SGOU
Higher Education for All

CYBER CRIME

COURSE CODE: B21CA13DE

Bachelor of Computer Applications
Discipline Specific Elective Course
Self Learning Material



SREENARAYANAGURU OPEN UNIVERSITY

SREENARAYANAGURU OPEN UNIVERSITY

The State University for Education, Training and Research in Blended Format, Kerala

SREENARAYANAGURU OPEN UNIVERSITY

SGOU

Vision

To increase access of potential learners of all categories to higher education, research and training, and ensure equity through delivery of high quality processes and outcomes fostering inclusive educational empowerment for social advancement.

Mission

To be benchmarked as a model for conservation and dissemination of knowledge and skill on blended and virtual mode in education, training and research for normal, continuing, and adult learners.

Pathway

Access and Quality define Equity.

Cyber Crime

Course Code: B21CA13DE

Semester - VI

SGOU

Discipline Specific Elective Course
Undergraduate Programme
Bachelor of Computer Applications
Self Learning Material

(With Model Question Paper Sets)

SREENARAYANAGURU
OPEN UNIVERSITY

SREENARAYANAGURU OPEN UNIVERSITY

The State University for Education, Training and Research in Blended Format, Kerala

SREENARAYANAGURU
OPEN UNIVERSITY

CYBER CRIME

Course Code: B21CA13DE
Semester- VI
Discipline Specific Elective Course
Bachelor of Computer Applications

Academic Committee

Dr. M.V. Judy
Dr. Aji S.
Dr. Vishnukumar S.
Rajesh R.
Dr. Rafidha Rehiman K.A.
P.M. Ameera Mol
Dr. Ajitha R.S.
Dr. Bindu Lal T.S.
Dr. Sreeja S.

Development of the Content

Block 1: Greeshma P.P.
Block 2: Subi Priya Laxhmi S.B.N.
Block 3: Shamin S.
Block 4: Sreerekha V.K.
Block 5: Dr. Kanitha D.K.
Block 6: Aswathy V.S.

Review and Edit

ICT Academy of Kerala

Proofreading

ICT Academy of Kerala

Scrutiny

Greeshma P.P., Dr. Kanitha D.K.,
Sreerekha V.K., Shamin S.,
Sub Priya Laxhmi S.B.N.,
Aswathy V.S.

Cover Design

Jobin J.

Co-ordination

Director (IC), MDDC :
Dr. Sajeevkumar G.
Coordinator, Development:
Dr. Anfal M.
Coordinator, Distribution:
Dr. Abdul Razak Kunnathodi

Scan this QR Code for reading the SLM on a digital device.

Edition
September 2026

Copyright
© Sreenarayanaguru Open University

ISBN 978-81-903304-4-2

9 788190 330442

SGOU

All rights reserved. No part of this work may be reproduced in any form, by mimeograph or any other means, without permission in writing from Sreenarayanaguru Open University. Printed and published on behalf of Sreenarayanaguru Open University by Registrar, SGOU, Kollam.

www.sgou.ac.in

Visit and Subscribe our Social Media Platforms

MESSAGE FROM VICE CHANCELLOR

Dear

With immense joy and excitement, I extend my heartfelt greetings to all of you and warmly welcome you to Sreenarayanaguru Open University.

Established in September 2020 as a state-driven initiative, Sreenarayanaguru Open University is dedicated to advancing higher education through open and distance learning. Our vision is guided by the principle of "access and quality define equity," laying the foundation for a celebration of excellence in education. I am delighted to share that we are steadfast in our commitment to uphold the highest standards and refrain from compromising on the quality of education we offer. The university draws its inspiration from the legacy of Sreenarayana Guru, a revered figure in the Indian renaissance movement. His name serves as a constant reminder for us to prioritize quality in all our academic endeavors.

Sreenarayanaguru Open University operates within the practical framework of the widely recognized "blended format." Acknowledging the constraints faced by distance learners in accessing traditional classroom settings, we have curated a pedagogical approach centered on three main components: Self Learning Material, Classroom Counselling, and Virtual Modes. This comprehensive blend is poised to deliver dynamic learning and teaching experiences, maximizing engagement and effectiveness. Our unwavering commitment to quality ensures excellence across all aspects of our educational initiatives.

The University aims to offer you an engaging and stimulating educational environment that fosters active learning. The SLM is designed to offer a comprehensive and cohesive learning experience, fostering a deep interest in the study of technological advancements in IT. Careful consideration has been given to ensure a logical progression of topics, facilitating a clear understanding of the discipline's evolution. The curriculum is thoughtfully crafted to provide ample opportunities for students to navigate through the current trends in information technology. Furthermore, this course is designed to provide essential insights into computer hardware, software classification, and foundational HTML concepts crucial for web development.

We assure you that the university student support services will closely stay with you for the redressal of your grievances during your studentship. Feel free to write to us about anything that seems relevant regarding the academic programme.

Wish you the best.



Regards,
Dr. Jagathy Raj V.P.

01-09-2026

SGOU

Contents

Block 01	**Cyber Crime Overview**	**1**
Unit 1	Internal and External Attacks	2
Unit 2	Cyber Crimes against Individuals	13
Unit 3	Cyber Crime against Women and Children	30
Unit 4	Cyber Crime against Government	43
Block 02	**Cyber Crime Against Organizations**	**57**
Unit 1	Network and System based Cyber Attacks	58
Unit 2	Evolving Cybercrime Techniques	74
Unit 3	Cyber Crime in Social Environments	88
Unit 4	Financial and Intellectual Property Cyber Frauds	100
Block 03	**A Global Perspective of Cyber Crimes**	**115**
Unit 1	Phases of Cyber Attack	116
Unit 2	Types of Cyber Attacks	130
Unit 3	Methods of Gaining and Sustaining Unauthorized Access	153
Unit 4	Lateral Movement and Detection Avoidance	174
Block 04	**Cyber Crime and Cloud Computing**	**186**
Unit 1	Tools and Methods used for Cyber Crime	187
Unit 2	Password Security and Remote Threats	202
Unit 3	Viruses and its Types	212
Unit 4	Cyber Criminal Syndicates and Nation-State Groups	226
Block 05	**Regulatory Framework of IT Act 2000**	**240**
Unit 1	Legal Framework	241
Unit 2	Electronic Records and Governance	251
Unit 3	Regulatory Authorities	263
Unit 4	Cyber Law Applications and E-Commerce	277
Block 06	**Offenses and Penalties Information Technology (Amendment) Act 2008**	**294**
Unit 1	Overview of Cyber Law and Jurisdiction	295
Unit 2	Cyber Crimes and Legal Penalties	306
Unit 3	Penal Provisions for Cyber Offenses	323
Unit 4	Human Rights in Cyberspace	344
Model Question Paper Sets		**365**

SGOU



BLOCK 1

Cyber Crime Overview

SGOU



UNIT 1 Internal and External Attacks

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- define cyber attacks and explain their basic concepts
- classify cyber attacks into internal and external attacks
- explain the different types of internal and external attacks with examples
- summarize the impact and consequences of cyber attacks on individuals and organizations

Prerequisites

Every day, you are using digital technologies such as mobile phones, online banking, social media, and email services. While using these, you may have come across situations like receiving suspicious messages, unknown links, or warnings about account security. Sometimes, you might have heard about incidents where someone's account was hacked or money was stolen through online fraud.

These everyday experiences show that while technology makes life easier, it also brings certain risks. Have you ever wondered how such attacks happen, who carries them out, and how systems get compromised?

This unit builds on what you already know and introduces you to the concept of cyber attacks. It helps you understand the different types of attacks, how they occur, and how they can affect individuals, organizations, and governments. By learning this, you will be better prepared to identify threats and understand the importance of cybersecurity in the digital world.

Key concepts

Cyber attacks, Internal attacks, External attacks, Phishing, DoS, Malicious insider attacks

SGOU

Discussion

1.1.1 Introduction to Cyber Attacks

In the present digital age, computers, mobile devices, and the internet have become an essential part of everyday life. People depend on digital technologies for various activities such as banking, online shopping, communication, education, and accessing government services. Due to this widespread usage, a large amount of sensitive information including personal details, financial data, and official records is stored and transmitted through computer systems and networks.

As dependence on digital systems increases, the chances of misuse and unauthorized activities also rise. Some individuals attempt to take advantage of system vulnerabilities or human weaknesses for illegal purposes. They may target software flaws, weak passwords, or even trick users into revealing confidential information. Such harmful and unauthorized activities are referred to as cyber attacks.

Cyber attacks have become one of the most serious challenges in the field of information technology because they can lead to data loss, financial damage, and privacy violations. These attacks not only affect individuals but can also disrupt organizations and government services.

A common example of a cyber attack is a phishing scam. In this type of attack, the attacker creates a fake website that closely resembles a genuine banking website. When users unknowingly enter their login credentials on this fake site, the attacker captures the information. This stolen data is then used to access the victim's bank account and carry out fraudulent transactions.

1.1.2 Definition of Cyber Attacks

A cyber attack can be defined as a deliberate and unauthorized attempt to access, alter, damage, or destroy computer systems, networks, or data. Such attacks are usually carried out with the intention of causing harm, stealing information, or gaining some form of benefit.

Cyber attacks mainly affect three important aspects of information security, namely confidentiality, integrity, and availability. These three principles are essential for maintaining the security and proper functioning of any information system. The three principles of information security are collectively known as the CIA Triad, as shown in Figure 1.1.1.

Confidentiality refers to the protection of sensitive information from unauthorized access. It ensures that data such as personal details, passwords, and financial information is accessible only to authorized users. When attackers gain access to such private information without permission, confidentiality is violated. Example: Stealing login credentials from a user's account.

Integrity refers to maintaining the accuracy and reliability of data. It ensures that information is not modified, deleted, or tampered with by unauthorized users. When attackers change or manipulate data, it affects the integrity of the system.

SGOU

Example: Altering student marks in a university database.



Fig. 1.1.1 CIA Triad

Availability ensures that computer systems and data are accessible to authorized users whenever required. Cyber attacks that disrupt services or make systems unavailable directly affect availability.

Example: A website becoming inaccessible due to a cyber attack such as a denial of service attack.

1.1.3 Types of Cyber Attacks

Cyber attacks can be classified into different types based on the source and method of the attack. Understanding these types helps in identifying threats and taking appropriate security measures. In general, cyber attacks are broadly divided into two main categories: internal attacks and external attacks as shown in Figure 1.1.2.

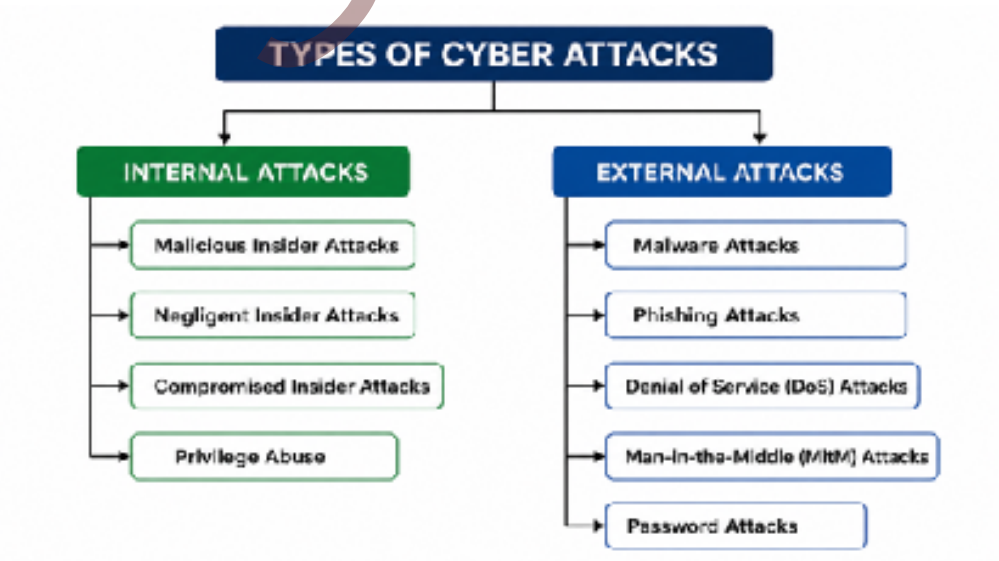


Fig. 1.1.2 Types of Cyber Attacks

SGOU

1.1.3.1 Internal attacks

An internal attack, also known as an insider attack, is a type of cyber attack that is carried out by a person who is part of an organization and has authorized access to its systems, networks, or data. These individuals may include employees, system administrators, contractors, or business partners.

Unlike external attackers, insiders already have permission to access the system. However, they misuse this access either intentionally or unintentionally, which can lead to serious security issues. Internal attacks are considered highly dangerous because insiders are familiar with the organization's structure, security policies, and system weaknesses.

Internal attacks can occur due to various reasons such as personal dissatisfaction, financial gain, revenge, or lack of awareness about security practices. In some cases, employees may not intend to cause harm but may still create security risks due to negligence or carelessness.

One of the major challenges with internal attacks is that they are difficult to detect. Since the attacker is an authorized user, their activities often appear normal, making it harder for security systems to identify suspicious behavior.

Internal attacks can result in several consequences, including:

- loss of confidential data,
- damage to systems or files,
- financial loss to the organization, and
- harm to the organization's reputation.

Consider the situation, in an organization the employees are frequently granted access to important systems, which they may subsequently misuse either intentionally or through negligence.

For instance, an employee who has access to a company's database containing confidential customer information may copy this data and share it with competitors for personal gain. Such actions can lead to financial loss and damage to the organization's reputation. This is considered an internal attack because the individual is part of the organization and misuses their authorized access.

Types of Internal Attacks

Internal attacks are carried out by individuals within an organization who have authorized access to systems and data. These attacks can occur either intentionally or unintentionally. Based on the nature and intention of the attacker, internal attacks can be classified into the following types:

1. Malicious Insider Attack

A malicious insider attack occurs when an employee or an authorized user intentionally

SGOU

misuses their access privileges to harm the organization. In this type of attack, the individual is fully aware of their actions and deliberately performs activities that can damage the organization's systems, data, or reputation.

Such attacks usually arise due to reasons such as financial gain, personal revenge, job dissatisfaction, or conflicts within the workplace. Since the attacker already has access to the system, they can easily carry out harmful activities without raising immediate suspicion.

Malicious insiders may engage in activities such as copying confidential data, leaking sensitive information to competitors, deleting important files, or introducing harmful software into the system. These actions can result in serious consequences, including financial loss, loss of trust, and legal issues for the organization. For example, an employee who is unhappy with the organization copies confidential customer data and sells it to a competitor company for money.

2. Negligent Insider Attack

A negligent insider attack occurs when an employee unintentionally causes a security breach due to carelessness or lack of awareness about cybersecurity practices. In this case, the individual does not have any intention to harm the organization, but their actions still lead to security issues.

This type of attack commonly occurs when employees fail to follow basic security guidelines. For instance, using weak passwords, sharing login credentials, clicking on suspicious links, or downloading files from untrusted sources can expose the system to cyber threats. Negligent insider attacks highlight the importance of user awareness and training, as even a small mistake can lead to serious consequences such as data breaches or malware infections. For example, an employee receives a fake email and clicks on a malicious link, which installs malware on the system and allows attackers to access sensitive data.

3. Compromised Insider Attack

A compromised insider attack occurs when an external attacker gains unauthorized access to an insider's account by stealing their login credentials. Once the attacker gains access, they use the account to perform malicious activities within the system.

In this situation, the actual employee may not be aware that their account has been compromised. Since the attacker is using a valid account, the system treats them as a legitimate user, making it difficult to detect the attack.

This type of attack often occurs through phishing, password attacks, or malware that captures login information. It can lead to serious security breaches, as attackers can access confidential data and perform unauthorized actions. For example, a hacker sends a phishing email to an employee and steals their login credentials. The hacker then uses these credentials to access the company's system and download sensitive information.

4. Privilege Abuse

Privilege abuse occurs when an individual misuses their authorized access rights beyond

SGOU

what is permitted. This type of attack is common among users who have higher-level privileges, such as system administrators, managers, or database administrators.

These users have the ability to access and control critical parts of the system. If they misuse their privileges, they can modify, delete, or misuse important data. Privilege abuse can be either intentional or done for personal benefit.

This type of attack is particularly dangerous because high-level users have greater control over the system, and their actions may not be easily questioned or monitored. For example, a system administrator intentionally deletes important company records or alters sensitive data without proper authorization.

1.1.3.2 External Attacks

An external attack is a type of cyber attack that is carried out by individuals or groups who are outside an organization and do not have authorized access to its systems, networks, or data. These attackers attempt to gain access by exploiting system vulnerabilities or by using various hacking techniques.

External attackers may include hackers, cyber criminals, or organized groups who target individuals, organizations, or government systems. These attacks are usually performed over the internet and can affect a large number of users at the same time.

The main objectives of external attacks are to:

- gain unauthorized access to systems,
- steal sensitive or confidential information,
- damage or disrupt services, and
- misuse data for financial or other benefits.

External attacks may be easier to detect at the network perimeter, though sophisticated attacks can remain undetected for long periods. However, they can still cause serious damage if proper security measures are not in place. External attackers use different techniques such as malware, phishing, denial of service attacks, password attacks, and man-in-the-middle attacks to achieve their goals.

For example, a hacker sends a phishing email that appears to be from a bank. The user clicks on the link and enters their login details on a fake website. The attacker collects this information and uses it to access the user's bank account.

Types of External Attacks

External attacks are carried out by attackers who are outside an organization and do not have authorized access to its systems. These attackers use various techniques to gain access, steal information, or disrupt services. The common types of external attacks are explained below:

1. Malware Attack

A malware attack involves the use of malicious software designed to damage, disrupt,

SGOU

or gain unauthorized access to computer systems. Malware includes different forms such as viruses, worms, trojans, and ransomware. These programs are usually spread through infected email attachments, unsafe downloads, or malicious websites.

Once malware enters a system, it can perform harmful actions such as deleting files, stealing sensitive data, monitoring user activities, or locking the system. Some malware, like worms, can spread automatically across networks, affecting multiple systems. Ransomware is particularly dangerous as it encrypts files and demands payment to restore access. For example, a user downloads free software from an untrusted website. The software contains hidden malware that encrypts all files on the computer and displays a message demanding money to unlock them.

2. Phishing Attack

A phishing attack is a social engineering technique used by attackers to trick users into revealing sensitive information such as usernames, passwords, bank details, or OTPs. Attackers pretend to be a trusted source, such as a bank, company, or government agency.

Phishing attacks are commonly carried out through emails, SMS messages, or fake websites that closely resemble legitimate ones. Users are often asked to click on a link and enter their details, which are then captured by the attacker. These attacks exploit human trust rather than technical weaknesses.

For example, a user receives an email that appears to be from their bank, asking them to verify their account details. The link in the email leads to a fake website where the user enters their login information, which is then stolen by the attacker.

3. Denial of Service (DoS) Attack

A Denial of Service (DoS) attack is an attempt to make a computer system, server, or network unavailable to its intended users. This can be achieved by flooding the system with a large number of requests, exhausting its resources, or exploiting a vulnerability that causes the system or service to slow down or crash.

In some cases, attackers use multiple computers to carry out the attack simultaneously. This is known as a Distributed Denial of Service (DDoS) attack. These attacks mainly target the availability of systems and do not necessarily involve data theft. DoS attacks can disrupt business operations, affect online services, and lead to financial losses. For example, an attacker sends a huge number of requests to a company's website, causing the server to crash. As a result, genuine users are unable to access the website.

4. Man-in-the-Middle (MitM) Attack

A Man-in-the-Middle (MitM) attack occurs when an attacker secretly intercepts communication between two parties without their knowledge. The attacker positions themselves between the sender and the receiver and can monitor, capture, or even alter the information being exchanged.

This type of attack is common in unsecured networks, especially public Wi-Fi, where data transmission is not properly encrypted. Attackers can steal sensitive information

SGOU

such as login credentials, credit card details, or personal messages.

For example, a user connects to a public Wi-Fi network at a café. An attacker on the same network intercepts the communication and captures the user's login details when they access their bank account.

5. Password Attack

A password attack involves attempts by attackers to gain unauthorized access to systems by guessing or cracking user passwords. Attackers use various techniques such as brute force attacks, where all possible combinations are tried, and dictionary attacks, where commonly used passwords are tested.

Weak or easily guessable passwords make it easier for attackers to succeed. Once the attacker gains access, they can steal data, modify information, or perform unauthorized actions. For example, a hacker uses automated software to try multiple password combinations on a user's account until the correct password is found, gaining unauthorized access.

Recap

- Cyber attacks are unauthorized attempts to access, damage, or disrupt computer systems and networks.
- Cyber attacks exploit system vulnerabilities as well as human weaknesses such as lack of awareness.
- Cyber attacks can affect individuals, organizations, and governments by causing financial loss, data theft, and service disruption.
- A cyber attack is defined as a deliberate attempt to access, alter, or destroy systems and data without permission.
- The main objectives of cyber attacks include stealing sensitive information, damaging systems, and gaining financial or personal benefits.
- Information security is based on three important principles known as confidentiality, integrity, and availability.
- Confidentiality ensures that sensitive information is accessed only by authorized users.
- Integrity ensures that data remains accurate and is not modified or tampered with by unauthorized users.
- Availability ensures that systems and data are accessible to authorized users whenever required.
- Cyber attacks are broadly classified into internal attacks and external attacks based on their source.

SGOU

- Internal attacks are carried out by individuals within an organization who have authorized access to systems.
- Internal attacks are difficult to detect because the attacker is a trusted user within the organization.
- Malicious insider attacks occur when an employee intentionally misuses access privileges to harm the organization.
- Negligent insider attacks occur when an employee unintentionally causes a security breach due to carelessness.
- Compromised insider attacks occur when an attacker gains access to an employee's account and misuses it.
- Privilege abuse occurs when a user misuses their authorized access rights beyond permitted limits.
- External attacks are carried out by attackers outside the organization without authorized access.
- External attackers use various techniques to gain access, steal data, or disrupt services.
- Malware attacks involve the use of malicious software to damage or control systems.
- Phishing attacks trick users into revealing sensitive information through fake messages or websites.
- Denial of Service attacks make systems or services unavailable by flooding them with excessive traffic, exhausting resources, or exploiting vulnerabilities.
- Man-in-the-Middle attacks involve intercepting communication between two users to steal data.
- Password attacks involve guessing or cracking passwords to gain unauthorized access.
- Internal attacks may be more difficult to detect because attackers have authorized access, while external attacks are carried out by attackers outside the organization.

SGOU

Objective Type Questions

1. What is an unauthorized attempt to access or damage a computer system called?
2. Which principle ensures that data is accessible when needed?

3. Which principle protects data from unauthorized access?
4. Which principle ensures that data remains accurate and unaltered?
5. What type of attack is performed by an employee within an organization?
6. What type of attack is performed by outsiders without authorized access?
7. Which internal attack involves intentional harm by an employee?
8. Which internal attack occurs due to carelessness?
9. Which attack involves stealing login credentials and misusing an account?
10. What type of attack involves misuse of access rights?
11. Which external attack uses harmful software?
12. Which attack tricks users through fake emails or websites?
13. Which attack makes a system unavailable by flooding traffic?
14. Which attack intercepts communication between two users?
15. Which attack involves guessing or cracking passwords?

Answers to Objective Type Questions

1. Cyber attack
2. Availability
3. Confidentiality
4. Integrity
5. Internal
6. External
7. Malicious insider attack
8. Negligent insider attack
9. Compromised insider attack
10. Privilege abuse
11. Malware

SGOU

12. Phishing

13. DoS

14. Man-in-The-Middle attack

15. Password attack

Assignments

1. Explain the concept of cyber attacks and discuss their impact on individuals and organizations with examples.

2. Describe the principles of information security (Confidentiality, Integrity, and Availability) with suitable examples.

3. Differentiate between internal attacks and external attacks with examples.

4. Explain the different types of internal attacks with examples.

5. Describe the common types of external attacks and explain any two with examples.

Suggested Reading

1. Godbole, Nina, and Sunit Belapure. *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*. Wiley India, 2011.

2. Brooks, Charles J., et al. *Cybersecurity Essentials*. Wiley, 2018.

3. Stallings, William. *Network Security Essentials: Applications and Standards*. Pearson.

Reference

1. India. *The Information Technology Act, 2000*. Government of India.

2. National Institute of Standards and Technology. *Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce, 2024.

3. Cybersecurity and Infrastructure Security Agency. *Cybersecurity Resources*. U.S. Department of Homeland Security.

SGOU



UNIT 2 Cyber Crimes against Individuals

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- define cyber crimes against individuals and explain their impact
- identify and describe different types of email-based cyber crimes
- explain various forms and methods of phishing attacks
- classify different types of online frauds and spamming techniques
- explain the concepts of cyber defamation, cyberstalking, and cyber bullying

Prerequisites

In your daily life, you are already using digital technologies such as email, social media, online shopping platforms, and messaging applications for communication, learning, entertainment, and financial transactions. You may check your email regularly, receive messages on your phone, browse social media feeds, or make payments online. While doing so, you might have noticed certain unusual situations such as receiving messages from unknown sources, emails asking for personal details, or attractive offers that seem too good to be true.

At times, you may also hear about incidents where people lose money due to fake online offers, become victims of fraud, or face problems because someone misused their personal information. You might have even experienced unwanted messages, spam emails, or suspicious links that made you feel unsure about their authenticity. These common experiences show that along with the convenience of digital technologies, there are also risks involved in using them.

As the use of the internet continues to grow, cyber criminals are finding new ways to target individuals by taking advantage of both technical weaknesses and human trust. They use methods such as fake emails, fraudulent websites, misleading messages, and social engineering techniques to deceive users. Many of these attacks appear genuine, making it difficult for users to identify them easily.

This unit introduces you to various types of cyber crimes that specifically target individuals, including email spoofing, online frauds, phishing and its forms, spamming, cyber defamation, cyberstalking, and cyber bullying. By studying these topics, you will gain a clear understanding of how such attacks are carried out, how they affect individuals, and why it is important to be aware of them.

SGOU

Key concepts

Cyber crimes, Email spoofing, Phishing, Online frauds, Cyber bullying.

Discussion

1.2.1 Introduction to Email-Based Cyber Crimes

In today's digital world, email has become one of the most widely used communication tools for personal, professional, and official purposes. People use email to send important information, documents, and financial details. However, the widespread use of email has also made it a common target for cyber criminals.

Attackers use various techniques to misuse email systems in order to deceive users and steal sensitive information. These attacks are designed to appear genuine so that users trust them without suspicion. One of the most common forms of such attacks is email spoofing.

1.2.2 Email Spoofing

Email spoofing is a type of cyber crime in which an attacker sends an email that appears to come from a trusted or legitimate source. In this method, the sender's email address is falsified so that the message looks genuine to the receiver. As a result, the receiver believes that the email is from a known organization such as a bank, company, or service provider.

In practice, email spoofing takes advantage of the way email systems allow the sender information to be modified. Attackers manipulate the "From" field of the email so that it displays a fake identity. Since the email appears authentic, users may not suspect any risk and may trust the message without verification.

The main purpose of email spoofing is to deceive users into performing certain actions. These actions may include providing personal or financial information, clicking on harmful links, or downloading malicious attachments. In many cases, email spoofing is used along with phishing attacks to collect sensitive information such as usernames, passwords, and banking details.

Email spoofing can lead to serious consequences. It may result in identity theft, financial loss, and unauthorized access to personal or organizational accounts. Therefore, it is considered a major threat to individuals in the digital environment.

A common example of email spoofing is when a person receives an email that appears to be from their bank, requesting urgent verification of account details. The email may contain a link that directs the user to a fake website. When the user enters their login credentials, the attacker captures this information and uses it to access the victim's account and carry out fraudulent activities.

1.2.2.1 Prevention Methods

Email spoofing can be reduced by following appropriate security practices. The following

SGOU

methods can help users and organizations identify and prevent email spoofing.

1. Verify the Sender's Email Address

Users should carefully check the sender's complete email address before responding to an email or clicking on any links or attachments. The display name may look familiar even when the actual email address belongs to an attacker. Users should verify that the email address belongs to the expected organization and be cautious of unfamiliar or slightly altered addresses.

2. Check Email Headers

Email headers contain technical information about the sender, recipient, and servers through which the email was transmitted. Checking the headers can help identify suspicious or forged emails by providing additional information about the actual source and path of the message. This can be particularly useful when the sender's displayed address appears suspicious.

3. Sender Policy Framework (SPF)

Sender Policy Framework (SPF) is an email authentication mechanism that allows a domain owner to specify which mail servers are authorized to send emails on behalf of that domain. Receiving mail servers can check the SPF information to determine whether the sending server is authorized. This helps reduce the use of a domain for unauthorized or spoofed emails.

4. DomainKeys Identified Mail (DKIM)

DomainKeys Identified Mail (DKIM) is an email authentication method that uses a digital signature to verify that an email was sent by an authorized domain and that the message has not been altered during transmission. The receiving mail server can verify the signature using information published by the sender's domain.

5. Domain-based Message Authentication, Reporting and Conformance (DMARC)

Domain-based Message Authentication, Reporting and Conformance (DMARC) works with SPF and DKIM to provide an additional layer of email authentication. It allows domain owners to specify how receiving mail servers should handle emails that fail authentication checks. Depending on the configured policy, suspicious messages may be monitored, quarantined, or rejected.

6. Avoid Sharing Sensitive Information

Users should not provide passwords, banking details, OTPs, or other sensitive information in response to unexpected or suspicious emails. If an email requests such information, users should independently verify the request through the organization's official website or another trusted communication channel.

7. Report Suspicious Emails

Suspicious or fraudulent emails should be reported to the appropriate organization or cybercrime reporting authority. Reporting such messages can help prevent other users

SGOU

from becoming victims of similar attacks and supports efforts to identify fraudulent activities.

1.2.3 Online Frauds

Online fraud refers to any illegal activity carried out over the internet with the intention of deceiving individuals to gain money or sensitive information. In such crimes, attackers use digital platforms such as websites, emails, and social media to trick users.

Online frauds mainly depend on deceiving users rather than breaking technical systems. Attackers create fake websites, messages, or offers that appear genuine and attractive. These may include online shopping deals, lottery winnings, job offers, or investment schemes.

Users are often influenced by offers that seem too good to be true. Attackers create urgency by using messages like "limited time offer" or "act immediately," which forces users to make quick decisions without proper verification. As a result, users may share personal details or make payments, leading to financial loss.

1.2.3.1 Types of Online Frauds

1. E-commerce Fraud

E-commerce fraud refers to fraudulent activities carried out during online buying and selling with the intention of obtaining money, goods, services, or sensitive information through deception or unauthorized transactions. It can occur on both fake and legitimate e-commerce platforms. Attackers may use fake websites or product listings, stolen payment or credit card information, unauthorized transactions, fraudulent refunds or chargebacks, and other deceptive techniques to commit fraud.

These websites often display attractive offers, discounts, and branded products to gain the trust of customers. Once the user places an order and makes the payment, the product is either not delivered or a fake/low-quality product is sent. In many cases, the website becomes inactive after collecting money from users. E-commerce fraud can also occur on legitimate platforms, for example, through the use of stolen payment card information, unauthorized purchases, or fraudulent refund and chargeback claims. E-commerce fraud mainly targets users who do not verify the authenticity of the website before making a purchase.

For example, a person orders a branded mobile phone from a website offering huge discounts. After making the payment, the product is never delivered, and the website disappears.

2. Lottery Scam

A lottery scam is a type of online fraud in which users receive messages or emails claiming that they have won a lottery or prize. The message often appears to come from a well-known organization or international company.

The attacker asks the user to pay a certain amount as a processing fee, tax, or service charge to claim the prize. In reality, there is no prize, and the attacker's main aim is

SGOU

to collect money from the victim. These scams often create excitement and urgency, making users act without verifying the information.

For example, a person receives an email stating that they have won an international lottery worth a large amount of money. To claim the prize, they are asked to pay a small fee. After paying, they receive no reward.

3. Job Fraud

Job fraud involves fake job offers provided by attackers to deceive individuals, especially job seekers. In this type of fraud, attackers create fake job advertisements or send emails offering attractive job opportunities with high salaries.

Once the user shows interest, the attacker may ask for money for registration, training, or document processing. In some cases, personal information such as certificates and identity details may also be collected. Job fraud takes advantage of people who are actively searching for employment and are eager to secure a job quickly.

For example, a person receives an email offering a high-paying job in a reputed company. The sender asks for a registration fee to process the application. After the payment is made, no job is provided.

4. Investment Fraud

Investment fraud is a type of online fraud in which attackers promote fake investment schemes that promise high returns with little or no risk. These schemes are designed to attract individuals who are looking for quick financial gains.

Attackers may use websites, social media platforms, or messages to advertise these schemes. They may show fake testimonials or past success stories to convince users. Once the victim invests money, the attacker either disappears or stops communication. Such frauds exploit the greed or financial expectations of individuals.

For example, a person invests money in an online scheme that promises to double the investment within a short period. After the payment is made, the scheme becomes inactive, and the money is lost.

1.2.4 Phishing

Phishing is a type of cyber crime in which attackers attempt to obtain sensitive information such as usernames, passwords, bank details, or OTPs by pretending to be a trusted entity like a bank, company, or service provider.

Phishing attacks mainly rely on deceiving users rather than exploiting technical weaknesses. Attackers create fake emails, messages, or websites that look very similar to genuine ones. These messages often create a sense of urgency, such as warning about account suspension or offering attractive rewards, to make users act quickly without thinking.

When users click on links or provide information, the attacker captures the data and uses it for illegal purposes such as financial fraud or identity theft. Phishing is one of the most common cyber attacks targeting individuals.

SGOU

The typical flow of a phishing attack is illustrated in Figure 1.2.1.

A phishing attack generally follows a sequence of steps. First, the attacker prepares a deceptive message that appears to come from a trusted source and sends it to the target user. The message may contain a link or attachment designed to attract the user's attention. When the user clicks the link, they may be directed to a fake website that closely resembles a genuine one. The user may then be asked to enter sensitive information such as a username, password, bank details, or OTP. The attacker captures the submitted information and may use it for unauthorized access, financial fraud, identity theft, or other illegal activities. In some cases, malicious attachments may also install harmful software on the user's device.

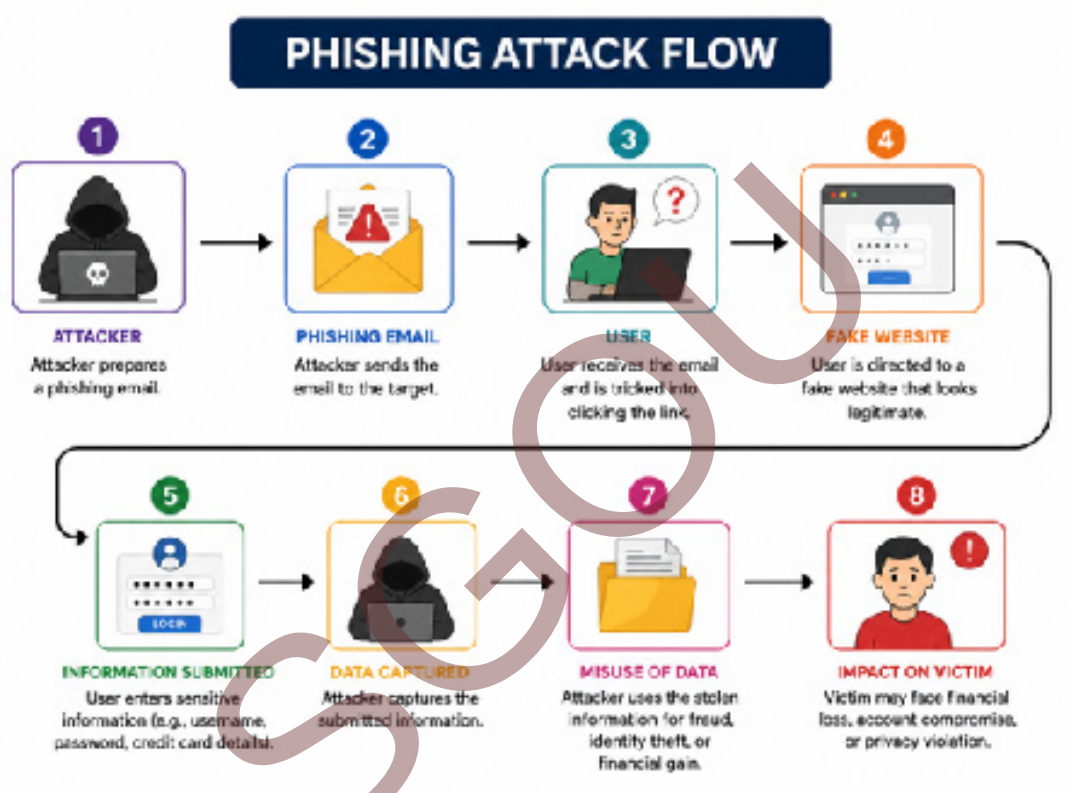


Fig. 1.2.1 Phishing attack flow

Methods Used to Carry Out Phishing

Phishing attacks can be carried out using different methods that trick users into revealing sensitive information or installing malicious software. Some of the common methods used in phishing are explained below:

1. Clicking on an Unknown File or Attachment

One of the common methods used in phishing is sending malicious files or attachments through emails. Attackers send emails that appear to be from trusted sources and include attachments such as documents, PDFs, or links. When the user opens these files, they may unknowingly install malware on their system or be prompted to enter confidential information. These attachments are often found in spam emails or fake

SGOU

corporate communications and are designed to look genuine, making users trust and open them without suspicion.

2. Wi-Fi Phishing

Wi-Fi phishing involves creating a fake or deceptive wireless network to trick users into providing sensitive information. Attackers may use Captive Portals or Evil Twin attacks to present users with fake login pages.

a. Captive Portals

A Captive Portal is a web page that appears when a user connects to a Wi-Fi network and asks the user to provide information or accept certain terms before accessing the internet. In a phishing attack, an attacker can create a fake captive portal that looks like the login page of a genuine Wi-Fi service, hotel, airport, or other organization. The user may be asked to enter an email address, username, password, or other sensitive information. The attacker can then capture the information entered by the user.

Example: A user connects to a public Wi-Fi network and is shown a page that appears to be the official login page of the service provider. The user enters their email address and password, which are then captured by the attacker.

b. Evil Twin Attack

An Evil Twin attack involves creating a fake Wi-Fi network that has a name or appearance similar to a legitimate wireless network. The attacker may give the fake network a name similar to the network available in a hotel, airport, café, or other public place. When users connect to the fake network, the attacker may display a fraudulent login page, such as a captive portal, to trick them into entering their credentials.

Example: A genuine café Wi-Fi network is named “Cafe_WiFi”. An attacker creates a fake network named “Cafe_WiFi_Free”. A user connects to the fake network and is presented with a login page requesting their username and password.

3. Responding to Social Media Requests

Social media platforms are often used by attackers to carry out phishing through social engineering techniques. Attackers create fake profiles and send friend requests or messages to users. Once the request is accepted, the attacker gains the user’s trust and may start collecting personal information. Users may unknowingly share private details such as contact information, photos, or other personal data, which can later be used for targeted phishing attacks or identity theft.

4. Clicking on Unauthenticated Links or Ads

Another common phishing method involves clicking on fake or unauthenticated links and advertisements. These links are designed to look similar to legitimate websites and often appear in emails, pop-up ads, or unsafe websites. When users click on such links, they are redirected to fake websites where they are asked to enter sensitive information such as usernames, passwords, or financial details. Since the websites closely resemble genuine ones, users may not realize that they are being deceived.

SGOU

1.2.4.1 Forms of Phishing

1. Email Phishing

Email phishing is the most common type of phishing in which attackers send fake emails to a large number of users. These emails are designed to look as if they are sent from trusted organizations such as banks, online services, or companies.

The attacker carefully designs the email using official logos, formatting, and language to make it appear genuine. The email usually contains a message that creates urgency, such as a warning about account suspension or a request to verify account details. It may also include a link that directs the user to a fake website or an attachment that installs malware. When the user clicks on the link and enters personal information, the attacker captures this data and uses it for fraudulent activities.

For example, a user receives an email that appears to be from a bank asking to verify account details. The link provided leads to a fake website where the user unknowingly enters their login credentials.

2. Spear Phishing

Spear phishing is a more advanced and targeted form of phishing in which attackers focus on a specific individual or organization. Unlike email phishing, which targets many users, spear phishing attacks are carefully planned using personal information about the victim.

Attackers may collect details such as the victim's name, job role, or organization to make the message appear more authentic. Because of this personalization, the victim is more likely to trust the message and respond to it. Spear phishing is commonly used to steal confidential information or gain access to organizational systems.

For example, an employee receives an email that appears to be from their manager requesting confidential company data. Since the email looks genuine, the employee shares the information.

3. Smishing

Smishing is a type of phishing that is carried out through SMS (text messages). Attackers send messages that appear to come from trusted sources such as banks, courier services, or government agencies.

These messages often contain a link or a request for urgent action, such as updating account details or claiming a reward. The message creates a sense of urgency so that the user responds quickly without verifying the source. When the user clicks the link or shares information, the attacker collects the data.

For example, a user receives an SMS stating that their bank account will be blocked and is asked to click a link to verify details. The link leads to a fake website.

4. Vishing

Vishing is phishing carried out through voice calls. In this method, attackers call the

SGOU

victim pretending to be officials from banks, customer service centers, or government organizations.

The attacker speaks in a convincing manner and may use fear or urgency to pressure the victim into sharing sensitive information such as OTPs, PINs, or account details. Since the communication happens directly through a phone call, victims may trust the caller more easily. Vishing is dangerous because it involves direct interaction, making it more difficult for victims to recognize the fraud.

For example, a person receives a call claiming to be from the bank, asking for OTP details to resolve an issue. After sharing the OTP, money is withdrawn from the account.

5. Whaling

Whaling is a highly targeted form of phishing that specifically targets high-ranking individuals such as senior executives, government officials, or other influential persons. Attackers carefully research the target and create convincing messages that appear to come from a trusted person or organization. The aim may be to obtain sensitive information, gain unauthorized access to accounts, or persuade the target to authorize financial transactions.

Example: An attacker may send a carefully prepared email to a senior executive, pretending to be a government authority or business partner, and request confidential information or an urgent financial transaction.

1.2.5 Spamming

Spamming refers to the act of sending a large number of unwanted, irrelevant, or unsolicited messages to users through electronic communication systems such as email, messaging platforms, or social media.

Spamming is one of the most common cyber crimes that targets individuals. In this method, attackers send bulk messages to many users without their consent. These messages are often advertisements, promotional content, or fraudulent offers. In many cases, spam messages may also contain malicious links or attachments that can harm the user's system.

Spammers collect email addresses or contact details from various sources and use automated tools to send messages in large volumes. Since these messages are sent to a wide audience, even if a small number of users respond, attackers can gain benefits.

Spamming not only causes inconvenience by filling inboxes with unnecessary messages but also creates security risks. Users who click on links or download attachments from spam messages may become victims of phishing attacks, malware infections, or online frauds.

1.2.5.1 Types of Spamming

1. Email Spam

Email spam is the most common form of spamming in which a large number of unwanted emails are sent to users without their permission. These emails are usually promotional

SGOU

in nature and may advertise products, services, or fake offers.

Spammers use automated tools to send bulk emails to thousands of users at once. Many of these emails may contain misleading subject lines to attract attention. In some cases, they also include malicious links or attachments that can lead to phishing attacks or malware infections. Email spam can overload a user's inbox, making it difficult to identify important messages.

For example, a user receives multiple emails every day promoting unknown products or fake discount offers, even though they never subscribed to such services.

2. SMS Spam

SMS spam refers to unwanted messages sent to mobile phones. These messages are often promotional or fraudulent and may include links, contact numbers, or instructions to claim offers.

Attackers use SMS spam to promote fake schemes, lottery winnings, or urgent account updates. These messages often create a sense of urgency, encouraging users to respond quickly without verification. SMS spam is particularly dangerous because users tend to trust messages received on their personal mobile devices.

For example, a user receives a message stating that they have won a prize and are asked to click a link or call a number to claim it.

3. Social Media Spam

Social media spam involves sending or posting unwanted messages, advertisements, or links on platforms such as social networking sites, messaging apps, or online communities.

Spammers may create fake accounts or use bots to send friend requests, post links, or share promotional content. These messages may contain harmful links that redirect users to fake websites or malicious downloads. Social media spam can spread quickly due to the large number of users on these platforms.

For example, a user receives repeated messages or friend requests from unknown profiles promoting fake offers or suspicious links.

4. Comment Spam

Comment spam refers to posting irrelevant or promotional messages in the comment sections of websites, blogs, or online forums. These comments are usually unrelated to the actual content and are posted to advertise products or redirect users to other websites.

Spammers often include links in these comments to increase website traffic or promote malicious content. In some cases, automated programs are used to post large numbers of such comments. Comment spam reduces the quality of online discussions and may expose users to security risks.

For example, a blog post contains multiple unrelated comments promoting products or

SGOU

including links to unknown websites.

1.2.6 Cyber Defamation

Cyber defamation is the act of damaging a person's reputation by spreading false or harmful information about them through digital platforms such as social media, websites, blogs, or emails. It involves publishing statements online that are not true and that negatively affect a person's image, character, or credibility.

In the online environment, such information can spread very quickly and reach a large number of people within a short time. This makes cyber defamation more harmful than traditional forms of defamation, as it is difficult to completely remove the content once it is shared.

For example, if a person posts false accusations about someone on social media without any proof, and this information harms the person's reputation, it is considered cyber defamation.

Types of Cyber Defamation

1. Social Media Defamation

Social media defamation occurs when false or harmful information about a person is posted or shared on social media platforms. Since social media allows instant sharing, such content can quickly reach a large audience, increasing its impact.

In many cases, individuals may post false accusations, rumors, or offensive comments about someone out of anger, jealousy, or personal conflict. Even sharing or forwarding such content without verification can also contribute to defamation. This type of defamation is particularly dangerous because once the content goes viral, it becomes very difficult to control or remove completely.

For example, a person posts false allegations about a colleague on a social media platform, which spreads widely and damages the colleague's reputation.

2. Website or Blog Defamation

Website or blog defamation occurs when defamatory content is published on websites, blogs, or online articles. This type of content may appear as written posts, reviews, or comments that contain false information about an individual.

Such content may remain available online for a long time, making it accessible to a wide audience. It can affect a person's professional image, especially if the content appears in search results. In some cases, attackers create entire websites or blogs dedicated to spreading false information about a person.

For example, a blog publishes false information about a businessperson's activities, which affects their professional reputation.

3. Email Defamation

Email defamation occurs when false or harmful information about a person is shared

SGOU

through emails with others. This type of defamation often targets individuals within organizations, workplaces, or social groups.

The attacker may send emails containing false accusations or misleading information to colleagues, clients, or friends of the victim. Even though the audience may be smaller compared to social media, the impact can still be serious, especially in professional environments. Email defamation can damage trust, relationships, and career opportunities.

For example, an individual sends emails to office staff falsely accusing a colleague of misconduct, affecting the colleague's reputation at the workplace.

1.2.7 Cyberstalking

Cyberstalking is a type of cyber crime in which a person is repeatedly harassed, threatened, or monitored using digital platforms such as social media, emails, or messaging applications. It involves continuous and unwanted online behavior that causes fear, discomfort, or emotional distress to the victim.

In cyberstalking, the attacker may send repeated messages, track the victim's online activities, spread false information, or try to control and intimidate the victim. Since these actions are carried out over the internet, they can occur at any time and may be difficult to stop.

For example, if a person continuously sends threatening messages and keeps monitoring another person's social media activities even after being blocked, it is considered cyberstalking.

Types of Cyberstalking

1. Email Stalking

Email stalking is a form of cyberstalking in which the attacker repeatedly sends unwanted emails to the victim. These emails may contain threatening messages, abusive language, or disturbing content intended to create fear or discomfort.

The attacker may send emails frequently, sometimes from different email addresses, to avoid being blocked. Even if the victim ignores or blocks the sender, the attacker may continue the behavior using new accounts. This continuous flow of unwanted communication can cause mental stress and anxiety to the victim.

For example, a person receives multiple threatening emails every day from an unknown sender. Even after blocking the email address, the attacker continues sending messages using different accounts.

2. Social Media Stalking

Social media stalking occurs when an attacker continuously monitors and interacts with a person through social media platforms without their consent. The attacker may send repeated messages, comment on posts, or track the victim's activities online.

SGOU

In many cases, the attacker may create fake accounts to continue the harassment if they are blocked. This type of stalking invades the victim's privacy and can make them feel unsafe while using social media.

For example, an individual repeatedly sends unwanted messages and comments on a person's posts. Even after being blocked, the attacker creates new profiles to continue the behavior.

3. Online Harassment

Online harassment involves sending abusive, insulting, or threatening messages through digital communication platforms such as chat applications, forums, or messaging services. This type of cyberstalking may occur publicly or privately. The attacker's intention is to emotionally disturb or intimidate the victim. Continuous harassment can negatively affect the victim's mental health and confidence. For example, a person sends repeated abusive and insulting messages to another person through a messaging app, causing emotional distress.

4. Monitoring and Tracking

Monitoring and tracking is a more serious form of cyberstalking in which the attacker secretly observes the victim's online activities, location, or personal data. This may be done using spyware, tracking tools, or by collecting information from online platforms.

The attacker may use this information to control, threaten, or manipulate the victim. This type of stalking is dangerous because the victim may not be aware that they are being monitored.

For example, an attacker installs spyware on a victim's device and tracks their location and online activities without their knowledge.

1.2.8 Cyber Bullying

Cyber bullying is a form of cyber crime in which a person is intentionally harassed, insulted, threatened, or embarrassed using digital technologies such as social media, messaging applications, online forums, or gaming platforms. It involves using the internet or electronic devices to harm another person emotionally or socially.

In cyber bullying, the attacker may engage in activities such as sending abusive messages, spreading false rumours, posting embarrassing photos or videos, or making offensive comments online. These actions are often repeated and targeted, which increases their impact on the victim.

Unlike traditional bullying, cyber bullying can occur at any time and does not require face-to-face interaction. The anonymity provided by digital platforms may allow attackers to hide their identity and continue the behaviour without being easily identified.

Cyber bullying can have serious effects on the victim, including stress, anxiety, loss of confidence, social isolation, and emotional distress. Since content shared online can spread quickly to a large audience, its impact can be more severe and long-lasting.

SGOU

Types of Cyber Bullying

1. Harassment

Harassment involves repeatedly sending abusive, insulting, threatening, or unwanted messages to a person through digital platforms. The attacker may use social media, messaging applications, email, or online forums to repeatedly disturb or intimidate the victim.

Example: A person repeatedly sends insulting and threatening messages to another person through a messaging application, even after being asked to stop.

2. Exclusion

Exclusion involves deliberately leaving a person out of online groups, conversations, gaming activities, or social activities with the intention of making the person feel isolated or rejected. It may also involve intentionally preventing someone from participating in an online community.

Example: A group of students creates an online group for a class activity but deliberately excludes one student and discusses the activity in the group to make the student feel isolated.

3. Outing

Outing involves sharing a person's private, personal, or embarrassing information, photographs, messages, or other content online without their permission. The purpose may be to embarrass, humiliate, or harm the person.

Example: A person shares another individual's private photographs or personal messages in a social media group without permission, causing embarrassment to the victim.

4. Impersonation

Impersonation involves pretending to be another person online by using their name, photograph, or other identifying information. The attacker may create a fake account and post messages or content that could damage the victim's reputation or relationships.

Example: A person creates a fake social media account using another student's name and photograph and posts offensive messages pretending to be that student.

5. Trolling

Trolling involves deliberately posting provocative, insulting, or offensive comments online to upset, anger, or provoke another person. Trolls may repeatedly comment on social media posts, forums, or online discussions to create conflict or emotional distress.

Example: A person repeatedly posts insulting comments under another person's social media posts with the intention of provoking and embarrassing them.

SGOU

Recap

- Email is widely used for communication but has become a common target for cyber crimes.
- Email spoofing is a cyber crime where attackers send emails that appear to come from trusted sources.
- Online fraud refers to illegal activities carried out through the internet to deceive users and gain money or sensitive information.
- Common types of online frauds include e-commerce fraud, lottery scams, job fraud, and investment fraud.
- Phishing is a cyber attack in which attackers trick users into sharing confidential information by pretending to be trusted entities.
- Phishing attacks are carried out using methods such as malicious attachments, fake Wi-Fi networks, social media interactions, and unauthenticated links.
- Forms of phishing include email phishing, spear phishing, smishing, and vishing.
- Spamming is the act of sending large numbers of unwanted messages through email, SMS, social media, or other platforms.
- Types of spamming include email spam, SMS spam, social media spam, and comment spam.
- Cyber defamation involves damaging a person's reputation by spreading false information online.
- Cyber defamation can occur through social media, websites or blogs, and emails.
- Cyberstalking is the repeated harassment or monitoring of a person using digital platforms.
- Types of cyberstalking include email stalking, social media stalking, online harassment, and monitoring or tracking.
- Cyber bullying involves using digital platforms to intentionally harm, insult, or embarrass a person.

SGOU

Objective Type Questions

1. What is sending fake emails with a forged sender address called?
2. What type of cyber crime involves deceiving users to gain money online?
3. What is the fake message technique used to steal user information called?

4. Which type of phishing is carried out through SMS?
5. Which type of phishing is done through voice calls?
6. What is the act of sending bulk unwanted messages called?
7. What type of fraud involves fake online shopping websites?
8. What type of fraud involves fake job offers?
9. What is damaging someone's reputation online called?
10. What type of cyber crime involves repeated online harassment?
11. What is continuous monitoring of a person online called?
12. What is using digital platforms to insult or harm someone called?
13. What type of phishing targets a specific individual?

Answers to Objective Type Questions

1. Email spoofing
2. Online fraud
3. Phishing
4. Smishing
5. Vishing
6. Spamming
7. E-commerce fraud
8. Job fraud
9. Cyber defamation
10. Cyberstalking
11. Monitoring and Tracking.
12. Cyberbullying
13. Spear phishing

SGOU

Assignments

1. Explain the concept of email spoofing and discuss its impact with an example.
2. Describe different types of online frauds and explain any two in detail with examples.
3. What is phishing? Explain its various forms and methods used to carry out phishing attacks.
4. Define spamming and discuss its different types with suitable examples.
5. Explain the concepts of cyber defamation, cyberstalking, and cyber bullying with examples.

Suggested Reading

1. Brooks, Charles J., et al. *Cybersecurity Essentials*. Wiley, 2018.
2. Yar, Majid. *Cybercrime and Society*. SAGE Publications.
3. Godbole, Nina, and Sunit Belapure. *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*. Wiley India.
4. Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. *Cybercrime and Digital Forensics: An Introduction*. Routledge.

Reference

1. India. *The Information Technology Act, 2000*. Government of India.
2. India. *The Bharatiya Nyaya Sanhita, 2023*. Government of India.
3. Government of India. *National Cyber Crime Reporting Portal*. Ministry of Home Affairs.

SGOU



UNIT 3 Cyber Crime against Women and Children

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- define cyber crimes against women and children
- explain online sexual harassment and its forms
- describe the stages of online grooming
- summarize effects and prevention of child sexual exploitation and abuse material (CSEAM)
- explain digital human trafficking methods

Prerequisites

Think about your daily life. You chat with friends, share photos, watch videos, and explore new things online. The digital world feels friendly, fast, and full of opportunities. It connects you to people and information in just a few seconds, making life easier and more enjoyable.

But have you ever paused to think, can this same space sometimes become unsafe? Just like in the real world, not everyone online has good intentions. Some people misuse digital platforms to harm others, especially those who are more trusting or less aware. A simple action like accepting a friend request, replying to a message, or sharing a photo may seem harmless, but in certain situations, it can lead to uncomfortable or even dangerous experiences.

Many times, these risks are not very obvious. They may begin as friendly conversations, attractive offers, or supportive interactions. Gradually, they can turn into situations that affect a person's privacy, safety, and emotional well-being. This is why it is important to understand not only how to use technology, but also how to use it safely and responsibly.

In this unit, you will explore the lesser-known side of the digital world, where technology is misused to target individuals, especially women and children. You will learn about different types of harmful online activities, how they occur, and how they impact people's lives. More importantly, this unit will guide you in recognizing warning signs and adopting simple practices to stay safe, aware, and confident while using digital platforms.

SGOU

Key concepts

Cyber safety, Online harassment, Child protection, Digital threats, Human trafficking

Discussion

1.3.1 Introduction

In today's digital world, the use of the internet, smartphones, and social media has become an essential part of everyday life. People use these technologies for communication, education, entertainment, and accessing various online services. While these advancements have made life easier, they have also created new opportunities for misuse and exploitation.

Among all users, women and children are considered more vulnerable to cyber crimes due to factors such as lack of awareness, trust in online interactions, and exposure to unknown individuals through digital platforms. Cyber criminals take advantage of these vulnerabilities to carry out harmful activities that affect the safety, privacy, and dignity of individuals.

Crimes against women and children in the digital environment include activities such as online sexual harassment, online grooming, child sexual exploitation and abuse material (CSEAM), and human trafficking through digital platforms. These crimes are often carried out using social media, messaging applications, websites, and other online tools. Many of these attacks involve manipulation, deception, and exploitation rather than direct technical attacks.

Such crimes can have serious consequences, including emotional distress, psychological trauma, social isolation, and in some cases, long-term harm to the victim's well-being. Since digital content can spread quickly and widely, the impact of these crimes is often more severe and difficult to control.

This unit aims to provide a clear understanding of different types of cyber crimes that specifically target women and children. It helps in identifying how these crimes are carried out, understanding their impact, and recognizing the importance of awareness and preventive measures. By studying this unit, you will be able to better understand the risks involved in using digital platforms and the need for responsible and safe online behavior. Let us now discuss each of these topics in detail

1.3.2 Online Sexual Harassment

Online sexual harassment is a significant form of cyber crime that involves unwanted, inappropriate, or offensive behavior of a sexual nature carried out through digital platforms such as social media, emails, and messaging applications. It includes actions that violate the dignity and privacy of individuals and cause discomfort, fear, or emotional distress.

In the digital environment, the misuse of online platforms has led to the rise of such

SGOU

cyber crimes, particularly targeting women and young individuals. Offenders may send explicit messages, share inappropriate content, or make offensive remarks without consent.

A major factor contributing to this cyber crime is the anonymity provided by the internet, which allows offenders to hide their identity and continue their actions without immediate detection.

Online sexual harassment can occur in both public and private digital spaces, including social media posts, private messages, and emails. In some cases, even known individuals may engage in such behavior, making it more difficult to address.

1.3.2.1 Forms of Online Sexual Harassment

Table 1.3.1 Forms of Online Sexual Harassment

S l no	Form of Cyber Crime	Explanation	Example
1	Sending Unwanted Sexual Messages	This form of cyber crime involves sending sexually explicit or inappropriate messages without the consent of the recipient. These messages are often repeated and cause discomfort.	A person repeatedly sends inappropriate messages through a messaging app despite being ignored.
2	Sharing Obscene Images or Videos	In this type of cyber crime, explicit images or videos are sent or shared without permission, violating the victim's privacy.	An individual sends explicit images to another person through social media without consent.
3	Posting Inappropriate Comments on Social Media	This cyber crime involves posting offensive or sexually suggestive comments on a person's online posts or profiles, which may be publicly visible.	Posting inappropriate remarks on someone's photo on a social media platform.
4	Online Stalking with Sexual Intent	This form of cyber crime includes repeatedly following, monitoring, and contacting a person online with sexual intentions.	A person continuously sends messages and tracks a user's online activity
5	Threats and Blackmail	This is a serious cyber crime where the offender threatens to share private content unless the victim complies with their demands.	An offender threatens to leak private photos to force the victim to obey.

SGOU

1.3.2.2 How to Prevent Online Sexual Harassment

Online sexual harassment is a serious cyber crime, but it can be reduced by following safe and responsible practices while using digital platforms. The following measures can help individuals protect themselves and ensure a safer online experience:

1. **Do not share personal information:** Avoid sharing sensitive details such as phone numbers, addresses, passwords, or private photos with unknown individuals online.

2. **Use privacy settings effectively:** Adjust privacy settings on social media platforms to control who can view your profile, posts, and personal information.

3. **Avoid interacting with strangers:** Be cautious while accepting friend requests or responding to messages from unknown people, as they may have harmful intentions.

4. **Block and report offenders:** If someone behaves inappropriately, immediately block the user and report the incident using the appropriate reporting mechanism. Cyber crime complaints can be reported through the National Cyber Crime Reporting Portal at https://cybercrime.gov.in/. The portal provides a dedicated Women/Children Related Crime category for reporting cyber crimes involving women and children. Complaints can be registered through the available reporting options on the portal.

5. **Do not respond to harassment:** Ignoring inappropriate messages can prevent encouraging the offender and reduce further interaction.

6. **Save evidence of harassment:** Keep screenshots, messages, or emails as proof, which can be useful while reporting the issue to authorities.

7. **Be aware of cyber safety practices:** Understanding common cyber threats and safe online behavior helps in identifying and avoiding risky situations.

1.3.2.3 Legal Provisions Related to Online Sexual Harassment

Online sexual harassment and related cyber offences may have legal consequences under the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita (BNS), 2023. The following provisions are relevant to some of the activities discussed in this section.

1. Section 66E of the Information Technology Act, 2000 – Violation of Privacy

Section 66E of the Information Technology Act, 2000 deals with the violation of privacy. It applies to specified acts involving the intentional or knowing capture, publication, or transmission of the image of a private area of a person without consent, in circumstances covered by the provision.

This provision is particularly relevant to cases involving the unauthorized capture or sharing of private images.

SGOU

Example: If a person's private image is captured and transmitted electronically without consent, the act may attract Section 66E, depending on the facts and circumstances of the case.

2. Section 67 of the Information Technology Act, 2000 – Obscene Material in Electronic Form

Section 67 deals with publishing or transmitting obscene material in electronic form. It is relevant to situations where obscene content is circulated through websites, social media platforms, messaging applications, or other electronic communication systems.

Example: Sharing obscene material through a social media platform may attract the provisions of Section 67, depending on the nature of the material and the circumstances of the case.

3. Section 67A of the Information Technology Act, 2000 – Sexually Explicit Material in Electronic Form

Section 67A deals with publishing or transmitting material containing a sexually explicit act or conduct in electronic form. It is relevant to serious cases involving the electronic transmission or publication of sexually explicit content.

Example: Uploading or transmitting sexually explicit material through a digital platform may attract Section 67A, subject to the applicable legal conditions.

4. Section 77 of the Bharatiya Nyaya Sanhita, 2023 – Voyeurism

Section 77 of the Bharatiya Nyaya Sanhita, 2023 deals with voyeurism. It addresses specified acts involving watching or capturing the image of a woman engaged in a private act where she would ordinarily expect privacy, and the subsequent dissemination of such an image in circumstances covered by the provision.

Example: Secretly recording a woman while she is engaged in a private act and sharing the recording without her consent may constitute an offence covered by Section 77, subject to the facts and circumstances of the case.

5. Section 78 of the Bharatiya Nyaya Sanhita, 2023 – Stalking

Section 78 of the Bharatiya Nyaya Sanhita, 2023 deals with stalking. It includes specified forms of repeatedly following or attempting to contact a woman despite a clear indication of disinterest, as well as monitoring a woman's use of the internet, email, or other forms of electronic communication, subject to the conditions specified in the provision.

Example: Repeatedly monitoring a woman's online activities or electronic communications despite her clear disinterest may fall within the scope of Section 78.

1.3.3 Online grooming

Online grooming is a serious form of cyber crime in which an adult establishes a relationship with a child through digital platforms with the intention of exploiting,

SGOU

manipulating, or abusing the child. This process involves gaining the child's trust over time and using that trust for harmful purposes.

In the digital environment, children frequently use social media, online games, and messaging applications for communication and entertainment. Cyber offenders take advantage of this by creating fake identities and pretending to be friendly individuals, often posing as someone of a similar age. This makes it easier to approach and interact with children without raising suspicion.

Online grooming is usually a gradual process. The offender begins by initiating contact and engaging in casual conversations to build rapport. Over time, the offender gains the child's trust by showing care, offering emotional support, or sharing common interests. Once trust is established, the offender may begin to request personal information, private images, or engage the child in inappropriate discussions.

In more serious cases, the offender may use emotional manipulation, threats, or blackmail to control the child and force them into harmful activities. Since these interactions take place online, children may not easily recognize the danger, making them more vulnerable to such cyber crimes.

1.3.3.1 Stages of Online Grooming

Online grooming occurs in a sequence of steps through which the offender gradually gains the trust of the child and exploits them. The main stages of online grooming are illustrated in Figure 1.3.1



Fig. 1.3.1 Stages of Online Grooming

1. Initiation

In this stage, the offender establishes contact with the child through social media, online games, or messaging applications. The offender may send friend requests or start casual conversations. Often, they pretend to be of a similar age or share common interests to gain attention and reduce suspicion.

2. Trust Building

The offender develops a friendly relationship by communicating regularly and gaining the child's confidence. They may show care and emotional support, making the child feel comfortable and secure. Over time, the child begins to trust the offender.

3. Exploitation

Once trust is established, the offender starts asking for personal information or private photos. They may also involve the child in inappropriate conversations. The child may share such information due to the trust developed.

4. Control and Manipulation

In this stage, the offender uses threats, emotional pressure, or blackmail to control the child. They may threaten to share private information if the child does not cooperate, making the child feel afraid and trapped.

1.3.4 Child Sexual Exploitation and Abuse Material (CSEAM)

Child sexual exploitation and abuse material (CSEAM) refers to visual or other recorded material that depicts or represents the sexual exploitation or sexual abuse of children. CSEAM is a serious form of cyber crime and represents a severe violation of the rights, dignity, privacy, and safety of children.

The term CSEAM is used in place of the earlier expression "child pornography." The Supreme Court of India, in *Just Rights for Children Alliance v. S. Harish* (2024), directed that the term "child pornography" should not be used in judicial orders or judgments and that the term "child sexual exploitation and abuse material (CSEAM)" should be used instead. The Court observed that the terminology should reflect the exploitative and abusive nature of such material rather than suggesting consensual activity.

CSEAM may involve the creation, distribution, possession, or viewing of sexually explicit material involving children through digital platforms. Such material may be created, stored, and shared through websites, social media platforms, messaging applications, or other online channels.

Offenders may exploit children by forcing, manipulating, or deceiving them into participating in the creation of such material. In many cases, children may not fully understand the consequences of their actions, making them more vulnerable to exploitation.

This cyber crime is highly dangerous because digital content can be easily copied and distributed to a large audience within a short period. Once such material is shared online, it becomes extremely difficult to remove completely, which can lead to continuous and repeated harm to the victim.

CSEAM is often linked with other cyber crimes such as online grooming, where offenders build trust with children before exploiting them. The availability and circulation of such material can encourage further criminal activities and increase the risk of child abuse.

SGOU

1.3.4.1 Effects of Child sexual exploitation and abuse material (CSEAM)

CSEAM, as a serious form of cyber crime, can have severe and long-lasting effects on victims. These effects can impact the physical, emotional, psychological, and social well-being of children.

1. **Emotional Trauma:** Victims may experience fear, shame, anxiety, and depression due to exploitation and abuse.

2. **Psychological Stress:** Victims may suffer from emotional distress, loss of confidence, and difficulties in trusting others.

3. **Social Isolation:** Fear of judgment, embarrassment, or exposure may cause victims to withdraw from friends, family, and society.

4. **Damage to Reputation:** Since digital content can spread rapidly, the victim's dignity and privacy may be affected.

5. **Long-Term Harm:** The continued circulation of CSEAM can repeatedly harm the victim, even after the original incident has occurred.

1.3.4.2 How to Prevent Child sexual exploitation and abuse material (CSEAM)

1. **Educate Children about Online Safety:** Children should be made aware of the risks associated with sharing personal information, photos, or videos online.

2. **Parental Supervision:** Parents and guardians should monitor children's online activities while respecting their privacy and encouraging open communication.

3. **Avoid Sharing Private Content:** Children should be advised not to share private images or videos with strangers or unknown persons online.

4. **Use Privacy Settings:** Appropriate privacy and security settings should be enabled on social media platforms and other online services.

5. **Report Suspicious Activities:** Suspicious online interactions, attempts to obtain private images, or suspected exploitation should be reported to the appropriate platform and authorities.

6. **Create Awareness:** Schools, parents, educational institutions, and society should create awareness about online exploitation and responsible digital behavior.

7. **Preserve Evidence:** Relevant messages, screenshots, URLs, usernames, and other digital evidence should be preserved when reporting suspected exploitation.

SGOU

1.3.5 Human Trafficking through Digital Platforms

Human trafficking through digital platforms is a form of cyber crime in which offenders use online technologies such as social media, websites, and messaging applications to recruit, deceive, transport, or exploit individuals for illegal purposes such as forced labor or sexual exploitation.

In the modern digital environment, traffickers make use of online platforms to identify and target vulnerable individuals. They often create fake profiles, post attractive job offers, or send messages promising better opportunities such as employment, education, or a better lifestyle. These offers appear genuine and convincing, which makes victims trust the offenders.

Once the victim responds, the trafficker gradually manipulates or deceives them and may eventually exploit them. Digital platforms make this cyber crime more dangerous because offenders can easily hide their identity and reach a large number of people within a short time. This type of crime is especially harmful as victims may not realize the danger until they are trapped, leading to serious physical, emotional, and psychological consequences.

1.3.5.1 Methods Used in Digital Human Trafficking

Human trafficking through digital platforms is carried out using various deceptive methods. These methods are designed to attract, manipulate, and exploit victims through online technologies.

1. Fake Job Offers

Traffickers post attractive job advertisements on websites and social media platforms, offering high salaries and better opportunities. These offers often appear genuine and target individuals who are searching for employment. Once the victim shows interest, they are misled and eventually exploited.

2. Social Media Manipulation

Offenders create fake profiles on social media platforms to approach and communicate with potential victims. They build trust by engaging in friendly conversations and gradually manipulate the victim. This method is similar to online grooming and is commonly used to trap individuals.

3. Online Advertisements

Traffickers use misleading online advertisements to attract victims by offering unrealistic benefits such as free travel, education, or job opportunities. These advertisements are designed to appear legitimate and encourage individuals to respond without verification.

4. Messaging and Communication Applications

Private messaging platforms are used by traffickers to communicate secretly with victims. They use these platforms to control, influence, and monitor the victim's actions without attracting attention.

SGOU

5. Online Grooming and Relationship Building

Traffickers may use online platforms to establish relationships with potential victims and gradually gain their trust. They may communicate regularly, show concern, offer emotional support, or pretend to share common interests. After gaining the victim's trust, traffickers may manipulate or deceive them and eventually exploit them for forced labour, sexual exploitation, or other purposes.

1.3.5.2 Legal Provisions Related to Human Trafficking

Human trafficking is a serious criminal offence involving the recruitment, transportation, transfer, harbouring, or receiving of persons for the purpose of exploitation. In India, human trafficking and certain related forms of exploitation are addressed through the Bharatiya Nyaya Sanhita (BNS), 2023 and the Immoral Traffic (Prevention) Act (ITPA), 1956.

1. BNS Section 143 – Trafficking of Person

Section 143 of the Bharatiya Nyaya Sanhita, 2023 deals with trafficking of persons. It covers recruiting, transporting, harbouring, transferring, or receiving a person for exploitation through means such as threats, force, coercion, abduction, fraud, deception, abuse of power, or inducement. The provision includes forms of exploitation such as physical exploitation, sexual exploitation, slavery or practices similar to slavery, servitude, beggary, and forced removal of organs.

Example: A person uses a fake job advertisement on social media to deceive an individual and recruit them for exploitation. Such conduct may fall within the scope of Section 143, depending on the facts and circumstances of the case.

2. BNS Section 144 – Exploitation of a Trafficked Person

Section 144 of the Bharatiya Nyaya Sanhita, 2023 deals with the exploitation of a trafficked person. It specifically addresses sexual exploitation of a trafficked person and provides stronger protection where the trafficked person is a child.

Example: A person who knowingly or having reason to believe that a person has been trafficked engages that person for sexual exploitation may attract Section 144 of the BNS, subject to the facts and circumstances of the case.

3. Immoral Traffic (Prevention) Act, 1956 – Sections 3 to 6

The Immoral Traffic (Prevention) Act, 1956 (ITPA) addresses activities connected with prostitution and related exploitation. The following provisions are relevant to understanding trafficking-related activities involving prostitution:

- **Section 3** – Keeping a brothel or allowing premises to be used as a brothel: This provision deals with maintaining or managing a brothel or knowingly allowing premises to be used as a brothel.
- **Section 4** – Living on the earnings of prostitution: This provision deals with persons who knowingly live, wholly or partly, on the earnings of prostitution of another person, subject to the conditions specified in the Act.

SGOU

- **Section 5** – Procuring, inducing or taking a person for the sake of prostitution: This provision addresses specified acts of procuring, inducing, taking, or causing a person to be taken for the purpose of prostitution.
- **Section 6** – Detaining a person in premises where prostitution is carried on: This provision deals with the detention of a person in premises where prostitution is carried on, under the circumstances specified in the Act.

Recap

- People use the internet, smartphones, and social media every day.
- Women and children are the most vulnerable to cyber crimes.
- Cyber crimes can cause emotional and mental harm to victims.
- Online sexual harassment includes unwanted messages, sharing obscene content, posting bad comments, stalking, and making threats.
- To prevent harassment, people should use privacy settings, avoid strangers, block or report offenders, save evidence, and stay alert.
- Online grooming happens when adults build trust with children to exploit them.
- The stages of grooming are starting contact, building trust, exploiting, and controlling the child.
- Child sexual exploitation and abuse material (CSEAM) involves making, sharing, or keeping sexual content involving minors.
- Child sexual exploitation and abuse material (CSEAM) can cause emotional trauma, mental stress, social isolation, damage to reputation, and long-term harm.
- Prevention of child pornography includes teaching children about safety, supervising their online activity, avoiding sharing private content, using privacy settings, reporting suspicious activity, and raising awareness.
- Human trafficking through digital platforms happens using fake jobs, social media tricks, misleading ads, and messaging apps to exploit victims, Online Grooming and Relationship Building.
- Human trafficking is addressed under BNS Section 143, while BNS Section 144 deals with the exploitation of trafficked persons.
- The Immoral Traffic (Prevention) Act, 1956 (ITPA) contains relevant provisions relating to prostitution and related exploitation, including Sections 3, 4, 5, and 6.

SGOU

Objective Type Questions

1. What term describes harmful online actions against women and children?
2. What is sending unwanted sexual messages called?
3. What term refers to building trust with a child to exploit them?
4. Which stage of grooming involves asking for personal information?
5. What does CSEAM refer to?
6. What is the act of repeatedly following someone online called?
7. What is the online crime of tricking victims with fake jobs?
8. Which practice can help prevent CSEAM?
9. Which section of the BNS deals with trafficking of persons?

Answers to Objective Type Questions

1. Cybercrime
2. Harassment
3. Grooming
4. Exploitation
5. Child Sexual Exploitation and Abuse Material
6. Stalking
7. Trafficking
8. Educating children about online safety
9. Section 143

Assignments

1. Explain online sexual harassment. Describe its different forms and how it affects women and children in the digital environment. Give examples for better understanding.

2. What is online grooming? Explain the stages involved in online grooming and how children can become vulnerable to such crimes.

SGOU

3. Describe child sexual exploitation and abuse material (CSEAM). Discuss its effects on the physical, emotional, psychological, and social well-being of children and suggest measures to prevent it.

4. Explain human trafficking through digital platforms. Describe the methods used by traffickers to exploit victims online and give examples of how they operate.

5. Discuss the preventive measures that can be taken to protect women and children from cyber crimes. Explain why awareness and responsible online behavior are important.

Suggested Reading

1. Brooks, Charles J., et al. *Cybersecurity Essentials*. Wiley, 2018.

2. Yar, Majid. *Cybercrime and Society*. SAGE Publications.

3. Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. *Cybercrime and Digital Forensics: An Introduction*. Routledge.

4. Godbole, Nina, and Sunit Belapure. *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*. Wiley India.

Reference

1. India. *The Information Technology Act, 2000*. Government of India.

2. India. *The Bharatiya Nyaya Sanhita, 2023*. Government of India.

3. India. *The Protection of Children from Sexual Offences Act, 2012*. Government of India.

4. India. *The Immoral Traffic (Prevention) Act, 1956*. Government of India.

5. Government of India. *National Cyber Crime Reporting Portal*. Ministry of Home Affairs.

SGOU



UNIT 4 Cyber Crime against Government

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- explain the concept of cyber terrorism and its methods
- describe website defacement, its causes, and effects
- explain attacks on critical infrastructure and their impact
- describe unauthorized access to government data and its consequences
- explain espionage, surveillance, and common attacks on government networks

Prerequisites

In your daily life, you regularly use digital technologies such as mobile phones, the internet, online banking, social media, and government websites for communication and accessing services. You may already be aware of basic cyber threats such as hacking, phishing, malware, and online frauds that affect individuals and organizations. These concepts help you understand how attackers misuse digital platforms to steal information or cause harm.

Now, think about how important systems like electricity supply, transportation, healthcare services, and government databases also depend on similar digital technologies. Just like personal systems, these large-scale systems can also become targets of cyber attacks. However, when such systems are attacked, the impact is much greater, affecting not just one person but a large number of people and even the entire country.

In this unit, you will build on your existing knowledge of cyber security and explore how cyber crimes are carried out against government systems and national infrastructure. You will learn about serious threats such as cyber terrorism, website defacement, attacks on critical infrastructure, unauthorized access to government data, espionage, and surveillance. You will also understand common attack methods used against government networks.

SGOU

By connecting your prior understanding of basic cyber threats with these advanced concepts, you will be able to clearly understand the importance of protecting government systems, ensuring data security, and maintaining public safety in the digital age. This knowledge will help you develop a broader perspective on cyber security and its role in national development.

Key concepts

Cyber terrorism, Website defacement, Critical infrastructure attacks, Unauthorized access, Espionage, Surveillance

Discussion

1.4.1 Cyber Terrorism

Cyber terrorism is a serious form of cyber crime in which computer systems, networks, and digital technologies are used to carry out attacks that threaten national security, disrupt essential services, and create fear among the public.

In the modern digital environment, governments rely heavily on information systems for administration, communication, defense, and the delivery of public services. This dependence makes government systems vulnerable to cyber attacks. Cyber terrorists exploit weaknesses in these systems to gain unauthorized access, disrupt operations, or damage critical infrastructure.

The primary objective of cyber terrorism is not only to cause technical damage but also to create panic, instability, and insecurity within society. These attacks are often planned and may be motivated by political, ideological, or religious factors. In many cases, cyber terrorism involves organized groups that use advanced technological tools and techniques.

Cyber terrorism can take various forms, including unauthorized access to government networks, disruption of communication systems, spreading of false information, and attacks on critical infrastructure such as power grids or transportation systems. Due to the anonymous nature of the internet, identifying and preventing such attacks can be challenging.

An example of cyber terrorism is an attack on a country's power grid, where cyber attackers gain access to control systems and disrupt electricity supply across major regions. This can affect hospitals, transportation, and communication systems, leading to widespread panic and disruption.

Legal Reference: Section 66F of the Information Technology Act, 2000

Cyber attacks that threaten the security and integrity of a country can have serious consequences. In India, Section 66F of the Information Technology Act, 2000 deals

SGOU

specifically with cyber terrorism.

The provision covers certain acts involving unauthorized access to or attempts to access computer resources when carried out with the intention of threatening the unity, integrity, security, or sovereignty of India, or causing or likely to cause damage to critical information infrastructure. It also covers certain unauthorized access or disruption of computer resources that may cause harm to national security or other essential interests.

Cyber terrorism is therefore considered a serious cyber offence because it can target important computer systems and digital infrastructure and may pose a threat to national security.

The detailed legal provisions and penalties for cyber offences, including the relevant provisions of the Information Technology Act, 2000, are discussed further in Block VI.

1.4.1.1 Methods of Cyber Terrorism

Cyber terrorism involves the use of various techniques to attack government systems, disrupt essential services, and create fear among the public. These methods are carefully planned and executed using advanced digital tools and technologies.

1. Denial of Service (DoS) Attacks:

A Denial-of-Service (DoS) attack is a cyber attack in which an attacker attempts to make a computer system, network, server, or online service unavailable to legitimate users. The attack may be carried out by overwhelming the target with a large number of requests or by exploiting weaknesses in the system that consume its available resources.

DoS attacks can occur through different methods, including:

1. **Flooding:** The attacker sends a very large number of requests or data packets to the target system. The excessive traffic consumes network bandwidth or processing capacity, making the service slow or unavailable to legitimate users.

2. **Resource Exhaustion:** The attacker deliberately consumes limited system resources such as memory, processing power, network connections, or storage. When these resources are exhausted, the system may become slow, unstable, or unavailable.

3. **Vulnerability-Based DoS:** The attacker exploits a weakness or vulnerability in software, a network protocol, or a system service to cause it to crash, become unresponsive, or consume excessive resources. Unlike a flooding attack, this type of DoS attack may succeed even without generating a very large volume of traffic.

2. Malware Attacks:

Cyber terrorists use malicious software such as viruses, worms, and ransomware to damage systems or gain unauthorized access. Malware can delete files, steal sensitive data, or block access to important systems, causing serious disruption.

SGOU

3. Unauthorized Access (Hacking):

In this method, attackers exploit security vulnerabilities to gain illegal access to government systems or databases. Once inside, they may steal, modify, or destroy confidential information.

4. Website Defacement:

Cyber terrorists may hack government websites and change their content to display false information, propaganda, or threatening messages. This can damage the reputation of the government and create fear among citizens.

5. Attacks on Critical Infrastructure:

Cyber terrorists target essential services such as power grids, transportation systems, healthcare systems, and communication networks. Disrupting these services can affect daily life and create large-scale panic.

6. Data Theft and Cyber Espionage:

Attackers secretly access and steal sensitive government data such as defense information, strategic plans, or confidential records. This information may be misused for political or strategic advantage.

1.4.2 Website Defacement

Website defacement is a form of cyber crime in which an unauthorized individual gains access to a website and modifies its content without permission. In this attack, the original information displayed on the website is replaced with false, offensive, or misleading content.

This type of attack commonly targets government and organizational websites because they are widely accessed by the public. By altering the content, attackers aim to damage the credibility and reputation of the organization. In some cases, website defacement is used to spread political messages, propaganda, or warnings to a large audience.

Website defacement usually occurs due to security weaknesses such as poor authentication mechanisms, unpatched software vulnerabilities, or improper access control. Even a small security gap can allow attackers to gain control of the website and make unauthorized changes.

1.4.2.1 Causes of Website Defacement

1. **Weak Passwords or Poor Authentication:** The use of simple or easily guessable passwords, along with inadequate authentication mechanisms, makes it easier for attackers to gain unauthorized access to the website.
2. **Unpatched Software or Outdated Systems:** Websites that use outdated software or fail to install security updates remain vulnerable to known threats, which attackers can exploit to access and modify content.
3. **Lack of Proper Security Measures:** Absence of essential security controls

SGOU

such as firewalls, intrusion detection systems, and secure configurations increases the risk of unauthorized access.

4. **Vulnerabilities in Web Applications:** Security flaws in web applications, such as improper input validation or coding errors, can be exploited by attackers to gain control over the website.

1.4.2.2 Effects of Website Defacement

Table 1.4.1 Effects of Website Defacement

Sl no	Effect	Description
1	Loss of Reputation	Website defacement damages the image of a government or organization. Users may lose trust when they see that the website has been hacked, reducing confidence in its security.
2	Spread of False Information	Attackers may display incorrect or harmful information on the website. Users may believe this information, leading to confusion or wrong decisions.
3	Service Disruption	The normal functioning of the website may be affected. Important services may become unavailable, causing inconvenience to users.
4	Security Concerns	A defaced website shows that there are security weaknesses. This increases the risk of further attacks such as data theft or malware infections.

1.4.2.3 Preventive Measures of Website Defacement

Protecting a website from defacement is similar to protecting a house from intruders. Just as we lock doors, install security systems, and regularly check for safety, websites also need proper protection to prevent unauthorized access.

1. Use Strong Passwords and Authentication Methods:

Just like a strong lock protects a house, strong passwords protect a website. Using complex passwords and additional security methods like two-factor authentication makes it difficult for attackers to break in.

2. Regularly Update and Patch Software:

Software updates act like repairs for weak points in a system. If a website uses outdated software, attackers can easily find and exploit known weaknesses. Regular updates help in closing these security gaps.

SGOU

3. Implement Proper Security Controls and Monitoring:

Installing security tools such as firewalls and monitoring systems is like having CCTV cameras and security guards. These tools help detect suspicious activities and prevent attacks before they cause damage.

4. Conduct Regular Security Audits and Testing:

Regular checking of the system helps identify hidden weaknesses. Just like periodic inspections ensure safety in buildings, security audits help in finding and fixing vulnerabilities in websites.

1.4.3 Attacks on Critical Infrastructure

Attacks on critical infrastructure are a type of cyber crime in which attackers target essential systems and services such as electricity, transportation, healthcare, and communication networks with the aim of disrupting their normal functioning.

Critical infrastructure refers to the basic systems that are necessary for the smooth functioning of a country. When cyber attackers target these systems, they attempt to damage, control, or disrupt these services using digital technologies.

These attacks can lead to serious problems such as power failures, communication breakdowns, or disruption of healthcare services. Since a large number of people depend on these systems, even a small attack can affect many individuals and create panic in society.

1.4.3.1 Types of Critical Infrastructure Attacks

1. Power Grid Attacks

Power grid attacks target the electricity supply systems of a country, which are controlled by digital technologies. Attackers may gain access to these control systems and shut down or manipulate the power supply. Such attacks can lead to large-scale blackouts, affecting homes, industries, hospitals, and communication systems. For example, if attackers hack into a city's power control system and disrupt electricity supply, it can affect traffic signals, hospital operations, and daily life.

2. Transportation System Attacks

Transportation system attacks focus on digital systems used in railways, airports, traffic signals, and public transport. These systems depend on computer networks for scheduling and communication. Attackers may disrupt these systems, causing delays, confusion, or accidents. For example, if a railway signaling system is manipulated, trains may be delayed or misrouted, leading to serious operational issues.

3. Healthcare System Attacks

Healthcare systems include hospitals and medical databases that store important patient information. Cyber attacks on these systems can disrupt medical services and delay treatments. In some cases, attackers may block access to patient records, making it difficult for doctors to provide proper care. For instance, a ransomware attack on a hospital system can prevent access to patient data during emergencies, affecting treatment decisions.

SGOU

4. Communication Network Attacks

Communication networks such as internet services, telephone systems, and emergency communication channels are essential for information sharing. Attackers may target these networks to disrupt communication, leading to confusion and delays in response. For example, if a cyber attack disables internet and phone services in a region, it can affect communication between people and emergency services during critical situations.

1.4.4 Unauthorized Access to Government Data

Unauthorized access to government data is a type of cyber crime in which an individual or group gains access to confidential or sensitive government information without permission. This data may include citizens' personal details, financial records, official documents, or information related to national security. Such unauthorized access usually occurs through methods like hacking, weak passwords, phishing attacks, or malware.

Once access is gained, attackers may steal, modify, or misuse the data for personal, financial, or political gain. This can lead to serious consequences such as data breaches, identity theft, financial loss, and threats to national security. In some cases, the stolen data may also be sold or shared with other attackers, increasing the risk further.

This type of cyber crime not only affects individuals whose data is exposed but also damages the credibility and trust of government institutions. Therefore, protecting government data from unauthorized access is essential to ensure security, privacy, and proper functioning of public systems.

1.4.4.1 Effects of Unauthorized Access to Government Data

1. Loss of Confidential Information

Unauthorized access can lead to the exposure or leakage of sensitive government data. This may include personal details of citizens, official records, or classified information. Such data, once leaked, can be difficult to recover or control. For example, if an attacker gains access to a government database containing citizens' personal information, such as Aadhaar or financial records, the data may be leaked or misused.

2. Threat to National Security

When attackers access confidential information related to defense, intelligence, or strategic operations, it can pose a serious threat to national security. Such information can be used against the country. For example, if defense-related data or military plans are accessed by unauthorized individuals, it may weaken the country's security and give advantage to hostile entities.

3. Identity Theft and Misuse of Data

Stolen personal data can be used by attackers to impersonate individuals and carry out illegal activities. This includes financial fraud, opening fake accounts, or committing crimes using someone else's identity. For instance, if an attacker obtains personal details such as name, address, and ID numbers from a government database, they may use this information to perform fraudulent transactions.

SGOU

4. Financial Loss

Unauthorized access can result in financial damage to both individuals and the government. Attackers may manipulate financial data, steal funds, or carry out fraud. For example, if attackers access a government financial system, they may transfer funds illegally or alter financial records, leading to economic loss.

5. Loss of Trust in Government Systems

When government data is compromised, people may lose confidence in the system's ability to protect their information. This can affect the credibility and reliability of government institutions. For example, if a data breach exposes citizens' personal information, people may hesitate to use government digital services in the future.

1.4.5 Espionage

Espionage means secretly collecting important or confidential information without permission. In the context of cyber crime, this is called cyber espionage, where attackers use computers, networks, and the internet to access sensitive government data.

The main goal of espionage is to obtain valuable information such as defense plans, government policies, confidential reports, or strategic decisions. Attackers usually carry out these activities silently and over a long period of time so that they are not detected.

To perform espionage, attackers may use techniques such as hacking into secure systems, sending phishing emails to gain login details, or installing malware to access data. Once the information is collected, it may be used for political, military, or economic advantage, or even shared with other unauthorized parties.

Espionage is considered very dangerous because it can weaken national security and expose sensitive information that should remain confidential.

For example, if a hacker gains access to a government defense system and secretly collects information about military strategies over several months without being detected, it is an act of cyber espionage.

1.4.6 Surveillance

Surveillance means continuously monitoring a person, system, or network to observe activities and collect information. In cyber crime, unauthorized surveillance occurs when someone monitors another person's digital activities without their knowledge or permission.

Attackers may use tools such as spyware, tracking software, or monitoring programs to observe emails, messages, browsing history, or even location data. This allows them to collect personal or sensitive information about the victim.

While surveillance can be used legally by governments for security purposes, illegal surveillance becomes a cyber crime when it violates privacy. It can be used to control, threaten, or misuse the collected information.

Continuous monitoring can also create fear and discomfort for the victim, as they may feel that their privacy is being invaded.

SGOU

For example, if an attacker installs spyware on a person's computer or mobile phone and secretly tracks their messages, calls, and online activities, it is considered illegal surveillance.

1.4.7 Use Cases – Common Attacks on Government Networks

Government networks are widely used to store, process, and manage important information and services. Due to the sensitive nature of this data, these networks are common targets for cyber attackers. Various types of cyber attacks are carried out on government systems to steal information, disrupt services, or create panic among the public.

The following are some of the most common attacks on government networks:

1. Phishing Attacks

Phishing attacks are one of the most common methods used to target government employees. In this attack, fake emails or messages are sent that look like they come from trusted sources such as senior officials, departments, or service providers. These messages usually create urgency and ask the user to click a link or provide login details.

If the employee trusts the message and enters their information, the attacker collects the data and gains access to government systems. This type of attack mainly depends on human error rather than technical weakness.

For example, a government employee may receive an email that appears to be from their department asking them to update their password. When they click the link and enter the details, the attacker captures the login credentials.

2. Malware Attacks

Malware attacks involve the use of harmful software such as viruses, worms, or ransomware to damage systems or steal data. Attackers usually send malicious files through email attachments or links. When the user opens the file, the malware gets installed in the system.

Once inside, the malware can delete files, steal information, or even block access to important data. In government systems, this can disrupt services and affect important operations.

For instance, if a government employee opens an infected attachment, ransomware may lock all important files and demand payment to restore access.

3. Denial of Service (DoS) Attacks

A Denial-of-Service (DoS) attack is a cyber attack in which an attacker attempts to make a computer system, network, server, or online service unavailable to legitimate users. The attack may be carried out by overwhelming the target with a large number of requests or by exploiting weaknesses in the system that consume its available resources.

DoS attacks can occur through different methods, including:

1. **Flooding:** The attacker sends a very large number of requests or data packets

SGOU

to the target system. The excessive traffic consumes network bandwidth or processing capacity, making the service slow or unavailable to legitimate users.

2. **Resource Exhaustion:** The attacker deliberately consumes limited system resources such as memory, processing power, network connections, or storage. When these resources are exhausted, the system may become slow, unstable, or unavailable.

3. **Vulnerability-Based DoS:** The attacker exploits a weakness or vulnerability in software, a network protocol, or a system service to cause it to crash, become unresponsive, or consume excessive resources. Unlike a flooding attack, this type of DoS attack may succeed even without generating a very large volume of traffic.

The main objective of a DoS attack is to disrupt the availability of a service and prevent legitimate users from accessing it. For example, an attacker may exploit a vulnerability in a web server, causing the server to crash whenever a specially crafted request is received.

DoS attacks can affect websites, online applications, banking services, communication systems, and other critical digital services. Therefore, organizations should regularly update software, fix security vulnerabilities, monitor network activity, and implement appropriate security controls to reduce the risk of DoS attacks.

4. Unauthorized Access (Hacking)

Unauthorized access, or hacking, occurs when attackers gain access to government systems without permission by exploiting security weaknesses. Once they enter the system, they can view, change, or delete important data.

This type of attack is dangerous because it directly affects the confidentiality and integrity of government information.

For example, a hacker may break into a government database and access sensitive information such as citizen records or official documents.

5. Website Defacement

Website defacement is an attack where the content of a government website is changed without permission. Attackers may replace the original content with false information, messages, or images.

This affects the reputation of the government and may mislead users who visit the website. It also shows that the system is not secure.

For example, the homepage of a government website may be replaced with unauthorized or offensive content by attackers.

6. Insider Attacks

Insider attacks occur when individuals within the organization misuse their access

SGOU

to systems. These individuals may be employees, staff members, or anyone who has authorized access.

They may intentionally leak confidential information or accidentally cause security issues by sharing login details. Since insiders already have access, these attacks are difficult to detect.

For example, a staff member may share confidential government data with unauthorized persons or misuse it for personal benefit.

Recap

- Cyber terrorism is a cyber crime that targets government systems to create fear and disrupt national security.
- It uses methods such as DoS attacks, malware, hacking, website defacement, and attacks on critical infrastructure.
- Website defacement involves unauthorized modification of website content to damage reputation and spread false information.
- It occurs due to weak passwords, outdated software, lack of security measures, and application vulnerabilities.
- Website defacement leads to loss of trust, spread of misinformation, service disruption, and security risks.
- Attacks on critical infrastructure target essential services like electricity, transportation, healthcare, and communication.
- These attacks cause large-scale disruption and create panic among the public.
- Unauthorized access to government data involves illegal access to sensitive information without permission.
- It results in data theft, identity misuse, financial loss, and threats to national security.
- Espionage refers to secretly collecting confidential information for advantage.
- Surveillance involves continuous monitoring of activities, often violating privacy.
- Government networks are targeted through phishing, malware, DoS attacks, hacking, website defacement, and insider attacks.

SGOU

Objective Type Questions

1. What type of cyber crime aims to create fear and threaten national security?
2. Which attack floods a server with excessive requests?
3. What is the unauthorized modification of a website called?
4. What type of software is used to damage or disrupt systems?
5. What is illegal access to a system known as?
6. What type of attack targets electricity and transport systems?
7. What is the secret collection of confidential information called?
8. What is continuous monitoring of activities known as?
9. What attack tricks users into revealing login details?
10. Which type of cyber attack targets essential services such as power grids, transportation systems, and communication networks?
11. Which section of the Information Technology Act, 2000 deals with cyber terrorism?
12. What type of attack is carried out by authorized users?
13. Name one critical infrastructure that can be targeted by cyber terrorists.

SGOU

Answers to Objective Type Questions

1. Cyberterrorism
2. DoS
3. Website Defacement
4. Malware
5. Hacking
6. Infrastructure
7. Espionage
8. Surveillance

9. Phishing
10. Attacks on Critical Infrastructure
11. Section 66F
12. Insider
13. Power Grid

Assignments

1. Explain the concept of cyber terrorism as a form of cyber crime. Describe the various methods used in cyber terrorism and discuss their impact on government systems.
2. Define website defacement and explain its causes and effects. Also discuss the preventive measures that can be taken to protect websites from such attacks.
3. What are attacks on critical infrastructure? Explain the different types of critical infrastructure attacks with suitable examples.
4. Explain unauthorized access to government data and discuss its major effects on individuals and national security with examples.
5. Describe espionage and surveillance in the context of cyber crime. Also explain common attacks on government networks such as phishing, malware, and insider attacks.

SGOU

Suggested Reading

1. Brooks, Charles J., et al. *Cybersecurity Essentials*. Wiley, 2018.
2. Stallings, William. *Network Security Essentials: Applications and Standards*. Pearson.
3. Kizza, Joseph Migga. *Guide to Computer Network Security*. Springer.
4. Godbole, Nina, and Sunit Belapure. *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*. Wiley India.

Reference

1. India. *The Information Technology Act, 2000*. Government of India.

2. India. *The Bharatiya Nyaya Sanhita, 2023*. Government of India.

3. Indian Computer Emergency Response Team. *Cyber Security Advisories and Guidelines*. Ministry of Electronics and Information Technology, Government of India.

4. National Institute of Standards and Technology. *Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce, 2024.

5. Government of India. *National Cyber Crime Reporting Portal*. Ministry of Home Affairs.

SGOU



BLOCK 2

Cyber Crime Against Organizations

SGOU



Network and System based Cyber Attacks

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- understand the concept of network and system-based cyber attacks and their impact
- explain different types of attacks such as DoS, DDoS, Backdoors, Malware, and MitM
- analyze how these attacks work and identify their effects on systems and networks
- apply appropriate prevention and security measures to protect systems from cyber threats

Prerequisites

Understanding network and system-based cyber attacks is important because modern systems are highly dependent on digital communication and online services. Attacks such as DoS, DDoS, malware, backdoors, and MitM can disrupt services, steal sensitive data, and cause financial loss. In real life, incidents like large-scale DDoS attacks on popular websites or malware infections through email attachments have shown how vulnerable systems can be. For example, when users access public Wi-Fi without proper security, attackers can intercept their data, leading to identity theft or financial fraud.

Traditional security methods such as firewalls, antivirus software, and basic encryption play a crucial role in protecting systems. These methods provide advantages like early threat detection, prevention of unauthorized access, and protection against common malware. Although they may not stop all advanced attacks, they form the first line of defense and significantly reduce risks when combined with modern security practices.

Keywords

Traffic Flooding, SYN Flood, Application Layer Attack, Backdoor, Malware, Virus, Worm, Trojan Horse, Ransomware, Spyware, Botnet, Rootkit, Man-in-the-Middle(MitM) Attack, ARP Spoofing, DNS Spoofing, Session Hijacking, SSL Stripping

SGOU

Discussion

2.1.1 Introduction

With the increasing use of computer networks and information systems in various sectors, cybersecurity has become an important concern. Network and system-based cyber attacks are malicious activities that target computer networks, servers, and systems to disrupt services, steal information, or gain unauthorized access. These attacks exploit vulnerabilities in network infrastructure, software, and communication protocols.

Some common types of network- and system-based cyber attacks include Denial-of-Service (DoS) attacks, Distributed Denial-of-Service (DDoS) attacks, Backdoors and Malware, and Man-in-the-Middle (MitM) attacks. A DoS attack attempts to make a system or service unavailable to legitimate users by exhausting its resources, such as bandwidth, connections, or processing capacity. When such attacks are carried out using multiple compromised devices simultaneously, they become DDoS attacks, which are more powerful and difficult to control.

Malware refers to malicious software designed to damage or disrupt systems, while backdoors allow attackers to bypass security mechanisms and gain unauthorized access to a system. Another significant threat is the Man-in-the-Middle (MitM) attack, where an attacker secretly intercepts communication between two parties to steal or manipulate sensitive information.

Understanding these attacks is essential for improving network security and protecting systems from potential cyber threats.

2.1.2 Denial-of-Service (DoS) Attack

A Denial-of-Service (DoS) attack is a type of cyber attack in which an attacker attempts to make a system, server, network, or application unavailable to legitimate users by exhausting its network bandwidth, system resources, or application-level resources. A DoS attack does not necessarily depend on sending a large volume of traffic or requests; different DoS techniques can target different resources of the victim system.

The main types of DoS attacks include Traffic Flooding Attacks, SYN Flood Attacks, and Application Layer Attacks.

Types of DoS Attacks

Some common types of DoS attacks include:

1. Traffic Flooding Attack

A traffic flooding attack attempts to overwhelm the target network or server by sending a very large amount of traffic. The excessive traffic consumes available bandwidth and network resources, making it difficult for legitimate users to access the service.

Example: An attacker continuously sends a large number of data packets to a web server. As the server receives more traffic than it can handle, its resources become exhausted and legitimate requests may be delayed or rejected.

SGOU

2. SYN Flood Attack

A SYN flood attack exploits the TCP connection establishment process. The attacker sends a large number of SYN requests to the target server but does not complete the TCP three-way handshake. The server keeps resources reserved for these incomplete connections, eventually exhausting its connection capacity.

Example: An attacker sends thousands of SYN requests using spoofed or unreachable source addresses. The server waits for the remaining handshake messages, causing its connection queue to fill and preventing legitimate users from establishing connections.

3. Application Layer Attack

An application layer attack targets a specific application or service rather than simply overwhelming the network with high-volume traffic. The attacker sends specially crafted or repeated requests that consume the application's processing resources, connections, or other limited resources.

Example – Slowloris: Slowloris opens many HTTP connections to a web server and keeps them alive by sending partial HTTP requests very slowly. The server keeps these connections open while waiting for the requests to be completed. As the available connection pool becomes exhausted, legitimate users may be unable to establish new connections. Slowloris is particularly important because it can cause a denial of service while using very little bandwidth, demonstrating that a DoS attack does not necessarily require high-volume traffic.

Effects of DoS Attack

- Slowing down of network services
- Server crash or shutdown
- Temporary unavailability of websites or applications
- Financial loss and service disruption

Suppose an attacker continuously sends thousands of requests to a university website server within a short period. The server becomes overloaded while processing these requests, preventing legitimate students from accessing the website.

In the fig 2.1.1, the attacker system generates continuous high traffic toward the web server, causing it to become slow or crash due to excessive load.

As a result, legitimate users are unable to access the service and receive error messages such as “No Access” or “Service Unavailable.” The main aim of this attack is to disrupt the normal functioning of the server rather than to steal data.

Prevention Methods

Some common methods to prevent DoS attacks include::

- **Traffic filtering and rate limiting** – Restrict excessive or abnormal traffic and limit the number of requests accepted from a source.

SGOU

- **Load balancing and resource management** – Distribute requests across multiple servers and allocate resources efficiently to prevent a single system from becoming overloaded.
- **Network monitoring and anomaly detection** – Identify unusual traffic patterns and sudden increases in requests so that mitigation can begin quickly

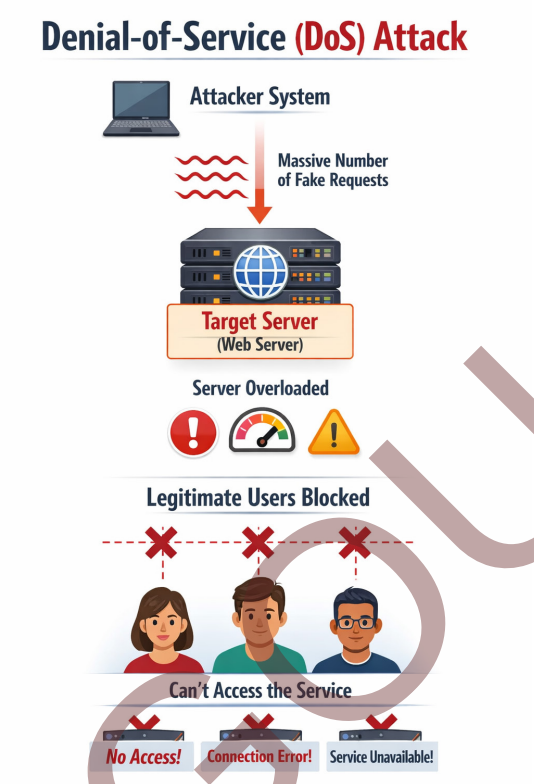


Fig 2.1.1 Denial-of-Service (DoS) Attack

A Denial-of-Service attack is designed to disrupt the availability of network services by overwhelming a system with excessive traffic. Proper security mechanisms and network monitoring are necessary to detect and mitigate such attacks.

2.1.3 Distributed Denial-of-Service (DDoS) Attack

A Distributed Denial-of-Service (DDoS) attack is a type of cyber attack in which multiple compromised computers or devices are used simultaneously to flood a target system, server, or network with a large amount of traffic. The goal of the attack is to overwhelm the system resources and make the service unavailable to legitimate users.

Unlike a Denial-of-Service (DoS) attack that originates from a single source, a DDoS attack uses many distributed systems, making it more powerful and difficult to detect and prevent.

How DDoS Attack Works

In a DDoS attack, the attacker first infects multiple computers or devices with malicious

software. These compromised devices are known as bots or zombies. A large group of such infected devices forms a botnet.

The attacker then remotely controls the botnet and instructs all the bots to send a massive number of requests or data packets to the target server at the same time. This overwhelms the server's processing power and bandwidth, causing the service to slow down or completely stop functioning.

Components of a DDoS Attack

- **Attacker (Botmaster)** – The person who controls the attack
- **Botnet** – A network of infected computers used to perform the attack
- **Target Server** – The system or network being attacked

Types of DDoS Attacks

1. Volume-Based Attacks

These attacks aim to consume the bandwidth of the target network by sending huge amounts of traffic.

2. Protocol Attacks

These attacks exploit weaknesses in network protocols such as TCP or ICMP.

3. Application Layer Attacks

These attacks target specific applications such as web servers or databases.

Effects of DDoS Attack

- Website or online service becomes inaccessible
- Network congestion and slowdown
- Server crash or system failure
- Business and financial losses

In 2016, the Dyn DNS service was attacked by a large-scale DDoS attack using thousands of infected Internet of Things (IoT) devices. This attack disrupted major websites such as Twitter, Netflix, and Reddit for several hours.

In the fig 2.1.2, several bots (Bot 1 to Bot 6) are shown sending a large number of requests simultaneously toward the target server. These bots are usually infected computers controlled remotely by a single attacker.

Because the traffic comes from many different sources at the same time, the target server becomes heavily overloaded and cannot handle legitimate user requests. This results in slow performance or complete service failure. Unlike a simple DoS attack from one system, a DDoS attack is more powerful and difficult to stop because the attack traffic is distributed across multiple systems.

SGOU

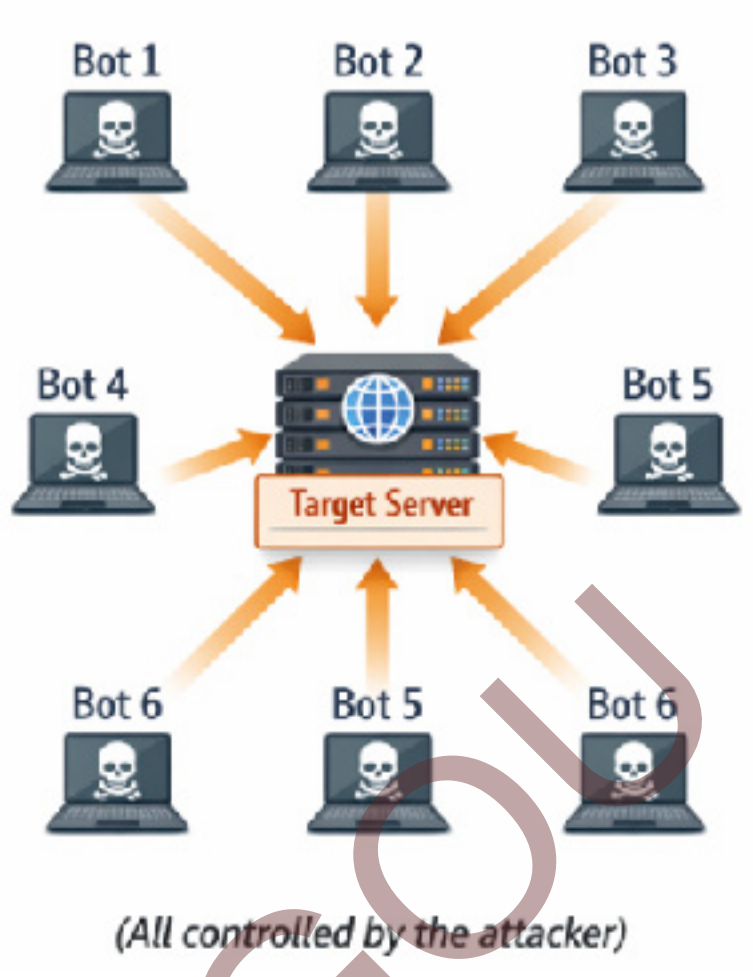


Fig 2.1.2 Distributed Denial-of-Service (DDoS) Attack

Prevention Methods

Some techniques used to mitigate DDoS attacks include:

- **Traffic filtering and rate limiting** – Identify and restrict malicious or excessive traffic before it reaches the target server.
- **Content Delivery Networks (CDNs) and DDoS protection services** – Distribute traffic across geographically distributed infrastructure and absorb large traffic volumes.
- **Load balancing and redundant servers** – Distribute incoming requests across multiple servers and maintain service availability during an attack.
- **Continuous network monitoring** – Detects unusual traffic patterns and identifies large-scale distributed attacks early.

A Distributed Denial-of-Service attack uses multiple compromised devices to overwhelm a target system with massive traffic. Due to its distributed nature, it is more difficult to detect and mitigate compared to a standard DoS attack, making it one of the most serious threats to online services.

SGOU

2.1.4 Backdoors

A Backdoor is a hidden method or mechanism that allows attackers to bypass normal authentication and security controls in a computer system, application, or network. It provides unauthorized access to a system without using the standard login process.

Backdoors are often installed by attackers after compromising a system, allowing them to access the system remotely at any time without being detected.

How Backdoors Work

A backdoor usually works by creating a secret entry point into a system. After gaining initial access through a vulnerability or malware, the attacker installs a backdoor program. This program allows the attacker to reconnect to the system whenever needed without repeating the original hacking process.

The backdoor may operate as a hidden service, modified software component, or malicious script that listens for commands from the attacker.

Types of Backdoors

1. Software Backdoors

Hidden code intentionally placed inside software that allows unauthorized access.

2. Malware-Based Backdoors

Malware such as Trojans installs backdoors that allow attackers to control infected systems remotely.

3. Hardware Backdoors

Hidden vulnerabilities or secret access mechanisms embedded in hardware devices.

4. Web Application Backdoors

Malicious scripts inserted into web servers that allow attackers to control the server remotely.

5. Hardcoded or Default Credentials

Hardcoded or default credentials are manufacturer-set usernames and passwords that attackers can exploit to gain unauthorized access, especially in IoT devices.

Example: The Mirai botnet exploited devices using weak or default credentials and incorporated them into large-scale DDoS attacks.

Risks of Backdoors

- Unauthorized access to systems
- Data theft and privacy violations
- Installation of additional malware

SGOU

- Remote control of compromised systems
- System manipulation or sabotage

Example: An attacker exploits a vulnerability in a web server and uploads a hidden script that allows remote access. Even if the vulnerability is later fixed, the attacker can still access the server through the backdoor.

Fig 2.1.3 shows the difference between a normal and unauthorized way of accessing a server. In the legitimate path, a user must pass through an authentication process (such as login credentials) before gaining access to the server, ensuring security and proper verification.

In contrast, Fig 2.1.3 also illustrates a backdoor path where an attacker uses a hidden entry point to bypass the authentication mechanism and directly access the server. This type of access is unauthorized and poses serious security risks, as it allows attackers to exploit the system without detection.

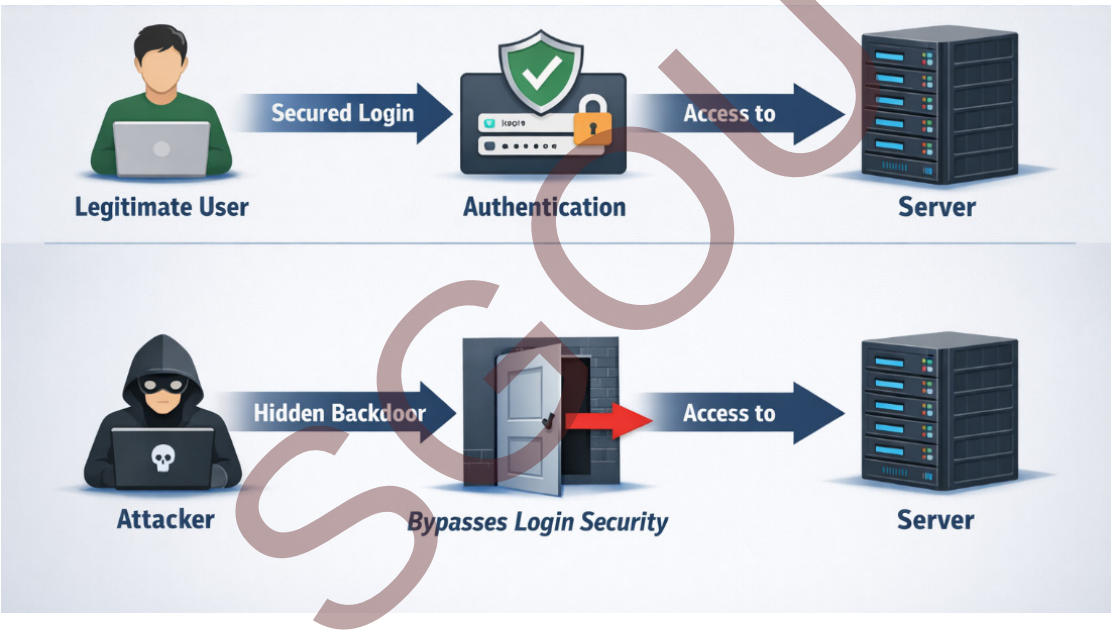


Fig 2.1.3 Backdoor access

Prevention Methods

- **Integrity monitoring of system binaries and configuration files** – Monitor important system files and configurations so that unauthorized modifications to software components can be detected.
- **Review scheduled tasks, services, and startup entries** – Regularly examine scheduled tasks, system services, startup programs, and similar locations where attackers may establish persistence.
- **Egress filtering and outbound traffic monitoring** – Restrict and monitor outbound connections to detect a backdoor communicating with an external attacker or command-and-control server.

- **Regular software updates and security patches** – Fix known vulnerabilities that attackers could exploit to install or maintain backdoors.
- **Strong authentication and access control** – Restrict unauthorized access and reduce the opportunity for attackers to install persistent access mechanisms.

Backdoors are hidden entry points that allow attackers to bypass security mechanisms and gain unauthorized access to systems. They are often installed after a system compromise and can enable long-term control of the affected system if not detected and removed.

2.1.5 Malware

Malware (Malicious Software) refers to any software intentionally designed to harm, exploit, or gain unauthorized access to computer systems, networks, or data. Cyber attackers use malware to damage systems, steal sensitive information, monitor user activities, or disrupt normal operations.

Malware can infect computers, mobile devices, servers, and network systems, making it one of the most common cyber threats.

How Malware Spreads

Malware can spread through several methods, including:

- Downloading infected software or files
- Opening malicious email attachments
- Visiting compromised or malicious websites
- Using infected USB drives or external devices
- Exploiting vulnerabilities in operating systems or applications

Once installed, malware may run secretly in the background and perform harmful activities without the user's knowledge.

Types of Malware

1. Virus

A virus is a type of malware that attaches itself to legitimate files or programs. It spreads when the infected file is executed and can damage data or system files.

2. Worm

A worm is self-replicating malware that can spread automatically through networks without requiring the user to execute an infected file.

3. Trojan Horse

A Trojan disguises itself as legitimate software or a useful file but secretly performs malicious activities, such as stealing information or installing additional malware.

SGOU

4. Ransomware

Ransomware encrypts or blocks access to a victim's files or systems and demands payment in exchange for restoring access.

5. Spyware

Spyware secretly monitors user activities and may collect sensitive information such as passwords, browsing history, and personal data.

6. Bot or Botnet Malware

Bot malware infects a computer or other device and places it under the remote control of an attacker. A large group of infected devices controlled together is called a **botnet**. Attackers can use botnets to perform activities such as DDoS attacks, spam distribution, credential attacks, or other malicious operations.

Example: An attacker infects thousands of vulnerable IoT devices with bot malware and remotely commands them to send traffic to a target website. The collection of infected devices forms a botnet and can be used to conduct a DDoS attack.

7. Adware

Adware is software that displays unwanted advertisements, often through pop-ups or browser redirections. Some forms of adware may also track user activity or collect information without adequate user consent.

8. Fileless Malware

Fileless malware relies primarily on memory-based execution and legitimate system tools rather than conventional malicious executable files stored on disk. This can reduce traditional disk-based indicators and make detection more difficult.

9. Rootkit

A rootkit is malware designed to obtain or maintain privileged access while hiding its presence and the activities of other malicious programs. Some rootkits operate at the operating-system kernel level, making them particularly difficult to detect.

Effects of Malware

- Data theft or loss
- System damage or corruption
- Unauthorized access and privilege escalation
- Monitoring of user activities
- Evasion of security and detection mechanisms
- Financial loss and privacy violations
- Disruption of business operations

SGOU

A user receives an email with an attachment that appears to be an invoice. When the user opens the attachment, it installs ransomware that encrypts all files on the computer and demands payment to unlock them.

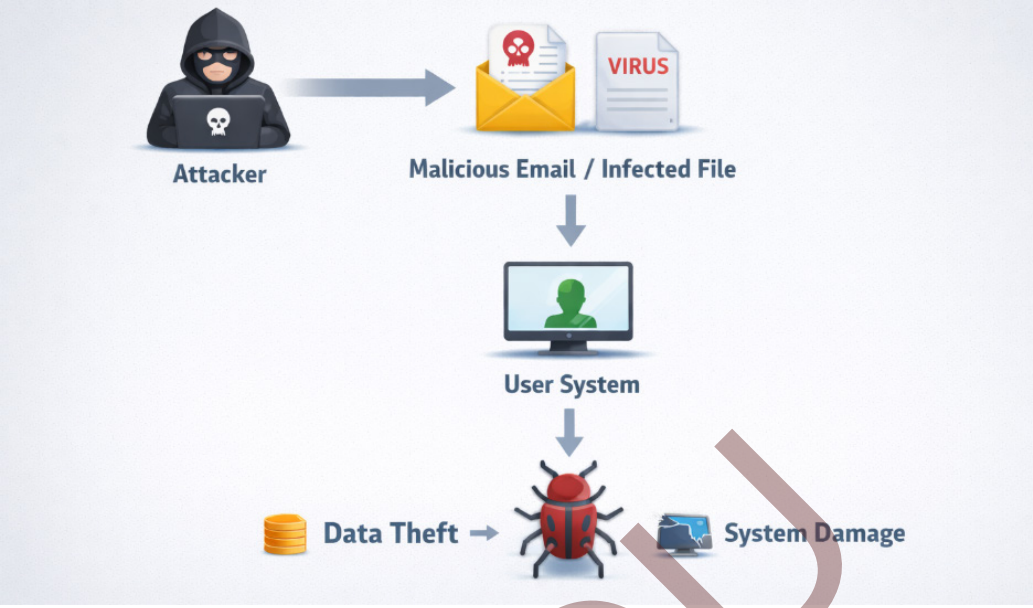


Fig 2.1.4 Malware Infection Process

Fig 2.1.4 illustrates how a malware attack spreads from an attacker to a user's system and causes harm. The process begins when the attacker sends a malicious email or infected file to the user. When the user opens or downloads it, the malware gets installed on the system without the user's knowledge.

Once installed, the malware starts performing harmful activities such as stealing sensitive data or causing system damage. This figure highlights how simple actions like opening unknown emails or files can lead to serious security threats, emphasizing the importance of user awareness and system protection.

Prevention Methods

- Install and regularly update endpoint security and antivirus software.
- Keep operating systems and applications updated with security patches.
- Avoid downloading files or software from untrusted sources.
- Be cautious with email attachments, links, and macros.
- Use application allowlisting and restrict unnecessary scripting tools.
- Monitor unusual processes, memory activity, and system behavior.
- Use endpoint detection and response (EDR) solutions to identify suspicious activity.
- Regularly verify system integrity to detect unauthorized modifications.

SGOU

Malware is malicious software used by attackers to damage systems, steal information, or gain unauthorized access. Understanding different types of malware and adopting proper security practices can help prevent infections and protect computer systems.

2.1.6 Man-in-the-Middle (MitM) Attacks

A Man-in-the-Middle (MitM) attack is a type of cyber attack in which an attacker secretly intercepts and possibly alters the communication between two parties who believe they are directly communicating with each other. In this attack, the attacker positions themselves between the sender and the receiver, allowing them to monitor, capture, or manipulate the exchanged data.

How Man-in-the-Middle Attack Works

In a MitM attack, the attacker first gains access to the communication channel between two systems. This often happens on unsecured or public networks such as public Wi-Fi. Once the attacker is positioned between the two parties, they can intercept messages, read sensitive data, and even modify the information before forwarding it to the intended recipient. The communication appears normal to both parties, making the attack difficult to detect.

Common Techniques Used in MitM Attacks

1. ARP Spoofing (ARP Cache Poisoning)

ARP spoofing sends forged ARP replies to associate the attacker's MAC address with the gateway's IP address, causing the victim's network traffic to be delivered to the attacker instead of directly to the gateway.

2. DNS Spoofing

DNS spoofing provides a forged DNS response so that the victim is directed to an attacker's server while believing that they are connecting to the genuine website.

3. Packet Sniffing

Packet sniffing involves capturing network packets transmitted between systems to obtain information such as login credentials, messages, or other sensitive data, particularly when communication is not adequately protected.

4. Session Hijacking

Session hijacking occurs when an attacker obtains or takes control of a user's active session, potentially allowing the attacker to act as the legitimate user.

5. SSL Stripping

In an SSL stripping attack, the attacker positions themselves between the victim and the website and attempts to downgrade the connection from HTTPS to HTTP, allowing the attacker to relay and potentially observe the communication in less-protected form.

SGOU

6. Rogue Wi-Fi Hotspots

An attacker creates a fake wireless network that appears legitimate and persuades users to connect to it, allowing the attacker to monitor or manipulate their network communication.

Effects of MitM Attacks

- Theft of login credentials
- Credit card and banking information theft
- Data manipulation or tampering
- Identity theft and privacy violations

A user connects to a free public Wi-Fi network in a café and logs into an online banking website. The attacker intercepts the communication and captures the user's login credentials and financial information.

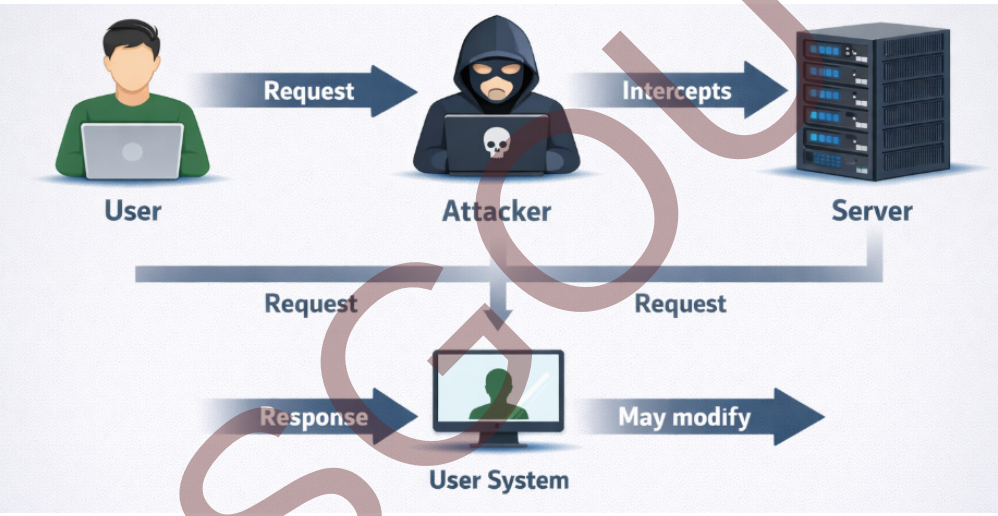


Fig 2.1.5 Man-in-the-middle attack

Fig 2.1.5 illustrates how an attacker secretly intercepts communication between a user and a server. When the user sends a request to the server, it first passes through the attacker, who can monitor or capture the data before forwarding it to the server. The server then sends a response, which again goes through the attacker before reaching the user.

During this process, the attacker may eavesdrop, steal sensitive information, or even modify the data being transmitted. This makes the communication unsafe, as both the user and server may believe they are directly communicating with each other, while in reality the attacker is controlling the exchange.

Prevention Methods

- **Use HTTPS with HSTS (HTTP Strict Transport Security)** – HTTPS encrypts communication between the user and server, while HSTS instructs the browser to use HTTPS and helps prevent attackers from downgrading

SGOU

the connection to HTTP through SSL stripping or similar downgrade attacks.

- **Use secure and trusted networks** – Avoid connecting to unknown or unsecured public Wi-Fi networks and verify the legitimacy of wireless networks before connecting.
- **Use VPNs on untrusted networks** – A properly configured VPN can provide an additional encrypted communication channel when using potentially unsafe networks.
- **Enable multi-factor authentication (MFA)** – MFA provides an additional layer of protection if login credentials are intercepted or compromised.
- **Use strong encryption and certificate validation** – Ensure that applications properly validate digital certificates and do not ignore browser or certificate-security warnings.
- **Keep browsers and operating systems updated** – Security updates help protect against known vulnerabilities that may facilitate interception or downgrade attacks.

A Man-in-the-Middle attack occurs when an attacker secretly intercepts communication between two parties to steal or manipulate data. Implementing secure communication practices and encryption techniques is essential to protect systems and users from such attacks.

Recap

- Cyber attacks target networks, servers, and systems to disrupt or steal data.
- 'DoS attacks make a service unavailable by exhausting the resources of a target from a single source.
- DDoS attacks use multiple infected devices (botnets) to overwhelm a system.
- Backdoors allow attackers to bypass authentication and gain hidden access.
- Malware is malicious software that damages or controls systems.
- MitM attacks intercept communication between users and servers.
- Security measures like firewalls, encryption, and awareness help prevent attacks.

SGOU

Objective Type Questions

1. What is the attack that disrupts service availability?
2. What is a group of infected computers called?
3. What is malicious software known as?
4. What is hidden unauthorized access called?
5. Which attack intercepts communication between two parties?
6. Which malware is self-replicating?
7. Which malware demands payment from users?
8. What is a fake network used in attacks called?
9. Which type of DoS attack exploits the TCP connection establishment process by sending many incomplete SYN requests?
10. Which malware spies on user activities?

Answers to Objective Type Questions

1. DoS
2. Botnet
3. Malware
4. Backdoor
5. MitM
6. Worm
7. Ransomware
8. Rogue Wi-Fi
9. SYN Flood
10. Spyware

SGOU

Assignments

1. Explain network and system-based cyber attacks with examples.
2. Differentiate between DoS and DDoS attacks.
3. Describe the working mechanism of a DoS attack.
4. Explain the concept of botnets in DDoS attacks.
5. What are backdoors? Discuss their types and risks.
6. Describe different types of malware with examples.
7. Explain Man-in-the-Middle (MitM) attack and its prevention methods.

Suggested Reading

1. Easttom, C. (2019). *Computer security fundamentals* (4th ed.). Pearson.
2. Andress, J. (2019). *The basics of information security* (3rd ed.). Syngress.
3. Grimes, R. A. (2017). *Hacking the hacker: Learn from the experts who take down hackers*. Wiley.
4. Goodrich, M. T., & Tamassia, R. (2014). *Introduction to computer security*. Pearson.

Reference

1. Stallings, W. (2018). *Effective cybersecurity: A guide to using best practices and standards*. Pearson.
2. Kurose, J. F., & Ross, K. W. (2021). *Computer networking: A top-down approach* (8th ed.). Pearson.
3. Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.
4. Peltier, T. R. (2016). *Information security policies, procedures, and standards*. Auerbach Publications.

SGOU



UNIT 2 Evolving Cybercrime Techniques

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- understand the concept of cybercrime and evolving cyber attack techniques
- explain different types of cybercrimes such as E-mail Bombing, Salami Attack, Software Piracy, Industrial Espionage, and Intruder Attacks
- analyze the working mechanisms, effects, and risks of these cyber attacks
- apply suitable prevention and security measures to protect systems and data

Prerequisites

With the rapid expansion of digital systems, online services, and interconnected networks, cybercrime has become more advanced and diverse. Understanding modern cybercrime techniques is important because attackers no longer rely on simple methods; instead, they use intelligent, automated, and often hidden approaches to exploit systems. Awareness of these techniques helps individuals and organizations recognize potential threats early and take appropriate security measures to protect sensitive data and ensure safe digital operations.

In real-life situations, cybercrime techniques are widely observed, for example, a company may suffer losses due to small unnoticed financial manipulations (salami attacks), or an organization's confidential data may be stolen by competitors through industrial espionage. Similarly, users may experience email service disruption due to email bombing or unknowingly use pirated software that contains hidden malware. These examples highlight how cyber attacks directly impact everyday digital activities, making it essential to understand and address them effectively.

However, earlier or traditional security methods such as basic passwords, simple anti-virus software, and limited monitoring systems have several limitations. They often fail to detect sophisticated and evolving attacks, especially those involving insider threats, social engineering, or small unnoticed changes over time. These methods are usually reactive rather than proactive and may not provide complete protection against modern cyber threats, emphasizing the need for advanced and continuous security practices.

SGOU

Keywords

Masquerader, Misfeasor, Clandestine User, Cybercrime, Unauthorized Access, Data Theft

Discussion

2.2.1 Introduction

Cybercrime refers to criminal activities carried out using computers, networks, or the internet. With the rapid growth of information technology, digital communication, and online services, cybercriminals continuously develop new and sophisticated methods to exploit vulnerabilities in computer systems. These changing and improving methods are known as evolving cybercrime techniques.



Fig 2.2.1 Types of Cyber Attacks

In the early days, cyber attacks were simple and mainly involved unauthorized access to computer systems or spreading basic viruses. However, as technology advanced and the use of the internet increased, cybercrime also evolved into more complex, organized, and financially motivated activities. Modern cybercriminals use advanced tools, automated programs, and social engineering techniques to target individuals, organizations, and governments.

The growth of online banking, e-commerce, cloud computing, and digital communication has increased the risk of cyber attacks. As a result, attackers continuously develop new techniques to bypass security systems and steal sensitive information, disrupt services, or gain unauthorized access to networks.

Some common cybercrime techniques include E-mail Bombing, Salami Attacks, Software Piracy, Industrial Espionage, and Intruder Attacks. These techniques demonstrate how cybercriminals exploit digital systems in different ways to achieve their malicious goals.

SGOU

Understanding these evolving cybercrime techniques is essential for developing effective cybersecurity measures, protecting sensitive information, and ensuring the safe use of digital technologies.

2.2.2 E-mail Bombing

E-mail bombing is a type of cyber attack in which a large number of emails are sent to a particular email address or mail server within a short period of time. The main purpose of this attack is to overload the victim's mailbox or email server, making it difficult or impossible for the user to access legitimate emails.

In this attack, the attacker uses automated programs or scripts to send thousands or even millions of emails to a single email account. As a result, the email inbox becomes flooded with messages, consuming storage space and network resources. This may lead to system slowdown, denial of service, or temporary shutdown of the email service.

E-mail bombing is often used as a form of harassment, disruption, or denial-of-service (DoS) attack. It can also be used to hide important emails by burying them under a large number of unwanted messages.



Fig 2.2.2 E-mail Bombing

As shown in Fig 2.2.2, the attacker continuously sends massive volumes of emails, which flood the target inbox. Due to this excessive load, the mail server may become slow, crash, or display error messages such as "Inbox Full" or "Server Error." This results in denial of service, preventing normal communication and disrupting email services.

Types of E-mail Bombing

1. **Mass Mailing** – Sending a huge number of identical or unwanted emails to a single email address.

2. **Subscription Bombing** – Repeatedly subscribing a victim's email address to numerous legitimate mailing lists, newsletters, or online services, causing the inbox to receive a large volume of unwanted subscription messages. It is also sometimes referred to as an email cluster bomb.

3. **Zip Bombing** – Sending a specially crafted compressed file that expands to an extremely large size when decompressed, potentially consuming excessive storage or system resources.

Effects of E-mail Bombing

- Overloading of the email server
- Loss of important emails
- Slowing down of the system
- Temporary denial of email services

Prevention Methods

- Using spam filters and email security systems
- Limiting the number of emails received per minute
- Blocking suspicious email sources
- Implementing strong email server protection mechanisms

E-mail bombing is considered a malicious cyber activity and can cause significant disruption to individuals and organizations if proper security measures are not in place.

2.2.3 Salami Attack

A Salami Attack is a type of cybercrime in which an attacker makes small, unnoticed changes to financial transactions, reward points, or other forms of value. Each individual deduction is very small and may go unnoticed, but when repeated across a large number of transactions or users, the accumulated amount can become significant.

The name "Salami Attack" comes from the idea of cutting a salami into many very thin slices. Each slice is small, but together they form a substantial amount. Similarly, in a salami attack, an attacker takes tiny amounts of value repeatedly while attempting to avoid detection.

Traditionally, salami attacks were illustrated using banking systems in which fractions of a cent were diverted from numerous transactions. In modern digital environments, the same principle can be applied to reward schemes, loyalty points, digital wallets, and micro-transactions. For example, an attacker may manipulate a loyalty programme so that a very small number of reward points from thousands of customer transactions are redirected to an unauthorized account. Although the loss to each individual customer may be negligible, the accumulated value can become substantial.

SGOU

Examples of Salami Attacks

- **Reward-Scheme Skimming:** Small amounts of reward value are secretly diverted from many customer transactions into an unauthorized account.
- **Micro-Loyalty Point Skimming:** Tiny fractions of loyalty points or rewards are removed from multiple customer accounts and accumulated by the attacker.
- **Payroll Rounding Manipulation:** A payroll system may be manipulated so that tiny rounding differences from many salary calculations are diverted to an unauthorized account.
- **UPI Micro-Transaction Manipulation:** A transaction-processing system could be manipulated to divert extremely small amounts from a large number of digital transactions. Such manipulation would require unauthorized access to or compromise of the relevant financial system.



Fig 2.2.3 Salami Attack

Fig 2.2.3 illustrates a Salami Attack (Salami Slicing Attack) in a banking system. It shows multiple customer accounts such as Account A, B, C, and D, where each account initially has a certain balance (₹1000, ₹2000, ₹1500, ₹3000) and then a very small amount (₹0.10) is deducted from each. These tiny deductions are so small that individual users usually do not notice them. The image then highlights that all these small amounts are collected together and transferred to a hacker's account, resulting in a total of ₹0.40 from just four accounts. In real-world situations, the attacker targets thousands or even lakhs of accounts, allowing them to accumulate a large sum of money without raising suspicion. The hacker shown with a laptop represents the use of malicious programs or

code to automate this process. Overall, the image clearly conveys the idea that a Salami Attack works by stealing very small amounts repeatedly from many users, making it difficult to detect but highly profitable over time.

Characteristics of Salami Attack

- Involves very small and repeated deductions or modifications.
- Individual losses are difficult to notice.
- Can target money, reward points, loyalty benefits, or other forms of value.
- May exploit automated transaction or processing systems.
- The accumulated value can become significant over a large number of transactions.
- Requires strong auditing and transaction monitoring for detection.

Prevention Methods

- Regular auditing of financial transactions
- Strong access control and monitoring systems
- Code review and secure software development practices
- Continuous monitoring of unusual transaction patterns

Salami attacks highlight the importance of strict security controls and monitoring mechanisms in financial and information systems.

2.2.4 Software Piracy

Software piracy refers to the illegal copying, distribution, or use of software without the permission of the software owner or without a valid license. It is one of the most common forms of cybercrime and results in significant financial losses for software developers and companies.

Software is protected by copyright laws, and users must purchase a license or obtain proper authorization to use it. When individuals or organizations install, share, or sell software without paying for the license, it is considered software piracy.

Software piracy often occurs through unauthorized downloads from the internet, sharing software copies with others, or using cracked or modified versions of software that involve DRM (Digital Rights Management) circumvention.

Fig 2.2.4 illustrates the illegal copying, distribution, or use of software without proper authorization or license. In the figure, original software is duplicated and shared through unauthorized methods such as illegal downloads, counterfeit CDs/DVDs, or cracked versions.

This act violates copyright laws and causes financial losses to software developers and companies. Software piracy not only affects businesses but also increases the risk of

SGOU

malware infections, as pirated software often contains hidden malicious code.



Fig 2.2.4 Software Piracy

Types of Software Piracy

1. **Softlifting** – Installing a single licensed software on multiple computers or sharing it with others.
2. **Counterfeiting** – Creating and selling fake copies of copyrighted software.
3. **Internet Piracy** – Downloading or distributing software illegally through websites or peer-to-peer networks.
4. **Hard Disk Loading** – Selling computers with illegal copies of software already installed.

Effects of Software Piracy

- Financial loss to software developers and companies
- Reduced revenue for the software industry
- Security risks due to malware in pirated software
- Legal consequences for individuals or organizations using illegal copies

Prevention Methods

- Using genuine and licensed software
- Implementing software license management systems
- Increasing awareness about copyright laws
- Strengthening digital rights management (DRM) technologies

SGOU

Software piracy not only violates legal and ethical standards but also exposes users and organizations to security threats and legal penalties.

2.2.5 Industrial Espionage

Industrial Espionage, also known as corporate espionage, is a form of cybercrime in which confidential information belonging to a company or organization is illegally obtained for commercial, strategic, or competitive advantage. The targeted information may include trade secrets, research and development (R&D) data, product designs, intellectual property, business strategies, and other sensitive information.

In modern cybersecurity environments, sophisticated industrial and state-sponsored espionage campaigns are often associated with Advanced Persistent Threats (APTs). An APT is a well-resourced threat actor or group that gains unauthorized access to a target network and attempts to maintain long-term, stealthy access while continuously collecting valuable information. Unlike a "smash-and-grab" attack, in which an attacker quickly gains access, steals information, and leaves, an APT campaign may remain undetected within an organization's network for an extended period.

APTs may use techniques such as spear phishing, exploitation of vulnerabilities, credential theft, malware, and compromised accounts to establish and maintain access. Once inside the network, attackers may move between systems, escalate privileges, identify valuable information, and gradually extract data while attempting to avoid detection.

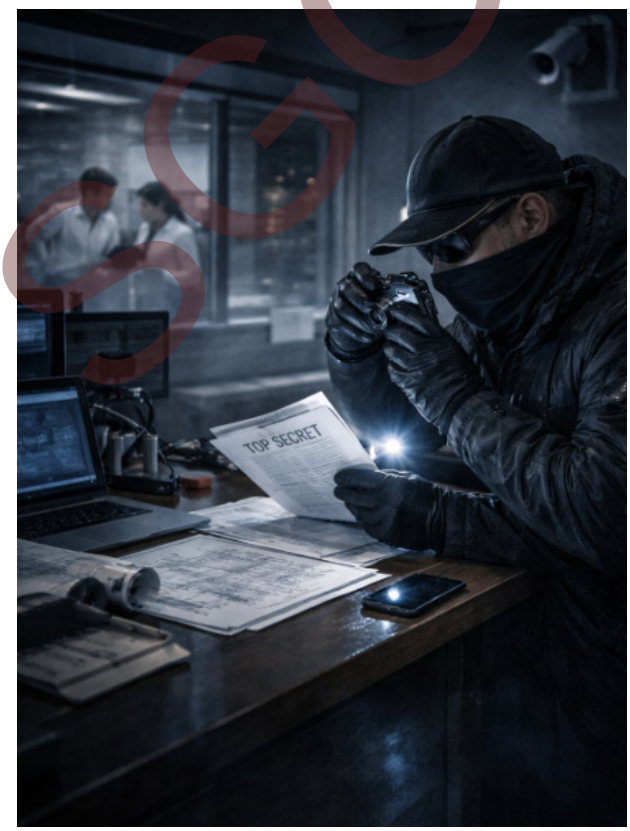


Fig 2.2.5 Industrial Espionage

Examples of Industrial Espionage

- Stealing confidential product designs from a competing company
- Accessing an organization's R&D data
- Obtaining confidential marketing or business strategies
- Stealing proprietary software or manufacturing processes
- Extracting trade secrets through a long-term APT campaign

Methods Used in Industrial Espionage

- **Spear Phishing** – Targeted messages designed to obtain credentials or deliver malware.
- **Exploitation of Vulnerabilities** – Taking advantage of weaknesses in software or network systems.
- **Credential Theft** – Obtaining legitimate usernames and passwords to access organizational resources.
- **Malware** – Using malicious software to establish access, monitor systems, or steal information.
- **Insider Threats** – Employees or other authorized individuals deliberately or unintentionally exposing confidential information.

Effects of Industrial Espionage

- Loss of trade secrets and intellectual property
- Loss of competitive advantage
- Financial losses
- Damage to organizational reputation
- Exposure of confidential R&D and business information

Prevention Methods

- Implement strong access controls and multi-factor authentication.
- Keep operating systems and applications regularly updated.
- Monitor networks for unusual or persistent activities.
- Use endpoint detection and response (EDR) and other security monitoring mechanisms.
- Conduct regular security awareness training, particularly for targeted phishing attacks.

SGOU

- Apply network segmentation to limit the movement of attackers within the network.

Industrial espionage poses a serious threat to businesses and industries because it can compromise confidential information and affect long-term business growth and innovation.

2.2.6 Intruder Attacks

An Intruder Attack refers to an unauthorized attempt by an individual (called an intruder or hacker) to gain access to a computer system, network, or data without permission. The main objective of an intruder may be to steal sensitive information, modify data, disrupt system operations, or misuse system resources.

Intruders exploit security weaknesses or vulnerabilities in software, networks, or system configurations to enter a system. Once access is obtained, they may monitor activities, copy confidential data, install malicious software, or damage important files.

Intruder attacks can target individual computers, corporate networks, financial systems, government databases, and online services.

Types of Intruders

- **Masquerader** – A person who gains unauthorized access by pretending to be an authorized user, usually by stealing login credentials.
- **Misfeasor** – A legitimate user who misuses their authorized access to perform malicious activities.
- **Clandestine User** – An attacker who gains administrative control and hides their activities to avoid detection.

Methods Used in Intruder Attacks

- Password cracking
- Exploiting software vulnerabilities
- Phishing and social engineering
- Installing malware or spyware

Effects of Intruder Attacks

- Unauthorized access to confidential data
- Data modification or destruction
- Financial loss
- Disruption of system operations

Prevention Methods

- **Strong authentication and access control** – Use strong passwords, multi-

SGOU

factor authentication, and least-privilege access to prevent unauthorized users from entering systems.

- **Regular software updates and security patches** – Fix known vulnerabilities that intruders could exploit to gain access.
- **Account and login monitoring** – Monitor failed login attempts, unusual login locations, privilege changes, and other suspicious account activity.
- **Security awareness and physical access controls** – Train users to recognize phishing and social engineering attempts and protect physical devices and restricted areas.

Intruder attacks are a major cybersecurity concern because they can compromise the confidentiality, integrity, and availability of information systems.

Physical and Social-Engineering Intrusion

Intruder attacks can also occur through physical access and social-engineering techniques, rather than through direct network exploitation. Tailgating occurs when an unauthorized person follows an authorized employee into a restricted area without completing the required authentication. Similarly, an unattended unlocked workstation can provide an intruder with direct access to confidential information, applications, or organizational resources. Unauthorized access to server rooms or other restricted facilities can allow an intruder to access network equipment, servers, or storage devices and potentially obtain the same level of access that could result from a successful network compromise.



Fig 2.2.6 Intruder Attack

Fig. 2.2.6 illustrates physical and social-engineering methods through which an intruder may gain unauthorized access to an organization.

- **Tailgating:** An intruder follows an authorized person through a secure door without proper authentication.
- **Physical Break-In:** An attacker forcibly enters a restricted area to gain access to systems, equipment, or sensitive information.
- **Unlocked Devices:** An unattended and unlocked laptop or workstation can allow an unauthorized person to access data or organizational resources.

Overall, the image highlights that intruder attacks can occur through human mistakes, physical force, or negligence, emphasizing the importance of strong security practices like proper authentication, physical security controls, and locking devices when not in use.

Recap

- Cybercrime involves illegal activities using computers and networks.
- E-mail bombing floods inboxes with massive emails causing service disruption.
- Salami attacks steal small amounts repeatedly to gain large profits over time.
- Software piracy is illegal copying and distribution of software.
- Industrial espionage involves theft of confidential business information.
- Intruder attacks involve unauthorized access to systems or networks.
- Strong security measures like authentication, monitoring, and awareness are essential.

SGOU

Objective Type Questions

1. What is the attack that floods an inbox with emails?
2. What is the attack involving small repeated theft?
3. What is illegal copying of software called?
4. What is the theft of business secrets known as?
5. What is unauthorized system access called?
6. What type of intruder uses a fake identity?
7. What type of attack involves insider misuse?

8. What is a hidden administrator attacker called?

9. What type of e-mail bombing involves sending a specially crafted compressed file that expands to an extremely large size when decompressed?

10. What type of intruder gains administrative control of a system and attempts to hide their activities?

Answers to Objective Type Questions

1. Email Bombing
2. Salami Attack
3. Software Piracy
4. Industrial Espionage
5. Intrusion
6. Masquerader
7. Misfeasor
8. Clandestine User
9. Zip Bombing
10. Clandestine User

SGOU

Assignments

1. Define cybercrime and explain evolving cybercrime techniques.
2. Describe the working and effects of E-mail Bombing.
3. Explain Salami Attack with a suitable example.
4. What is Software Piracy? Discuss its types and impacts.
5. Explain Industrial Espionage and its methods.
6. Describe different types of Intruder Attacks.
7. Discuss prevention methods for cybercrime techniques.

Suggested Reading

1. Easttom, C. (2019). *Computer security fundamentals* (4th ed.). Pearson.
2. Andress, J. (2019). *The basics of information security* (3rd ed.). Syngress.
3. Grimes, R. A. (2017). *Hacking the hacker*. Wiley.
4. Goodrich, M. T., & Tamassia, R. (2014). *Introduction to computer security*. Pearson.

Reference

1. Stallings, W. (2018). *Effective cybersecurity*. Pearson.
2. Kurose, J. F., & Ross, K. W. (2021). *Computer networking: A top-down approach* (8th ed.). Pearson.
3. Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.
4. Peltier, T. R. (2016). *Information security policies, procedures, and standards*. Auerbach Publications.

SGOU



Cyber Crime in Social Environments

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- understand the concept of cyber crime in social environments
- identify different types of security policy violations and their consequences
- recognize common social media-related cyber crimes and their impact
- explain various ATM-related cyber crimes and methods to prevent them

Prerequisites

Many users lack awareness about online safety and often share personal information without proper caution. They may trust unknown sources on social media or digital platforms, making them easy targets for cybercriminals. For example, a person might receive a message from a fake social media account asking for money or click on a suspicious link pretending to be from a bank, which can lead to financial loss or account hacking.

Similarly, careless behavior while using digital services can increase risks. For instance, using an ATM without checking for unusual devices or not covering the PIN while entering it can result in fraud. These real-life situations show that limited awareness and over-trust in digital environments make individuals vulnerable to cybercrime, emphasizing the need to understand and prevent such threats.

Keywords

Security Policy Violation, Fake Profiles, Cyberbullying, Phishing, Malware, ATM Skimming, Card Cloning, Cash Trapping, Shoulder Surfing, Identity Theft, Online Fraud, Data Leakage

SGOU

Discussion

2.3.1 Introduction

The rapid growth of the internet, social networking platforms, and digital banking systems has significantly transformed the way people communicate, interact, and conduct financial transactions. However, this increased dependence on digital technologies has also created new opportunities for cybercriminals to exploit individuals and organizations. Cybercrimes that occur within these digital interactions and online communities are referred to as cybercrime in social environments.

In social environments, cybercriminals often target users by exploiting human behavior, trust, and lack of awareness rather than only focusing on technical vulnerabilities. Many people share personal information on online platforms, making them vulnerable to various forms of cyber attacks and online fraud.

Cybercrime in social environments includes activities such as security policy violations within organizations, crimes related to social media platforms, and ATM-related cyber frauds. Security policy violations occur when users or employees fail to follow established security guidelines, which may lead to unauthorized access, data leakage, or misuse of organizational resources.

Social media platforms have also become common targets for cybercriminals. Attackers may create fake accounts, spread malicious links, conduct online harassment, steal personal information, or perform identity theft. Similarly, ATM-related cybercrimes involve techniques such as ATM skimming, card cloning, and unauthorized withdrawal of money, which can cause financial loss to individuals and banks.

Understanding cybercrime in social environments is important because these crimes affect individual privacy, financial security, and organizational safety. Increasing awareness, following proper security practices, and implementing strong cybersecurity policies can help reduce the risks associated with these cyber threats.

2.3.2 Security Policy Violations

Security policy violations occur when individuals or employees fail to follow the established security rules, guidelines, or procedures of an organization. Security policies are created to protect computer systems, networks, and sensitive data from unauthorized access, misuse, or damage. When these policies are ignored or violated, it can lead to serious cybersecurity risks.

In many cases, security policy violations happen due to lack of awareness, negligence, or intentional misuse of system resources. These violations can expose confidential information, weaken system security, and create opportunities for cybercriminals to exploit vulnerabilities.

Examples of Security Policy Violations

- Sharing passwords with others
- Using weak or easily guessable passwords

SGOU

- Installing unauthorized software on office computers
- Accessing restricted data without permission
- Using organizational systems for personal or illegal activities
- Connecting insecure external devices (such as USB drives) to the network

Causes of Security Policy Violations

- Lack of cybersecurity awareness among users
- Carelessness or negligence by employees
- Intentional misuse of privileges by insiders
- Poor enforcement of security policies

Consequences of Security Policy Violations

- Data leakage or loss of confidential information
- Unauthorized system access
- Financial and reputational damage to organizations
- Increased vulnerability to cyber attacks

Prevention Methods

- Creating clear and well-defined security policies
- Conducting regular cybersecurity awareness training
- Implementing strong authentication and access control
- Monitoring system activities and enforcing policy compliance

Security policy violations highlight the importance of user responsibility and adherence to security guidelines to ensure the safety and integrity of organizational information systems.

SGOU

2.3.3 Crimes Related to Social Media

Social media platforms such as Facebook, Instagram, WhatsApp, and X allow people to communicate, share information, and interact online. However, these platforms are also used by cybercriminals to perform various illegal activities.

Crimes related to social media involve the misuse of social networking platforms to harass individuals, steal personal information, commit fraud, spread misinformation, or damage someone's reputation.

Below are some common types of social media cybercrimes with examples and explanations.

2.3.3.1 Fake Profiles / Impersonation

A fake profile is created when a cybercriminal uses another person's name, photos, or

identity to create a false account on social media. This is often done to deceive others, collect personal information, or commit fraud.

How it works

- The attacker copies photos and details from a real person's profile.
- A new fake account is created using those details.
- The attacker sends friend requests to the victim's friends.
- They may ask for money, share malicious links, or spread false information.

Example: A criminal creates a fake profile of a student and sends messages to the student's friends asking for emergency financial help. Since the account looks genuine, some friends may send money.

Effects

- Identity theft
- Damage to reputation
- Financial fraud

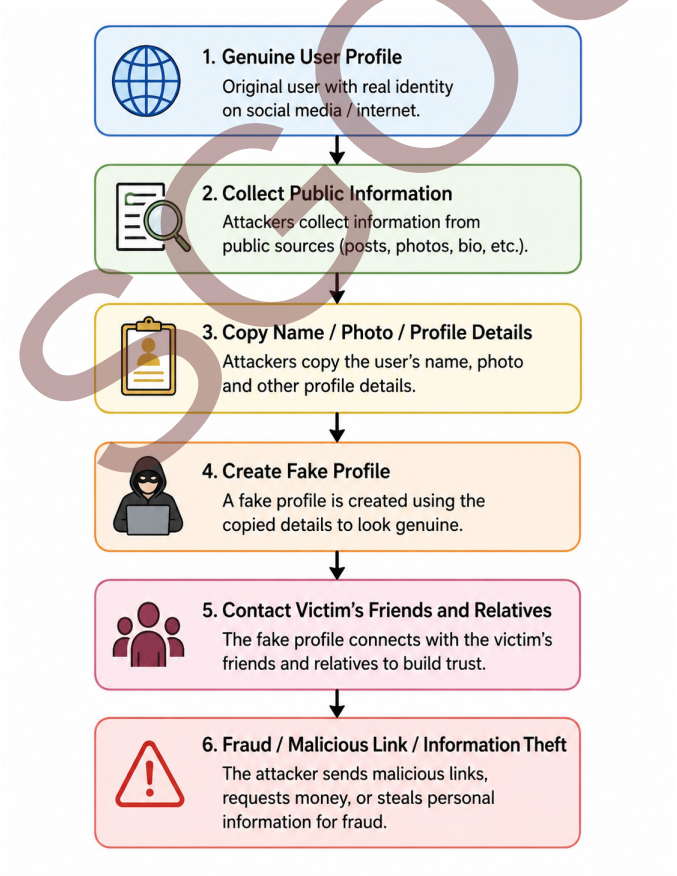


Fig 2.3.1 Fake Profile Creation and Impersonation

Fig 2.3.1 illustrates how a fake social media profile can be created using information

obtained from a genuine user's profile. The process begins when an attacker collects publicly available information such as the victim's name, profile photograph, and other personal details. The attacker then creates a fake profile that appears similar to the genuine account and uses it to send friend requests or messages to the victim's contacts. The attacker may subsequently use the fake identity to request money, distribute malicious links, or obtain additional personal information. The figure highlights how publicly available information can be misused to impersonate a person and deceive their contacts.

2.3.3.2 Cyberbullying and Online Harassment

Cyberbullying is the act of using social media to harass, threaten, or humiliate someone online. This type of crime is especially common among teenagers and young users.

Common forms

- Posting insulting or abusive comments
- Sharing embarrassing photos or videos without permission
- Spreading rumors or false information
- Sending threatening messages

Example: A group of users repeatedly posts abusive comments and memes targeting a particular student on social media platforms.

Effects

- Emotional stress and depression
- Damage to personal reputation
- Social isolation

2.3.3.3 Phishing and Online Scams

In social media phishing, attackers send fake messages or links pretending to be from trusted organizations or friends.

How it works

- A user receives a message such as *"Your account will be suspended. Click this link to verify."*
- The link leads to a fake login page.
- When the user enters their username and password, the attacker steals the information.

Example: A fake page pretending to be a bank or popular brand sends messages offering prizes or asking users to verify their accounts.

SGOU

Effects

- Account hacking
- Financial fraud
- Theft of personal data

2.3.3.4 Spreading Malware through Social Media

Cybercriminals may share malicious links, infected files, or fake apps through social media posts or private messages.

For example, a user receives a message saying *"Watch this shocking video of you!"* with a link. When the link is clicked, malware is installed on the victim's device.

Consequences

- Device infection
- Data theft
- Unauthorized control of the user's account

Prevention Methods of Social Media-Related Cybercrimes

- Review and restrict privacy settings.
- Verify profiles and confirm unusual requests through another channel.
- Report and block suspicious accounts.
- Be cautious with shortened or unexpected links.
- Enable two-factor authentication.
- Do not install applications received through social media messages.

2.3.4 ATM Related Cybercrimes

ATM (Automated Teller Machine) fraud is a type of cybercrime where criminals use different techniques to steal bank card information, PIN numbers, or money from ATM users. With the increasing use of debit and credit cards, ATM machines have become common targets for cybercriminals.

Attackers often install fraudulent devices, hidden cameras, or malicious software on ATM machines to capture card details and PIN numbers. These stolen details are later used to create duplicate cards or withdraw money from victims' accounts.

ATM fraud includes a range of physical, observational, and technical attacks, including physical tampering with the ATM, observation of customers while they enter or use their PINs, and attacks that target the ATM's software or dispensing system.

2.3.4.1 ATM Skimming

ATM skimming is one of the most common ATM cybercrimes. In this method, criminals

SGOU

attach a skimming device to the card slot of an ATM machine. This device secretly reads and stores the data from the magnetic stripe of a card when the user inserts it.

How the Attack Works

- The attacker installs a fake card reader (skimmer) on the ATM slot.
- When the user inserts the card, the skimmer copies the card information.
- Criminals may install a PIN pad overlay over the legitimate ATM keypad to capture the customer's PIN.
- The criminal later retrieves the stored data and creates a duplicate ATM card.
- The duplicate card is used to withdraw money from the victim's account.

Example

A person withdraws money from an ATM in a shopping mall. The ATM has a hidden skimming device and a tiny camera placed above the keypad. The device records the card details while the camera records the PIN. Later, criminals use this information to withdraw money from the victim's bank account.



Fig 2.3.2 ATM Skimming Devices

Fig 2.3.2 illustrates common physical devices that criminals may attach to an ATM to capture card and PIN information. A skimming device fitted over or inside the card-reader area can capture information from a payment card, while a PIN pad overlay placed over the genuine keypad can record the numbers entered by the user. Some attacks may also involve hidden cameras positioned near the keypad. The figure helps users recognize suspicious modifications to the card reader and keypad and emphasizes the importance of checking an ATM before using it.

Shimming is a technique used to target EMV chip-based payment cards. In a shimming attack, a thin, unauthorized device is inserted inside the ATM's card reader to intercept data exchanged between the payment card's chip and the ATM. Unlike traditional skimming, which primarily targets magnetic-stripe data, shimming is designed to target communication associated with chip-based cards. Including shimming alongside skimming reflects the evolution of ATM fraud as payment-card technology has moved from magnetic stripes toward EMV chip technology.

2.3.4.2 Card Cloning

Card cloning occurs when criminals use stolen ATM card data to create a duplicate or fake card. This cloned card works like the original card and can be used for unauthorized withdrawals or purchases.

How it Happens

- Card details are stolen using skimming devices or malware.
- The stolen data is copied onto a blank magnetic stripe card.
- The cloned card is used at ATMs or POS machines to withdraw money.

Example

A criminal steals card details using a skimming device and creates a cloned card. Using this cloned card and the stolen PIN, the attacker withdraws money from multiple ATMs.

2.3.4.3 ATM Malware and Logical Attacks (Jackpotting)

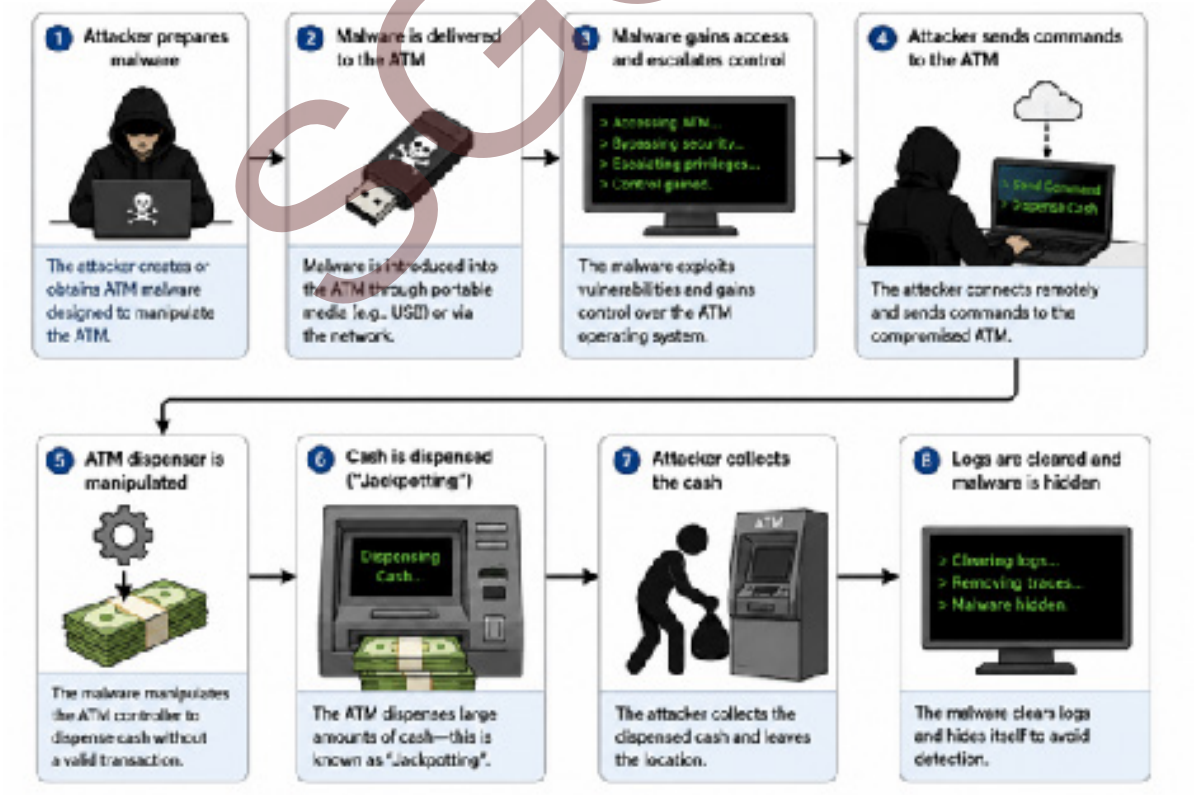


Fig 2.3.3 ATM Malware Jackpotting Attack

SGOU

ATM malware and logical attacks, commonly known as jackpotting, target the software and cash-dispensing mechanisms of an ATM rather than the customer's bank account or card. In such attacks, criminals may gain physical access to the internal components of an ATM and install malicious software or connect an unauthorized device that sends commands to the cash dispenser. The compromised ATM can then be instructed to dispense cash without requiring a legitimate bank card or a customer's account transaction. This demonstrates how cybercriminals can combine physical access with malware or unauthorized control of ATM systems to cause direct financial loss.

Figure 2.3.3 illustrates how an ATM can be compromised through a logical attack. Unlike skimming or shoulder surfing, which target customer information or PINs, jackpotting targets the ATM itself and can cause the machine to dispense cash without a normal customer transaction.

2.3.4.4 Shoulder Surfing

Shoulder surfing is a simple but effective ATM fraud method where criminals secretly watch a user entering their PIN number.

Example: A criminal stands near an ATM and observes a person entering their PIN. Later, the criminal steals the victim's card or uses other techniques to access the account.

2.3.4.5 What to Do If ATM Fraud Happens

If an ATM or card fraud incident occurs, the user should take the following steps immediately:

1. **Contact the bank immediately** through its official customer-care channel and request that the card be blocked and the unauthorized transaction reported.

2. **Report the incident through the National Cyber Crime Reporting Portal** at cybercrime.gov.in.

3. **Call 1930**, the national cyber-fraud helpline, to report the financial cyber fraud and initiate the appropriate response.

Important: Users should report unauthorized transactions as soon as possible and preserve transaction messages, screenshots, transaction IDs, and other evidence for the investigation.

Customer Protection

The Reserve Bank of India's Customer Protection framework provides for zero customer liability in specified circumstances involving unauthorized electronic banking transactions. Where the loss results from a third-party breach and the customer reports the transaction to the bank within three working days of receiving the bank's communication about the transaction, the customer's liability may be zero, subject to the applicable conditions.

SGOU

Recap

- Cybercrime in social environments targets human behavior and trust.
- Security policy violations weaken organizational cybersecurity.
- Social media crimes include fake profiles, cyberbullying, phishing, and malware attacks.
- ATM-related cybercrimes include skimming, cloning, cash trapping, and shoulder surfing.
- Lack of awareness is a major cause of cybercrime.
- Following security practices can reduce cyber risks.

Objective Type Questions

1. Which social media crime involves repeatedly sending unwanted messages or requests to a user's account?
2. Which attack creates an unusually large compressed file that expands to consume excessive system resources?
3. Which attack divides a small amount of value into many tiny deductions that may go unnoticed?
4. Which activity involves unauthorized copying, distribution, or use of copyrighted software?
5. Which cybercrime involves obtaining confidential information about a company or organization for competitive or strategic advantage?
6. Which type of intruder gains access to a system by pretending to be an authorized user?
7. Which malware attaches itself to a legitimate file and spreads when the file is executed?
8. Which ATM fraud copies card data using an unauthorized reader placed at the card slot?
9. Which ATM fraud uses a device or obstruction to prevent cash from being dispensed to the customer?
10. Which technique involves observing a person while they enter their PIN or other confidential information?

SGOU

11. Which social media crime uses another person's photographs and identity to create a deceptive account?

12. Which social engineering attack attempts to deceive users into revealing sensitive information through fraudulent messages or links?

13. Which form of online abuse involves repeatedly threatening, harassing, or humiliating a person through digital platforms?

14. Which ATM attack uses malware or an unauthorized device to command the ATM to dispense cash without a legitimate transaction?

15. Which security-related offence occurs when a person deliberately violates an organization's established security rules or procedures?

Answers to Objective Type Questions

1. Email Bombing
2. Zip Bombing
3. Salami Attack
4. Software Piracy
5. Industrial Espionage
6. Masquerader
7. Virus
8. Skimming
9. Cash Trapping
10. Shoulder Surfing
11. Fake Profile
12. Phishing
13. Cyberbullying
14. Jackpotting
15. Security Policy Violation

SGOU

Assignments

1. Define cybercrime in social environments. Explain its impact on individuals and organizations.
2. What are security policy violations? Discuss their causes and consequences.
3. Explain different types of security policy violations with examples.
4. Describe various crimes related to social media with suitable examples.
5. What is cyberbullying? Explain its effects on individuals.
6. Explain phishing and malware attacks in social media. How can users protect themselves?
7. Explain ATM-related cybercrimes such as ATM skimming, card cloning, cash trapping, and shoulder surfing. Also suggest preventive measures to avoid these crimes.

Suggested Reading

1. Shinde, A. (2019). *Introduction to cyber security*. Tech Publications.
2. Chander, H. (2020). *Cyber laws and IT protection*. Universal Law Publishing.
3. National Cyber Security Centre. (2021). *Cyber security guidance*. NCSC Publications.
4. Reserve Bank of India. (2023). *Safe digital banking practices*. RBI.

Reference

1. Brooks, C. J. (2018). *Cyber security essentials*. Wiley.
2. National Council of Educational Research and Training (NCERT). (2020). *Information technology textbook*. NCERT.
3. Indian Computer Emergency Response Team (CERT-In). (2021). *Cyber security awareness guide*. Government of India.
4. Reserve Bank of India (RBI). (2022). *Guidelines on ATM and digital payment security*. RBI.

SGOU



UNIT 4 Financial and Intellectual Property Cyber Frauds

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- understand the concept of financial and intellectual property cyber frauds
- identify different types of cyber frauds such as software piracy, trademark infringement, and copyright violation
- analyze the effects and risks associated with cyber frauds
- apply preventive measures to protect financial data and intellectual property

Prerequisites

Basic awareness of digital activities such as online banking, e-commerce, and social media usage is important for studying financial and intellectual property cyber frauds. Familiarity with concepts like passwords, OTPs, malware, and data privacy helps individuals recognize suspicious activities and take safer actions while using digital platforms.

However, basic awareness alone is often not enough to prevent cyber frauds. Many users follow general safety practices but still become victims due to advanced and deceptive techniques used by cybercriminals. For example, a person may know that OTPs should not be shared, but may still provide it after receiving a convincing call pretending to be from a bank official. Similarly, a user may avoid illegal activities but still download free software from an untrusted source and unknowingly install malware. These situations show that limited awareness and lack of careful judgment can lead to cyber fraud, highlighting the need for cautious behavior in digital environments.

Keywords

PIN Theft, PIN Pad Overlay, Cash Trapping, Shoulder Surfing, ATM Jackpotting, Social Media Crimes, Fake Profiles, Cyberbullying, Security Policy Violation

SGOU

Discussion

2.4.1 Introduction

Financial and intellectual property cyber frauds are major categories of cybercrime that have grown rapidly with the expansion of the internet, digital communication, and online financial systems. As people increasingly rely on online platforms for banking, shopping, and sharing information, cybercriminals exploit these systems to carry out illegal activities. These frauds not only cause financial loss but also affect privacy, trust, and the protection of creative works.

Financial cyber frauds mainly include online fraud and banking fraud. Online fraud involves deceptive activities such as phishing emails, fake websites, and online scams designed to trick users into revealing sensitive information like passwords, credit card details, or OTPs. SIM Swapping transfers a victim's mobile number to an attacker-controlled SIM, allowing the attacker to receive SMS-based OTPs. SS7 exploitation abuses weaknesses in cellular signalling systems to intercept or redirect SMS messages, potentially exposing OTPs without user interaction. Banking fraud includes unauthorized access to bank accounts, illegal fund transfers, ATM-related frauds, and misuse of debit or credit cards. These crimes often occur due to a lack of awareness, weak security practices, and over-trust in digital systems.

On the other hand, intellectual property cyber frauds involve the unauthorized use or theft of original creations and brand identity. Software piracy is a common issue where paid software is illegally copied, distributed, or used without a license, leading to financial loss for developers and security risks for users. Trademark and logo infringement occurs when counterfeit products use well-known brand names or logos to mislead customers and gain profit. Additionally, copyright violations on online platforms involve the illegal uploading, downloading, or sharing of digital content such as movies, music, eBooks, and software without the permission of the rightful owner.

Overall, financial and intellectual property cyber frauds highlight the importance of cybersecurity awareness, legal protection, and responsible use of digital technologies. Understanding these concepts helps individuals and organizations protect their financial assets and intellectual rights in the digital environment.

2.4.2 Online and Banking Fraud

Online and banking fraud refers to the use of digital technologies, communication networks, and deceptive techniques to illegally obtain money, banking credentials, payment information, or access to financial accounts. These frauds may target debit and credit cards, UPI and payment applications, internet banking accounts, and mobile banking services.

Types of Online and Banking Fraud

- **Card-Present Fraud:** Fraud involving the physical use of a stolen, lost, or counterfeit debit or credit card at an ATM or point-of-sale terminal.
- **Card-Not-Present Fraud:** Fraud in which the physical card is not required.

SGOU

Attackers misuse stolen card numbers, expiry dates, CVV numbers, or other payment details for online transactions.

- **UPI and Payment-App Fraud:** Attackers may send fraudulent UPI collect requests, manipulate users into scanning malicious QR codes, or deceive them into approving transactions.
- **Net Banking Fraud and Account Takeover:** Attackers obtain login credentials through phishing, malware, social engineering, or other methods and use them to gain unauthorised access to the victim's bank account.
- **Vishing and OTP Fraud:** Attackers use phone calls or other deceptive communication to persuade victims to reveal OTPs, PINs, or banking credentials.
- **SIM Swapping:** An attacker obtains a replacement SIM associated with the victim's mobile number and uses it to receive OTPs and other banking messages.
- **Fake Payment Links:** Attackers send fraudulent links that imitate legitimate banking, shopping, or payment websites and trick users into entering credentials or payment information.

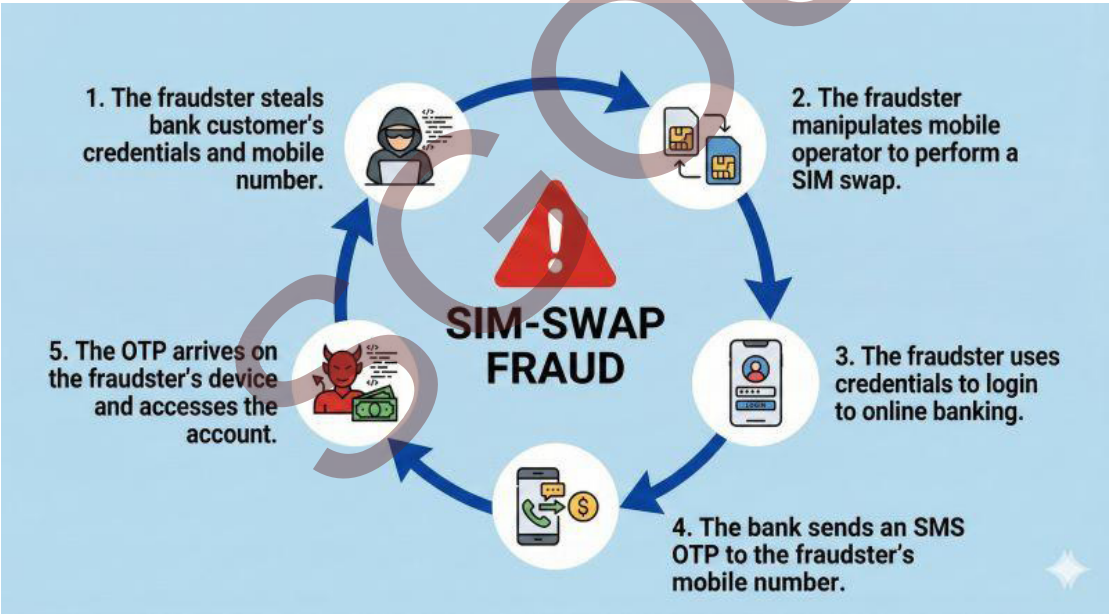


Fig 2.4.1 Major Types of Online and Banking Fraud

Online and banking fraud can involve different stages, from deceiving the victim to obtaining authentication information and finally performing an unauthorised transaction.

Effects of Online and Banking Fraud

- Financial loss to individuals and organisations
- Theft of banking and payment credentials
- Unauthorised transactions and account takeover

- Loss of privacy and personal information
- Identity theft and misuse of financial accounts
- Emotional stress and loss of trust in digital payment systems

Prevention Methods

- Never share OTPs, PINs, passwords, CVV numbers, or banking credentials with anyone.
- Verify UPI collects requests and QR codes before approving or scanning them.
- Avoid clicking unexpected payment links received through messages or social media.
- Use official banking and payment applications and websites.
- Enable two-factor authentication wherever available.
- Monitor bank statements and transaction alerts regularly.
- Contact the bank immediately when an unauthorized transaction is detected.
- Protect the mobile number and contact the telecom provider if a sudden loss of mobile service suggests possible SIM swapping.
- Report suspected financial cyber fraud promptly through the appropriate official reporting channels.

Example: An attacker sends a fake payment link claiming that a refund is waiting for the user. When the user opens the link, it displays a fraudulent banking page and asks for login credentials and an OTP. The attacker uses the stolen information to access the account and initiate an unauthorized transaction.

2.4.3 Intellectual Property Frauds

Intellectual Property (IP) refers to creations of the human mind, such as inventions, software, literary and artistic works, music, films, photographs, designs, symbols, names, and logos used in business. Intellectual property is protected by laws that give creators, authors, developers, and organisations certain rights over the use, reproduction, distribution, and commercial exploitation of their creations. In the digital environment, intellectual property can be copied, modified, stored, and distributed quickly and at very low cost. This has created new opportunities for the unauthorised use and distribution of intellectual property.

Intellectual Property Frauds are unlawful activities in which a person's or organisation's intellectual property is copied, distributed, modified, accessed, or used without proper authorisation or in violation of the owner's rights. Cybercriminals may exploit websites, file-sharing platforms, social media, cloud storage, and other digital technologies to distribute or misuse protected content.

Common forms of intellectual property fraud include software piracy, copyright

SGOU

infringement, trademark infringement, unauthorised distribution of digital content, and DRM circumvention. For example, illegally downloading and distributing a copyrighted software application, sharing a paid movie through an unauthorised website, or using a company's logo to create a fake website can constitute forms of intellectual property infringement.

Intellectual property fraud can affect both individual creators and organisations. Creators may lose income when their work is copied or distributed without permission, while organisations may suffer financial losses, damage to their reputation, and loss of competitive advantage. In addition, pirated software and digital content obtained from unauthorised sources may contain malware, ransomware, spyware, or other malicious components, creating additional cybersecurity risks for users.

The growth of cloud services, social media, streaming platforms, digital marketplaces, and file-sharing technologies has made intellectual property protection increasingly important. Therefore, users should understand the difference between legitimate use and unauthorised use, respect licensing and copyright requirements, and obtain software and digital content from authorised sources.

2.4.3.1 Software Piracy

Software piracy is the illegal copying, installation, distribution, or use of software without proper permission or license from the original developer or owner. It is one of the most common forms of intellectual property cyber fraud and occurs when users access paid software for free through unauthorized means. This practice violates copyright laws and results in significant financial losses for software companies and developers.

Software piracy can occur in several ways. Users may download cracked or modified versions of software from illegal websites, use a single licensed copy on multiple devices without permission, or share licensed software with others. In many cases, pirated software is distributed through torrent sites or unauthorized platforms that offer “free” downloads of paid applications. Although such software may appear attractive because it is free, it often contains hidden malware, viruses, or spyware that can harm the user’s system and compromise sensitive data.

DRM (Digital Rights Management) circumvention refers to the unauthorised bypassing or removal of technological measures used to control access to or use of licensed software. Informally, this may be described as bypassing licensing systems or using tools such as a key generator (keygen) or a modified licence key.

A common real-life situation involves a user downloading a cracked version of a paid application from an untrusted website instead of purchasing it legally. While the software may work initially, it can later expose the system to viruses or allow hackers to access personal data. This not only creates security risks but also discourages software developers by reducing their revenue and recognition for their work.

The effects of software piracy are serious. It leads to financial loss for developers and companies, legal penalties for users, and increased cybersecurity risks. Pirated software often lacks updates and technical support, making systems more vulnerable to

SGOU

attacks. Therefore, it is important to use only genuine and licensed software, download applications from trusted sources, and respect intellectual property rights to ensure safety and ethical use of digital resources.

Fig 2.4.1 illustrates the concept of software piracy and how it occurs in the digital environment. It shows the unauthorised acquisition and use of software, highlighting the violation of software licensing and copyright requirements and the potential security risks associated with obtaining software from unauthorised sources.

At the center of the image, a person using a computer represents an unauthorized user involved in illegal activities. The screen displaying "cracked software" indicates the use of modified or pirated programs that bypass licensing systems.

On the left side, the "free download" sign and pirated copies (CDs and USB devices) show how illegal software is distributed through websites and storage devices. On the right side, the diagram of connected computers represents illegal sharing of software across multiple users or networks.



Fig 2.4.1 Software Piracy

Warning symbols such as malware and virus icons highlight the risks associated with software piracy, including data theft and system damage. The presence of legal symbols, such as a judge's gavel, indicates that software piracy can lead to legal consequences. Additionally, the broken license key and key generator (keygen) represent the unauthorized methods used to activate pirated software.

Effects of Software Piracy

- Financial loss to software developers and companies
- Legal penalties for users and organizations

- Increased risk of malware, viruses, and spyware
- Lack of software updates and technical support
- Reduced innovation in the software industry

Prevention of Software Piracy

- Always use genuine and licensed software.
- Download software only from official or trusted websites.
- Avoid using cracked or pirated versions of software.
- Do not share licensed software with others illegally.
- Install antivirus software to detect harmful pirated files.
- Follow organizational policies regarding software usage.

Legal Framework for Software Piracy in India

In India, software is protected under the Copyright Act, 1957. Under Section 2(o), a computer programme is included within the definition of a *literary work*. Therefore, unauthorised copying, distribution, or use of copyrighted software can constitute copyright infringement.

Section 63 provides that knowing infringement or abetment of infringement of copyright is an offence. The provision prescribes imprisonment of six months to three years and a fine of ₹50,000 to ₹2 lakh, subject to the qualifications provided by the Act.

Section 63B specifically addresses the knowing use of an infringing copy of a computer programme on a computer. It provides a separate offence and a lower penalty where the infringing use was not for gain or in the course of trade or business.

The Information Technology Act, 2000 may also become relevant where software piracy involves unauthorised access to, downloading from, copying from, or extraction of data from a computer, computer system, or computer resource. Section 43 provides for compensation for specified unauthorised acts, while Section 66 addresses certain acts under Section 43 when committed dishonestly or fraudulently.

Important: The exact application of these provisions depends on the facts of the case and the nature of the conduct. Students should therefore understand that software piracy is not merely a violation of a software licence; it can also involve copyright offences and, in appropriate circumstances, offences under the Information Technology Act, 2000.

2.4.3.2 Trademark and Logo Infringement

Trademark and logo infringement is a type of intellectual property fraud in which an individual or organization uses a registered brand name, logo, or symbol without permission. This is done to mislead customers into believing that the product or service is genuine. Such activities are illegal and violate trademark laws.

This type of fraud commonly occurs in both online and offline markets. Cybercriminals

SGOU

or counterfeit manufacturers create fake products that closely resemble popular brands by copying their logos, colors, packaging, or design. Customers may find it difficult to distinguish between original and fake products, especially when they are sold at lower prices or through unverified online platforms.

Trademark infringement can also occur through fake websites that imitate well-known companies. These websites may use similar logos and layouts to trick users into making purchases or sharing personal information.



Fig 2.4.2 Example of Trademark Infringement Using a Fictitious Brand

For instance, a customer may purchase shoes online that appear to belong to a popular brand, but after receiving the product, they realize it is a duplicate with a copied logo and lower quality.

Fig 2.4.2 clearly illustrates the concept of trademark and logo infringement by comparing an original branded product with a counterfeit (fake) product. On the left side, the original shoe represents a genuine product with an authentic brand logo, proper design, and high-quality appearance. On the right side, the fake shoe shows a slightly altered logo, which is intentionally designed to confuse customers.

The warning symbol placed between the two products indicates the risk of deception and highlights that such practices are illegal.Additionally, the labels “Original Brand Logo” and “Copied Brand Logo” emphasize the misuse of intellectual property. The

fake product may look similar to the original but usually has lower quality materials and performance. This not only misleads customers but also damages the reputation and sales of the original brand.

In real-world situations, such counterfeit products are often sold at lower prices through unauthorized websites, street markets, or unverified online sellers. Many customers unknowingly purchase these fake products thinking they are genuine. This results in financial loss for both consumers and companies and may also involve legal consequences for those involved in producing or selling counterfeit goods.

Legal Framework for Trademark Infringement in India

In India, trademark infringement is primarily governed by the Trade Marks Act, 1999. Section 29 specifies the circumstances in which the use of a registered trademark can constitute infringement. It provides protection against unauthorised use of a mark that is identical or deceptively similar to a registered trademark in relation to relevant goods or services.

Section 102 deals with falsifying and falsely applying a trademark. It covers conduct involving the unauthorised application or alteration of a trademark with the intention of presenting goods or services as being associated with the genuine trademark owner.

Sections 103 and 104 provide criminal penalties for applying false trademarks and for selling or possessing goods bearing false trademarks. The offences may attract imprisonment of six months to three years and a fine of ₹50,000 to ₹2 lakh, subject to the provisions and circumstances specified in the Act.

When trademark infringement involves online impersonation, fake websites, or fraudulent digital representations of a brand, provisions of the Information Technology Act, 2000 may also become relevant. Section 66C addresses identity theft, while Section 66D addresses cheating by personation using a computer resource or communication device.

Therefore, students should understand that trademark infringement in India is primarily governed by the Trade Marks Act, 1999, while the Information Technology Act, 2000 may additionally apply when the infringement involves online impersonation, identity misuse, or computer-based fraud.

Effects of Trademark and Logo Infringement

- Damage to brand reputation and trust
- Financial loss to original companies
- Customer deception and confusion
- Sale of low-quality counterfeit products
- Legal consequences for counterfeit sellers

Prevention of Trademark and Logo Infringement

- Purchase products only from authorized sellers or official websites.

SGOU

- Verify brand logos, packaging, and product details before buying.
- Avoid buying products at unusually low prices from unknown sources.
- Check reviews and ratings of online sellers.
- Companies should register trademarks and monitor misuse.
- Report counterfeit products or fake websites to authorities.

2.4.3.3 Copyright Violation in Online Platforms

Copyright violation in online platforms refers to the illegal use, copying, sharing, or distribution of digital content without permission from the original creator or owner. This type of intellectual property fraud commonly affects content such as movies, music, videos, software, eBooks, and images. With the growth of the internet and streaming platforms, it has become easier for users to access and share content, but this also increases the risk of copyright violations.

These violations often occur when users upload or download content from unauthorized websites, share paid content for free, or stream movies and music from illegal platforms. Many websites provide pirated content to attract users, often without the knowledge that such actions are illegal. This not only affects the earnings of creators but also discourages creativity and innovation.



Fig 2.4.3 Copyright Violation in Online Platforms

Fig 2.4.3 represents how copyright violation occurs in online platforms. It typically shows a digital device such as a laptop or smartphone displaying a website that offers

free access to movies, music, or software. These websites often use attractive messages like “Free Download” or “Watch Now” to lure users.

The presence of warning signs or piracy symbols in the image indicates that the content being accessed is illegal. It highlights how users may unknowingly or knowingly engage in copyright violation by using such platforms. These websites may also contain hidden risks such as malware, viruses, or data theft.

The image emphasizes that digital content shared without proper authorization is a violation of copyright laws. It also shows how easy access to pirated content can lead to misuse of intellectual property.

In real-life situations, many users visit such websites to watch newly released movies or download paid content for free. Although it may seem convenient, it results in financial loss for creators, producers, and companies, and discourages creativity and innovation.

Legal Framework for Copyright Infringement in India

In India, copyright protection is primarily governed by the Copyright Act, 1957. Section 14 gives the copyright owner exclusive rights over specified uses of the work, including reproduction and communication of the work to the public. Therefore, unauthorised uploading or making a copyrighted work available online may infringe the owner's rights, subject to the exceptions and limitations provided by the Act.

Section 63 makes knowing infringement or abetment of copyright infringement a criminal offence. It provides for imprisonment of six months to three years and a fine of ₹50,000 to ₹2 lakh, subject to the qualifications and exceptions specified in the provision.

What Can a Copyright Owner Do if the Work Is Uploaded Without Permission?

A creator whose copyrighted work has been uploaded without permission can take several steps:

1. Send a written copyright complaint/takedown notice to the platform. Under the procedure in the proviso to Section 52(1)(c) and Rule 75 of the Copyright Rules, 2013, a copyright owner can submit a written complaint containing details identifying the work, establishing ownership, identifying the infringing copy and its location, and providing the required undertaking to approach the competent court. Where the Rule 75 procedure applies and the intermediary is satisfied that the copy is infringing, access is to be restricted for 21 days, or until a court order is received, whichever is earlier. The copyright owner must produce the competent court's order within that period; otherwise, access may be restored.

2. Use the platform's grievance mechanism. Intermediaries are required to prominently publish the name and contact details of their Grievance Officer and the mechanism through which users or victims can submit complaints. The current IT Rules also prescribe timelines for acknowledging and resolving grievances, including specific treatment for certain removal requests.

SGOU

3. Report the matter through the National Cyber Crime Reporting Portal. Affected persons can submit a cybercrime complaint through the Government of India's National Cyber Crime Reporting Portal at cybercrime.gov.in. The portal provides facilities for reporting different categories of cybercrime, including online and social-media-related offences.

4. Important: The creator must comply with the Rule 75 procedure and produce the required competent-court order within the prescribed twenty-one-day period if continued restriction of access is sought; otherwise, the storage provider may restore access and is not obliged to respond to a further notice from the same complainant concerning the same work and location.

Effects

- Financial loss to creators, producers, and companies
- Legal consequences for users involved in piracy
- Reduction in creativity and innovation
- Increased risk of malware, viruses, and data theft
- Loss of trust in digital platforms

Prevention

- Use only legal and authorized streaming or downloading platforms
- Avoid visiting suspicious or pirated websites
- Respect copyright laws and intellectual property rights
- Install antivirus software to protect devices
- Spread awareness about the risks of piracy

SGOU

Recap

- Financial cyber fraud includes online fraud and banking fraud.
- Intellectual property fraud involves misuse of creative works and brand identity.
- Software piracy refers to illegal use or distribution of software.
- Trademark infringement involves copying brand logos to deceive customers.
- Copyright violation occurs when digital content is shared without permission.
- These cybercrimes cause financial loss, legal issues, and security risks.
- Awareness and proper cybersecurity practices help in prevention.

Objective Type Questions

1. Which type of intellectual property fraud involves the illegal copying, installation, distribution, or use of software without proper permission or a valid license?

2. Which type of fraud uses deceptive messages, fake websites, or fraudulent links to obtain sensitive information such as passwords, banking credentials, or OTPs?

3. Which intellectual property fraud involves the unauthorized use of a registered brand name, logo, or symbol to mislead customers?

4. Which type of intellectual property violation involves the unauthorized copying, uploading, sharing, or distribution of digital content such as movies, music, eBooks, or photographs?

5. Which type of fraud involves the unauthorized use of stolen debit or credit card information to make transactions when the physical card is not present?

6. What is the term for a fake product that uses a brand name, logo, packaging, or design without authorization?

7. Which type of malicious software can be hidden in pirated or unauthorized software and may steal data, damage systems, or monitor users?

8. What is the term for a fraudulent request or transaction designed to deceive a user into transferring money or revealing financial information?

9. What term describes creations of the human mind, such as inventions, software, literary works, music, films, designs, symbols, names, and logos, that receive legal protection?

10. What security code is commonly sent to a registered mobile device or generated by an authentication system to verify a user's identity during a digital transaction or login?

SGOU

Answers to Objective Type Questions

1. Software Piracy

2. Phishing

3. Trademark Infringement

4. Copyright Violation

5. Card-Not-Present Fraud
6. Counterfeit Product
7. Malware
8. Online Fraud
9. Intellectual Property
10. One-Time Password (OTP)

Assignments

1. Explain financial cyber frauds with examples.
2. Describe software piracy and its effects.
3. What is trademark and logo infringement? Explain with examples.
4. Discuss copyright violation in online platforms.
5. Explain the prevention methods of cyber frauds.
6. Compare financial fraud and intellectual property fraud.
7. Discuss the impact of cyber frauds on individuals and organizations.

Suggested Reading

1. Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.
2. Stallings, W. (2018). *Effective cybersecurity: A guide to using best practices and standards*. Addison-Wesley.
3. Kizza, J. M. (2017). *Guide to computer network security* (5th ed.). Springer.
4. Chander, A. (2013). *The electronic silk road: How the web binds the world together in commerce*. Yale University Press.

SGOU

Reference

1. Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.

2. Easttom, C. (2019). *Computer security fundamentals* (4th ed.). Pearson.

3. Kumar, A., & Singh, S. (2020). Cybercrime and its impact on society. *International Journal of Cyber Security*, 5(2), 45–52.

4. National Crime Records Bureau. (2022). *Cyber crime in India report*. Government of India.

SGOU



BLOCK 3

A Global Perspective of Cyber Crimes

SOU



UNIT 1 Phases of Cyber Attack

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- outline the phases of a cyber attack and their objectives
- differentiate the activities performed during each phase of a cyber attack
- illustrate the progression of a cyber attack from reconnaissance to data exfiltration using practical examples
- implement appropriate security practices to reduce risks at different phases of a cyber attack

Prerequisites

Learners should understand the purpose of IP addresses, servers, databases, and web applications, and how security mechanisms such as firewalls, antivirus software, intrusion detection systems, and access controls help protect computer systems from unauthorized access. They should also appreciate the importance of regular software updates, timely security patching, strong passwords, multi-factor authentication, and continuous system monitoring in reducing security risks. This foundational knowledge helps learners understand that cyber attacks are usually carried out in a series of planned stages rather than through a single action. For example, consider a hospital that stores confidential patient records on its network. An attacker may begin by gathering publicly available information about the hospital (reconnaissance), identify vulnerable systems through network scanning (scanning), exploit a security weakness to gain unauthorized access (gaining access), establish long-term control over the compromised system (maintaining access), remove logs and other evidence to avoid detection (covering tracks), and finally transfer sensitive patient records outside the organization (data exfiltration). Understanding these phases helps learners recognize how attackers systematically compromise systems and highlights the importance of implementing effective security controls at every stage to protect an organization's information and digital assets.

SGOU

Key concepts

Authentication, Persistence, Reconnaissance, Malware, Exfiltration, malicious attackers, Privilege Escalation

Discussion

Ethical hacking follows a systematic and well-defined approach to detect vulnerabilities in systems, networks, and applications before they can be exploited by malicious attackers. This process enables security professionals to replicate real-world attack scenarios in a controlled and authorized environment, thereby enhancing overall cybersecurity measures.

Identifies potential security weaknesses before they are exploited by attackers

Simulates real-world cyber attacks in a safe and legally approved environment

Helps organizations strengthen and improve their security infrastructure.

3.1.1 The Phases of hacking

The hacking process consists of five structured phases used to identify and exploit system vulnerabilities. It begins with reconnaissance and scanning, where information is collected and potential weaknesses are identified. Next, the attacker gains access and maintains it by exploiting vulnerabilities and ensuring continued control over the system. Finally, the attacker covers tracks by removing evidence to avoid detection. See fig. 3.1.1.



Fig. 3.1.1 Phases of Ethical Hacking

3.1.1.1 Reconnaissance (Footprinting Phase)

Reconnaissance is the initial stage of ethical hacking in which security experts collect relevant information about the target system or organization. The main objective of this phase is to gain a clear understanding of the target environment and identify possible

SGOU

entry points for further security analysis. See fig. 3.1.2.

- Gathers details such as domain names, IP addresses, and DNS information
- Identifies the technologies, servers, and network infrastructure used by the target
- Relies on publicly available sources like websites, search engines, and social media platforms
- Enables ethical hackers to understand the system before proceeding with deeper security testing

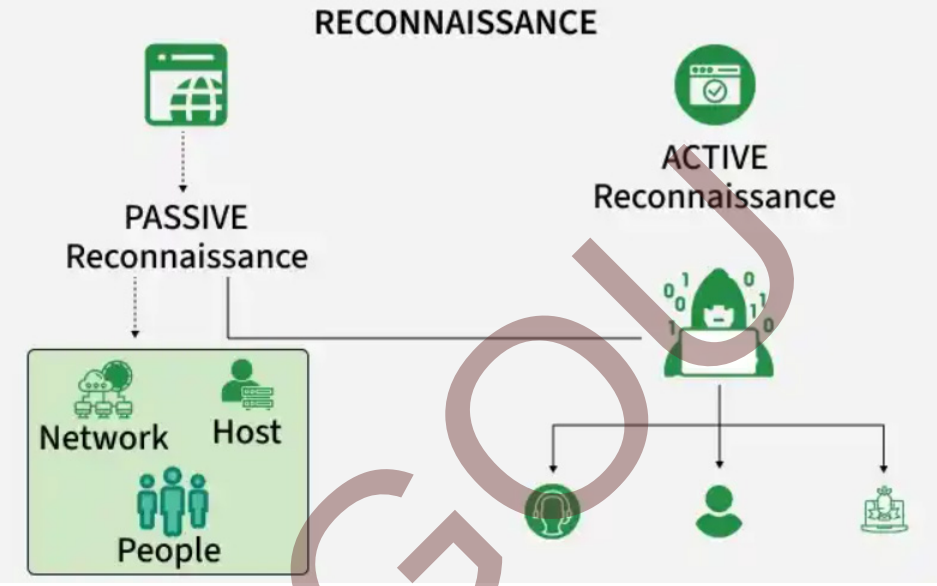


Fig. 3.1.2 Reconnaissance

Types of Reconnaissance

1. Passive Reconnaissance

Passive reconnaissance refers to collecting information about a target without directly interacting with its systems, making it difficult to detect. The attacker relies entirely on publicly available data to understand the target environment. For example, an ethical hacker may search a company's website and Google results to gather basic details, check employee roles and email patterns on LinkedIn, review DNS records to understand domain structure, or use WHOIS services to identify domain ownership and registration details.

2. Active Reconnaissance

Active reconnaissance involves directly interacting with the target system to obtain more detailed technical information. Since it includes probing the system, it is more likely to be detected. For example, an ethical hacker may perform a ping sweep to identify which devices are active on a network, send DNS queries to discover servers associated with a domain, or conduct network scanning to detect open ports and running services on a company's server.

SGOU

Tools Used in Reconnaissance

Various tools are used to support information gathering during this phase. WHOIS is used to obtain domain registration details such as owner and hosting provider. Maltego helps visualize relationships between domains, IP addresses, and organizations in a graphical format. theHarvester is useful for collecting email addresses and domain-related information from public sources. Recon-ng is a comprehensive framework for conducting reconnaissance tasks.

Google Dorking is a methodology that uses advanced search techniques to discover sensitive or hidden information available on websites.

Consider a company that hires an ethical hacker to evaluate its security. The hacker begins by gathering publicly available information such as the company's domain details, hosting provider, and server infrastructure using WHOIS and DNS lookup tools. They may also analyze employee profiles on LinkedIn to understand organizational roles and identify potential targets for phishing simulations, thereby preparing for the next stages of security testing.

3.1.1.2 Scanning

Scanning is the second stage of ethical hacking, where the information collected during reconnaissance is analyzed to identify potential weaknesses in the target system. In this phase, ethical hackers examine the network to detect open ports, active services, and possible security gaps that could be exploited. See fig. 3.1.3.

- Detects open ports and running services on the target system
- Identifies operating systems and software versions in use
- Discovers vulnerabilities and configuration issues that may be exploited
- Helps in identifying possible entry points for further testing

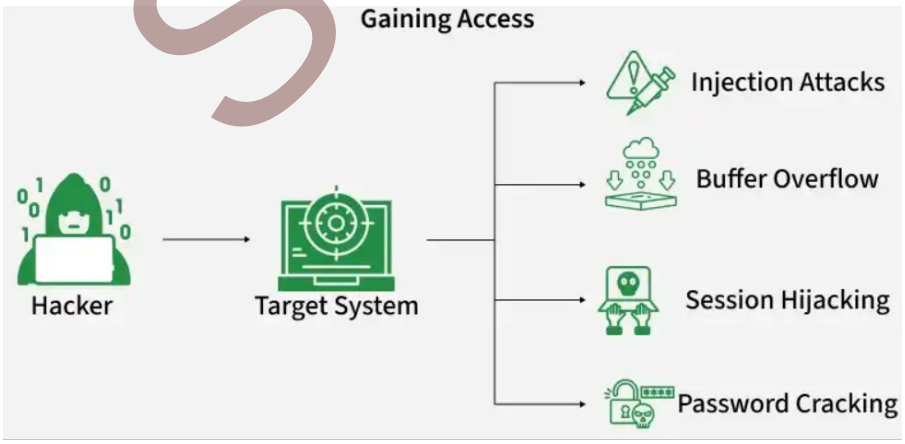


Fig. 3.1.3 Scanning

Types of Scanning

1. **Port Scanning:** This technique is used to identify open ports and the services associated with them on a system.

SGOU

2. **Vulnerability Scanning:** It detects known security flaws in operating systems, applications, and network services.

3. **Network Mapping:** This process identifies devices connected to the network and analyzes how they interact with each other.

Tools Used in Scanning

Nmap is a widely used tool for detecting open ports and services. Nikto is used to scan web servers for vulnerabilities. OpenVAS is a comprehensive vulnerability scanning framework, while Nessus is a popular tool for vulnerability assessment.

For example, an ethical hacker may scan a company's web server using Nmap and find that ports 80 (HTTP) and 443 (HTTPS) are open. The scan may also reveal that the server is running an outdated version of Apache, which contains known vulnerabilities that could be targeted in further testing.

Netdiscover is an Address Resolution Protocol (ARP)-based tool that helps identify active devices within a network.

3.1.1.3 Gaining Access

In this stage, the ethical hacker attempts to take advantage of the vulnerabilities identified during the scanning phase to check whether they can be exploited to gain unauthorized entry into the system. The objective is to simulate real-world cyber attacks in a controlled and authorized environment to assess the system's security.

Common Exploitation Techniques

SQL Injection involves manipulating database queries to access or modify data.

Cross-Site Scripting (XSS) allows attackers to inject malicious scripts into web applications.

Password Cracking focuses on breaking weak or poorly protected passwords.

Buffer Overflow attacks exploit weaknesses in memory handling to execute unauthorized code.

Outdated software vulnerabilities are targeted to gain access through unpatched systems. See fig. 3.1.4.

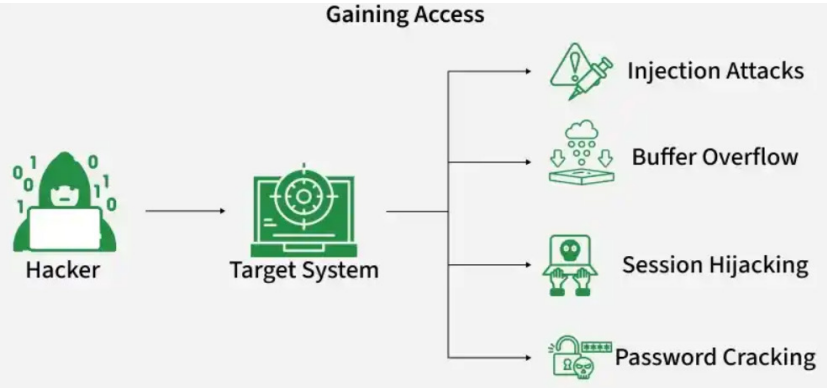


Fig. 3.1.4 Gaining Access

SGOU

Tools Used in Exploitation

The Metasploit Framework is widely used for testing and exploiting vulnerabilities.

SQLmap automates the process of detecting and exploiting SQL injection flaws.

Burp Suite is used for testing the security of web applications.

Hydra is commonly used for password cracking.

BeEF (Browser Exploitation Framework) targets vulnerabilities in web browsers.

For example, if a login page is found to have a SQL Injection vulnerability during scanning, the ethical hacker may use SQLmap to verify whether it can be exploited. If the attack is successful, it may allow access to sensitive information stored in the database, demonstrating the potential risk.

3.1.1.4 Maintaining Access

Maintaining Access is the stage in ethical hacking where the tester examines how long an attacker can remain within a compromised system without being detected. The purpose of this phase is to evaluate the extent of damage that could be caused and the level of control an attacker might achieve over the system. See fig. 3.1.5.

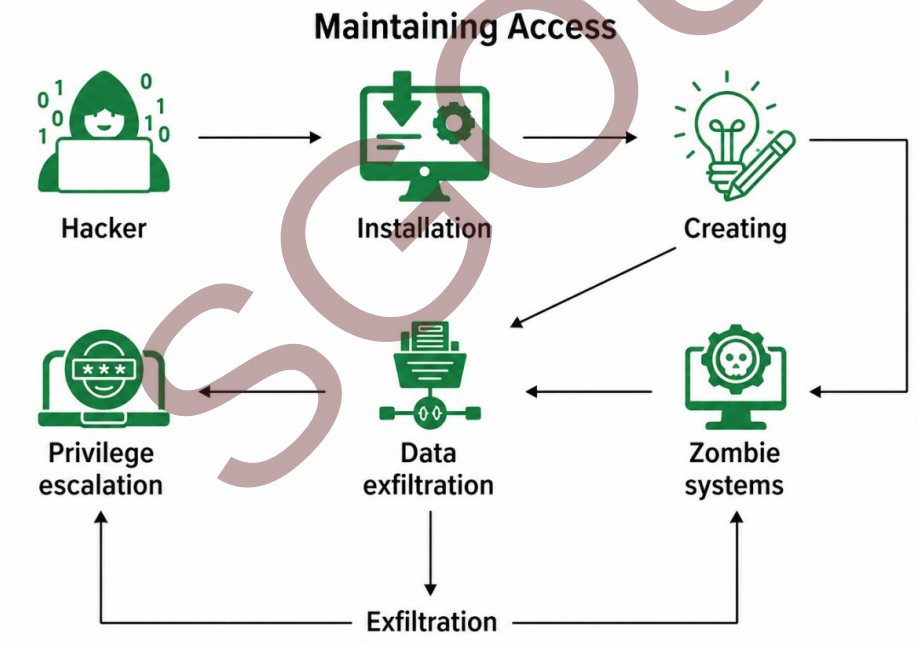


Fig. 3.1.5 Maintaining Access

- Verifies whether user privileges can be elevated to administrator or root level
- Determines if the attacker can move across multiple systems within the network
- Identifies whether sensitive or confidential data can be accessed
- Assesses the duration for which unauthorized access can be sustained

Activities Performed in Maintaining Access

- **Privilege Escalation:** Obtaining higher-level permissions such as administrator or root access
- **Lateral Movement:** Expanding access from one compromised system to other systems within the network
- **Persistence:** Establishing mechanisms to retain long-term access to the system
- **Data Exfiltration:** Accessing and potentially extracting sensitive information

Tools Used in Post-Exploitation

- Meterpreter: Enables advanced control over compromised systems
- Mimikatz: Retrieves credentials from system memory
- Empire: Supports post-exploitation operations
- PowerSploit: Provides PowerShell-based exploitation features

After successfully gaining access to a server, an ethical hacker may attempt to elevate privileges using tools like Mimikatz to extract login credentials. This process helps determine whether an attacker could obtain full administrative control and maintain prolonged access to the system.

3.1.1.5 Covering Tracks

Covering tracks is the stage in which an attacker tries to conceal their actions after successfully gaining unauthorized access to a system. The main objective is to eliminate or manipulate evidence so that security personnel find it difficult to detect, trace, or analyze the intrusion. See fig. 3.1.6.

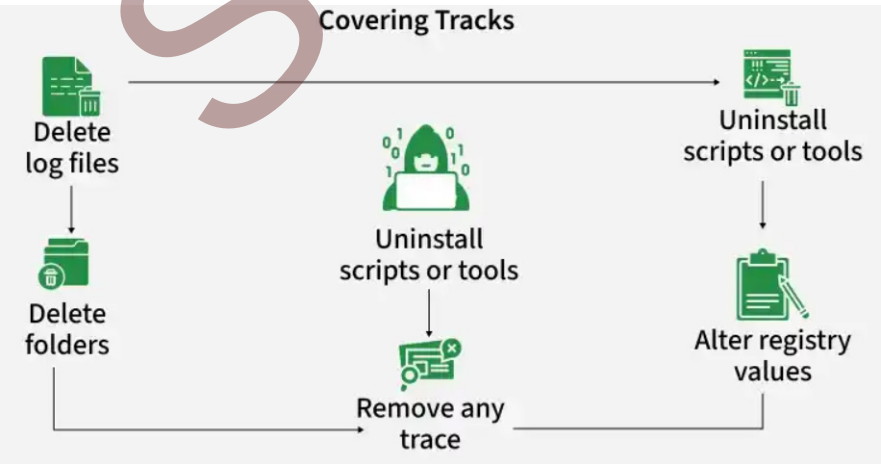


Fig. 3.1.6 Covering Tracks

- Removes or alters system logs to erase evidence of the attack
- Conceals malicious files, running processes, or backdoors from detection tools

SGOU

- Modifies file timestamps to mislead forensic analysis
- Enables the attacker to remain hidden and continue operating within the system unnoticed

Activities Carried Out in This Phase

- **Log Removal:** Attackers delete or modify system logs to eliminate traces of their actions.
- **Concealing Files and Processes:** Malicious files and running processes are hidden to evade detection by security systems.
- **Timestamp Alteration:** File timestamps are changed to obscure the actual time of the attack.
- **Backdoor Hiding:** Backdoors or persistent access mechanisms are concealed to maintain unnoticed access to the system.

Tools Commonly Used for Covering Tracks

- **Rootkits:** Employed to hide files, processes, and system activities from detection.
- **Metasploit (Clearev module):** Used to erase Windows event logs.
- **Timestomp:** Alters file timestamps to disguise the attack timeline.
- **Log Cleaning Scripts:** Custom scripts designed to remove or modify log entries.

After gaining unauthorized access to a company server, an attacker removes system logs and alters file timestamps to conceal evidence of the breach. They may also deploy a rootkit to hide malicious processes and retain access without being noticed by system administrators.

Once this phase is complete, it indicates that the ethical hacker has successfully accessed the system, exploited its vulnerabilities, and exited without leaving detectable traces. After completing all five phases, the ethical hacker prepares a detailed report outlining the identified vulnerabilities along with recommended solutions, enabling the organization to strengthen its overall security posture.

3.1.1.6 Data Exfiltration – The Stage Where the Actual Damage Occurs

Data exfiltration is the final and one of the most critical stages of a cyber attack. At this stage, the attacker transfers confidential or sensitive information from the victim's network to a location under the attacker's control. The stolen data may include customer records, financial information, intellectual property, login credentials, business documents, medical records, or other valuable organizational data.

After successfully gaining access to the target system, escalating privileges, and locating valuable information, the attacker begins extracting the data without the knowledge

SGOU

of the organization. To avoid detection, attackers often use stealth techniques such as compressing and encrypting the data before transmission or transferring it in small batches over an extended period. In some cases, attackers may rapidly exfiltrate large volumes of data if they believe their presence is about to be detected.

Common Methods of Data Exfiltration

Attackers employ various techniques to secretly move data outside the organization's network, including:

- **Encrypted Outbound Traffic:** Sensitive data is encrypted before transmission, making it difficult for security systems to inspect the contents of the outgoing traffic.
- **Cloud Storage Services:** Public cloud storage platforms are frequently misused to upload stolen information because they appear as legitimate internet traffic.
- **Compromised Third-Party Platforms:** Attackers may route stolen data through compromised websites, remote servers, or trusted third-party services to conceal the final destination.
- **Email and File Transfer Protocols:** In some attacks, confidential files are sent through email attachments or transferred using FTP, SFTP, or similar protocols.
- **Command-and-Control (C2) Servers:** Data may also be transmitted directly to servers controlled by the attacker through an established command-and-control channel.

Impact of Data Exfiltration

By the time an organization detects data exfiltration, the confidential information has often already been copied and transferred outside its control. Recovering the stolen data is usually impossible, and the consequences can be severe. The attackers may:

- Sell the stolen information on dark web marketplaces.
- Leak confidential data publicly.
- Use the information for identity theft or financial fraud.
- Demand ransom payments by threatening to publish sensitive information.
- Exploit the stolen data for corporate espionage or future cyber attacks.

Business Consequences

Data exfiltration represents the point at which a cyber attack causes measurable business damage. Organizations may suffer:

- Significant financial losses due to recovery costs, legal penalties, and regulatory fines.

SGOU

- Loss of customer trust and confidence.
- Damage to brand image and corporate reputation.
- Business disruption and operational downtime.
- Legal actions from customers, partners, or regulatory authorities.
- Long-term competitive disadvantages resulting from the theft of intellectual property and trade secrets.

Data exfiltration is the final objective of many cyber attacks and marks the stage where the impact becomes most severe. Once sensitive information leaves the organization's network, the damage is often irreversible. Therefore, organizations must implement strong security controls such as data loss prevention (DLP) systems, network monitoring, encryption, access control, and continuous threat detection to identify and prevent unauthorized data transfers before valuable information is lost.

Recap

- Ethical hacking is an authorized security assessment performed to identify and fix vulnerabilities before malicious attackers can exploit them.
- The ethical hacking process phases: Reconnaissance, Scanning, Gaining Access, Maintaining Access, and Covering Tracks.
- Reconnaissance (Footprinting) is the information-gathering phase where details such as domains, IP addresses, DNS records, technologies, and employee information are collected.
- Passive reconnaissance gathers publicly available information without interacting with the target, while active reconnaissance directly probes the target system and is more likely to be detected.
- Common reconnaissance tools include WHOIS, Maltego, theHarvester, Recon-ng, and Google Dorking.
- Scanning analyzes the collected information to identify open ports, running services, operating systems, software versions, and known vulnerabilities.
- The three primary types of scanning are port scanning, vulnerability scanning, and network mapping, using tools such as Nmap, Nessus, OpenVAS, Nikto, and Netdiscover.
- During Gaining Access, ethical hackers safely exploit discovered vulnerabilities to verify whether unauthorized access is possible.
- Common exploitation techniques include SQL Injection, Cross-Site Scripting (XSS), Password Cracking, Buffer Overflow, and exploiting outdated software vulnerabilities.

SGOU

- Popular exploitation tools include Metasploit Framework, SQLmap, Burp Suite, Hydra, and BeEF.
- Maintaining Access evaluates whether an attacker can retain long-term control by performing privilege escalation, lateral movement, persistence, and data exfiltration.
- Post-exploitation tools such as Meterpreter, Mimikatz, Empire, and PowerSploit help assess the level of control an attacker could achieve.
- Covering Tracks involves hiding evidence of the attack by deleting logs, concealing malicious files and processes, modifying timestamps, and hiding backdoors using tools like Rootkits, Timestomp, and Metasploit Clearev.
- Data Exfiltration is the stage where attackers secretly transfer sensitive information outside the organization's network using encrypted traffic, cloud storage, email, file transfer protocols, or command-and-control (C2) servers.
- Organizations can reduce cyber risks by implementing Data Loss Prevention (DLP), continuous network monitoring, encryption, strong access control, timely patch management, vulnerability assessments, and continuous threat detection to prevent unauthorized access and data theft.

Objective Type Questions

1. Which phase of ethical hacking involves collecting information about the target before launching an attack?
2. Which type of reconnaissance gathers information without directly interacting with the target system?
3. Which tool is commonly used to retrieve domain registration information?
4. Which scanning technique identifies open ports on a target system?
5. Which tool is widely used for network scanning and port discovery?
6. Which attack technique exploits weaknesses in SQL queries?
7. Which framework is commonly used for exploiting vulnerabilities during penetration testing?
8. Which post-exploitation technique allows attackers to obtain administrator or root privileges?
9. What is the process of moving from one compromised system to another within the same network called?

SGOU

10. Which tool is commonly used to extract Windows credentials from system memory?

11. What is the process of secretly transferring confidential data outside an organization's network called?

12. Which type of server is commonly used by attackers to receive stolen data from compromised systems?

13. Which tool is used to modify file timestamps to hide evidence of an attack?

14. Which malicious software hides files, processes, and attacker activities from the operating system?

15. Which security solution is specifically designed to prevent unauthorized transfer of sensitive information outside an organization?

Answers to Objective Type Questions

1. Reconnaissance
2. Passive
3. WHOIS
4. Port Scanning
5. Nmap
6. SQL Injection
7. Metasploit
8. Privilege Escalation
9. Lateral Movement
10. Mimikatz
11. Data Exfiltration
12. Command-and-Control (C2)
13. Timestomp
14. Rootkit
15. DLP

SGOU

Assignments

1. Explain the phases of ethical hacking with a neat diagram. Discuss the objectives, activities, and significance of each phase in securing computer systems.

2. Differentiate between passive reconnaissance and active reconnaissance. Explain the techniques, tools, advantages, and limitations of each with suitable examples.

3. Describe the scanning phase of ethical hacking. Explain the different types of scanning, commonly used scanning tools, and their role in identifying system vulnerabilities.

4. Explain the gaining access phase of ethical hacking. Discuss various exploitation techniques and the tools used by ethical hackers to verify system vulnerabilities.

5. Describe the maintaining access phase in ethical hacking. Explain privilege escalation, lateral movement, persistence, and data exfiltration with suitable examples.

6. What is data exfiltration? Explain the common methods used by attackers to transfer sensitive information outside an organization's network and discuss its impact on business operations.

7. Assume you are an ethical hacker assigned to perform a security assessment for an organization. Explain how you would execute each phase of ethical hacking, including the tools used, expected outcomes, and recommendations for improving the organization's security posture.

SGOU

Suggested Reading

1. Godbole, Nina, and Sunit Belapure. *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*. Wiley India Pvt. Ltd., 2011.

2. Brooks, Charles J., et al. *Cybersecurity Essentials*. Wiley, 2018

3. Wu, Chwan-Hwa (John), and J. David Irwin. *Introduction to Cyber Security*. CRC Press, 2016.

Reference

1. Jain, Atul. *Cyber Crime: Issues, Threats and Management*. Isha Books, 2004.

2. Yar, Majid. *Cybercrime and Society*. Sage Publications, 2006.

3. Chaubey, R. K. *Cyber Crimes and Law*. Kamal Law House, 2012.

SGOU



UNIT 2 Types of Cyber Attacks

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- differentiate between passive attacks and active attacks based on their characteristics and impact
- classify common cyber attack techniques such as scanning, footprinting, and enumeration according to their purpose in ethical hacking
- apply basic footprinting and scanning techniques to gather information about a target system in an authorized environment
- use appropriate tools and methods to enumerate network resources and identify potential security weaknesses

Prerequisites

The learner should know how computers communicate over a network and how users access online services using usernames and passwords. For example, when a person connects to a public Wi-Fi network at an airport or coffee shop, an attacker may silently monitor network traffic (a passive attack) or actively attempt to intercept or modify communications (an active attack). Similarly, before attacking an organization, cyber-criminals often collect publicly available information about its website and network through footprinting and scanning. Understanding these basic concepts helps learners recognize how cyber attacks are planned and why organizations use security measures to detect and prevent them.

Key concepts

Interception, Authentication, Integrity, Reconnaissance, Vulnerability, Spoofing, Timestamps

SGOU

Discussion

Attack classification based on data and resources: Network attacks are classified into passive attacks and active attacks based on how they affect data and network resources.

3.2.1 Passive Attacks

In a **passive attack**, an attacker secretly monitors or intercepts network communications without modifying the data or disrupting system operations. The primary objective is to collect sensitive information, such as login credentials, confidential documents, or communication details, while remaining unnoticed. Because no changes are made to the data or network resources, passive attacks are often difficult to detect and can continue for long periods without raising suspicion. See fig. 3.2.1.

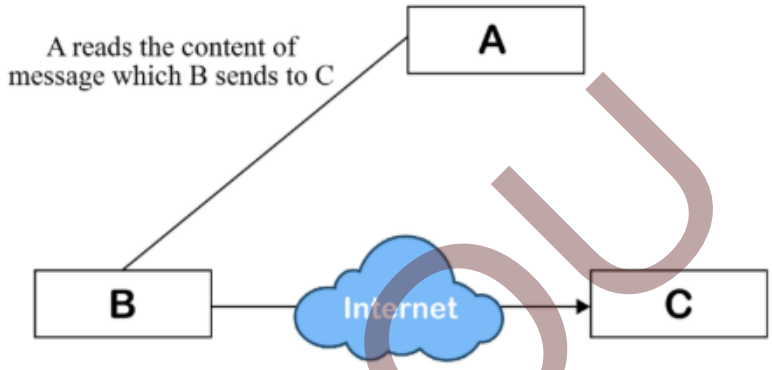


Fig. 3.2.1 Passive Attacks

3.2.1.1 Traffic Analysis

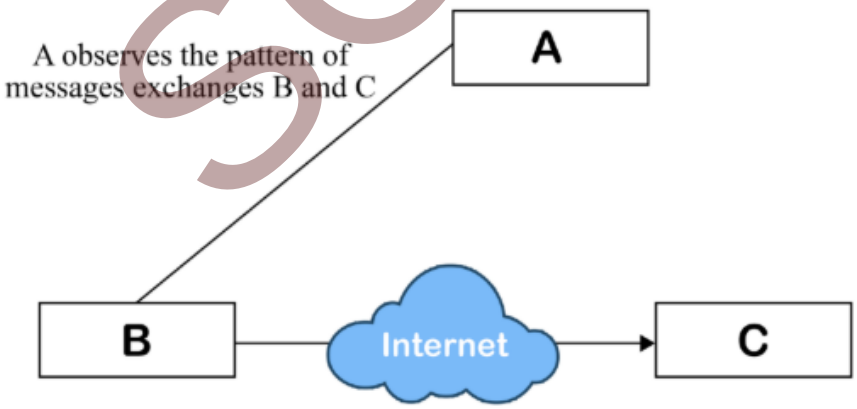


Fig. 3.2.2 Traffic Analysis

Traffic analysis is a passive attack in which an attacker observes the volume, timing, and patterns of data exchanged between communicating systems without altering the transmitted information. By examining communication behavior, attackers can infer valuable details such as user activity, operational schedules, communication frequency, and the importance of specific interactions. For example, a sudden increase

SGOU

in network traffic may indicate an emergency, a critical business operation, or the transfer of sensitive information, while reduced traffic may suggest inactivity or system downtime. This information can help attackers plan targeted cyber attacks or social engineering campaigns at the most effective time. Since traffic analysis relies on monitoring rather than modifying data, it is difficult to detect. Organizations can reduce this risk by implementing encryption, traffic padding, secure communication protocols, and continuous network monitoring to conceal communication patterns and identify suspicious activities.

3.2.1.2 Eavesdropping

Eavesdropping is a passive cyber attack in which an unauthorized person secretly intercepts and listens to communications between two parties to obtain sensitive information such as usernames, passwords, financial details, personal data, or confidential business information. Attackers may perform eavesdropping by exploiting insecure network connections, weaknesses in communication protocols, or malware capable of capturing transmitted data.

Unlike traffic analysis, which focuses only on communication patterns and data flow, eavesdropping captures the actual content of the communication. As a result, attackers can directly access confidential information that may be used for identity theft, financial fraud, espionage, or other malicious activities. For example, if an attacker intercepts an online banking session over an unsecured network, they may obtain login credentials and gain unauthorized access to the victim's account.

Eavesdropping can occur in both digital and physical environments. It may involve intercepting emails, phone calls, or network traffic, as well as overhearing private conversations or using hidden listening devices. The widespread use of wireless networks, mobile devices, and online communication platforms has significantly increased the opportunities for such attacks, particularly when users rely on unsecured public Wi-Fi networks.

To protect against eavesdropping, organizations and individuals should use strong encryption techniques, secure communication protocols, multi-factor authentication, and virtual private networks (VPNs). Regular software updates, secure network configurations, user awareness programs, and continuous security monitoring further help prevent unauthorized interception of sensitive communications and strengthen overall information security.

3.2.2 Active Attacks

Active attacks involve unauthorized attempts to access a network with the objective of altering, disrupting, or destroying data and system resources. Unlike passive attacks, they directly interfere with normal network operations by modifying transmitted data, interrupting services, or compromising system functionality, making them easier to detect but significantly more harmful.

3.2.2.1 Repudiation Attacks

A repudiation attack is a type of cyber attack in which an attacker performs an action and later denies having carried it out. These actions may include sending messages,

SGOU

executing transactions, or modifying data. The attacker exploits weaknesses in authentication, logging, or auditing mechanisms to avoid accountability and make it difficult to prove who performed the action. As a result, organizations may face challenges in identifying the source of malicious activities, resolving disputes, and conducting forensic investigations.

Repudiation attacks commonly occur when systems lack proper authentication, digital signatures, secure logs, or audit trails. Without reliable evidence, attackers can deny their involvement, making it difficult to enforce security policies or establish legal accountability. Implementing non-repudiation mechanisms ensures that every action performed within a system can be traced back to its legitimate source.

Types of Repudiation Attacks

1. Message Repudiation

In a message repudiation attack, an attacker sends an email, message, or other form of communication and later denies sending it. This is often achieved by using forged sender identities or exploiting systems that do not verify the sender's identity. For example, an attacker may send a phishing email using a spoofed email address and later deny responsibility because the system lacks proper authentication or digital signatures.

2. Transaction Repudiation

Transaction repudiation occurs when an attacker performs an online transaction and later claims that they never authorized or initiated it. Such attacks are common in banking and e-commerce systems that lack strong authentication or transaction verification mechanisms. Examples include unauthorized fund transfers, fraudulent online purchases, or fake payment transactions that lead to financial disputes and losses.

3. Data Repudiation

Data repudiation involves modifying, deleting, or tampering with information and then denying responsibility for those changes. This attack is especially dangerous in environments where data integrity is critical, such as healthcare, banking, and government systems. For instance, an attacker may alter customer records or financial data and later deny making the changes if the system lacks secure logging and auditing.

Prevention of Repudiation Attacks

Organizations can reduce the risk of repudiation attacks by implementing strong authentication methods, digital signatures, secure audit logs, access controls, encryption, and non-repudiation mechanisms. Maintaining tamper-proof logs and continuously monitoring user activities helps ensure that every action performed within the system can be accurately traced to the responsible user, thereby improving accountability and supporting forensic investigations after a security incident.

3.2.2.2 Modification of Messages

Modification of messages is an active attack in which an attacker intercepts and deliberately alters, delays, reorders, or inserts messages during communication. Unlike passive attacks that only observe data, this attack compromises the integrity of

SGOU

information by changing its original content, making the received message unreliable or misleading. Attackers may manipulate data packets, modify communication sequences, or inject fraudulent messages to disrupt normal operations and deceive the recipient. For example, a message stating, "Allow JOHN to access confidential file X," can be altered to "Allow SMITH to access confidential file X," granting unauthorized access to sensitive information. Such attacks can lead to financial fraud, unauthorized transactions, denial-of-service conditions, or the compromise of critical business processes. To defend against message modification attacks, organizations should implement strong encryption, digital signatures, message integrity checks, and secure authentication mechanisms to ensure that any unauthorized changes are detected and prevented. See fig. 3.2.3.

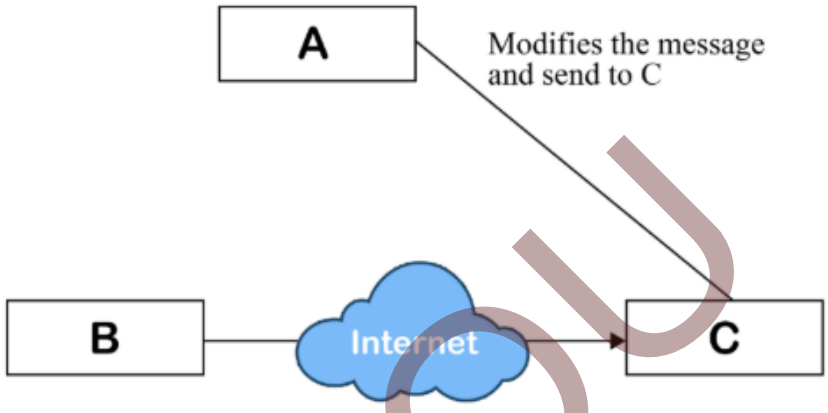


Fig. 3.2.3 Modification of messages

3.2.2.3 Replay Attacks

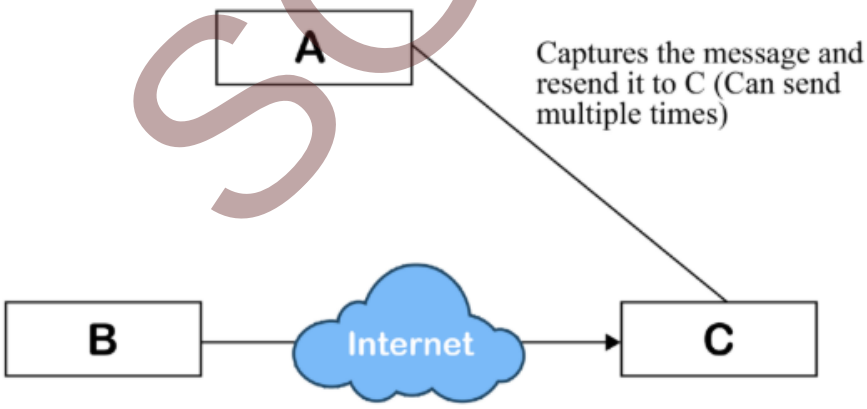


Fig. 3.2.4 Replay Attacks

A replay attack is an active network attack in which an attacker captures a legitimate communication and retransmits it later to deceive a system into accepting it as a valid request. Instead of modifying the original data, the attacker reuses previously captured messages to impersonate an authorized user and gain unauthorized access. For example, if an attacker intercepts a user's login request or authentication token, they can resend the same information to the server and potentially gain access without knowing

SGOU

the user's password. Replay attacks are particularly dangerous when authentication tokens, session IDs, or cryptographic keys remain valid for long periods without proper validation. In financial systems, a replay attack could result in duplicate transactions or unauthorized fund transfers by resending previously authorized requests. To prevent replay attacks, organizations should implement security measures such as timestamps, nonces (single-use random values), challenge-response authentication, and session expiration mechanisms. Secure communication protocols such as TLS, along with continuous monitoring of authentication activities, further help ensure that intercepted messages cannot be reused successfully.

3.2.2.4 Masquerade Attacks

A masquerade attack is an active cyber attack in which an attacker pretends to be a legitimate user to gain unauthorized access to systems, networks, or sensitive information. Instead of exploiting software vulnerabilities directly, the attacker typically obtains valid user credentials through techniques such as phishing, social engineering, shoulder surfing, or keylogging. Once these credentials are acquired, the attacker logs in as the authorized user, making the malicious activity appear legitimate and bypassing many traditional security controls. For example, an attacker may send a fake email that appears to come from the organization's IT department, directing employees to a fraudulent login page where their usernames and passwords are stolen. After successfully logging in, the attacker can access confidential information, modify or delete data, perform unauthorized transactions, or misuse the victim's privileges to compromise additional systems. Masquerade attacks are especially dangerous when high-privilege accounts are targeted, as they provide attackers with extensive control over organizational resources. To reduce the risk of such attacks, organizations should enforce strong passwords, implement multi-factor authentication (MFA), provide regular security awareness training to help users recognize phishing attempts, and continuously monitor user activities for unusual login patterns or suspicious behavior. See fig. 3.2.5.

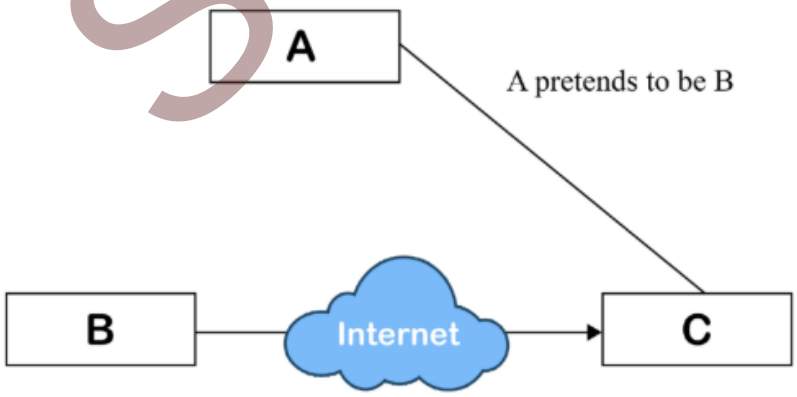


Fig. 3.2.5 Masquerade Attack

There are several common types of masquerade attacks, each involving different techniques to deceive users and systems:

Username and Password Masquerade: In this type of attack, the attacker uses stolen,

SGOU

guessed, or compromised usernames and passwords to impersonate a legitimate user and gain unauthorized access to a system. Such attacks commonly occur through phishing, credential theft, or password guessing, allowing the attacker to access confidential information or perform unauthorized activities while appearing to be an authorized user.

IP Address Masquerade: An IP address masquerade attack occurs when an attacker forges or spoofs their IP address to appear as a trusted device or network. This enables the attacker to bypass IP-based security controls, conceal their true identity, evade detection, or launch attacks such as Distributed Denial-of-Service (DDoS) attacks using fake source addresses.

Website Masquerade: In a website masquerade attack, the attacker creates a counterfeit website that closely resembles a legitimate one, such as an online banking portal, shopping website, or government service. The fake website is designed to trick users into entering sensitive information such as usernames, passwords, credit card numbers, or personal details, which are then captured and misused by the attacker.

Email Masquerade: An email masquerade attack involves sending fraudulent emails that appear to originate from a trusted individual or organization. These emails often contain malicious links, fake login pages, or infected attachments that trick recipients into revealing confidential information or installing malware. Spoofed sender addresses make these emails appear authentic and increase the likelihood of successful deception.

Masquerade attacks are highly effective because they exploit the trust users place in legitimate identities, websites, and communication channels. Understanding these different forms of masquerade attacks helps individuals and organizations recognize suspicious activities and implement appropriate security measures to reduce the risk of impersonation-based attacks.

3.2.2.5 Denial of Service (DoS) attacks

A Denial of Service (DoS) attack is an active cyber attack that aims to make a server, application, or network unavailable by overwhelming it with an excessive number of requests or data packets. In a typical DoS attack, a single attacking system continuously sends large volumes of traffic, exhausting the target's resources such as processing power, memory, or bandwidth. As a result, legitimate users are unable to access the affected service, leading to service disruption, financial losses, and reputational damage. For example, an attacker may use an automated tool or script to generate thousands of requests to a website, causing it to become overloaded and eventually crash. See fig. 3.2.6.

There are various types of Denial of Service (DoS) attacks, each designed to disrupt a network or system's functionality:

1. **Flood attacks:** In a flood attack, the attacker generates an extremely large volume of network traffic or service requests to exhaust the target system's resources, preventing it from responding to legitimate users.

2. **Amplification attacks:** In an amplification attack, the attacker exploits

SGOU

vulnerable third-party servers to multiply the amount of attack traffic, causing a much larger volume of data to be directed toward the target and increasing the impact of the attack.

To protect against DoS attacks, organizations can adopt several strategies:

1. **Firewalls and Intrusion Detection Systems (IDS):** These security mechanisms continuously inspect network traffic to identify and block suspicious or malicious activities before they affect the system.

2. **Connection Limiting:** Restricting the number of incoming requests or simultaneous connections helps prevent attackers from exhausting system resources.

3. **Load Balancing and Distributed Systems:** These techniques distribute network traffic across multiple servers, ensuring that no single server becomes overloaded during an attack.

4. **Network Segmentation and Access Control:** Dividing the network into smaller, isolated segments and enforcing strict access permissions helps contain attacks and reduces their overall impact.

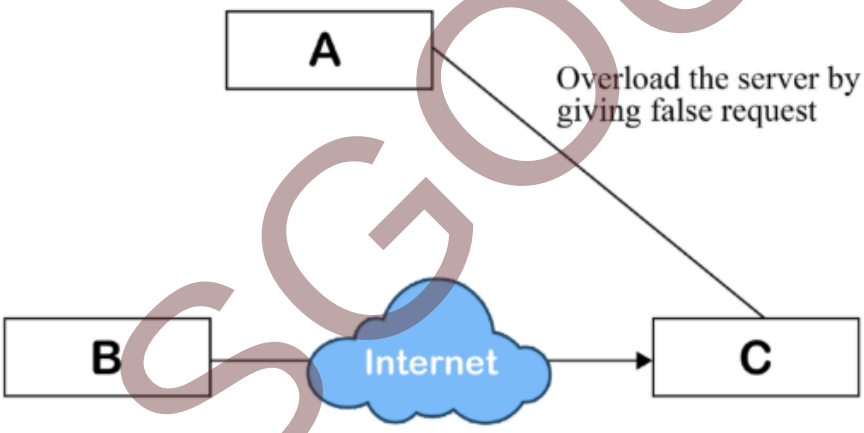


Fig. 3.2.6 Denial of Service

SGOU

3.2.2.6 Distributed Denial of Service (DDoS)

A Distributed Denial of Service (DDoS) attack is an advanced form of DoS attack in which multiple compromised computers simultaneously flood a target server, network, or service with an enormous volume of traffic. These compromised devices, collectively known as a botnet, are remotely controlled by the attacker to launch coordinated attacks from different locations. Since the malicious traffic originates from numerous systems rather than a single source, identifying and blocking the attack becomes significantly more difficult. As a result, DDoS attacks can severely disrupt online services, consume network resources, and prevent legitimate users from accessing the targeted system. See fig. 3.2.7.

Both DoS and DDoS attacks can cause significant disruption to organizations by

making critical services unavailable, resulting in operational downtime, financial losses, and reduced customer confidence. Online businesses, e-commerce platforms, healthcare providers, and financial institutions are particularly vulnerable because service availability is essential to their operations. In some cases, attackers use DDoS attacks as a distraction while simultaneously carrying out other malicious activities, such as data theft, malware deployment, or unauthorized system access.

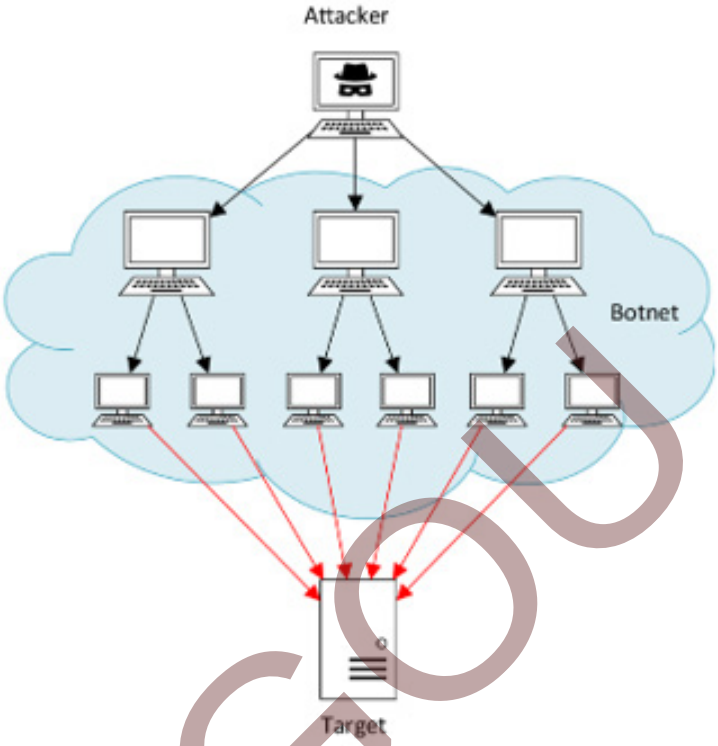


Fig 3.2.7 DDoS Attack

Protecting against these attacks requires multiple security measures, including firewalls, intrusion detection and prevention systems (IDS/IPS), and network traffic monitoring to identify abnormal traffic patterns. Many organizations also rely on cloud-based DDoS mitigation services that can filter or absorb malicious traffic before it reaches the target infrastructure. In addition, having a well-defined incident response plan enables security teams to respond quickly and minimize the impact of an attack.

Organizations should also educate employees about the indicators of DoS and DDoS attacks and promote good cybersecurity practices to improve overall preparedness. As these attacks continue to become more frequent and sophisticated, adopting a proactive security strategy, implementing robust defensive technologies, and continuously monitoring network activity are essential for protecting digital assets and ensuring uninterrupted access to services for legitimate users.

3.2.2.7 MitM Attacks

A Man-in-the-Middle (MitM) attack is an active cyber attack in which an attacker secretly intercepts and relays communication between two parties who believe they are communicating directly with each other. By positioning themselves between the sender

SGOU

and the receiver, the attacker can monitor, capture, modify, or manipulate the exchanged information without either party detecting the intrusion. This enables attackers to steal sensitive information such as usernames, passwords, banking details, personal messages, and confidential business data. For example, while a user is accessing an online banking website, an attacker may intercept the communication and redirect the user to a fake website that closely resembles the legitimate one, allowing login credentials to be stolen.

Attackers use several techniques to carry out MitM attacks. HTTPS spoofing involves presenting a fake secure website by using fraudulent digital certificates, making users believe their connection is encrypted. DNS poisoning manipulates DNS records so that users are redirected from legitimate websites to malicious ones without their knowledge. Another common method is exploiting unsecured public Wi-Fi networks, where attackers intercept data transmitted between users and the internet. Specialized attack tools further automate these techniques, enabling attackers to capture credentials, monitor communications, and alter transmitted data with minimal effort.

The consequences of MitM attacks can be severe, including identity theft, financial fraud, unauthorized account access, and the compromise of confidential organizational information. In some cases, attackers perform session hijacking, where they steal or take control of an active user session, allowing them to impersonate the victim and perform unauthorized actions without requiring login credentials.

Organizations can reduce the risk of MitM attacks by implementing strong security measures such as end-to-end encryption, HTTPS with valid digital certificates, multi-factor authentication (MFA), and secure communication protocols. Users should avoid connecting to untrusted public Wi-Fi networks or use a Virtual Private Network (VPN) when doing so. Regular security awareness training and continuous monitoring of network communications further help detect and prevent Man-in-the-Middle attacks before they cause significant damage. See fig. 3.2.8.

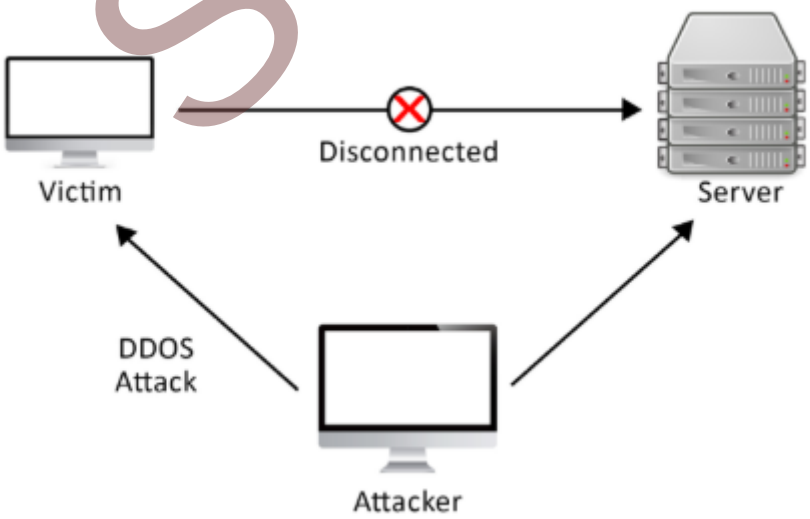


Fig. 3.2.8 Man-in-the-Middle (MitM) Attack

Organizations can strengthen their defenses against Man-in-the-Middle (MitM) attacks

by deploying Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to continuously monitor network traffic for suspicious activities and unauthorized interception attempts. Regular security audits, vulnerability assessments, and timely patch management help identify weaknesses that attackers could exploit. In addition, promoting cybersecurity awareness among users and implementing proactive security practices are essential for minimizing the risk of MitM attacks and protecting the confidentiality and integrity of network communications.

3.2.3 Port Scanning Techniques Using Nmap

Nmap (Network Mapper) is a widely used open-source tool for network discovery and security auditing. It helps identify active hosts, open ports, running services, operating systems, and software versions by sending packets to target systems and analyzing their responses. One of its primary functions is port scanning, which determines whether network ports are open, closed, or filtered.

Example:

nmap -sS 192.168.0.1-52

This command performs a TCP SYN scan on the specified IP address range.

Port Status

- **Open:** A service is actively running and accepting connections.
- **Closed:** No service is listening on the port, but the host is reachable.
- **Filtered:** A firewall or security device blocks the scan, making the port status unknown.

3.2.3.1 Nmap Port Scanning Techniques

1. TCP Connect Scan (-sT)

TCP Connect Scan establishes a complete TCP three-way handshake to determine whether a port is open or closed. If the port is open, the connection is completed; if it is closed, the target responds with a TCP Reset (RST) packet. Since the full connection is established, this scan is accurate but easily detected and logged by the target system.

Advantages

- Accurate and reliable.
- Does not require administrator privileges.

Disadvantages

- Slower than SYN scan.
- Easily detected and logged.

2. TCP SYN Scan (-sS)

TCP SYN Scan, also called Half-Open or Stealth Scan, sends only a SYN packet to the

SGOU

target. If the port is open, the target replies with SYN/ACK, and Nmap immediately sends an RST packet instead of completing the handshake. This makes the scan faster and less likely to appear in system logs.

Advantages

- Fast and efficient.
- Less detectable than TCP Connect Scan.

Disadvantages

- Requires administrator/root privileges.

3. UDP Scan (-sU)

UDP Scan checks UDP ports by sending UDP packets. Since UDP is connectionless, open ports usually do not respond, while closed ports return an ICMP "Port Unreachable" message. Because of the lack of responses, UDP scanning is slower and less accurate than TCP scanning.

Advantages

- Detects UDP services such as DNS, DHCP, and SNMP.

Disadvantages

- Slow and sometimes inconclusive.

4. TCP NULL Scan (-sN)

NULL Scan sends a TCP packet with no flags set. Closed ports respond with an RST packet, while open ports usually do not respond. This technique can sometimes bypass simple firewall rules.

5. TCP FIN Scan (-sF)

FIN Scan sends a packet with only the FIN flag set. Closed ports reply with an RST packet, whereas open ports ignore the packet. It is mainly used for stealth scanning.

6. TCP XMAS Scan (-sX)

XMAS Scan sends a packet with the URG, PSH, and FIN flags enabled. Closed ports return an RST packet, while open ports generally do not respond. The packet resembles a "Christmas tree" in packet analyzers, giving the scan its name.

Nmap supports several port scanning techniques, each designed for different purposes. TCP Connect Scan is accurate but easily detected, TCP SYN Scan is faster and stealthier, UDP Scan identifies UDP services, while NULL, FIN, and XMAS scans are specialized techniques used to bypass simple firewall rules and perform stealth reconnaissance.

3.2.4 Footprinting

Footprinting is an important information-gathering activity performed during the early

SGOU

stages of ethical hacking and penetration testing. It is closely related to reconnaissance, which is the broader process of collecting information about a target to support further security assessment or potential attack planning. Footprinting focuses on identifying and documenting relevant details about the target, such as domain names, IP addresses, DNS information, network infrastructure, exposed services, operating systems, software, and web application components. These activities help security professionals understand the target's environment and identify its potential attack surface. NIST identifies information gathering and scanning as key activities within the discovery phase of penetration testing, while OWASP describes web-application footprinting as probing and exploring an application to understand its composition, configuration, and entry points.

The information obtained through reconnaissance and footprinting helps ethical hackers plan subsequent security testing more effectively and enables organizations to identify unnecessary information exposure. By understanding what information and services are publicly accessible, organizations can reduce information leakage and strengthen their overall security posture.

3.2.4.1 Types of Footprinting

Footprinting can be classified into **passive footprinting** and **active footprinting** based on the method used to collect information.

Passive Footprinting

Passive footprinting involves collecting information about a target without directly interacting with its systems or network. Since there is no direct communication with the target, this method is difficult to detect and leaves almost no evidence of reconnaissance activities. Ethical hackers rely on publicly available information obtained from search engines, company websites, social media platforms, domain registration databases, public documents, and archived web pages. Although passive footprinting may not always provide complete or real-time information, it offers valuable background knowledge about the organization and serves as the starting point for further investigation.

Active Footprinting

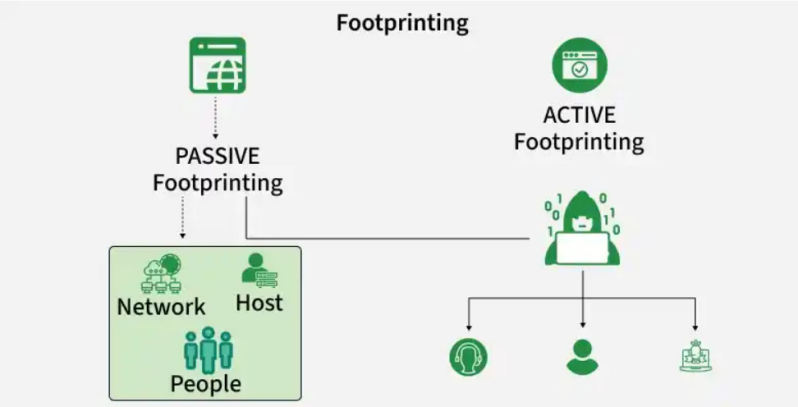


Fig. 3.2.9 Footprinting

Active footprinting involves directly communicating with the target system or network to

SGOU

obtain technical information. This may include sending requests to servers, performing network scans, querying DNS servers, or scanning for open ports and running services. Because active footprinting directly interacts with the target, it can be detected by firewalls, intrusion detection systems, or security monitoring tools. However, it provides more accurate and up-to-date information than passive footprinting and helps identify active hosts, accessible services, and network configurations. See fig. 3.2.9.

3.2.4.2 Information Gathered During Footprinting

During the footprinting process, ethical hackers collect information from multiple sources to develop a comprehensive understanding of the target environment. One of the most important areas is **domain information**, which includes identifying the organization's primary domain name, associated subdomains, DNS records, and domain registration details. Examining DNS records such as A, MX, TXT, CNAME, and NS records provides information about web servers, mail servers, name servers, and domain configurations. WHOIS databases further reveal details about domain registration, including the registrar, registration dates, and administrative contacts.

Another important aspect is **network information**. Ethical hackers identify the organization's public IP addresses, network ranges, routers, gateways, firewalls, VPN servers, and other publicly accessible systems. This information helps create a map of the organization's network infrastructure and identifies systems that may require further security testing.

Footprinting also involves collecting **system information** to identify the technologies used by the target organization. This includes determining the operating systems running on servers and workstations, identifying web servers, application frameworks, content management systems, database servers, programming languages, and software versions. Knowing the versions of operating systems and applications helps security professionals identify whether any known vulnerabilities may exist.

Another valuable source of information is **employee information**. Publicly available information about employees can reveal organizational structure, department names, management hierarchy, official email address formats, and professional roles. Information gathered from company websites, conference presentations, research publications, and professional networking platforms may assist attackers in preparing targeted social engineering or phishing attacks. Ethical hackers collect such information to evaluate the organization's exposure and recommend appropriate security measures.

3.2.4.3 Sources of Information for Footprinting

A significant amount of footprinting information can be obtained from publicly available sources.

- **Social media platforms** are one of the richest sources of organizational information. Employees frequently share details about their job roles, work locations, company activities, technologies they use, and ongoing projects. Such information can unintentionally reveal valuable insights into an organization's internal environment. In some cases, attackers create fake social media profiles to establish trust with employees and gather confidential information through conversation.

SGOU

- **Job portals** also provide valuable technical information. Organizations often mention the programming languages, software frameworks, cloud platforms, databases, operating systems, and cybersecurity technologies used within the company while advertising job vacancies. These details help ethical hackers understand the organization's technical environment and identify technologies that may require security assessment.

- **Search engines**, particularly Google, play an important role in footprinting. Advanced search operators such as *site:*, *filetype:*, *intitle:*, and *inurl:* enable security professionals to locate publicly available documents, login pages, directories, reports, and configuration files. A specialized technique known as **Google Dorking** uses carefully constructed search queries to discover sensitive information that has been unintentionally exposed online, including backup files, spreadsheets, PDF reports, and publicly accessible administrative interfaces.

- **Social engineering**, which focuses on obtaining information by interacting with or observing people rather than attacking computer systems. Techniques such as eavesdropping on conversations, shoulder surfing while users enter passwords, and carefully crafted conversations may reveal sensitive organizational information. Ethical hackers study these techniques to assess the organization's awareness and preparedness against human-based attacks.

- **Archive.org** the historical versions of websites available through Archive. org, it also serves as valuable sources of information. Archived webpages may contain employee information, technical documentation, server structures, contact details, or documents that have been removed from the current website but remain accessible through historical snapshots. Such information may provide insights into the organization's previous infrastructure and reveal data that should no longer be publicly available.

- **The official website of the organization** itself remains one of the primary sources of footprinting information. Company websites often provide detailed information about products, services, business partners, office locations, contact information, employee directories, annual reports, press releases, and technical documentation. Even the source code and metadata of web pages may reveal information about the technologies, frameworks, or content management systems used by the organization.

- WHOIS Lookup: WHOIS is an Internet service that provides registration information about domain names. A WHOIS lookup reveals details such as the domain owner, domain registrar, registration and expiration dates, administrative and technical contacts, domain status, and the authoritative name servers associated with the domain. This information is useful during the initial stages of reconnaissance because it helps identify the organization responsible for a particular domain and provides insights into its domain infrastructure.

SGOU

3.2.5 Enumeration

Enumeration is the phase of ethical hacking that follows footprinting and scanning. During this phase, the ethical hacker actively communicates with the target system to extract detailed information about its resources, services, users, and network configuration. Unlike footprinting, which primarily gathers publicly available information, enumeration involves direct interaction with the target to obtain specific details that are not easily accessible through passive methods.

The primary objective of enumeration is to identify as much information as possible about the target system so that potential security weaknesses can be assessed. Information gathered during this stage may include usernames, user groups, shared folders, network devices, operating systems, running services, service versions, open ports, domain information, and possible vulnerabilities. This information provides a comprehensive understanding of how the target network operates and helps identify areas that require further security testing.

Enumeration depends heavily on the information collected during footprinting. Without prior knowledge of the organization's domains, IP addresses, network ranges, and publicly accessible systems, the enumeration process would become time-consuming and inefficient. Therefore, footprinting serves as the foundation upon which enumeration is performed.

3.2.5.1 Role of Footprinting in the Enumeration Phase

Footprinting provides the background information necessary for successful enumeration by identifying important details such as domain names, IP address ranges, DNS records, publicly accessible servers, network infrastructure, and technologies used by the target organization. This preliminary information enables ethical hackers to understand the target environment and prepare a structured approach for the next phase of security assessment.

The information collected during reconnaissance helps ethical hackers determine where to focus their efforts, which systems require further investigation, and which network services are most likely to contain security weaknesses. As a result, enumeration becomes more efficient, targeted, and accurate, reducing unnecessary scanning while improving the overall effectiveness of the penetration testing process.

3.2.5.2 Building a Map of the Target Network

One of the first objectives of enumeration is to understand the overall structure of the target network. Information obtained during footprinting, such as domain names, IP addresses, subnet ranges, and DNS records, helps create an initial map of the organization's network. By using techniques such as WHOIS lookups, DNS queries, and IP address analysis, ethical hackers can identify the systems that are connected to the Internet and understand how they are organized.

Knowing the network ranges used by an organization allows the ethical hacker to concentrate enumeration activities on relevant systems instead of scanning unrelated networks. Information about public-facing servers, routers, gateways, and firewalls also helps determine the most appropriate systems for further investigation.

SGOU

3.2.5.3 Identifying Network Services and Applications

Footprinting often reveals the services and applications that are publicly available within the organization's network. These may include web servers, email servers, FTP servers, DNS servers, database servers, and remote access services. During enumeration, these services are examined in greater detail to determine their configuration, software versions, authentication mechanisms, and potential security weaknesses.

For example, if footprinting indicates that the target organization uses an Apache or Nginx web server, the enumeration process focuses on identifying the server version, installed modules, enabled directories, and possible vulnerabilities associated with that software. Similarly, if an FTP server is discovered, the ethical hacker may enumerate user accounts, shared directories, and access permissions to evaluate the security of the service.

3.2.5.4 Gathering Information About User Accounts

User account information plays an important role in security assessments because user credentials are often targeted during cyber attacks. During footprinting, publicly available information such as employee names, email addresses, job titles, and organizational structure may be collected from company websites, professional networking platforms, research publications, and social media.

This information becomes valuable during enumeration, where the ethical hacker attempts to identify valid usernames, user groups, login policies, and authentication mechanisms implemented within the target system. Understanding user account structures enables security professionals to evaluate the effectiveness of password policies and authentication controls while identifying potential weaknesses that could be exploited by attackers.

3.2.5.5 Discovering Open Ports and Running Services

Footprinting provides preliminary information about systems that are accessible over the network. During enumeration, these systems are examined more thoroughly by identifying open ports and the services running on them. Tools such as Nmap are commonly used to determine which ports are open and which network services are active.

For example, if ports 80 (HTTP) and 443 (HTTPS) are found to be open, further enumeration may focus on identifying web applications, server configurations, SSL/TLS settings, and application frameworks. Similarly, if ports associated with file sharing, remote administration, or database services are discovered, those services are examined to determine whether they contain configuration weaknesses or outdated software versions.

Determining the exact version of a service is particularly important because many software products have publicly documented vulnerabilities that can be identified and patched during a security assessment.

3.2.5.6 Identifying Operating Systems and System Architecture

Another important objective of enumeration is identifying the operating systems and

SGOU

hardware architecture used by the target organization. Information collected during footprinting often provides clues regarding whether systems are running Windows, Linux, UNIX, or other operating systems.

Enumeration techniques and operating system fingerprinting tools help confirm these details by analyzing network responses and service characteristics. Knowing the operating system allows ethical hackers to understand the security mechanisms available on the target and identify vulnerabilities specific to that platform. Similarly, identifying whether systems are hosted on cloud platforms or traditional on-premises infrastructure provides additional context for the security assessment.

3.2.5.7 Examining Network Devices

Footprinting also helps identify network infrastructure devices such as routers, switches, firewalls, wireless access points, and gateways. During enumeration, these devices are examined to gather more detailed configuration information, management interfaces, firmware versions, routing protocols, and authentication mechanisms.

For example, identifying the presence of enterprise networking equipment enables ethical hackers to verify whether secure management practices are implemented. Similarly, discovering a directory service such as a domain controller allows further enumeration of domain information, user groups, shared resources, and network policies. This information helps assess whether network devices have been configured securely.

3.2.5.8 Identifying Security Mechanisms

Enumeration also attempts to identify the security controls protecting the target environment. Information collected during footprinting may indicate the presence of firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), web application firewalls (WAF), virtual private networks (VPN), endpoint protection software, or other defensive technologies.

Understanding the organization's security mechanisms enables ethical hackers to evaluate how effectively these controls protect the network. For example, identifying a web application firewall allows the security assessment to verify whether it is correctly configured to detect and prevent common web-based attacks. Similarly, recognizing the presence of intrusion detection systems helps evaluate their ability to identify suspicious activities. This information assists organizations in strengthening existing security controls and addressing configuration weaknesses.

3.2.5.9 Importance of Enumeration

Enumeration is one of the most valuable phases of ethical hacking because it provides detailed technical information that cannot usually be obtained through passive reconnaissance alone. The information gathered enables security professionals to understand the structure of the target environment, verify the configuration of systems and services, identify publicly accessible resources, and detect security weaknesses before they can be exploited by malicious attackers. Accurate enumeration also reduces unnecessary testing by allowing security assessments to focus on systems and services that present the highest security risk.

SGOU

Enumeration is an active information-gathering process performed after footprinting and scanning. It involves communicating directly with the target system to obtain detailed information about users, operating systems, network services, shared resources, security mechanisms, and infrastructure. The success of enumeration largely depends on the quality of information collected during the footprinting phase, which provides the foundation for identifying systems that require detailed examination. Together, footprinting and enumeration enable ethical hackers to perform systematic security assessments and help organizations identify vulnerabilities, improve their security posture, and protect critical information assets.

Recap

- Network attacks are broadly classified into passive attacks and active attacks based on their impact on data and network resources.
- Passive attacks focus on monitoring communications and collecting sensitive information without modifying data or interrupting network operations.
- Traffic analysis examines communication patterns, timing, and data volume to infer user behavior, operational activities, and communication frequency.
- Eavesdropping involves secretly intercepting the actual contents of communications to obtain confidential information such as passwords, financial data, and business records.
- Strong encryption, VPNs, secure communication protocols, and multi-factor authentication help defend against passive attacks.
- Active attacks directly alter, disrupt, or destroy data and network resources, making them more damaging and easier to detect than passive attacks.
- Repudiation attacks allow attackers to deny sending messages, performing transactions, or modifying data by exploiting weak authentication and auditing mechanisms.
- Message modification attacks compromise data integrity by altering, delaying, reordering, or inserting messages during transmission.
- Replay attacks reuse previously captured legitimate communications to impersonate authorized users and gain unauthorized access.
- Masquerade attacks involve attackers impersonating legitimate users using stolen credentials obtained through phishing, social engineering, or other credential theft techniques.
- Denial of Service (DoS) attacks overwhelm a target system with excessive requests from a single source, making services unavailable to legitimate users.

SGOU

- Distributed Denial of Service (DDoS) attacks use multiple compromised devices (botnets) to generate massive traffic, making detection and mitigation more challenging.
- Man-in-the-Middle (MitM) attacks secretly intercept and manipulate communications between two parties to steal or modify sensitive information.
- Nmap is a widely used network scanning tool that identifies active hosts, open ports, running services, operating systems, and software versions using various port scanning techniques.
- Footprinting and enumeration are essential reconnaissance phases that systematically collect detailed information about domains, networks, users, services, operating systems, and security mechanisms to support effective security assessments.

Objective Type Questions

1. What type of attack secretly monitors network communication without modifying data?
2. Which passive attack studies communication patterns instead of message contents?
3. Which passive attack captures the actual contents of network communication?
4. Which type of attack modifies or disrupts transmitted data?
5. Which attack allows an attacker to deny performing a malicious action?
6. Which type of repudiation attack involves denying an online payment or transaction?
7. Which attack changes the content of transmitted messages during communication?
8. Which attack resends previously captured valid messages to gain unauthorized access?
9. Which attack involves pretending to be a legitimate user by using stolen credentials?
10. Which type of masquerade attack creates a fake website to steal user credentials?
11. Which cyber attack overwhelms a server using requests from a single attacking system?

SGOU

12. Which attack uses multiple compromised devices to flood a target with traffic?

13. Which attack secretly intercepts communication between two parties?

14. Which open-source tool is commonly used for network discovery and port scanning?

15. Which phase of ethical hacking actively gathers detailed information from a target system after footprinting?

Answers to Objective Type Questions

1. Passive
2. Traffic Analysis
3. Eavesdropping
4. Active
5. Repudiation
6. Transaction
7. Modification
8. Replay
9. Masquerade
10. Website
11. DoS
12. DDoS
13. MitM
14. Nmap
15. Enumeration

SGOU

Assignments

1. Explain passive and active attacks. Compare their characteristics, objectives, effects on data and network resources, and methods of detection with suitable examples.

2. What is traffic analysis? Explain how attackers can obtain useful information by observing communication patterns, timing, and traffic volume. Discuss suitable measures for protecting against traffic analysis.

3. Explain eavesdropping as a passive attack. Differentiate between eavesdropping and traffic analysis, and describe their common methods, consequences, and preventive measures.

4. What are repudiation attacks? Explain message repudiation, transaction repudiation, and data repudiation with suitable examples. Discuss the mechanisms used to prevent repudiation attacks.

5. Explain message modification, replay, and masquerade attacks. Describe how each attack works, provide suitable examples, and discuss appropriate countermeasures.

6. Explain Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. Compare their characteristics, methods, impact, and protection mechanisms.

7. What is footprinting, and how is it related to reconnaissance and enumeration? Explain passive and active footprinting and discuss the different sources of information used during footprinting.

8. Explain the major Nmap port scanning techniques, including TCP Connect, TCP SYN, UDP, NULL, FIN, and XMAS scans. Discuss their working principles, advantages, limitations, and applications in network security assessment.

SGOU

Suggested Reading

1. Godbole, Nina, and Sunit Belapure. *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*. Wiley India Pvt. Ltd., 2011.

2. Brooks, Charles J., et al. *Cybersecurity Essentials*. Wiley, 2018

3. Wu, Chwan-Hwa (John), and J. David Irwin. *Introduction to Cyber Security*. CRC Press, 2016.

Reference

1. Jain, Atul. *Cyber Crime: Issues, Threats and Management*. Isha Books, 2004.

2. Yar, Majid. *Cybercrime and Society*. Sage Publications, 2006.

3. Chaubey, R. K. *Cyber Crimes and Law*. Kamal Law House, 2012.

SGOU



Methods of Gaining and Sustaining Unauthorized Access

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- explain how attackers exploit vulnerabilities in computer systems
- identify common vulnerability exploitation techniques such as password cracking, SQL injection, Brute Force attacks, dictionary attacks, and privilege escalation
- use basic security measures to protect systems from vulnerability exploitation
- apply suitable methods to protect computer systems and networks

Prerequisites

Before learning about exploiting vulnerabilities, students should have a basic understanding of computer networks, user authentication, and common cybersecurity concepts such as vulnerabilities, threats, and attacks. They should also know how users log into systems, how data is transmitted over networks, and why software updates and security controls are important. For example, when a person uses an online banking website, entering a weak password or using an outdated browser may allow an attacker to exploit security weaknesses, steal login credentials, or gain unauthorized access to the account. Understanding these basic concepts helps learners appreciate how vulnerabilities are exploited and why secure system design, regular patching, and strong authentication are essential for protecting digital systems.

Key concepts

Credential Theft, Post-Exploitation, Malicious Code, Password Hash, Security Patches

SGOU

Discussion

Exploiting vulnerabilities is the stage of a cyber attack where attackers take advantage of security weaknesses in software, operating systems, networks, or applications to gain unauthorized access or perform malicious actions. After identifying vulnerabilities through reconnaissance and scanning, attackers attempt to exploit these weaknesses to compromise the target system. Successful exploitation allows attackers to execute malicious code, steal sensitive information, install malware, or gain higher privileges.

A vulnerability may arise from software bugs, outdated applications, weak passwords, improper system configurations, insecure network services, or coding errors. If these weaknesses remain unpatched, attackers can exploit them to bypass security controls and gain control over the system.

3.3.1 How Vulnerability Exploitation Works?

Vulnerability exploitation occurs when an attacker takes advantage of a weakness in software, hardware, an application, or a system configuration to perform an action that the system was not intended to permit. The exploitation process is not necessarily a fixed sequence, but it commonly involves identifying a vulnerability, determining whether it can be exploited, attempting exploitation, and assessing the level of access or control obtained. During authorized penetration testing, security professionals may deliberately exploit a confirmed vulnerability to verify its existence and determine its potential impact. NIST distinguishes vulnerability scanning, which identifies possible vulnerabilities, from the attack phase of penetration testing, in which exploitation can be used to confirm whether a vulnerability is actually exploitable.

3.3.1.1 Vulnerability Identification

The first step is to identify a potential weakness in the target environment. Information may be obtained through security assessments, vulnerability scanning, software-version analysis, configuration reviews, or publicly available vulnerability information. Common weaknesses include outdated software, insecure configurations, programming errors, and authentication or access-control failures. For example, a vulnerability assessment may identify an outdated server application associated with a known security vulnerability. The discovery of a vulnerability does not automatically mean that the system can be successfully compromised; further assessment is required to determine its actual exploitability.

3.3.1.2 Assessing and Selecting an Exploitation Technique

After identifying a vulnerability, an attacker or authorized security tester determines whether an appropriate exploitation technique exists and whether it is applicable to the target. The technique depends on the vulnerability, affected software, system configuration, privileges, and intended objective. MITRE ATT&CK, for example, documents different exploitation techniques for purposes such as exploiting public-facing applications, client applications, credential access, and privilege escalation. Therefore, exploitation is not limited to obtaining initial access; vulnerabilities can also be exploited after an attacker has already entered an environment.

SGOU

For example, a vulnerability in an Internet-facing application may be exploited to obtain initial access to an organization's network, whereas a vulnerability in a locally installed application may be exploited to execute code or obtain higher privileges after initial access has already been achieved.

3.3.1.3 Exploiting the Vulnerability

In this stage, the attacker attempts to trigger the identified weakness. If exploitation is successful, the vulnerable component may perform an unintended action, such as executing unauthorized code, bypassing an access-control restriction, disclosing information, or allowing unauthorized interaction with a resource. NIST notes that penetration testers may exploit vulnerabilities during the attack phase to confirm their existence and determine the level of access that could be obtained.

For example, a vulnerable application that fails to enforce access controls may allow a user to access information belonging to another user. OWASP identifies broken access control as a major application-security risk and notes that such weaknesses can result in unauthorized information disclosure, modification, deletion, or privilege escalation.

3.3.1.4 Obtaining or Expanding Access

The result of successful exploitation depends on the vulnerability and the privileges of the affected component. An attacker may obtain limited access to an application or system, execute code with the privileges of a vulnerable process, or potentially obtain higher privileges. MITRE ATT&CK describes exploitation for privilege escalation as taking advantage of vulnerabilities in programs, services, operating systems, or kernels to obtain greater permissions, such as moving from a user-level account to administrator or root privileges.

For example, exploitation of a vulnerable service running with elevated privileges may provide an attacker with more control than exploitation of an application operating with ordinary user permissions.

3.3.1.5 Post-Exploitation Activities

Successful exploitation may be followed by additional activities depending on the attacker's objectives. These may include privilege escalation, credential access, discovery of other systems, lateral movement, data collection, or data exfiltration. MITRE ATT&CK treats these activities as separate techniques and tactics rather than assuming that every exploitation attempt automatically results in all of them.

For example, after compromising a vulnerable server, an attacker may attempt to obtain higher privileges and then use the compromised system to access other systems within the network. In an authorized penetration test, such activities should be performed only within the agreed scope and rules of engagement.

3.3.2 Common Vulnerabilities Exploited by Attackers

Attackers may exploit weaknesses arising from outdated software, insecure configurations, vulnerable components, injection flaws, broken access controls, authentication failures, and other software or system weaknesses. OWASP's current Top

SGOU

10:2025 identifies Broken Access Control, Security Misconfiguration, Software Supply Chain Failures, Cryptographic Failures, Injection, Insecure Design, Authentication Failures, Software or Data Integrity, Logging and Altering Failures and Mishandling of Exceptional Conditions among other categories, as major web-application security risks.

For example, a misconfigured application may expose sensitive resources to unauthorized users, while an injection vulnerability may allow specially crafted input to be interpreted in an unintended manner. Similarly, outdated software may contain publicly documented vulnerabilities that attackers can exploit. CISA maintains a Known Exploited Vulnerabilities (KEV) Catalog containing vulnerabilities for which there is evidence of exploitation in the wild, highlighting the importance of prioritizing remediation of actively exploited vulnerabilities.

Common vulnerability categories include:

- Vulnerable or outdated software and components
- Security misconfigurations
- Broken access controls
- Authentication failures
- Injection vulnerabilities
- Insecure software or system design
- Vulnerable services exposed to the Internet
- Improperly configured cloud or network resources
- Insecure file and resource permissions
- Software vulnerabilities that permit unauthorized code execution

These categories should not be treated as an exhaustive list because vulnerabilities vary according to the technology, application, operating system, and deployment environment.

3.3.2.1 Impact of Vulnerability Exploitation

The impact of successful exploitation depends on the nature of the vulnerability and the privileges available to the compromised component. Possible consequences include unauthorized access, disclosure or modification of sensitive information, execution of unauthorized code, privilege escalation, installation of malicious software, disruption of services, and compromise of additional systems. Broken access-control vulnerabilities, for example, can allow unauthorized users to view, modify, or delete information or perform functions beyond their intended permissions.

A vulnerability in a public-facing service may also provide an attacker with an entry point into an organization's network. MITRE ATT&CK documents exploitation of remote services as a technique that can be used for lateral movement, demonstrating that exploitation can occur after initial access as attackers attempt to move between systems.

SGOU

The business impact may include operational disruption, data loss, financial losses, legal or regulatory consequences, and reputational damage. The actual impact, however, should be assessed based on the affected asset, the vulnerability's severity, the privileges obtained, the sensitivity of the data involved, and the organization's security controls.

3.3.2.2 Preventing Vulnerability Exploitation

Preventing vulnerability exploitation requires a combination of vulnerability management, secure configuration, access control, secure software development, monitoring, and timely remediation. Organizations should regularly identify vulnerabilities, assess their risk, prioritize important weaknesses, and apply appropriate security updates or other mitigations. NIST recommends technical security testing and assessment activities to help organizations identify vulnerabilities and develop mitigation strategies.

Organizations should prioritize vulnerabilities that present significant risk, particularly vulnerabilities known to be actively exploited. CISA's KEV Catalog provides a useful source for identifying vulnerabilities for which there is evidence of exploitation in the wild.

Strong authentication, including Multi-Factor Authentication (MFA), should be used for sensitive accounts and services. Unnecessary services and exposed resources should be disabled or restricted, while access controls should follow the principle of least privilege. OWASP recommends denying access by default where appropriate, implementing access controls in trusted server-side components, logging access-control failures, and limiting unnecessary exposure of application resources.

Secure coding practices, code review, vulnerability testing, configuration management, firewalls, intrusion detection and prevention mechanisms, security logging, and continuous monitoring can further reduce the likelihood and impact of exploitation. Organizations should also maintain appropriate incident-response procedures so that confirmed exploitation can be detected, contained, investigated, and remediated promptly.

Vulnerability exploitation is therefore the deliberate use of a security weakness to cause a system or application to perform an unauthorized action. Exploitation may be used to obtain initial access, execute code, obtain credentials, escalate privileges, or move between systems, depending on the vulnerability and the attacker's objective. Effective vulnerability management, timely security updates, secure configurations, strong access controls, secure software development, and continuous monitoring are essential for reducing the risk posed by exploitable vulnerabilities.

3.3.3 Password Cracking as Example for Exploiting Vulnerabilities

Password cracking is the process of recovering or guessing a user's password to gain unauthorized access to a computer system, network, or online account. Attackers use various techniques and automated tools to identify passwords, especially when users choose weak or predictable passwords. Password cracking is one of the most common methods used by cybercriminals to steal sensitive information, compromise systems, and perform unauthorized activities.

SGOU

3.3.3.1 Types of Password Cracking Attacks

Password cracking attacks can be classified into the following categories:

1. Online Attacks

In an online attack, the attacker repeatedly attempts to log in to a system by guessing passwords through the authentication interface. These attacks may use common passwords, automated tools, or password lists. Security measures such as account lockout, CAPTCHA, and multi-factor authentication help reduce the success of online attacks.

2. Offline Attacks

Offline attacks occur after an attacker obtains encrypted password hashes from a compromised system. The attacker attempts to recover the original passwords without interacting with the login system, making these attacks faster and more difficult to detect.

3. Social Engineering Attacks

Instead of guessing passwords, attackers manipulate users into revealing their credentials through phishing emails, fake websites, phone calls, or other deceptive techniques.

3.3.3.3 Common Password Cracking Tools

Several tools are commonly used during security testing and are also misused by attackers:

- **John the Ripper** – Password recovery tool that supports multiple hash formats.
- **Hashcat** – High-speed password-cracking tool supporting brute force, dictionary, and hybrid attacks.
- **Hydra** – Network login cracker used against services such as SSH, FTP, HTTP, and RDP.
- **Cain & Abel** – Windows-based password recovery and network analysis tool.
- **Aircrack-ng** – Tool for recovering Wi-Fi passwords from captured wireless traffic.

3.3.3.4 Prevention of Password Cracking

Organizations and users can reduce the risk of password cracking by following these best practices:

- Create strong and unique passwords with at least 12 characters.
- Use a combination of uppercase letters, lowercase letters, numbers, and special characters.
- Avoid common words, personal information, and predictable patterns.
- Enable Multi-Factor Authentication (MFA).

SGOU

- Use a different password for every account.
- Change passwords periodically or immediately after a suspected compromise.
- Store passwords securely using strong hashing algorithms and salting.

3.3.3.5 Is Password Cracking Legal?

Password cracking is legal when performed with proper authorization, such as during penetration testing, security audits, or password recovery for legitimate users. However, attempting to crack passwords without permission to gain unauthorized access to systems or data is illegal and punishable under cybercrime laws in many countries.

Strong passwords, multi-factor authentication, secure password storage, and user awareness are the most effective defenses against password cracking attacks.

3.3.4 SQL Injection (SQLi)

SQL Injection (SQLi) is a web application attack in which an attacker inserts malicious SQL statements into user input fields to manipulate database queries. If an application does not properly validate user input, attackers can access, modify, or delete sensitive information stored in the database. SQL injection is one of the most common and dangerous vulnerabilities affecting web applications.

Key Features

- Exploits improperly validated user input.
- Allows unauthorized access to database information.
- Can bypass authentication mechanisms.
- May modify or delete database records.
- Can lead to complete compromise of the database.

3.3.4.1 Levels of Application Vulnerability to SQL Injection

1. Low Security

At the low security level, user input is directly included in SQL queries without validation or filtering. As a result, the application is highly vulnerable to SQL injection attacks.

2. Medium Security

The application performs basic input filtering by escaping special characters. Although this prevents simple attacks, attackers may still bypass the protection using alternative SQL injection techniques.

3. High Security

The application uses prepared statements (parameterized queries), where user input is treated only as data and not as executable SQL code. This effectively prevents SQL injection attacks.

SGOU

3.3.4.2 Types of SQL Injection

1. Error-Based SQL Injection

Error-based SQL injection exploits database error messages to obtain information about the database structure. By deliberately entering invalid SQL input, attackers can force the database to display error messages containing useful information such as database type, table names, and column names.

Example:

Entering a single quotation mark (') into a vulnerable input field may generate a database syntax error, indicating that the application is susceptible to SQL injection.

2. Union-Based SQL Injection

Union-based SQL injection uses the UNION operator to combine the results of the original query with another query created by the attacker. This technique allows attackers to retrieve data from other database tables.

Before performing a UNION attack, the attacker determines the number of columns in the original query using statements such as:

ORDER BY 1

ORDER BY 2

ORDER BY 3

Once the correct number of columns is identified, the attacker can use the UNION SELECT statement to extract sensitive information.

3. Blind SQL Injection

Blind SQL injection occurs when the application does not display database errors or query results. Instead, attackers infer information by observing differences in the application's behavior.

There are two common types:

Boolean-Based Blind SQL Injection:

The attacker sends SQL conditions that evaluate to TRUE or FALSE and observes differences in the webpage response.

Time-Based Blind SQL Injection:

The attacker injects SQL commands that delay the database response (such as `SLEEP()`). The response time indicates whether the injected condition is true or false.

3.3.4.3 Impact of SQL Injection

A successful SQL injection attack can have serious consequences, including:

- Unauthorized access to confidential information.
- Modification or deletion of database records.

SGOU

- Bypassing user authentication.
- Compromising the entire database server.
- Financial losses and reputational damage.

3.3.4.4 Prevention of SQL Injection

The following security practices help protect applications against SQL injection attacks:

- Use prepared statements or parameterized queries.
- Validate and sanitize all user inputs.
- Use stored procedures where appropriate.
- Apply the principle of least privilege to database accounts.

  [Restrict database users and applications to only the exact permission needed for their specific tasks]
- Avoid displaying detailed database error messages to users.
- Regularly update and patch web applications and database servers.

SQL Injection (SQLi) is a critical web application vulnerability that allows attackers to manipulate SQL queries by injecting malicious input. Common types include Error-Based, Union-Based, and Blind SQL Injection. Secure coding practices such as prepared statements, input validation, and proper database access controls are the most effective methods for preventing SQL injection attacks.

3.3.5 Brute Force Attack

A Brute Force Attack is a password-cracking technique in which an attacker systematically tries every possible password combination until the correct one is found. Unlike attacks that exploit software vulnerabilities, brute force attacks rely entirely on repeated trial-and-error attempts. Although this method can be time-consuming, weak or short passwords can often be cracked quickly using powerful computers and automated tools. See fig. 3.3.1.

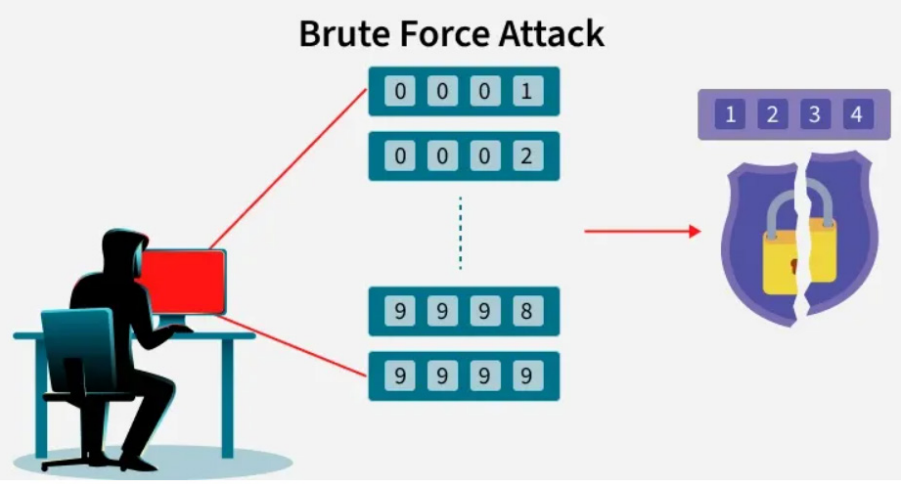


Fig. 3.3.1 Brute Force Attack

3.3.5.1 Types of Brute Force Attacks

Brute force attacks are mainly classified into simple brute force, dictionary attacks, and hybrid attacks. Each type uses different techniques to guess passwords or credentials by systematically trying possible combinations.

1. Simple Brute Force Attack

In a simple brute force attack, the attacker tries every possible combination of letters, numbers, and special characters until the correct password is discovered. No prior knowledge of the password is required.

2. Dictionary Attack

A dictionary attack uses a predefined list of common words, passwords, names, and leaked credentials instead of testing every possible combination. It is faster than a simple brute force attack but is limited to the passwords available in the wordlist.

3. Hybrid Brute Force Attack

A hybrid brute force attack combines dictionary words with additional characters such as numbers or symbols. For example, if the dictionary word is password, the attacker may try variations such as Password123, password@2025, or P@ssword1.

4. Reverse Brute Force Attack

In a reverse brute force attack, the attacker starts with a commonly used password and tests it against multiple usernames or user accounts. This technique is effective when many users choose the same weak password.

3.3.5.2 Working of Brute Force Attack

A brute force attack generally follows these steps:

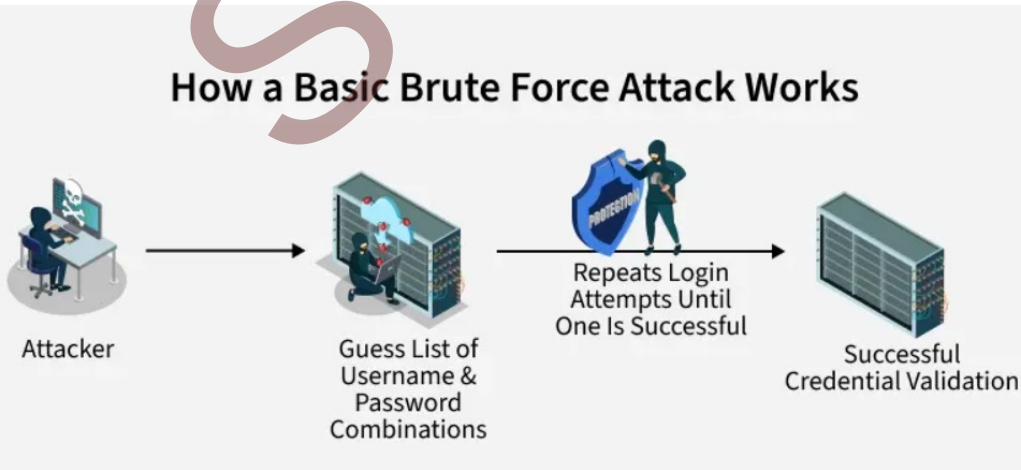


Fig. 3.3.3 Working of Brute Force Attack

1. Target Selection

The attacker selects a target such as a user account, login portal, network service, or encrypted file.

SGOU

2. Information Gathering

The attacker collects information such as usernames, common password patterns, or publicly available personal details that may help narrow the search.

3. Selecting the Attack Method

The attacker chooses the appropriate brute force technique, such as a simple brute force attack, dictionary attack, or hybrid attack, depending on the target. See fig. 3.3.3.

4. Using Automated Tools

Password-cracking tools such as John the Ripper, Hashcat, Hydra, Medusa, and Aircrack-ng automatically generate and test password combinations.

5. Password Testing

The tool systematically tries one password after another until the correct password is found or all possible combinations have been exhausted.

6. Gaining Access

If the correct password is discovered, the attacker gains unauthorized access to the account, system, or encrypted data.

3.3.5.3 Prevention of Brute Force Attacks

Organizations and users can reduce the risk of brute force attacks by implementing the following security measures:

- Use strong, long, and complex passwords.
- Avoid common words, names, dates, and predictable patterns.
- Use a unique password for every account.
- Enable Multi-Factor Authentication (MFA).
- Implement account lockout policies after multiple failed login attempts.
- Limit the number of login attempts and use CAPTCHA where appropriate.
- Change passwords periodically and immediately after a suspected compromise.
- Monitor login activities and detect repeated failed authentication attempts.

Brute force attacks can eventually succeed against weak passwords, they can be effectively prevented by using strong passwords, enabling Multi-Factor Authentication (MFA), enforcing account lockout policies, and continuously monitoring authentication activities.

3.3.6 Dictionary Attack

A Dictionary Attack is a password-cracking technique in which an attacker attempts

SGOU

to guess a password by systematically trying words from a predefined list, known as a dictionary or wordlist. Instead of testing every possible password combination, the attacker uses commonly used passwords, dictionary words, names, dates, and passwords obtained from previous data breaches. Since many users choose simple and predictable passwords, dictionary attacks are often faster and more efficient than Brute Force attacks.

3.3.6.1 Working of Dictionary Attack

A dictionary attack typically follows these steps:

1. Preparing the Wordlist

The attacker first creates or downloads a wordlist containing thousands or millions of commonly used passwords, dictionary words, names, keyboard patterns, and leaked passwords from previous security breaches.

2. Selecting the Target

The attacker selects the target system, which may be a login page, password hash database, Wi-Fi network, or any system that requires password authentication.

3. Testing Passwords

Each password in the wordlist is automatically tested one by one against the target account or password hash. This process continues until a matching password is found or the entire list has been exhausted.

4. Password Recovery

If one of the passwords matches the target password, the attacker successfully gains unauthorized access to the system or user account.

5. Attack Failure

If none of the passwords in the dictionary matches the target password, the attack fails. Unlike Brute Force attacks, a dictionary attack is limited to the passwords available in the wordlist.

3.3.6.2 Common Tools Used for Dictionary Attacks

1. John the Ripper

John the Ripper is a popular password-cracking tool used to recover passwords from encrypted password hashes. It compares passwords from a wordlist with stored password hashes until a match is found.

2. Aircrack-ng

Aircrack-ng is a wireless network security tool used to recover Wi-Fi passwords. It performs dictionary attacks by testing passwords from a wordlist against captured Wi-Fi authentication handshakes.

SGOU

3. Hydra

Hydra is a fast password-cracking tool used during penetration testing. It performs dictionary attacks against network services such as SSH, FTP, HTTP, Telnet, and RDP by trying multiple username and password combinations.

3.3.6.3 Dictionary Attack vs. Brute Force Attack

Dictionary Attack	Brute Force Attack
Uses a predefined list of common passwords.	Tries every possible password combination.
Faster because only likely passwords are tested.	Slower because all combinations are attempted.
Success depends on the quality of the wordlist.	Eventually succeeds if enough time and resources are available.
Less computationally expensive.	Requires significant processing time and computing power.
Effective against weak and commonly used passwords.	Can crack even complex passwords, given sufficient time.

3.3.6.4 Advantages

- Faster than Brute Force attacks.
- Requires less computational power.
- Highly effective against weak or commonly used passwords.
- Easy to automate using password-cracking tools.

3.3.6.5 Limitations

- Cannot crack passwords that are not present in the wordlist.
- Ineffective against long, complex, and randomly generated passwords.
- May fail if account lockout policies or multi-factor authentication (MFA) are enabled.

3.3.7 Privilege Escalation

Privilege escalation is a cyber attack technique in which an attacker gains higher permissions or access rights than those originally assigned to a user or application. After obtaining initial access to a system, the attacker exploits vulnerabilities, weak configurations, or stolen credentials to acquire administrative or root-level privileges. With elevated privileges, the attacker can control critical system resources, access sensitive data, install malicious software, and perform unauthorized actions.

SGOU

Privilege escalation is a crucial stage in the cyber attack lifecycle because it enables attackers to expand their control, maintain persistence, and launch further attacks within the network.

3.3.7.1 Aim of Privilege Escalation

When attackers first compromise a system, they usually obtain access as a standard or restricted user with limited permissions. Their objective is to increase these privileges and gain complete control over the system.

- In Windows, the goal is to obtain NT AUTHORITY\SYSTEM privileges, which provide the highest level of access.
- In Linux, the objective is to gain root privileges, giving unrestricted control over files, processes, and system configurations.

With elevated privileges, attackers can:

- Access confidential files and sensitive information.
- Extract passwords and password hashes.
- Disable antivirus and security software.
- Install malware or backdoors for persistent access.
- Create or modify user accounts.
- Move laterally to other systems within the network.

3.3.7.2 Types of Privilege Escalation

1. Horizontal Privilege Escalation

Horizontal privilege escalation occurs when an attacker gains access to another user's account while remaining at the same privilege level. Instead of becoming an administrator, the attacker accesses resources belonging to other users with similar permissions.

Example:

In a web application, if a user changes a URL parameter such as:

https://bank.com/account?user_id=1234

to

https://bank.com/account?user_id=1235

and is able to view another customer's account information without proper authorization, horizontal privilege escalation has occurred.

Consider a banking web application in which two customers, User A with user_id=1234 and User B with user_id=1235, have the same level of privileges. After User A logs in,

SGOU

the application displays User A's account using a URL containing the user_id parameter. If the application allows User A to change the user_id value to 1235 and view User B's account information without verifying whether User A is authorized to access that account, the application has a broken access control vulnerability. Because User A has accessed another user's resources while having the same level of privileges, this is an example of horizontal privilege escalation. This type of weakness is commonly associated with Insecure Direct Object Reference (IDOR), where a user-controlled identifier can be manipulated to access another user's resources without proper authorization.

2. Vertical Privilege Escalation

Vertical privilege escalation occurs when an attacker elevates access from a standard user account to an administrator or root account. This provides complete control over the operating system and its resources.

Example:

A Linux user exploits a vulnerability or misconfigured **sudo** permissions to obtain a root shell, allowing unrestricted access to the system.

3.3.7.3 Common Methods of Privilege Escalation

1. Social Engineering

Attackers trick users into revealing passwords or performing actions that provide elevated access. Phishing emails, fake login pages, and impersonation are common social engineering techniques.

2. Pass-the-Hash and Rainbow Table Attacks

Instead of discovering the actual password, attackers use stolen password hashes or precomputed hash tables to authenticate as legitimate users and gain higher privileges.

3. Exploiting Software Vulnerabilities

Attackers exploit software bugs, buffer overflows, or unpatched security vulnerabilities to execute malicious code with elevated privileges.

4. Misconfigured Systems

Weak passwords, excessive user permissions, improperly configured services, and insecure file permissions provide opportunities for attackers to gain administrative access.

See fig. 3.3.4.

5. Kernel Exploits

The operating system kernel runs with the highest privileges. Attackers exploit kernel vulnerabilities to obtain complete control over the system, bypassing normal security mechanisms.

SGOU



Fig. 3.3.4 Methods of Privilege Escalation

3.3.7.4 Common Tools Used for Privilege Escalation

Several tools assist security professionals during penetration testing and are also misused by attackers.

- **Metasploit** – Framework for exploiting vulnerabilities and privilege escalation.
- **Mimikatz** – Extracts passwords, hashes, and authentication tokens from Windows memory.
- **PowerUp** – Identifies Windows privilege escalation opportunities.
- **WinPEAS** – Automatically scans Windows systems for privilege escalation vulnerabilities.
- **BloodHound** – Analyzes Active Directory relationships to identify privilege escalation paths.
- **LinPEAS** – Detects common privilege escalation weaknesses in Linux systems.
- **Linux Exploit Suggester** – Recommends kernel exploits based on the Linux version.
- **GTFOBins** – Lists Linux commands that can be abused to bypass restrictions and gain elevated privileges.
- **Cobalt Strike** – A commercial security testing platform that includes post-exploitation and privilege escalation capabilities.

3.3.7.5 Prevention of Privilege Escalation

Organizations can reduce the risk of privilege escalation by implementing the following

SGOU

security measures:

- Apply security patches and software updates regularly.
- Enforce the principle of least privilege.
- Use strong authentication and Multi-Factor Authentication (MFA).
- Restrict administrator and root access.
- Monitor privileged account activities.
- Remove unnecessary services and permissions.
- Conduct regular vulnerability assessments and security audits.

Attackers use vulnerabilities, misconfigurations, stolen credentials, and kernel exploits to elevate their privileges from a normal user account to an administrator or root account. Once elevated privileges are obtained, attackers can disable security controls, steal sensitive data, install malware, and move laterally across the network. Implementing least-privilege access, timely patch management, strong authentication, and continuous security monitoring are essential defenses against privilege escalation attacks.

Recap

- Vulnerability exploitation involves taking advantage of weaknesses in software, hardware, applications, or system configurations to perform unauthorized actions.
- Vulnerabilities may result from outdated software, insecure configurations, coding errors, weak authentication, and improper access controls.
- Vulnerability identification can involve vulnerability scanning, configuration reviews, software-version analysis, and publicly available vulnerability information.
- Identifying a vulnerability does not necessarily mean that it can be successfully exploited; its actual exploitability and potential impact must be assessed.
- Exploitation techniques are selected according to the vulnerability, target environment, available privileges, and attacker's objective.
- Successful exploitation may allow unauthorized code execution, information disclosure, access-control bypass, or unauthorized interaction with system resources.

SGOU

- The level of access obtained through exploitation depends on the vulnerability and the privileges of the affected component.
- Post-exploitation activities may include privilege escalation, credential access, system discovery, lateral movement, data collection, and data exfiltration.
- Common vulnerabilities include broken access controls, security misconfigurations, injection flaws, authentication failures, vulnerable software, and improperly exposed services.
- Successful exploitation can affect the confidentiality, integrity, and availability of information systems and may result in data loss, service disruption, financial loss, or reputational damage.
- Effective vulnerability management includes identifying, assessing, prioritizing, and remediating vulnerabilities, with particular attention to vulnerabilities known to be actively exploited.
- Password cracking involves attempting to recover or guess passwords and may use techniques such as brute force, dictionary attacks, or other password-recovery methods.
- SQL Injection occurs when improperly handled input allows unintended SQL statements to affect database operations, potentially exposing or modifying sensitive data.
- Brute force and dictionary attacks can be reduced through strong unique passwords, Multi-Factor Authentication (MFA), rate limiting, account protections, and secure password storage.
- Privilege escalation occurs when an attacker obtains permissions beyond those originally assigned, including horizontal escalation between users with similar privileges and vertical escalation to higher privileges such as administrator or root.

SGOU

Objective Type Questions

1. Which process involves taking advantage of a weakness in a system to perform an unauthorized action?
2. Which activity is used to find weaknesses in a target system?
3. What is a method used to take advantage of a specific vulnerability called?
4. Which stage attempts to trigger a discovered vulnerability?

5. What is the term for gaining higher permissions after compromising a system?

6. Which type of attack uses a list of commonly used passwords to guess a password?

7. Which attack tries all possible combinations of characters to find a password?

8. Which web attack involves inserting malicious input into a database query?

9. Which vulnerability allows a user to access another user's resources without proper authorization?

10. Which attack involves capturing and reusing a valid authentication message?

11. Which security principle gives users only the permissions they need to perform their tasks?

12. Which authentication method requires more than one form of verification?

13. Which organization maintains the Known Exploited Vulnerabilities (KEV) Catalog?

14. Which type of privilege escalation involves gaining access to another user's resources at the same privilege level?

15. Which type of privilege escalation involves moving from a normal user account to an administrator or root account?

Answers to Objective Type Questions

1. Exploitation
2. Scanning
3. Exploit
4. Exploitation
5. Escalation
6. Dictionary
7. Brute Force
8. SQLi

SGOU

9. IDOR [Insecure Direct Object Reference]
10. Replay
11. Least-privilege
12. MFA [Multi - Factor Authentication]
13. CISA
14. Horizontal
15. Vertical

Assignments

1. Explain the stages involved in vulnerability exploitation and discuss how attackers progress from identifying vulnerabilities to performing post-exploitation activities.
2. Describe the various password cracking techniques and compare brute force, dictionary, rainbow table, and phishing attacks with suitable examples.
3. Explain SQL Injection (SQLi) attacks in detail. Discuss the different types of SQL injection attacks and the security measures used to prevent them.
4. Discuss the different types of brute force attacks. Explain the working process of a brute force attack and suggest effective methods to defend against it.
5. Describe the working mechanism of a dictionary attack. Compare dictionary attacks with brute force attacks, highlighting their advantages, limitations, and prevention techniques.
6. Explain the concept of privilege escalation in cybersecurity. Differentiate between horizontal and vertical privilege escalation with appropriate examples and prevention strategies.
7. Discuss the common vulnerabilities exploited by attackers and analyze the impact of successful vulnerability exploitation on organizational security.
8. Explain the various tools used for password cracking and privilege escalation. Discuss their legitimate use in ethical hacking as well as the ethical and legal considerations associated with their use.

SGOU

Suggested Reading

1. Godbole, Nina, and Sunit Belapure. *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*. Wiley India Pvt. Ltd., 2011.

2. Brooks, Charles J., et al. *Cybersecurity Essentials*. Wiley, 2018

3. Wu, Chwan-Hwa (John), and J. David Irwin. *Introduction to Cyber Security*. CRC Press, 2016.

Reference

1. Jain, Atul. *Cyber Crime: Issues, Threats and Management*. Isha Books, 2004.

2. Yar, Majid. *Cybercrime and Society*. Sage Publications, 2006.

3. Chaubey, R. K. *Cyber Crimes and Law*. Kamal Law House, 2012.

SGOU



Lateral Movement and Detection Avoidance

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- explain the concepts of lateral movement, credential dumping, and anti-forensics in cyber attacks
- identify common techniques used for lateral movement, credential dumping, and anti-forensics
- apply appropriate security measures to detect and prevent lateral movement and credential theft
- recognize suitable security practices to support digital forensic investigations

Prerequisites

Learners should have a basic understanding of how users access shared network resources, how authentication is performed using usernames, passwords, and other credentials, and why system logs are important for monitoring activities and detecting security incidents. They should also be familiar with the phases of ethical hacking and common cyber attacks to understand the actions that occur after an attacker gains initial access to a system.

Building on this foundation, this topic explains the post-exploitation phase of a cyber attack. It covers how attackers move laterally across a network, steal user credentials, elevate their privileges, and conceal their activities to avoid detection. For example, an attacker may gain access to a hospital employee's computer through a phishing email. Using the compromised credentials, the attacker can access file servers, patient record systems, and other critical resources, while attempting to avoid triggering security alerts. Before leaving the network, the attacker may delete or modify system logs to hide evidence of the intrusion.

By studying concepts such as lateral movement, credential dumping, privilege escalation, data exfiltration, and anti-forensics, learners will understand how modern cyber attacks spread within an organization. They will also learn how security professionals detect malicious activities, protect sensitive systems, investigate security incidents, and recover from cyber attacks through effective digital forensic techniques.

SGOU

Key concepts

Persistence, Kerberos Tickets, Authentication Credentials, Domain Controller, System Memory, Steganography, Obfuscation, Network Segmentation

Discussion

Lateral movement is a stage of a cyber attack in which an attacker moves from one compromised system to another within the same network. After gaining initial access, the attacker explores the network, collects information, escalates privileges, and searches for valuable systems containing sensitive data. Instead of attacking the final target directly, the attacker gradually expands access across multiple devices while attempting to remain undetected.

Lateral movement has become a common technique in modern cyber attacks, especially in Advanced Persistent Threats (APTs). Rather than causing immediate damage, attackers spend days, weeks, or even months moving through the network, gathering information and establishing long-term access before stealing data or disrupting operations.

Attackers often use legitimate administrator tools, valid user credentials, and normal network protocols during lateral movement. Because these activities resemble regular network operations, detecting lateral movement is one of the biggest challenges for cybersecurity professionals.

3.4.1 Purpose of Lateral Movement

The primary objective of lateral movement is to move deeper into the network and gain access to critical resources. Attackers perform lateral movement for several reasons.

3.4.1.1 Maintaining Persistence

One of the main goals is to maintain continuous access to the organization's network. Instead of relying on a single compromised computer, attackers infect multiple systems and establish several access points. If one compromised system is detected and removed, they can continue their attack using another infected machine. This allows attackers to remain inside the network for a long period without being completely removed.

3.4.1.2 Privilege Escalation

As attackers move through the network, they search for administrator accounts or systems with higher privileges. By obtaining elevated permissions, they gain access to more sensitive resources and can perform actions that ordinary users cannot. Privilege escalation enables attackers to control critical systems, modify security settings, and access confidential information.

3.4.1.3 Accessing Critical Resources

The ultimate objective of lateral movement is to locate valuable organizational assets. Attackers search for file servers, databases, domain controllers, cloud storage, financial

SGOU

systems, and backup servers that contain confidential information such as customer records, financial data, intellectual property, passwords, or business documents. Once these resources are located, attackers can steal, modify, or destroy the data.

3.4.1.4 Collecting Sensitive Information

Before launching the final attack, attackers often gather information about the network, users, applications, and security controls. This helps them identify the most valuable targets and avoid security mechanisms. The collected information may also be used for future attacks or cyber espionage.

3.4.1.5 Preparing for Data Exfiltration

Lateral movement allows attackers to position themselves close to the systems containing sensitive data. Once the desired information is identified, they collect and transfer it to attacker-controlled systems without attracting attention. This preparation makes data exfiltration more efficient and reduces the chances of detection.

3.4.2 Why Lateral Movement is Difficult to Detect?

Lateral movement is difficult to identify because attackers frequently use legitimate administrative tools such as Remote Desktop Protocol (RDP), PowerShell, Windows Management Instrumentation (WMI), Secure Shell (SSH), and file-sharing protocols. They also use stolen user credentials instead of malicious software whenever possible. As a result, their activities often appear similar to normal administrative tasks, making it challenging for security teams to distinguish malicious actions from legitimate network activity.

Lateral movement is a critical phase of a cyber attack in which attackers move across multiple systems after gaining initial access. Their objective is to maintain persistence, obtain higher privileges, discover valuable resources, and prepare for data theft or other malicious activities. Because attackers use legitimate credentials and trusted administrative tools, lateral movement often remains undetected for extended periods. Detecting unusual user behavior, monitoring privileged account activities, implementing network segmentation, and applying the principle of least privilege are essential measures for preventing and limiting lateral movement within an organization's network.

3.4.3 Common Techniques of Lateral Movement

Attackers use several techniques to move from one compromised system to another within a network while remaining undetected. Some of the most common techniques are described below.

3.4.3.1 Pass-the-Hash (PtH)

Pass-the-Hash is a technique in which attackers steal the hashed password of a user and use it to authenticate to other systems without knowing the actual password. By reusing these password hashes, attackers can access multiple computers and expand their control within the network.

3.4.3.2 Pass-the-Ticket (PtT)

Pass-the-Ticket is a technique that targets Kerberos authentication. Attackers steal valid

SGOU

Kerberos tickets from a compromised system and use them to access other network resources. Since the ticket is legitimate, the attacker can impersonate an authorized user without entering a password.

3.4.3.3 Remote Desktop Protocol (RDP) Abuse

Remote Desktop Protocol (RDP) allows users to remotely access another computer. Attackers who obtain valid RDP credentials can log into remote systems, execute commands, install malware, and access sensitive data as though they were legitimate users.

3.4.3.4 Windows Management Instrumentation (WMI)

Windows Management Instrumentation (WMI) is a Windows administration tool used to manage remote computers. Attackers misuse WMI to execute commands, run scripts, and install malicious software on remote systems without requiring physical access.

3.4.3.5 Exploiting Weak or Misconfigured Permissions

Attackers search for systems with weak passwords, excessive user privileges, insecure shared folders, or misconfigured access permissions. These weaknesses allow them to move between systems, gain unauthorized access, and compromise additional devices within the network.

Lateral movement techniques enable attackers to spread across a network after gaining initial access. Common methods include Pass-the-Hash, Pass-the-Ticket, RDP abuse, WMI, and exploiting weak or misconfigured permissions. Organizations can reduce the risk of lateral movement by enforcing strong authentication, applying the principle of least privilege, securing remote access services, and continuously monitoring network activities.

3.4.4 Credential Dumping

Credential dumping is a post-exploitation technique in which attackers extract stored user credentials from a compromised system. After gaining access to a computer, attackers retrieve authentication information such as passwords, password hashes, and Kerberos tickets from the system memory or storage. These credentials are then used to move to other systems, gain higher privileges, and access sensitive resources without needing to crack passwords.

Credential dumping is considered one of the most dangerous techniques because a single compromised computer can provide attackers with access to multiple systems across an organization's network.

3.4.4.1 Types of Credentials Obtained

Attackers commonly target the following authentication information:

- **Plaintext Passwords:** Actual user passwords stored in memory.
- **Password Hashes:** Encrypted representations of passwords used in **Pass-the-Hash (PtH)** attacks.

SGOU

- **Kerberos Tickets:** Authentication tickets used in **Pass-the-Ticket (PtT)** attacks within Windows Active Directory environments.

3.4.4.2 How Credential Dumping Works

Credential dumping is a multi-stage process in which attackers steal authentication credentials from a compromised system. These stolen credentials are then used to gain unauthorized access to additional systems, escalate privileges, and move laterally within the network. The process typically involves the following steps:

1. Initial Access

The first step is to gain access to the target system. Attackers may achieve this through phishing emails, malicious attachments, malware infections, stolen credentials, weak passwords, or by exploiting software vulnerabilities. At this stage, the attacker usually has limited access to the compromised machine.

2. Privilege Escalation

To access sensitive credential information, attackers require higher privileges. They attempt to obtain **Administrator** or **SYSTEM-level** access by exploiting local vulnerabilities, misconfigured permissions, or stolen administrator credentials. Elevated privileges allow attackers to access protected system files and memory areas that are inaccessible to ordinary users.

3. Accessing LSASS Memory

After obtaining sufficient privileges, the attacker targets the **Local Security Authority Subsystem Service (LSASS.exe)**. LSASS is a critical Windows process responsible for authenticating users and managing security policies. To support user authentication and single sign-on, Microsoft introduced **Credential Guard**, which uses **Virtualization-Based Security (VBS)** to isolate the **Local Security Authority Subsystem Service (LSASS)** and protect sensitive credentials from being exposed in memory. This modern security mechanism helps prevent attackers from extracting plaintext passwords and other authentication credentials. Attackers access the memory of this process to retrieve these authentication credentials. See fig. 3.4.1.

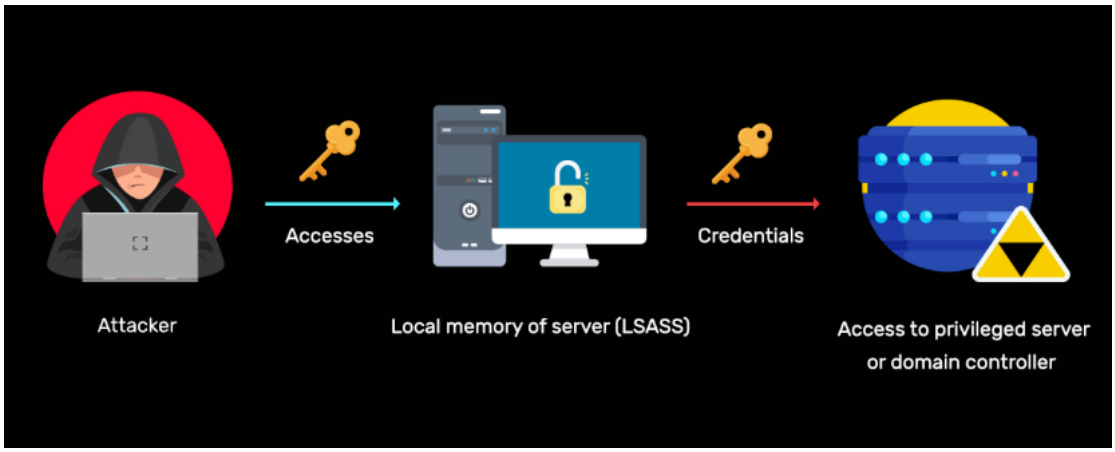


Fig. 3.4.1 Accessing Local Memory of Server

SGOU

4. Credential Extraction

Using specialized tools such as **Mimikatz** or **ProcDump**, attackers extract authentication data from the memory of the LSASS process. The extracted information may include plaintext passwords, NTLM password hashes, cached credentials, and Kerberos tickets. These credentials can then be used to authenticate without knowing the actual user passwords.

5. Lateral Movement

Once valid credentials have been obtained, attackers use them to access other computers, servers, and network resources. They authenticate as legitimate users, gain access to additional systems, elevate their privileges further, and continue expanding their control across the network. This process, known as **lateral movement**, enables attackers to locate sensitive information, compromise critical servers, and prepare for data theft or other malicious activities.

Credential dumping enables attackers to steal authentication information directly from system memory rather than attempting to crack passwords. By gaining initial access, escalating privileges, extracting credentials from **LSASS.exe**, and using the stolen credentials for lateral movement, attackers can compromise multiple systems within an organization's network. Protecting privileged accounts, restricting access to LSASS memory, enabling credential protection mechanisms, and continuously monitoring authentication activities are essential defenses against credential dumping attacks.

SGOU

3.4.4.3 Common Tools Used

Several tools are used to perform credential dumping:

- **Mimikatz:** The most widely used tool for extracting passwords, password hashes, and Kerberos tickets from Windows memory.
- **ProcDump:** A Microsoft utility that can create memory dumps of running processes, including LSASS, for offline credential extraction.

3.4.4.4 Key Features of Credential Dumping

- Extracts authentication credentials directly from system memory.
- Enables **Pass-the-Hash** and **Pass-the-Ticket** attacks.
- Supports lateral movement across the network.
- Helps attackers gain administrative privileges.
- Often difficult to detect because it uses legitimate system processes and administrative tools.

Credential dumping is a powerful post-exploitation technique used to steal authentication credentials from compromised systems. By extracting passwords, password hashes, and Kerberos tickets from **LSASS.exe**, attackers can move laterally, gain higher privileges,

and access sensitive resources. Protecting privileged accounts, enabling credential protection features, restricting administrative access, and monitoring access to LSASS memory are essential measures to defend against credential dumping attacks.

3.4.5 Anti-Forensics

Anti-forensics refers to the techniques and methods used to hide, alter, destroy, or manipulate digital evidence to make forensic investigation difficult or impossible. While **digital forensics** focuses on collecting and analyzing evidence after a cyber attack, anti-forensics aims to prevent investigators from finding or interpreting that evidence. Cybercriminals use anti-forensic techniques to conceal their activities, erase traces of attacks, and delay or mislead investigators.

In some legitimate situations, anti-forensic methods are used to securely erase confidential information and protect user privacy. However, these techniques are frequently abused by attackers to cover their tracks after compromising a system.

3.4.5.1 Goals of Anti-Forensics

The primary objectives of anti-forensics are to hide evidence and make forensic investigations more difficult. The main goals include:

- Avoid detection of unauthorized or malicious activities.
- Prevent or delay the collection of digital evidence.
- Increase the time and effort required for forensic analysis.
- Mislead investigators by altering or forging evidence.
- Bypass or disable forensic tools.
- Remove all traces indicating that anti-forensic tools were used.

3.4.5.2 Anti-Forensic Techniques

1. Data Destruction

Data destruction involves permanently removing digital evidence so that it cannot be recovered. Attackers use secure deletion techniques that overwrite files multiple times, making recovery impossible even with forensic software. They may also modify or delete file timestamps and metadata to hide when files were created, accessed, or modified.

2. Defense Evasion and In-Memory Execution

Instead of deleting evidence, attackers may use **Defense Evasion** techniques to avoid detection and reduce the forensic traces left on a compromised system. One approach is **In-Memory Execution**, in which malicious code operates primarily in system memory rather than being stored as a conventional file on disk. Techniques such as **Direct Kernel Object Manipulation (DKOM)** can also modify kernel data structures to hide malicious processes or other system objects from security tools. These techniques can make traditional file-based forensic analysis more difficult because fewer artifacts may be present on disk.

SGOU

3. Obfuscation and Artifact Hiding

Attackers may also use **Obfuscated Files or Information** and other artifact-hiding techniques to make malicious content difficult to identify or analyze. **Steganography** is one such technique, in which information is concealed within another file, such as an image, audio file, video, or document, so that the hidden content is not readily apparent. During forensic investigation, analysts may examine file structure, metadata, unusual file characteristics, and other indicators to identify potentially hidden information.

4. Encryption

Encryption protects stolen data and malicious files from being examined by investigators unless the correct decryption key is available.

5. Data Forgery

Data forgery involves creating fake logs, modifying records, or altering timestamps to mislead investigators. By inserting false evidence or changing existing information, attackers attempt to hide their actual activities and confuse forensic analysis.

6. Analysis Prevention

Attackers use techniques that prevent security tools and forensic software from analyzing malware or system activity. These include disabling logging services, detecting virtual machines or sandbox environments, terminating security software, and using anti-debugging techniques.

7. Online Anonymity

To conceal their identity, attackers often use anonymity tools such as **VPNs**, **proxy servers**, and the **Tor network**. These tools hide the attacker's real IP address, making it difficult for investigators to trace the source of an attack.

Anti-forensics consists of techniques used to hide, modify, or destroy digital evidence to prevent successful forensic investigation. Common techniques include data destruction, data concealment, data hiding, obfuscation, encryption, data forgery, analysis prevention, and online anonymity. Understanding these techniques helps cybersecurity professionals develop stronger detection mechanisms and conduct more effective digital forensic investigations.

SGOU

Recap

- Lateral movement allows attackers to move from one system to another within a network.
- The objective of lateral movement is to reach valuable systems and critical resources.
- Attackers may use stolen credentials to access additional systems.
- Privilege escalation helps attackers obtain higher levels of access.
- Defense evasion techniques are used to avoid detection by security tools.
- Attackers may attempt to reduce or manipulate forensic evidence.
- In-memory execution allows malicious code to operate primarily in system memory.
- Fileless or memory-based techniques can reduce traditional disk-based evidence.
- Direct Kernel Object Manipulation (DKOM) may be used to manipulate kernel-level objects.
- Attackers may attempt to hide processes or other malicious activities from security tools.
- Obfuscation makes malicious files or information more difficult to understand or analyze.
- Artifact hiding techniques attempt to conceal information from investigators and security tools.
- Steganography can hide information within images, audio, videos, or other files.
- Digital forensic investigators examine memory, files, metadata, and system artifacts for evidence.
- Understanding standard terminology such as Defense Evasion, In-Memory Execution, and Obfuscated Files or Information improves the accuracy of cybersecurity analysis.

SGOU

Objective Type Questions

1. What is the movement of an attacker from one compromised system to another called?
2. Which technique uses stolen password hashes for authentication?
3. Which authentication system is targeted in Pass-the-Ticket attacks?
4. Which protocol is commonly abused for remote access during lateral movement?
5. Which Windows administration tool can be misused to execute commands on remote systems?
6. What technique involves extracting stored authentication information from a compromised system?
7. Which Windows process is commonly targeted for credential extraction?
8. What type of security uses virtualization to protect sensitive credentials?
9. Which tool is widely known for extracting credentials from Windows memory?
10. What is the process of gaining higher-level permissions called?
11. What technique is used to hide, alter, or destroy digital evidence?
12. What technique permanently removes data to prevent its recovery?
13. What technique hides information inside another file such as an image or audio file?
14. What technique involves modifying or creating false evidence to mislead investigators?

SGOU

Answers to Objective Type Questions

1. Lateral Movement
2. Pass-the-Hash
3. Kerberos
4. RDP

5. WMI
6. Credential Dumping
7. LSASS
8. VBS
9. Mimikatz
10. Privilege Escalation
11. Anti-Forensics
12. Data Destruction
13. Steganography
14. Data Forgery

Assignments

1. Explain the purpose of lateral movement in a cyber attack and describe how attackers move between systems within a network.
2. Discuss the role of stolen credentials and privilege escalation in enabling lateral movement.
3. Explain the concept of defense evasion and describe why attackers use defense evasion techniques.
4. Describe in-memory execution and explain why it can make forensic investigation more challenging.
5. Explain Direct Kernel Object Manipulation (DKOM) and discuss its role in defense evasion.
6. Discuss the concept of obfuscation and explain how it makes malicious files or information difficult to analyze.
7. Explain artifact hiding techniques and describe the challenges they create for digital forensic investigators.
8. What is steganography? Explain how attackers may use it to hide information within digital files.

SGOU

Suggested Reading

1. Godbole, Nina, and Sunit Belapure. *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*. Wiley India Pvt. Ltd., 2011.

2. Brooks, Charles J., et al. *Cybersecurity Essentials*. Wiley, 2018

3. Wu, Chwan-Hwa (John), and J. David Irwin. *Introduction to Cyber Security*. CRC Press, 2016.

Reference

1. Jain, Atul. *Cyber Crime: Issues, Threats and Management*. Isha Books, 2004.

2. Yar, Majid. *Cybercrime and Society*. Sage Publications, 2006.

3. Chaubey, R. K. *Cyber Crimes and Law*. Kamal Law House, 2012.

SGOU



BLOCK 4

Cyber Crime and Cloud Computing

SOU



Tools and Methods used for Cyber Crime

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- explain the concept of cybercrime tools and techniques
- explain different types of network scanning and their purposes
- describe the working of keyloggers and Remote Access Trojans (RATs)
- discuss the role of packet sniffers and botnets in cyber activities

Prerequisites

Think about a situation where a system gets compromised, yet nothing unusual was noticed beforehand. No alarms, no visible damage, no obvious mistake. Later, it is discovered that information had been quietly collected over time, access had been established step by step, and the system had already been understood in detail before any real action took place.

This raises an interesting point. Cyber attacks are rarely random or immediate. They are often structured, moving through stages such as observing a network, identifying active systems, finding weak points, and then gradually gaining control. Each stage is supported by specific tools, and each tool plays a precise role in the overall process.

At the same time, these very tools are not exclusive to attackers. Security professionals use them to study systems, detect weaknesses, and strengthen defenses. This creates a dual nature where the same technique can either protect or exploit, depending on how it is used.

So, the real question is not just what these tools are, but how they fit into the sequence of an attack. When you begin to connect each tool to a particular stage, the entire process becomes clearer and more meaningful.

With this perspective, let us move into the topic and explore the tools and techniques that shape both cyber attacks and cybersecurity.

SGOU

Key concepts

Cybercrime tools, Network scanning, Port scanning, Vulnerability scanning, Keylogger, Remote Access Trojan (RAT), Packet sniffing, Botnet

Discussion

4.1.1 Introduction to Cyber Crime Tools and Techniques

Cybercrime does not occur as a sudden action. It develops through a sequence of steps, where each step is supported by specific tools. These tools help in observing systems, collecting information, gaining access, and sometimes controlling or exploiting resources.

At the beginning, it is helpful to stop for a moment and think about how an intrusion usually happens. Does an attacker start by attacking immediately? Or do they first try to understand the system?

In most cases, understanding comes first. That is why cybercrime tools are designed to work step by step, not all at once.

In this unit, attention is focused on a set of commonly used tools that operate at different stages of an attack. Some tools are used to gather information about systems, while others are designed to monitor user activity. Certain tools go further by enabling remote control, and some are capable of intercepting data as it travels across networks. There are also techniques that combine multiple compromised systems to carry out large-scale operations.

As each tool is introduced, it is useful to continuously ask: at which stage of an attack would this tool be used? This way of thinking helps in understanding not only how each tool works, but also how they are connected as part of a larger sequence.

With this perspective in mind, the discussion begins with tools that focus on discovering and analyzing systems within a network.

4.1.2 Network Scanners

Network scanning is a technique used to examine a network in order to identify active devices, available services, and possible points of entry. It plays a dual role. On one side, it helps security professionals monitor and protect systems. On the other side, the same technique can be used by attackers to discover weaknesses.

If a system is completely unknown, how can anyone attempt to attack it?

The answer lies in gathering information first. Network scanning provides this information. It reveals which devices are connected, how they communicate, and which parts of the system are exposed.

This is why network scanning is often considered the starting point of both cybersecurity and cyber attacks.

SGOU

4.1.2.1 Purpose of Network Scanning

Network scanning simplifies the process of monitoring and evaluating the security of a system. Instead of manually checking each device, it provides a structured way to observe the entire network.

As the scan progresses, it identifies live devices and the interactions between different components. This creates a clear picture of how the network is organized.

Now reflect on this idea:

If the structure of a network is clearly known, does it become easier to protect or easier to attack?

In reality, it becomes easier for both. Security professionals use this knowledge to strengthen defenses, while attackers use it to locate weaknesses.

Therefore, the purpose of network scanning is not limited to detecting vulnerabilities. It also supports continuous monitoring, helping maintain a secure and stable network environment.

4.1.2.2 Working Mechanism of Network Scanning

Network scanning works by sending requests to different parts of a network and analyzing the responses. Based on these responses, it identifies which systems are active and how they behave.

The process involves examining IP addresses and understanding how different devices are connected. This is done by using tools that send requests across the network and observe the responses. From these responses, it is possible to identify active devices, their IP addresses, and how they are linked within the network.

In simple terms, the tool "asks" the network questions, and the replies help in building a map of the system.

If a device responds freely to multiple requests, it may reveal more information than necessary. Such exposure can later be used for exploitation. This is why controlled responses and proper configuration are important in maintaining security.

The same scanning techniques are used by both administrators and attackers. Administrators use them to identify and fix vulnerabilities, while attackers use them to locate entry points. The difference lies in the intention behind their use.

4.1.2.3 Types of Network Scanning

Network scanning can be categorized based on the objective it serves. Each type focuses on a different aspect of the network and contributes to a deeper understanding of its structure and security.

In practice, these scanning techniques are often used in a sequential manner, where information gathered in one stage guides the next step. As this progression unfolds, the network gradually shifts from being unknown to something that can be clearly approached, examined, and potentially exploited in detail.

SGOU

1. Host (Ping) Scanning

From a cybercrime perspective, host scanning is used to identify which systems are alive and reachable within a network.

An attacker sends requests to multiple IP addresses and observes which ones respond. The systems that reply are considered active targets. Instead of blindly attacking every possible address, the attacker now has a refined list of potential victims.

This step is important because it avoids unnecessary noise and reduces the chances of detection. By focusing only on active systems, the attacker can proceed more strategically in the next stages of the attack.

2. Vulnerability Scanning

Once active systems are identified, attackers move to vulnerability scanning to discover known weaknesses in those systems.

This process involves comparing system details such as software versions, configurations, and services with publicly available databases of known vulnerabilities. If a match is found, the attacker gains insight into how the system can be exploited.

However, attackers are aware that this method has limitations. It only detects vulnerabilities that are already known. New or undiscovered weaknesses (often called zero-day vulnerabilities) may remain hidden. Because of this, attackers may combine vulnerability scanning with other techniques to increase their chances of success.

3. Port Scanning

Port scanning is used by attackers to map the entry points of a system by identifying open ports and the services running on them.

Every service (such as web servers, email servers, or databases) communicates through specific ports. By sending carefully crafted packets to these ports, an attacker observes the responses and classifies them as:

- **Open** – the service is active and accessible
- **Closed** – no service is running on that port
- **Filtered** – access is restricted, often by a firewall

Open ports are of particular interest because they indicate accessible services that may contain vulnerabilities. If a weakness exists in any of these services, it can be exploited to gain unauthorized access.

Through port scanning, attackers gain a clearer picture of the system's structure, allowing them to select the most promising path for intrusion.

4.1.2.4 Network Scanning Tools

Network scanning tools are software applications used to examine a network and gather information about connected devices, open ports, running services, and potential security

SGOU

weaknesses. These tools play an important role in both **network administration** and **cybersecurity**, as they help in understanding how a network is structured and how it can be protected.

In a typical scenario, a network scanning tool sends requests to different devices within a network and observes their responses. Based on these responses, it identifies which systems are active, what services they are running, and whether there are any vulnerabilities that could be exploited.

Some commonly used network scanning tools include:

- **Nmap**: One of the most popular tools used for discovering hosts and services on a network. It can perform port scanning, OS detection, and service identification.
- **Angry IP Scanner**: A fast and simple tool used to scan IP addresses and identify active devices on a network.
- **OpenVAS**: A vulnerability scanning tool used to detect security issues in network systems.

These tools are often used together in a step-by-step manner. For example, a user may first identify active devices, then scan for open ports, and finally check for vulnerabilities. This layered approach helps in building a complete picture of the network.

It is important to note that while network scanning tools are essential for maintaining security, they can also be misused if handled improperly. Therefore, they should always be used ethically and with proper authorization.

4.1.3 Spyware : Keyloggers

Spyware is a form of malicious software that secretly enters a device, collects information, and tracks user activity without the user's knowledge.

A keylogger, also known as a keystroke logger, is a tool that records everything a user types on a keyboard. It can capture letters, numbers, symbols, and even special keys such as Enter or Backspace.

This leads to an important understanding. Most interactions with a computer involve typing, logging into accounts, sending messages, entering personal details. Because of this, a keylogger can collect a large amount of information simply by recording keystrokes.

Keyloggers are not always used for harmful purposes. In some situations, they are used legally, such as monitoring employee activity, troubleshooting systems, or supervising usage on shared devices. However, in cybercrime, they are mainly used to secretly collect sensitive information.

Information Captured by Keyloggers

When a keylogger is active, it records every keystroke and stores it in a file or sends it to an external source.

SGOU

The type of information captured can include:

- login credentials such as usernames and passwords
- credit card details entered during online transactions
- messages, emails, and search queries
- websites visited and forms filled

Some advanced keyloggers go beyond keystrokes. They can capture screenshots at intervals or identify patterns in typing to quickly detect sensitive data like passwords.

This creates a critical situation. Even if strong passwords are used, they can still be exposed if they are recorded during typing.

4.1.3.1 How Keyloggers Work

Think of a keylogger like an invisible note-taker sitting beside a user while they type on a keyboard. Every time a key is pressed, it quietly writes it down without being noticed.

Once a keylogger is installed on a system, it starts recording all keystrokes:

- When a user types a password → it records it
- When a user sends a message → it records it
- When a user searches something → it records it

All this information is either:

- stored inside the system, or
- secretly sent to the attacker

Now, how does it enter the system?

The way a keylogger enters a system can be understood through simple situations. When a user clicks on a malicious link, it is similar to opening a door to something unsafe. Email attachments in phishing attacks act like disguised files that appear harmless but carry hidden threats. Software downloaded from untrusted sources may include a keylogger along with the actual program. In some cases, even visiting a compromised web page can allow hidden scripts to install such software without the user's knowledge.

After entering the system, the keylogger operates silently in the background. It does not interrupt normal activities or give visible signs of its presence. The user continues typing, browsing, and working as usual, while every keystroke is being recorded.

An important point to understand is that a keylogger does not aim to damage the system directly. Instead, it focuses on collecting information in a quiet and continuous manner. This ability to remain hidden while capturing sensitive data is what makes keyloggers particularly effective and dangerous.

4.1.3.2 Types of Keyloggers

Keyloggers can be broadly classified into two categories based on how they are

SGOU

implemented.

Hardware Keyloggers are physical devices attached to a system, often between the keyboard and the computer. They record keystrokes directly. Since they require physical access to install, they are less commonly used in large-scale cyber attacks.

Software Keyloggers are programs installed on a system. These are more commonly used because they can be distributed remotely.

Within software keyloggers, there are different forms:

- Some capture data entered into web forms

For example, when a user types login details into an online banking or email login page, the entered username and password can be recorded before the form is submitted.

- Some use scripts embedded in websites to record typing

For instance, a malicious website or a compromised webpage may include hidden scripts (such as JavaScript) that track keystrokes or form inputs as the user types, even if the form is not submitted.

- Some operate within applications using system-level functions

For example, a background program installed on a system may use operating system functions (like keyboard event listeners in Windows or Linux) to capture all keystrokes across applications such as text editors, browsers, or messaging apps.

4.1.4 Remote Access Trojan (RAT)

There are many legitimate tools that allow access to a computer from a distance. These are used in offices, technical support, and remote work environments.

If such access is possible for legitimate users, can it also be misused?

A Remote Access Trojan (RAT) is exactly that misuse. It is a type of malware that allows an attacker to access and control a computer or system from a remote location, without the knowledge or permission of the user.

The term “Trojan” itself comes from the idea of something that appears harmless but hides a threat inside. In the same way, a RAT enters a system by pretending to be a normal or useful program.

4.1.4.1 How RATs Work

A RAT does not usually force its way into a system. Instead, it relies on the user to unknowingly install it.

This can happen through:

- email attachments that appear legitimate
- links that lead to fake or infected websites
- software that looks genuine but contains hidden malware

SGOU

Once the file is opened or installed, the RAT silently becomes part of the system.

An important point to notice here is that the user often believes they are installing something useful. This makes RATs particularly dangerous.

After installation, a RAT behaves like a remote access tool, but with a hidden purpose.

It creates a connection between the infected system and the attacker. Through this connection, the attacker can control the system as if they were sitting in front of it.

This means:

- commands can be executed remotely
- files can be accessed or modified
- programs can be installed or removed

The most critical aspect is that all of this happens without the user being aware.

Unlike visible attacks, a RAT is designed to remain hidden. It may not appear in the list of active programs and can stay undetected for long periods. The main risk of a RAT lies in its level of control and its ability to remain hidden.

Since it operates silently, the user may continue normal activities without realizing that the system is compromised. During this time, sensitive information can be collected, modified, or misused.

RATs are often used in larger attack strategies. For example, attackers may first install a RAT and then use it to gather information, spread malware, or perform further actions.

They are especially dangerous in organizations, where a single infected system can lead to access to an entire network.

SGOU

4.1.4.2 Detecting a Remote Access Trojan (RAT) Infection

Detecting a Remote Access Trojan is not always easy. Even advanced security tools may sometimes fail to identify it because RATs are designed to remain hidden. However, certain unusual system behaviors can indicate a possible infection.

A noticeable slowdown in system performance can be one of the early signs. Since a RAT runs in the background, it consumes processing power, which may cause the system to lag without any clear reason. Similarly, if antivirus software starts behaving abnormally such as crashing frequently or responding very slowly, it may suggest interference from malicious software.

Another indication can be the presence of unfamiliar files or programs. If applications appear on the system without being installed intentionally, it raises suspicion. Changes in browser behavior, such as frequent redirects or web pages failing to load properly, may also point to underlying issues.

In some cases, hardware activity may provide clues. For example, if the webcam indicator light turns on without any application being used, it could mean that the system is being accessed remotely.

It is important to understand that these signs are not exclusive to RAT infections. A system may show some, all, or none of these symptoms. Because of this, identifying a RAT often requires detailed and thorough scanning. This highlights a key idea in cybersecurity: preventing such threats is always more effective than trying to detect them later.

4.1.5 Packet Sniffers

4.1.5.1 Understanding Packet Sniffing

When data is transmitted over a network, it does not travel as a single unit. Instead, it is broken into smaller parts called *packets*. These packets move through the network and are later reassembled at the destination.

Packet sniffing is the process of capturing and analyzing these data packets as they travel across a network.

This leads to an important understanding. If someone is able to observe these packets, they can understand what kind of data is being transmitted such as messages, login details, or browsing activity.

Packet sniffing itself is not always harmful. It is widely used by network administrators to monitor performance, detect issues, and ensure smooth communication.

However, the same technique can also be misused to secretly observe and steal sensitive information.

A packet sniffer can be either a software program or a hardware device that monitors data flowing through a network.

In a normal network, a device typically processes only the data packets addressed to it, along with certain broadcast or multicast traffic. A packet sniffer is a tool that captures and analyzes network packets that are visible to the device on which it is running.

This allows the sniffer to observe:

- communication between users
- websites being accessed
- data being transferred

If the data is not encrypted, it can be easily read and understood.

4.1.5.2 Types of Packet Sniffers

Now, packet sniffing can be understood in two simple ways.

First, based on how the data is captured.

In **hardware-based sniffing**, a separate physical device is connected to the network. This device sits quietly and captures packets directly from the flow of traffic. It is usually used in controlled environments such as labs or large organizations where detailed and accurate monitoring is required. You can imagine it as installing a dedicated camera on

SGOU

the road to record every movement clearly.

In **software-based sniffing**, instead of a physical device, we use programs installed on a computer. These programs capture and analyze the packets passing through the network interface. This method is more common today because it is flexible, easier to install, and does not require additional hardware. It is similar to using an app on your phone to monitor traffic instead of setting up a full camera system.

The second way to understand packet sniffing is based on how the sniffer behaves. It includes passive and active sniffing.

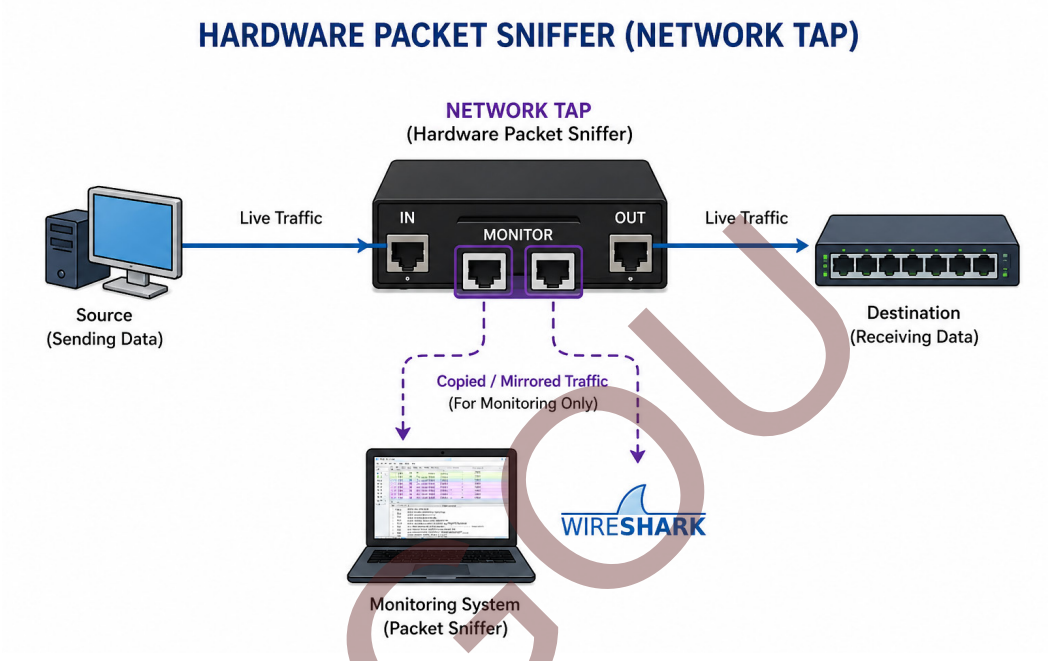


Fig. 4.1.1 Working of Packet Sniffer

In passive sniffing, the attacker behaves like a silent observer. They connect to the same network and simply listen to the traffic flowing through it. There is no interference with the communication process. Data packets move normally between sender and receiver, while the attacker quietly collects whatever is visible. This method is common in shared network environments, such as open Wi-Fi networks, where traffic can be observed without drawing attention. Because nothing is disturbed, it becomes very difficult to notice that monitoring is taking place.

In active sniffing, the situation is more intrusive. Here, the attacker does not just observe but actively tries to control or redirect the traffic. This can be done by creating a fake Wi-Fi hotspot that appears genuine, or by placing themselves between two communicating devices. This method is known as a Man-in-the-Middle attack, where the attacker secretly intercepts communication. By doing this, they can capture a much larger amount of data compared to passive sniffing.

Once the packets are captured, attackers use specialized tools to examine the data. If the information is not protected using encryption, it can be read easily in plain form. Sensitive details such as usernames, passwords, messages, and browsing activity may

SGOU

become visible. Even small pieces of information can be useful, as they help in building a clearer picture of a user's online behavior.

What makes this more concerning is the speed and invisibility of the process. Packet capture and analysis happen within seconds, and the user typically receives no indication that it is occurring. There are no alerts or visible signs. Because of this silent nature, understanding these techniques is essential for recognizing the importance of secure and protected communication.

Examples of Packet Sniffers

- **Wireshark** – one of the most popular tools for capturing and analyzing network traffic in detail.
- **Tcpdump** – a lightweight, command-line tool widely used in Unix/Linux systems.
- **Ettercap** – used for network monitoring as well as security testing and interception.
- **Kismet** – mainly used for detecting and analyzing wireless network traffic.
- **SolarWinds Network Performance Monitor** – a professional tool that includes packet analysis features along with network monitoring.

These tools can be used for legitimate purposes like troubleshooting and network analysis, but if misused, they can also be used to capture sensitive data from network traffic.

4.1.6 Botnets

A botnet is a group of computers or devices that have been infected with malicious software and are controlled remotely by an attacker. Each infected device is called a *bot* or sometimes a *zombie*, because it operates under someone else's control without the user knowing it.

These botnets are usually created using malware such as trojans, worms, or spyware. Once a device is infected, it becomes part of a larger network that is controlled from a central point. All the bots work together, often silently in the background, carrying out instructions given by the attacker.

One important aspect to notice is that the user of the infected device may not observe any major changes. The system may continue to function normally, while secretly participating in harmful activities.

4.1.6.1 Botnet Communication

After a system is infected, it needs to receive instructions. This is done through a mechanism known as Command and Control (C&C).

The infected device connects to a C&C server, which acts as the central system that sends commands. Through this connection, the attacker can control many devices at

SGOU

the same time. The communication usually uses common internet protocols so that it appears like normal network traffic, making it difficult to detect.

The process begins by identifying vulnerable systems. Devices with outdated software or weak security become easy targets. Malware is then introduced through methods such as phishing emails, malicious links, or unsafe downloads. Once installed, the system becomes part of the botnet and establishes a connection with the control server.

After this connection is established, commands are sent from the attacker to all infected devices. These commands may instruct the bots to perform specific tasks such as sending spam messages, launching attacks, or collecting data.

4.1.6.2 Types of Botnets

Botnets can be categorized based on how communication takes place between the bots and the control system.

In an IRC-based botnet, communication happens through chat servers. Bots join a specific channel and receive commands in the form of messages. This method is simple and easy to manage because everything is controlled from a single point.

A Peer-to-Peer (P2P) botnet works differently. Instead of relying on a central server, each infected device communicates with others. Every bot acts both as a client and a server. This decentralized structure makes it more difficult to detect and shut down.

In an HTTP/HTTPS botnet, communication takes place through web protocols. Bots connect to web servers at regular intervals to receive instructions. Since this communication looks similar to normal web browsing, it blends into regular traffic and becomes harder to identify.

Botnets are mainly used to perform large-scale attacks.

One common use is phishing, where bots send a large number of fake messages that appear to be from trusted sources. These messages trick users into revealing sensitive information.

Another major attack is the Distributed Denial of Service (DDoS) attack. In this case, multiple bots send a large number of requests to a server at the same time. This overloads the system and makes it unavailable to normal users.

Botnets are also used for spamming, where a large number of unwanted messages are sent automatically. These messages may contain malicious links or promote fake services.

In data theft, bots collect confidential information such as login details or financial data. This information can later be misused or sold.

Finally, botnets can be used for targeted intrusion, where a specific organization or individual is attacked. These attacks are often planned and may continue over a long period, causing serious damage.

SGOU

Recap

- Cybercrime follows a step-by-step process, not a sudden action. Tools are used at each stage such as scanning, monitoring, access, and control.
- Network scanning is the starting point for understanding a system. It identifies active devices, open ports, and available services. Scanning is used by both attackers and security professionals.
- Host scanning finds which systems are active. Port scanning identifies open and closed ports. Vulnerability scanning detects known weaknesses.
- Keyloggers record everything typed on a keyboard. They capture sensitive data like passwords and messages. They work silently in the background.
- Remote Access Trojans allow full control of a system from a distance. They enter systems by pretending to be legitimate software. They operate without the user's knowledge.
- Packet sniffing captures data traveling across a network. It can reveal sensitive information if data is not encrypted. Passive sniffing observes traffic, while active sniffing interferes with it.
- Botnets are networks of infected devices controlled by an attacker. Each device in a botnet is called a bot or zombie. Botnets are used for attacks like DDoS, spamming, and data theft.
- The same tools can be used for both security and attacks. Understanding these tools helps in improving cybersecurity awareness.

Objective Type Questions

1. What is the process of examining a network to identify active devices?
2. Which scanning type identifies active systems in a network?
3. Which scanning type detects open ports?
4. Which scanning type finds known weaknesses in systems?
5. What is the tool that records keystrokes?
6. What type of malware allows remote control of a system?
7. What is the technique of capturing data packets in a network?
8. What is a network of infected devices called?
9. What is each infected device in a botnet called?

SGOU

10. What type of sniffing only observes traffic without interference?

11. What type of sniffing involves interference in communication?

12. What is the central system that controls botnets called?

Answers to Objective Type Questions

1. Scanning
2. Host
3. Port
4. Vulnerability
5. Keylogger
6. RAT
7. Sniffing
8. Botnet
9. Bot
10. Passive
11. Active
12. C&C

SGOU

Assignments

1. Explain the step-by-step process of cybercrime activities and describe how different tools are used at each stage.
2. Describe the concept of network scanning and explain its types and purposes in detail.
3. Explain how keyloggers and Remote Access Trojans operate, and discuss the risks they pose to users.

4. Analyze how the same cybercrime tools can be used for both security and malicious purposes. What factors determine their ethical use?

5. Examine a scenario where a system is compromised without visible signs. Identify which tools or techniques might have been used at different stages and justify your reasoning.

Suggested Reading

1. Gupta, B. B., Martinez Perez, G., Agrawal, D. P., & Gupta, D. (2020). *Handbook of computer networks and cyber security: Principles and paradigms*. Springer.

2. Pramanik, S., Samanta, D., Vinay, M., & Guha, A. (2022). *Cyber security and network security*. Wiley-Scrivener.

3. Sadiqui, A. (2020). *Computer network security*. Wiley-ISTE.

4. Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.

Reference

1. Gupta, B. B., Martinez Perez, G., Agrawal, D. P., & Gupta, D. (2020). *Handbook of computer networks and cyber security: Principles and paradigms*. Springer.

2. Pramanik, S., Samanta, D., Vinay, M., & Guha, A. (2022). *Cyber security and network security*. Wiley-Scrivener.

3. Sadiqui, A. (2020). *Computer network security*. Wiley-ISTE.

4. Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.

SGOU



Password Security and Remote Threats

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- explain the concept of remote attacks and how they operate
- describe different remote attack methods such as brute force, dictionary, phishing, and credential stuffing
- explain the importance of random passwords in improving security
- differentiate between strong and weak passwords

Prerequisites

Imagine two users creating accounts on the same website. One chooses a simple password that is easy to remember. The other selects a complex and random one. Both feel their accounts are secure because access requires a password. After some time, one account is accessed without permission while the other remains safe. What made the difference?

The answer does not lie in luck. It lies in how passwords are created and how attackers approach them. Today, attacks are not always visible or forceful. Many of them happen quietly from a distance, using automated tools that can test thousands of possibilities or trick users into revealing their details. In such situations, even a small weakness in a password can become an easy entry point.

This leads to an important realization. Security is not only about having protection in place, but also about understanding how that protection can fail. When you begin to see how remote attacks target passwords, the role of password design becomes much clearer. You start to notice why some passwords fail quickly, while others resist even powerful attacks.

With this curiosity, let us explore how remote attacks work and how different types of passwords influence the strength of a system.

SGOU

Key concepts

Remote attacks, Brute force attack, Dictionary attack, Phishing, Credential stuffing, Random password, Strong password, Weak password

Discussion

4.2.1 Introduction

Consider how often access to systems depends only on a single step of verification. Once the correct password is entered, the system assumes the user is genuine and grants access without further questioning. This makes the password a critical point of trust.

Now think about this situation. If an attacker is not physically near the system, can they still attempt to break this trust? The answer lies in remote attacks, where access is attempted from a distance using automated methods and deceptive techniques.

This creates an important link between how passwords are designed and how they are attacked. If passwords are predictable or weak, remote attacks become easier and more effective. On the other hand, strong and carefully created passwords can significantly reduce these risks.

With this understanding, it becomes necessary to explore how remote attacks target passwords and how different types of passwords influence system security.

4.2.2 Remote Attacks

A **remote attack** is a type of cyber attack where the attacker does not need physical access to the system. Instead, they operate from a distant location using the internet or network connections.

This makes remote attacks highly dangerous, because:

- The attacker can be anywhere in the world
- The attack can happen silently
- It is often difficult to immediately identify the source

In most cases, attackers target authentication systems, especially passwords, because passwords act as the first line of defense in any system.

Think of a system like a house:

- Username → your house address
- Password → the key to your door

If the attacker gets the key, they don't need to break anything. They simply walk in. That's why most remote attacks focus on stealing or guessing passwords.

SGOU

4.2.2.1 Remote Attack Methods

Some common remote attack methods include:

1. Brute Force Attack

Brute force attacks are mainly used in situations where the attacker has no prior knowledge about the system. This is known as a zero knowledge approach.

In this method, the attacker does not need any details about the password or system. They simply try all possible combinations until they find the correct one. So, a brute force attack is a method where an attacker generates many possible password combinations and tests them one by one to gain access.

These combinations can include numbers, letters, and special characters. The process does not rely on intelligence or guessing patterns but on systematic trial and error.

This method can be applied to user accounts, encrypted files, websites, and wireless networks.

An important point to remember is that longer and more complex passwords take much more time to crack compared to short and simple ones.

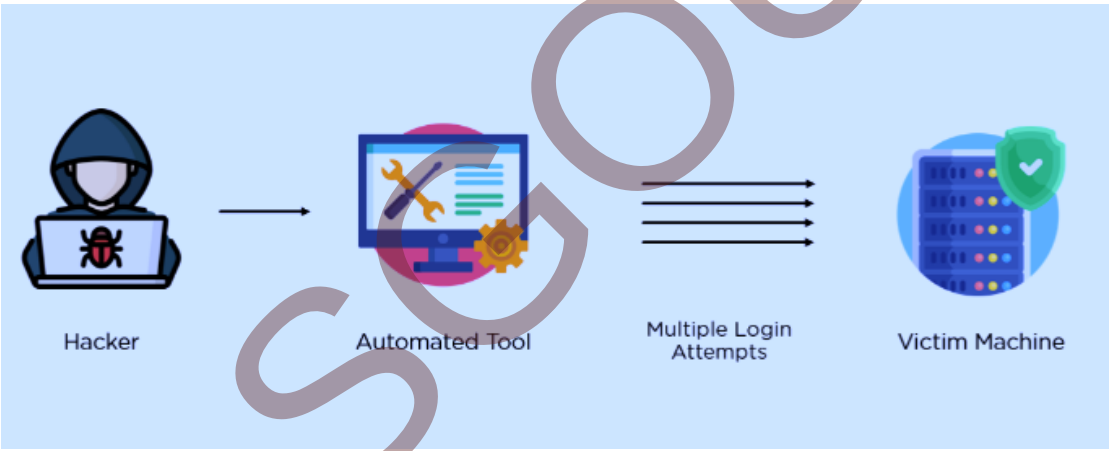


Fig. 4.2.1 How Brute force attack works

A brute force attack generally takes place in **three stages.**

First stage is choosing a tool: The attacker selects a software tool that can automatically test a large number of password combinations very quickly. Several tools are available, such as Hydra, John the Ripper, and Hashcat, which can perform brute force attacks on a wide range of targets, from encrypted files to secure web login forms.

The second stage is generating passwords: The tool creates multiple combinations of passwords. For example, a six digit numeric password can have around ten lakh combinations. Add alphabets and special characters to the mix, and we have a load of passwords to test.

Third stage is testing passwords: The generated passwords are tested against the target system. The tool keeps trying different combinations until the correct password is found or the system blocks further attempts.

SGOU

For example, in the case of a Wi Fi network, the tool repeatedly tries different passwords until it successfully connects.

2. Dictionary Attack

A dictionary attack is a method used by attackers to guess passwords using a prepared list of common words and passwords. In contrast to a brute force attack, which checks every possible combination of characters, a dictionary attack is more focused. It uses predefined lists of common words, previously leaked passwords, and simple variations such as adding numbers or symbols.

Because many users prefer simple and familiar passwords, this method becomes surprisingly effective.

Let us understand this step by step with a simple example.

Imagine a student named Arun creates an account on a website. He sets his password as “arun123”.

Now, an attacker wants to gain access to this account.

Step one is preparation of the wordlist

The attacker prepares a list of common passwords. This list may include words like arun, arun123, password, welcome123, and many others. These lists are often already available from previous data leaks.

Step two is target selection

The attacker selects the login page of the website where Arun has an account.

Step three is systematic testing

Using an automated tool, the attacker starts testing each password from the list. The tool enters one password after another into the login system.

So it tries:

arun

arun1

arun123

password

admin123

Step four is match found

When the tool tries “arun123”, it matches the correct password. The system accepts it, and the attacker gains access to Arun’s account.

3. Phishing Attack

A phishing attack is a technique in which the attacker manipulates users into revealing sensitive information such as passwords, banking details, or OTPs by pretending to be

SGOU

a trusted source.

Instead of breaking into a system technically, the attacker targets the human mind by creating a sense of urgency, fear, or trust.

In this method, attackers commonly use:

Fake emails that appear to come from banks, social media platforms, or official organizations

Fraudulent websites that closely resemble genuine login pages

Messages or links that encourage users to click and take immediate action

Imagine you receive an email saying:

"Your bank account will be suspended. Click here to verify your details."

The email looks official and includes a link. When you click the link, it takes you to a website that looks exactly like your bank's login page. Without realizing it is fake, you enter your username and password.

At that moment, the information is captured by the attacker, who can then use it to access your real account.

4. Credential Stuffing

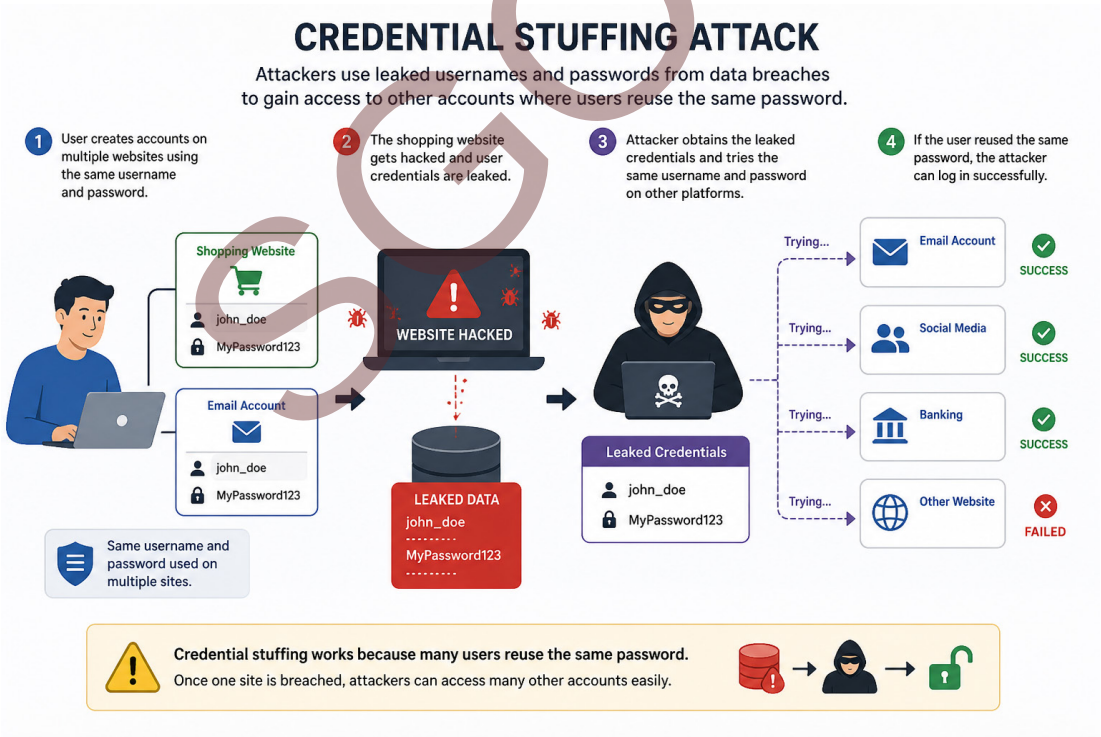


Fig. 4.2.2 Working of Credential Stuffing

Credential stuffing is an attack method where attackers use usernames and passwords that were leaked from previous data breaches to gain access to other accounts. This attack works mainly because many users reuse the same password across multiple websites.

Instead of guessing passwords, the attacker already has a list of valid credentials collected from hacked databases.

Suppose a user creates accounts on two websites: one shopping site and one email account. The user uses the same username and password for both.

Now imagine the shopping website gets hacked and user credentials are leaked. The attacker obtains this data and tries the same username and password on other platforms like email, social media, or banking services.

If the user has reused the same password, the attacker can easily log in without any effort.

4.2.3 Random Password

A random password is one that is created without any predictable pattern. It is usually generated using a combination of uppercase letters, lowercase letters, numbers, and special symbols.

Example

G7#kL9@pQ2

Such passwords do not resemble real words, names, or common patterns. Because of this, they are extremely difficult for attackers to guess.

Think of it like a lock where the key shape is completely irregular and unknown. There is no hint to guide the attacker.

Advantages of Random Passwords

Random passwords provide strong security for the following reasons.

They are resistant to guessing attacks. Since they do not follow common patterns, attackers cannot easily predict them.

They are difficult for dictionary attacks. Dictionary attacks rely on known words and patterns, which random passwords avoid completely.

They increase the time required for brute force attacks. Even if an attacker tries all combinations, the complexity of random passwords makes the process very time consuming.

Challenges of Random Passwords

While random passwords are secure, they also create practical difficulties.

They are hard to remember. Users may forget them easily because they have no meaningful pattern.

Users may store them insecurely. Some users write them down in notebooks or save them in plain text files, which introduces new security risks.

SGOU

4.2.3.1 Strong and Weak Passwords

Now let us clearly understand the difference between strong and weak passwords.

A weak password is one that can be easily guessed or cracked using simple techniques.

Examples

123456

password

abc123

Characteristics of weak passwords

- They are short in length
- They use common or easily guessable words
- They follow predictable patterns
- They may include personal information like name, date of birth, or phone number

Automated tools can test thousands of such passwords in seconds. Because these passwords are commonly used, attackers often succeed very quickly.

A strong password is designed to be difficult to guess and provides better protection against attacks.

Example

T9@rK!5mZ#2

Characteristics of strong passwords

- They are longer, usually 8 to 12 characters or more
- They include both uppercase and lowercase letters
- They contain numbers and special symbols
- They avoid common words and personal information

Strong passwords increase the number of possible combinations. This makes brute force and dictionary attacks much less effective, as the time required to crack them becomes very high.

SGOU

Recap

- Remote attacks are performed from a distant location without physical access. They mainly target authentication systems, especially passwords.
- A brute force attack tries all possible password combinations. It uses automated tools and takes more time for complex passwords.
- A dictionary attack uses a list of common words and known passwords. It is faster than brute force but limited to known patterns.
- A phishing attack tricks users into revealing sensitive information. It uses fake emails, messages, or websites that look genuine.
- Credential stuffing uses leaked usernames and passwords. It works when users reuse the same password across multiple sites.
- Random passwords have no predictable pattern. They are difficult to guess and resist most attacks.
- Weak passwords are short, simple, and easy to guess. They often include common words or personal details.
- Strong passwords are long and complex. They include letters, numbers, and special characters.
- Strong passwords increase the time required for attacks. Password complexity improves overall system security.

Objective Type Questions

1. What type of attack is performed from a distant location?
2. Which attack tries all possible password combinations?
3. Which attack uses a list of common passwords?
4. Which attack tricks users into revealing information?
5. Which attack uses leaked credentials?
6. What type of password has no predictable pattern?
7. What type of password is easy to guess?
8. What type of password is complex and secure?
9. What is the automated method of testing passwords called?
10. What is the fake website technique used in phishing called?

SGOU

Answers to Objective Type Questions

1. Remote
2. Brute force
3. Dictionary
4. Phishing
5. Credential stuffing
6. Random
7. Weak
8. Strong
9. Brute force
10. Spoofing

Assignments

1. Explain the concept of remote attacks and describe different methods such as brute force, dictionary attack, phishing, and credential stuffing.
2. Describe the characteristics, advantages, and challenges of random passwords.
3. Explain the differences between strong and weak passwords with suitable examples.
4. Analyze how password complexity influences the success of brute force and dictionary attacks.
5. Examine a scenario where a user reuses the same password across multiple websites. Analyze how this can lead to a credential stuffing attack and its consequences.

SGOU

Suggested Reading

1. Grimes, R. A. (2017). *Hacking the hacker: Learn from the experts who take down hackers*. Wiley.

2. Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.

3. Chapple, M., & Seidl, D. (2023). *CompTIA Security+ study guide: Exam SY0-601*. Wiley.

4. Nielsen, R. (2021). *Practical cybersecurity architecture: A guide to creating and implementing robust designs for cybersecurity architects*. Apress.

Reference

1. Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.

2. Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.

3. Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.

4. Kizza, J. M. (2020). *Guide to computer network security* (5th ed.). Springer.

SGOU



UNIT 3 Viruses and its Types

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- discuss the concept and functioning of computer viruses and malware
- summarize the different types of ransomware and their effects on systems
- explain the behavior and classification of worms and rootkits
- interpret the working of persistent and non-persistent web scripting attacks

Prerequisites

Computers and the internet have become a major part of modern life. From education and communication to banking, shopping, entertainment, and research, people depend on digital systems every day. Most users expect their computers to work smoothly and securely. However, there are times when systems suddenly slow down, important files disappear, unknown messages appear on the screen, or access to data becomes blocked. Such incidents often point to the presence of malicious software operating silently inside the system.

As technology continues to grow, cyber threats are also becoming more advanced and dangerous. Malware such as ransomware, worms, rootkits, and web scripting viruses can spread rapidly across networks, steal sensitive information, damage files, and even take control of entire systems. In many situations, a simple action such as clicking an unknown link, opening an email attachment, or downloading unsafe content may lead to a serious security attack.

One important question arises here: how do these malicious programs spread so effectively across computers and networks? Another equally important question is how users and organizations can protect themselves from such threats. Understanding these concepts is essential because cybersecurity is no longer a concern only for experts or large organizations. Every computer user needs awareness about digital threats and safe online practices.

SGOU

Studying computer viruses and malware helps learners understand the methods used by attackers, the impact of different cyber threats, and the importance of prevention techniques. Knowledge about ransomware, worms, rootkits, and web scripting viruses also helps users recognize suspicious activities and respond carefully when security risks appear.

This topic provides an opportunity to explore the fascinating and challenging world of cybersecurity threats and understand how modern systems can be protected against malicious attacks. Let us now begin the study of computer viruses and malware in detail.

Key concepts

Computer Virus, Malware, Ransomware, Worms, Rootkits, Web Scripting Viruses, Session Hijacking, Phishing

Discussion

4.3.1 Introduction to Computer Viruses

When we use computers in daily life, whether for teaching, research, communication, or entertainment, we often assume that the system will behave exactly as we expect. However, there are situations where the system behaves abnormally: files may disappear, programs may crash, or the system may slow down without any clear reason. Such unexpected behaviour often leads us to an important concept in cybersecurity: computer viruses.

A computer virus is a malicious program designed to enter a system without the user's knowledge, replicate itself, and cause harm either to data or to system performance. Unlike normal software, which performs useful tasks, a virus operates with hidden intent. It attaches itself to files or programs and becomes active when those files are executed. This ability to attach, replicate, and spread makes viruses particularly dangerous.

At this point, consider a simple question: if a virus spreads from one system to another, what enables that spread? In most cases, it is user interactions like opening infected files, downloading unsafe content, or clicking unknown links. This highlights an important idea: technology alone is not responsible for infections; user behavior plays a critical role.

4.3.2 Malware and its Categories

While the term "virus" is commonly used, it is actually a part of a larger category known as malware, which stands for malicious software. Malware includes various types of harmful programs, each designed with a specific purpose. Some aim to destroy

SGOU

data, others to steal information, and some to gain unauthorized control over a system.

Among the many forms of malware, ransomware, worms, rootkits, and web scripting viruses are particularly significant because of their widespread impact and distinct methods of operation. Each type behaves differently, and understanding these differences is essential for effective prevention and control.

4.3.2.1 Ransomware

Ransomware represents one of the most alarming forms of malware in recent years. It operates by denying users access to their own data, usually by encrypting files. Once the data is locked, the attacker demands a payment, often in digital currency, in exchange for restoring access.

To understand this better, imagine opening your system and finding that all your documents are inaccessible. A message appears stating that your files have been encrypted and can only be recovered by paying a certain amount. This is the typical behavior of ransomware.

Ransomware has an interesting origin. The first known example was created by Joseph L. Popp, a Harvard-trained biologist. He distributed infected floppy disks to participants at a conference organized by the World Health Organization in Stockholm. When users installed the program, it hid their file directories and demanded a payment of $189 to restore access. This attack became known as the AIDS Trojan.

Since then, ransomware has evolved significantly, but its main purpose remains the same: to extort money. Earlier, it spread through physical media like diskettes, but today it travels the internet through emails, malicious downloads, and even hidden content in images, audio, or video files.

Cryptojacking is a different type of cyberattack in which attackers secretly use a victim's computer resources to mine cryptocurrency. Unlike ransomware, which typically encrypts or blocks data and demands payment, cryptojacking mainly misuses the device's processing power and electricity for cryptocurrency mining. Attackers may sometimes use both ransomware and cryptojacking in the same attack, but they are separate types of malware. This process consumes system resources and electricity, benefiting the attacker without the user's knowledge.

A key question to consider is: does paying the ransom actually ensure you get your files back? In many cases, it does not. Attackers may not provide the decryption key even after payment, making prevention far more important than response.

Types of Ransomware

Ransomware can be understood more clearly by looking at its main types:

1. Scareware

Scareware is a type of malware that uses fear as a tool. It shows fake warnings, claiming that your computer is infected with viruses or serious threats. These messages are designed to create panic and pressure the user into buying unnecessary or fake security

SGOU

software. In most cases, there is no real infection. The safest approach is to ignore such alerts unless they come from a trusted and recognized antivirus service.

2. Screen Lockers

Screen lockers block access to your computer by locking the screen. Instead of your normal desktop, a message appears demanding payment to unlock the system. Sometimes, the message may pretend to be from a law enforcement agency to make it look more serious. However, these claims are false. Experts generally advise not to pay the ransom. Instead, restoring the system using a backup after cleaning the device is a safer solution.

3. Encrypting (Crypto) Ransomware

This is the most dangerous type of ransomware. It uses strong encryption techniques to lock the files on your system, making them inaccessible. A ransom note is then displayed with instructions on how to pay and recover the data. Even after payment, recovery is not guaranteed. In such cases, having a recent backup is often the only reliable way to restore files without paying the attacker.

Ransomware is not a static threat; it is continuously evolving and becoming more dangerous. As cybersecurity systems become stronger, attackers also develop new and smarter ways to break into computers and networks. This constant battle between security experts and cybercriminals has made ransomware one of the fastest-growing cyber threats today.

One of the most alarming developments is Ransomware-as-a-Service (RaaS). This works much like an online subscription service. Instead of creating ransomware themselves, attackers can purchase or rent ready-made ransomware tools from professional cybercriminal groups. In some cases, the profits earned from attacks are shared between the provider and the rattacker. This has made ransomware attacks easier to launch, even for people with limited technical knowledge.

Even though organizations like the United States Department of Justice actively work to track and stop cybercriminals, government system continue to be attractive targets. This is because disrepting government services can affect thousands of people.

For example, if a local government office is attacked, important public services such as records management, permits, or emergency response systems may stop functioning. Attackers take advantage of this pressure. Since restoring services quickly becomes a priority, organizations may feel forced to pay the ransom to resume operations. This is exactly why ransomware remains such a powerful weapon for cybercriminals. It combines technical attack methods with psychological pressure, making it both a technological and strategic threat.

Ransomware detection and prevention

Detecting ransomware early is very important. Organizations use a mix of training and tools to stay protected:

- Employee awareness plays a key role. Users should be trained to identify

SGOU

suspicious emails, unknown links, and unusual attachments, which are common entry points for attacks.

- Honeypots are used as traps. These are fake files or systems designed to attract attackers.
- When someone tries to access them, it signals a possible ransomware attempt.
- Network and system monitoring helps detect unusual behavior. For example, sudden file changes, unknown traffic, or abnormal user activity can indicate an attack.
- Security tools like antivirus and anti-ransomware software act as the first line of defense.They can block unsafe websites and alert users when threats are detected.
- Email filtering is another strong defense. Suspicious emails and harmful file types can be blocked before they reach users.

How to Respond to a Ransomware Attack

The first recommendation from authorities such as the Federal Bureau of Investigation is not to pay the ransom, as it may encourage further attacks. In India, victims should report cybercrime through the National Cyber Crime Reporting Portal and, in cases involving financial fraud, contact the 24×7 cybercrime helpline 1930. Cybersecurity incidents can also be reported to CERT-In (Indian Computer Emergency Response Team) as required under applicable rules.

Steps to respond include:

- **Identify scareware:** Fake alerts or pop-ups can often be removed with basic troubleshooting or support guidance.
- **Consult experts:** IT professionals may help contain the ransomware, recover affected systems, or identify available decryption tools, although success is not guaranteed and professional assistance may involve a cost.
- **Report the incident:** Victims in India should report the incident through the appropriate national cybercrime reporting channels and provide relevant details such as suspicious messages, payment information, and other available evidence.

Ransomware Removal

Removing ransomware involves:

- Isolating infected systems
- Identifying the type of attack
- Deleting malicious files

However, removal does not guarantee recovery of encrypted data. Recovery depends mainly on backups or available decryption keys.

SGOU

Prevention: The Best Strategy

Preventing ransomware is always better than dealing with it later. Key strategies include:

- Regular updates to fix security vulnerabilities
- Installing trusted software only and using authentication methods
- Using antivirus and firewalls for continuous protection
- Whitelisting applications so only approved programs run
- Maintaining regular backups for quick recovery
- Training employees to avoid mistakes
- Using multi-layered security systems that combine different protective techniques

4.3.2.2 Worms

Worms differ from traditional viruses in one key aspect: they do not require a host file to spread. A worm is a standalone program capable of replicating itself and spreading across networks without user intervention.

Consider how quickly information spreads on a network. Worms exploit this connectivity. Once a worm enters a system, it scans the network for other vulnerable systems and transfers copies of itself automatically. This rapid and autonomous spreading ability allows worms to infect large networks in a very short time.

For example, if one system in a network is infected, the worm can move to other connected systems without requiring any user action. This makes worms particularly dangerous in organizational environments where multiple systems are interconnected.

At this stage, think about the difference between a virus and a worm. A virus depends on user actions to spread, while a worm spreads independently. This distinction is crucial for understanding their behavior and designing appropriate defenses.

Classification of Worms

Computer worms are a category of malware that can replicate themselves and spread across systems and networks. While early worms are no longer active today, their underlying techniques continue to influence modern cyber threats. With the growth of the internet, cloud computing, and mobile technologies, worms have evolved in both method and impact.

1. Email Worms

Email worms spread through malicious attachments or links embedded in emails. They rely on social engineering techniques to trick users into opening infected content.

A well-known historical example is the ILOVEYOU worm, which spread rapidly by appearing as a harmless message.

SGOU

In the present day, such worms have evolved into phishing-based malware campaigns, where attackers use realistic emails, often impersonating banks, delivery services, or official institutions.

2. Network Worms

Network worms spread automatically by exploiting vulnerabilities in operating systems or network services, often without requiring user interaction.

The Conficker worm demonstrated how quickly such worms can infect millions of systems.

Today, similar techniques are used in automated cyberattacks targeting unpatched systems, especially in enterprise networks and Internet of Things (IoT) devices.

3. File-Sharing and Download-Based Worms

These worms spread through shared files, peer-to-peer networks, or software downloads by disguising themselves as legitimate content.

Earlier platforms like Napster experienced such threats. In modern environments, this method has evolved into malicious software downloads, cracked applications, and infected mobile apps, making it still highly relevant.

4. Messaging and Social Media Worms

Modern worms have expanded beyond traditional instant messaging to include social media platforms and chat applications.

The Kelvir worm is an early example of messaging-based propagation. Today, similar attacks occur through platforms like messaging apps and social networks, where malicious links are shared through compromised accounts.

5. Internet and Web-Based Worms

These worms target vulnerabilities in web servers, websites, and online applications. They spread by scanning the internet for weak systems.

The Code Red worm is a classic example that affected web servers globally. In modern systems, such attacks have evolved into web-based exploits, botnets, and large-scale automated attacks, often targeting cloud infrastructure and online services.

4.3.2.3 Rootkits

Rootkits represent a more sophisticated and hidden form of malware. Their primary purpose is not to damage the system directly, but to gain and maintain unauthorized access while remaining undetected.

A rootkit works by hiding its presence within the system, often at a deep level such as the operating system kernel. Once installed, it allows attackers to control the system remotely, access sensitive information, and even install additional malware without the user's knowledge.

SGOU

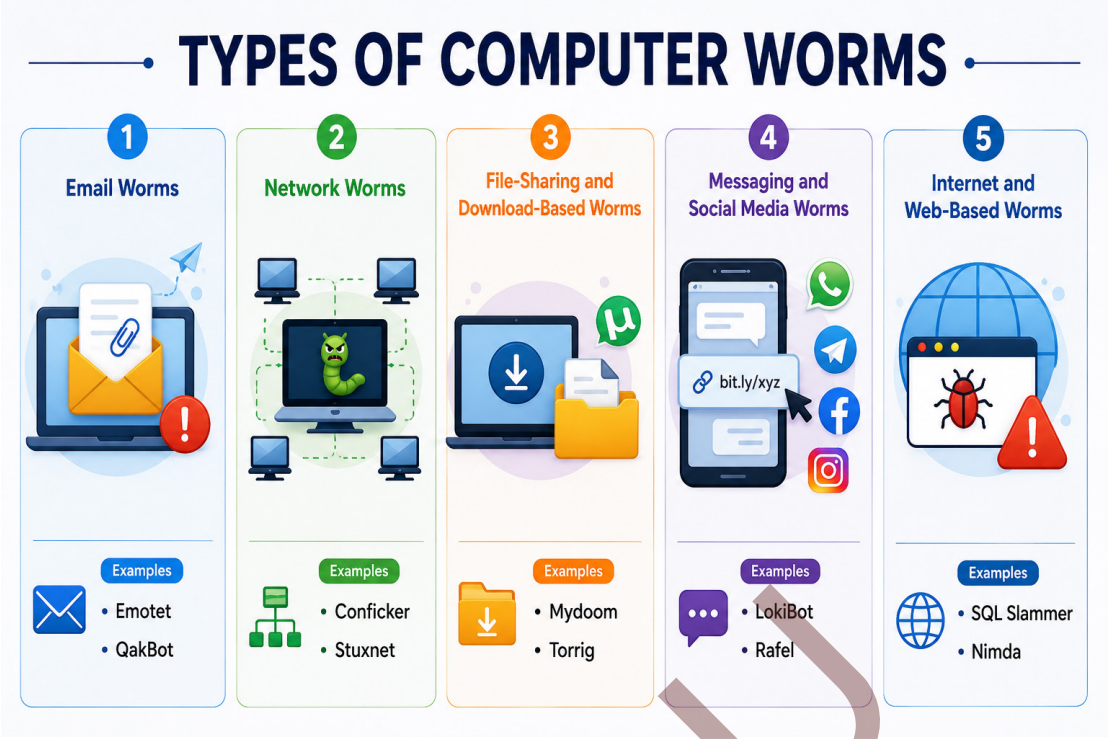


Fig. 4.3.1 Classification of Worms

What makes rootkits particularly dangerous is their ability to evade detection. Traditional antivirus software may not easily identify them because they manipulate system processes to conceal their existence. This means a system could be compromised for a long time without any visible signs.

Reflect on this idea: is a threat more dangerous when it is visible or when it is hidden? Rootkits demonstrate that hidden threats can be more harmful because they operate silently over extended periods.

1. Firmware Rootkits

These rootkits infect the firmware of a device, such as the BIOS or hardware components. They operate at a very deep level, making them difficult to detect and remove. They can even affect devices like routers or hard drives.

2. Bootloader Rootkits

Bootloader rootkits attack the system startup process by replacing the original bootloader with a malicious one. Since they activate before the operating system loads, they are hard to detect using standard security tools.

3. Memory Rootkits

Memory rootkits reside in the system's RAM. They are temporary and usually disappear when the system is restarted, but they can perform harmful activities while active and reduce system performance.

SGOU

4. Application Rootkits

These rootkits replace or modify legitimate application files. When users run common programs, the rootkit gets activated, allowing attackers to gain access without the user's knowledge.

5. Kernel Mode Rootkits

Kernel mode rootkits target the core part of the operating system. They provide deep control over the system, allowing attackers to manipulate system functions, steal data, or hide other malware. These are among the most dangerous and complex types of rootkits.

4.3.2.4 Web Scripting Viruses

Web scripting viruses are associated with web technologies and often exploit vulnerabilities in websites or browsers. These viruses typically use scripts written in languages such as JavaScript to execute malicious actions when a user visits a compromised webpage.

One common example is cross-site scripting (XSS), where malicious scripts are injected into trusted websites. When users access these sites, the script runs in their browser, potentially stealing data such as login credentials or session information.

Web scripting viruses are generally classified into two major types: persistent attacks and non-persistent attacks. Although both are harmful, they operate in different ways and affect users differently. Let us understand each type in a simple manner.

1. Persistent attacks, also known as stored attacks, occur when malicious code is permanently stored on a website's server, such as in a database, comment section, or forum post. Whenever a user visits the infected webpage, the harmful script automatically runs in the browser. In this way, the attacker can repeatedly target many users over a long period of time.

You can imagine this as a hidden trap placed inside a webpage. Every visitor who opens that page unknowingly activates the malicious script. One common activity in persistent attacks is cookie theft. Here, attackers steal browser cookies that may contain login information or session details. Using this information, attackers may pretend to be the actual user and gain unauthorized access to accounts.

Another dangerous activity is session hijacking. In this case, attackers capture session tokens or authentication details to take control of an active user session. Once the session is hijacked, the attacker can perform actions as the legitimate user, such as sending messages, changing account settings, or making unauthorized transactions. Since the malicious code remains stored on the server, persistent attacks can continue affecting every visitor until the infected content is removed.

2. Non-persistent attacks, also known as reflected attacks, occur when malicious code is not permanently stored on a website's server. Instead, the harmful script is included in a URL, search box, or form submission and becomes active only when the user clicks

SGOU

the infected link or submits the form. Because of this, the attack exists only for a short period and depends completely on user interaction.

In simple terms, the attacker creates a malicious link and tricks users into opening it. Once the victim clicks the link, the script immediately executes in the user's browser. These attacks are commonly used in phishing schemes, where attackers send fake emails or messages that appear genuine in order to attract users.

One important feature of non-persistent attacks is immediate execution. The malicious code works only at the moment the user accesses the link or submits the form. Unlike persistent attacks, the harmful script is not saved on the server, so it does not continue affecting future visitors to the website.

Another characteristic is that attackers do not need detailed knowledge about a particular user. They can simply distribute the malicious link to a large number of people through emails, social media, or messaging platforms, hoping that some users will click it without suspicion.

Although non-persistent attacks last for a shorter time compared to persistent attacks, they can still be very dangerous. They may steal sensitive information, interrupt active user sessions, or redirect users to fake websites designed to collect passwords and personal data.

The study of computer viruses and their types is not just about understanding threats, but about developing a mindset of caution and awareness in the digital world. As technology continues to evolve, so do the methods used by attackers. Therefore, continuous learning and vigilance are necessary.

The concepts of ransomware, worms, rootkits, and web scripting viruses provide a strong foundation for understanding modern cybersecurity challenges. With this knowledge, one is better prepared to use technology safely and responsibly.

SGOU

Recap

- A computer virus is a malicious program that spreads and damages systems or data.
- Viruses usually attach themselves to executable files or programs.
- Malware is a general term for all harmful software.
- Ransomware locks or encrypts files and demands payment for recovery.
- The AIDS Trojan was one of the earliest known ransomware attacks.
- Scareware creates fake warnings to frighten users.
- Screen lockers block access to the computer screen.

- Crypto ransomware encrypts files and is highly dangerous.
- Paying ransom does not guarantee file recovery.
- Ransomware often spreads through emails, downloads, and malicious links.
- Regular backups are important for ransomware recovery.
- Employee awareness helps reduce cyberattack risks.
- Honeypots are trap systems used to detect attackers.
- Antivirus and email filtering help prevent malware infections.
- Worms are standalone malware that spread without user action.
- Worms spread rapidly through networks and vulnerable systems.
- Viruses require user interaction, but worms spread automatically.
- Email worms spread through infected attachments or links.
- Network worms exploit security vulnerabilities in systems.
- File sharing and downloads can spread worms.
- Social media and messaging apps are common worm distribution channels.
- Rootkits hide inside systems and remain difficult to detect.
- Rootkits provide attackers with unauthorized remote access.
- Kernel mode rootkits target the core of the operating system.
- Firmware rootkits infect BIOS or hardware-level components.
- Memory rootkits operate temporarily in RAM.
- Web scripting viruses exploit browser and website vulnerabilities.
- Cross Site Scripting (XSS) injects malicious scripts into webpages.
- Persistent attacks store malicious scripts on servers.
- Persistent attacks affect every visitor to an infected webpage.
- Cookie theft steals browser session information.
- Session hijacking allows attackers to control active user sessions.
- Non persistent attacks use malicious links or forms.
- Reflected attacks become active only when users interact with them.
- Phishing attacks often use non persistent scripting attacks.
- Safe browsing habits reduce the risk of infection.
- Strong cybersecurity awareness is essential for all users.

SGOU

Objective Type Questions

1. What is the general term for harmful software?
2. Which type of malware encrypts files and demands payment?
3. What was the name of the first known ransomware attack?
4. Which ransomware type displays fake security warnings?
5. Which ransomware type locks the user's screen?
6. Which malware spreads without requiring a host file?
7. Which malware hides itself to avoid detection?
8. Which type of rootkit targets the operating system kernel?
9. Which rootkit infects BIOS or hardware firmware?
10. Which scripting attack stores malicious code on the server?
11. Which scripting attack becomes active only after clicking a link?
12. Which web attack injects malicious scripts into trusted websites?
13. What is stolen during cookie theft?
14. What is the process of taking control of a user session called?
15. Which technique uses fake systems to attract attackers?
16. Which worm spread through email attachments with a love message?
17. Which worm targeted web servers globally?
18. Which security method blocks suspicious emails?
19. Which type of ransomware uses encryption techniques?
20. Which malware category includes viruses, worms, and rootkits?

SGOU

Answers to Objective Type Questions

1. Malware
2. Ransomware
3. AIDS Trojan

4. Scareware
5. Screen Locker
6. Worm
7. Rootkit
8. Kernel Mode Rootkit
9. Firmware Rootkit
10. Persistent Attack
11. Non Persistent Attack
12. Cross Site Scripting
13. Cookies
14. Session Hijacking
15. Honeypot
16. ILOVEYOU
17. Code Red
18. Email Filtering
19. Crypto Ransomware
20. Malware

Assignments

1. Explain the concept of computer viruses and discuss the different categories of malware with suitable examples.
2. Describe the working of ransomware and explain its different types along with methods of prevention and recovery.
3. Discuss the characteristics, classification, and impact of worms, rootkits, and web scripting viruses in modern computer systems.
4. Analyze the differences between persistent and non persistent web scripting attacks in terms of operation, impact, and security risks.
5. Compare viruses, worms, and rootkits by analyzing their methods of spreading, system impact, and detection challenges.

SGOU

Suggested Reading

1. Bosworth, S., Kabay, M. E., & Whyne, E. (2014). *Computer security handbook* (6th ed.). Wiley.

2. Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). *Firewalls and internet security: Repelling the wily hacker* (2nd ed.). Addison Wesley.

3. Grimes, R. A. (2017). *Hacking the hacker: Learn from the experts who take down hackers*. Wiley.

4. Nicol, D. M., Sanders, W. H., & Trivedi, K. S. (2004). *Model based evaluation: From dependability to security*. IEEE Press.

5. Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.

Reference

1. Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.

2. Sikorski, M., & Honig, A. (2012). *Practical malware analysis: The hands on guide to dissecting malicious software*. No Starch Press.

3. Scarfone, K., & Mell, P. (2007). *Guide to malware incident prevention and handling for desktops and laptops*. National Institute of Standards and Technology.

4. Skoudis, E., & Zeltser, L. (2004). *Malware: Fighting malicious code*. Prentice Hall.

5. Vacca, J. R. (2017). *Computer and information security handbook* (3rd ed.). Elsevier.

SGOU



Cyber Criminal Syndicates and Nation-State Groups

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- explain the structure and operation of cybercriminal syndicates
- describe the characteristics of nation state cyber groups and attacks
- discuss the financial, political, and strategic motivations behind cyberattacks
- summarize the tools and techniques used by organized cybercrime groups

Prerequisites

Every day, millions of people use digital systems for communication, banking, education, shopping, entertainment, and business activities. Most users focus only on the convenience provided by technology and rarely think about the hidden threats operating behind the screens. However, cyberattacks occurring around the world show that digital systems are constantly targeted by highly organized groups working silently through networks and the internet.

News reports often mention incidents where hospitals lose access to patient records, companies suffer massive financial losses, government websites stop functioning, or confidential information gets leaked online. These incidents are not always caused by a single individual acting alone. In many cases, they are carried out by organized cybercriminal syndicates or nation state cyber groups with advanced technical skills, financial resources, and carefully planned strategies.

One interesting question naturally arises here. How do these groups manage to attack powerful organizations and government systems from distant locations? The answer lies in the organized nature of modern cybercrime. Today's cybercriminal groups often operate like professional companies. Different individuals handle different tasks such as developing malware, stealing credentials, managing illegal payments, creating fake websites, or maintaining secret communication systems. Some groups are motivated by money, while others work to achieve political, military, or strategic goals.

As technology continues to expand, cyber threats are also becoming more advanced and difficult to detect. Attackers use sophisticated tools, phishing techniques, ransomware,

SGOU

botnets, and social engineering methods to exploit both technical weaknesses and human behavior. This makes cybersecurity not only a technical challenge but also a social and strategic issue.

Understanding cybercriminal syndicates and nation state groups is important because it helps learners recognize how modern cyberattacks are organized, why they occur, and how digital systems can be protected. It also creates awareness about the motivations, strategies, and techniques used by attackers in the cyber world.

This topic offers an opportunity to explore the hidden structure of organized cybercrime and understand how cyber warfare and digital attacks are shaping the modern world. Let us now begin the study of cybercriminal syndicates and nation state groups in detail.

Key concepts

Cybercriminal Syndicates, Nation State Groups, Ransomware, Cyber Espionage, Botnets, Phishing, Social Engineering, Advanced Persistent Threats

Discussion

4.4.1 Introduction

A few decades ago, crimes were usually associated with physical actions such as robbery, theft, smuggling, or fraud carried out in the real world. Criminal groups operated in streets, markets, borders, and hidden locations. Today, however, the world has changed dramatically. Modern societies depend heavily on computers, networks, cloud systems, smartphones, digital banking, online communication, and interconnected infrastructures. As technology has evolved, crime has also evolved. Criminals no longer need to physically enter a bank to steal money. A single malicious program or carefully planned cyberattack can target organizations located thousands of kilometers away.

This transformation has given rise to organized cybercriminal syndicates and nation state cyber groups. These groups operate with planning, coordination, technical expertise, and financial resources. Some attack systems for financial profit, while others work to achieve political, military, or strategic objectives. Their operations affect governments, businesses, hospitals, educational institutions, financial organizations, and even ordinary individuals.

Think about this situation carefully. When a large company suddenly loses access to its systems because of ransomware, who is actually behind the attack? Is it a single hacker working alone in a dark room? In most cases, the answer is no. Modern cyberattacks are often conducted by highly organized groups where different individuals perform different responsibilities. Some create malicious software, some steal credentials, some manage financial transactions, while others handle negotiations with victims. Cybercrime has become an organized industry.

SGOU

Understanding these cybercriminal syndicates and nation state groups is important because cybersecurity is no longer only about protecting computers. It is also about understanding the people, motives, structures, and strategies behind attacks. Once we understand how attackers think and operate, we become better prepared to defend digital systems.

In this chapter, we will explore the structure and operation of cybercriminal syndicates, understand the motivations behind cyberattacks, and examine the tools and techniques used by organized cybercrime groups.

4.4.2 Understanding Cybercriminal Syndicates

A cybercriminal syndicate is an organized group of individuals involved in cybercrime activities. Unlike isolated hackers who may attack systems individually, syndicates operate in a coordinated and systematic manner. These groups may consist of programmers, network specialists, social engineering experts, money launderers, and negotiators working together toward common goals.

Cybercriminal syndicates often resemble legitimate business organizations. They may have leadership structures, division of responsibilities, technical support teams, financial departments, recruitment processes, and communication systems. Some even provide customer support for victims who pay ransom amounts.

At first, this may sound surprising. How can criminals operate like companies? Yet many modern cybercrime groups function exactly this way. Their operations are carefully planned, and many attacks are executed with professional efficiency.

Consider ransomware attacks. In several cases, attackers not only encrypt the victim's files but also provide detailed payment instructions and communication channels. Some groups even maintain help desks to guide victims through cryptocurrency payments. This demonstrates how cybercrime has become highly organized.

Cybercriminal syndicates usually operate across international borders. Members may live in different countries and communicate through encrypted platforms, anonymous networks, and dark web services. Because of this global nature, identifying and prosecuting cybercriminals becomes extremely difficult.

One important question arises here. Why do people join such syndicates? The answer varies. Some are attracted by financial rewards, others by power or influence, and some by ideological beliefs. In many cases, skilled programmers are recruited because cybercrime organizations offer large financial incentives.

4.4.3 Evolution of Organized Cybercrime

Cybercrime in its early stages was relatively simple. Early hackers often attacked systems to demonstrate technical skills, gain recognition, or satisfy curiosity. However, as the internet expanded and digital transactions increased, cybercriminals realized the enormous financial opportunities available online.

During the early days of the internet, attacks mainly focused on website defacement, spreading simple viruses, or disrupting systems. Over time, cybercrime evolved into

SGOU

a profitable business model. Today, cybercriminal syndicates target online banking systems, cryptocurrency platforms, healthcare databases, government networks, and multinational corporations.

The development of underground cybercrime markets accelerated this growth. The dark web became a marketplace where attackers could buy and sell stolen data, malware kits, hacking tools, and illegal services.

For example, instead of creating malware themselves, attackers can purchase ready made ransomware packages. This model is commonly called Ransomware as a Service. Here, experienced developers create ransomware tools and rent them to affiliates who carry out attacks. The profits are then shared between the developers and attackers.

This business style approach has significantly lowered the barrier for cybercrime. Individuals with limited technical knowledge can now launch sophisticated attacks using tools purchased online.

Another major development is the use of cryptocurrencies. Digital currencies allow cybercriminals to receive payments with a higher level of anonymity compared to traditional banking systems. This has encouraged the growth of ransomware operations and illegal online transactions.

As cybercrime evolved, governments also began recognizing cyberspace as an important domain of national security. This eventually led to the rise of nation state cyber groups.

4.4.4 Structure of Cybercriminal Syndicates

Cybercriminal syndicates are rarely random collections of attackers. Most successful syndicates operate with clear organizational structures. Each member performs specialized tasks that contribute to the overall operation.

1. Leadership and Coordination

At the top of the syndicate is usually a leadership group responsible for planning operations, selecting targets, managing finances, and coordinating activities. These leaders may not directly participate in attacks but instead supervise the overall organization.

The leadership decides which sectors to target. For instance, hospitals may be targeted because they rely heavily on immediate access to patient records. Financial organizations may be targeted because they handle sensitive financial data.

Leaders also determine attack strategies, allocate resources, and negotiate partnerships with other cybercriminal groups.

2. Malware Developers

Another important component of cybercriminal syndicates is the malware development team. These individuals design malicious software such as ransomware, spyware, keyloggers, trojans, worms, and botnet programs.

Developers continuously improve malware to bypass antivirus software and security

SGOU

systems. They study vulnerabilities in operating systems and applications to create more effective attacks.

Sometimes developers sell malware tools to other criminals through underground markets. This creates an entire economy around malicious software.

3. Social Engineering Specialists

Technical attacks alone are not always sufficient. Human behavior often becomes the weakest point in cybersecurity. This is where social engineering specialists play an important role.

These individuals create phishing emails, fake websites, fraudulent messages, and deceptive communication designed to trick victims into revealing sensitive information.

For example, a victim may receive an email appearing to come from a bank asking for password verification. Once the victim enters the credentials, attackers capture the information.

Social engineering attacks are highly successful because they exploit trust, fear, urgency, and curiosity.

4. Money Launderers

Cybercriminal syndicates also require financial specialists who manage stolen funds. Since illegally obtained money cannot easily be transferred through regular financial systems, money laundering techniques are used.

Money launderers may use cryptocurrency exchanges, fake accounts, shell companies, or online payment services to hide the origin of stolen funds.

This process makes it difficult for law enforcement agencies to trace financial transactions.

5. Infrastructure Managers

Some members specialize in maintaining technical infrastructure such as command and control servers, botnets, anonymous communication systems, and dark web platforms.

These individuals ensure that cybercriminal operations remain functional and hidden from investigators.

4.4.5 Nation State Cyber Groups

Unlike financially motivated cybercriminal syndicates, nation state cyber groups are generally linked to governments or national intelligence agencies. Their objectives often include espionage, surveillance, political influence, military advantage, or disruption of critical infrastructure.

Nation state cyber groups are among the most advanced cyber threat actors in the world. They usually possess significant financial resources, technical expertise, intelligence support, and long term strategic goals.

SGOU

One interesting point to consider is that cyber warfare has become an important component of modern international relations. Countries no longer rely only on traditional military power. Cyber capabilities are now considered essential for national defense and intelligence gathering.

Nation state cyber groups may target government systems, military networks, energy infrastructure, transportation systems, communication networks, research institutions, and technology companies.

In some cases, the goal is not immediate destruction but long term espionage. Attackers may remain hidden within systems for months or even years, silently collecting sensitive information.

4.4.5.1 Characteristics of Nation State Attacks

Nation state cyberattacks often differ from ordinary cybercrime in several ways.

1. Advanced Planning

These attacks are usually carefully planned over long periods. Attackers conduct extensive reconnaissance before launching operations.

They study the target's infrastructure, employee behavior, software vulnerabilities, and communication systems.

2. Advanced Persistent Threats

Nation state groups frequently use Advanced Persistent Threats, commonly called APTs. An APT is a long term cyberattack in which attackers gain unauthorized access to a network and remain undetected for an extended period.

Unlike ordinary attacks that aim for quick financial gain, APTs focus on continuous monitoring and data collection.

3. Use of Zero Day Vulnerabilities

Nation state groups often use zero day vulnerabilities. These are software flaws unknown to the software vendor or security community.

Since no security patches are available initially, zero day vulnerabilities provide attackers with powerful opportunities to infiltrate systems.

4. Stealth and Persistence

Nation state groups prioritize stealth. Their goal is often to remain undetected while collecting intelligence.

To achieve this, they use encryption, hidden communication channels, rootkits, and sophisticated malware.

4.4.6 Motivations Behind Cyberattacks

Understanding the motivations behind cyberattacks is essential because motives influence attack methods, target selection, and operational strategies.

SGOU

Cybercriminal syndicates and nation state groups may appear similar from a technical perspective, but their objectives often differ significantly.

4.4.6.1 Financial Motivations

Financial gain is the primary motivation for many cybercriminal syndicates.

Ransomware Attacks

Ransomware attacks generate enormous profits for attackers. Victims may include hospitals, schools, businesses, or government offices.

Since organizations rely heavily on digital systems, they may feel pressured to pay ransom amounts quickly.

Banking and Financial Fraud

Cybercriminals target banking systems, payment gateways, and online financial platforms to steal money directly. They may use phishing attacks, credential theft, or malware to gain unauthorized access.

Sale of Stolen Data

Personal data has become highly valuable in underground markets. Cybercriminals steal credit card details, passwords, social security numbers, medical records, and corporate information.

This stolen data can be sold to other criminals for identity theft or fraud.

Cryptojacking

Some attackers secretly use victims' computing resources to mine cryptocurrency. This process, known as cryptojacking, consumes system performance and electricity while benefiting attackers financially.

4.4.6.2 Political and Strategic Motivations

Nation state groups are often driven by political or strategic goals rather than direct financial profit.

Cyber Espionage

Governments seek sensitive intelligence related to defense, diplomacy, technology, economics, and national security. Cyber espionage allows countries to gather information without physical infiltration.

Political Influence

Cyber operations may attempt to influence elections, public opinion, or political stability. Attackers may spread misinformation, manipulate social media discussions, or leak confidential information.

Disruption of Critical Infrastructure

Critical infrastructure includes power grids, transportation systems, communication

SGOU

networks, healthcare services, and water supply systems. Disrupting such systems can create national level instability.

Military Advantage

Cyber capabilities are increasingly integrated into military strategies. Countries may use cyberattacks to weaken enemy communication systems, surveillance systems, or defense infrastructure.

4.4.6.3 Comparing Financial and Strategic Motivations

It is important to distinguish between financially motivated attacks and strategically motivated attacks.

Financially motivated attackers usually focus on rapid profits. Their attacks may target large numbers of victims and aim for quick returns.

Strategically motivated attackers, however, may focus on long term objectives. They often invest significant time and resources into maintaining hidden access to systems.

Another difference lies in target selection. Financial attackers frequently target businesses or individuals with monetary value, while nation state groups may target government agencies, research laboratories, military institutions, and strategic industries.

Understanding these differences helps cybersecurity professionals develop appropriate defense strategies.

4.4.7 Tools used by Organized Cybercrime Groups

Organized cybercrime groups and nation-state actors use specialized tools to conduct attacks on a large scale. These tools help them automate attacks, compromise multiple systems, steal information, and maintain long-term access.

Malware Kits

Organized groups may use malware kits that combine different malicious capabilities, such as ransomware, spyware, trojans, and botnet components. These kits allow attackers to conduct attacks more efficiently and may be customized for specific targets. Criminal groups may also purchase or rent such tools through underground marketplaces.

Exploit Kits

Exploit kits help attackers identify and exploit known vulnerabilities in targeted systems. Organized groups can use them to automate the delivery of malware to many vulnerable devices, reducing the effort required to compromise large numbers of victims.

Botnets

Organized groups may control large botnets containing thousands or even millions of compromised devices. Criminal groups can use these networks for activities such as large-scale DDoS attacks, spam campaigns, credential theft, and malware distribution. Nation-state actors may also use botnets or similar networks to support large-scale geopolitical or disruptive operations. Because the infected devices are controlled

SGOU

remotely, their owners may not realize that their systems are being used in an attack.

Phishing Toolkits

Organized groups use phishing toolkits to conduct large-scale campaigns that imitate trusted organizations and services. These toolkits can make it easier to create convincing fake login pages and communications, allowing attackers to target many victims and collect credentials or other sensitive information.

Keyloggers

Organized attackers may deploy keyloggers as part of broader campaigns to secretly collect credentials, financial information, or other sensitive data. Rather than using them as isolated tools, cybercrime groups may combine keyloggers with other malware to maintain access to compromised systems and transfer stolen information to attacker-controlled servers.

4.4.8 Techniques used by Organized Cybercrime Groups

Organized cybercrime groups use various techniques to manipulate people, gain unauthorized access, and steal sensitive information. Social engineering is a broad approach that exploits human behavior, trust, and emotions rather than only technical weaknesses.

Social Engineering

Social engineering involves manipulating victims by creating fear, urgency, trust, curiosity, or other emotional responses. Attackers use these psychological techniques to persuade victims to reveal information, click links, open attachments, or perform actions that compromise security.

Phishing

Phishing is a common social engineering technique in which attackers send fraudulent emails, messages, or other communications that appear to come from trusted sources. Victims may be directed to fake websites where their credentials or other sensitive information are collected.

Spear Phishing

Spear phishing is a targeted form of phishing. Instead of sending the same message to many people, attackers research specific individuals or organizations and create personalized messages to make the communication appear more genuine. This personalization can increase the likelihood that the victim will respond or disclose sensitive information.

Thus, social engineering is the broader concept, phishing is a common social engineering technique, and spear phishing is a targeted form of phishing.

The rise of cybercriminal syndicates and nation state cyber groups has transformed cybersecurity into one of the most important challenges of the digital age.

These groups operate with sophisticated structures, advanced tools, strategic planning,

SGOU

and global coordination. Some seek financial profit through ransomware, phishing, and fraud, while others pursue political, military, or strategic objectives.

Understanding the structure and operation of these groups helps learners recognize that cyberattacks are rarely random events. Behind many incidents are organized networks of individuals with specialized roles and carefully planned objectives.

The tools and techniques used by organized cybercrime groups continue to evolve rapidly. Malware kits, phishing campaigns, botnets, exploit kits, and social engineering attacks demonstrate the complexity of modern cyber threats.

At the same time, cybersecurity defenses must also evolve. Technical protection alone is not enough. Awareness, responsible behavior, international cooperation, ethical practices, and continuous learning are equally important.

As technology becomes increasingly integrated into daily life, the importance of cybersecurity will continue to grow. Understanding cybercriminal syndicates and nation state groups is therefore not only relevant for cybersecurity professionals but for everyone who uses digital technology in the modern world.

Recap

- Cybercriminal syndicates are organized groups involved in cybercrime activities.
- Modern cybercrime often operates like a professional business organization.
- Cybercriminal groups may include programmers, hackers, negotiators, and money launderers.
- Many cybercriminal syndicates operate across international borders.
- The dark web supports illegal cybercrime markets and services.
- Ransomware as a Service allows attackers to rent ransomware tools.
- Cryptocurrencies help cybercriminals perform anonymous financial transactions.
- Nation state cyber groups are usually linked to governments or intelligence agencies.
- Nation state attacks often focus on espionage and strategic objectives.
- Cyber warfare has become an important part of national security.
- Advanced Persistent Threats remain hidden in systems for long periods.
- Zero day vulnerabilities are unknown software weaknesses exploited by attackers.
- Stealth techniques help attackers avoid detection during cyber operations.

SGOU

- Financial gain is a major motivation behind organized cybercrime.
- Ransomware attacks target organizations that depend heavily on digital systems.
- Cybercriminals steal personal and financial information for illegal profit.
- Cryptojacking secretly uses victim systems for cryptocurrency mining.
- Political cyberattacks may attempt to influence elections and public opinion.
- Critical infrastructure includes power grids, healthcare systems, and communication networks.
- Nation state groups may target military and research organizations.
- Malware kits contain ready made malicious software tools.
- Exploit kits automatically identify and attack software vulnerabilities.
- Botnets are networks of infected devices controlled remotely by attackers.
- Phishing toolkits create fake websites and fraudulent login pages.
- Keyloggers secretly record keyboard activity and passwords.
- Social engineering attacks exploit human emotions and trust.
- Phishing attacks use fake emails and messages to steal information.
- Spear phishing targets specific individuals or organizations.
- Distributed Denial of Service attacks overload systems with traffic.
- Credential stuffing uses stolen passwords to access multiple accounts.
- Supply chain attacks compromise trusted software providers or vendors.
- Cybercriminals use anonymous communication and encrypted platforms.
- Law enforcement faces challenges because cybercrime crosses national borders.
- Multi factor authentication improves account security.
- Regular software updates reduce security vulnerabilities.
- Employee awareness is an important defense against cyberattacks.
- Regular backups help recover data after ransomware attacks.
- Cybersecurity requires both technical protection and responsible behavior.
- Continuous learning is essential because cyber threats constantly evolve.

SGOU

Objective Type Questions

1. What is an organized group involved in cybercrime called?
2. Which hidden part of the internet supports illegal cybercrime markets?
3. What type of malware locks files and demands payment?
4. Which model allows attackers to rent ransomware tools?
5. Which digital currency is commonly used in cybercrime transactions?
6. What are government linked cyberattack groups called?
7. What is the long term hidden cyberattack strategy used by nation state groups called?
8. What type of vulnerability is unknown to software vendors?
9. What technique manipulates human emotions to steal information?
10. What is a network of infected devices controlled remotely called?
11. Which toolkit creates fake websites and login pages?
12. What software secretly records keyboard activity?
13. What attack method uses fake emails to steal credentials?
14. What phishing technique targets specific individuals?
15. What attack overwhelms systems with excessive traffic?
16. What process secretly uses systems for cryptocurrency mining?
17. What term refers to secret information gathering by governments?
18. What type of malware collection contains ready made malicious tools?

SGOU

Answers to Objective Type Questions

1. Syndicate
2. Dark Web
3. Ransomware
4. RaaS

5. Cryptocurrency
6. Nation State Groups
7. APT
8. Zero Day Vulnerability
9. Social Engineering
10. Botnet
11. Phishing Toolkit
12. Keylogger
13. Phishing
14. Spear Phishing
15. DDoS
16. Cryptojacking
17. Espionage
18. Malware Kit

Assignments

1. Explain the structure and functioning of cybercriminal syndicates and discuss the roles performed by different members within these groups.
2. Describe the characteristics of nation state cyber groups and explain how their objectives differ from financially motivated cybercriminal organizations.
3. Discuss the various tools and techniques used by organized cybercrime groups to conduct cyberattacks on individuals and organizations.
4. Analyze the differences between financial motivations and political or strategic motivations behind cyberattacks with suitable examples.
5. Compare phishing, spear phishing, and social engineering attacks by analyzing their methods, targets, and impact on cybersecurity.

SGOU

Suggested Reading

1. Andress, J., & Winterfeld, S. (2013). *Cyber warfare: Techniques, tactics and tools for security practitioners* (2nd ed.). Elsevier.

2. Clough, J. (2015). *Principles of cybercrime* (2nd ed.). Cambridge University Press.

3. Goodman, M. (2015). *Future crimes: Everything is connected, everyone is vulnerable and what we can do about it*. Anchor Books.

4. Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

5. Shinder, D. L., & Tittel, E. (2002). *Scene of the cybercrime: Computer forensics handbook*. Syngress Publishing.

Reference

1. Furnell, S. (2021). *Cybersecurity*. Oxford University Press.

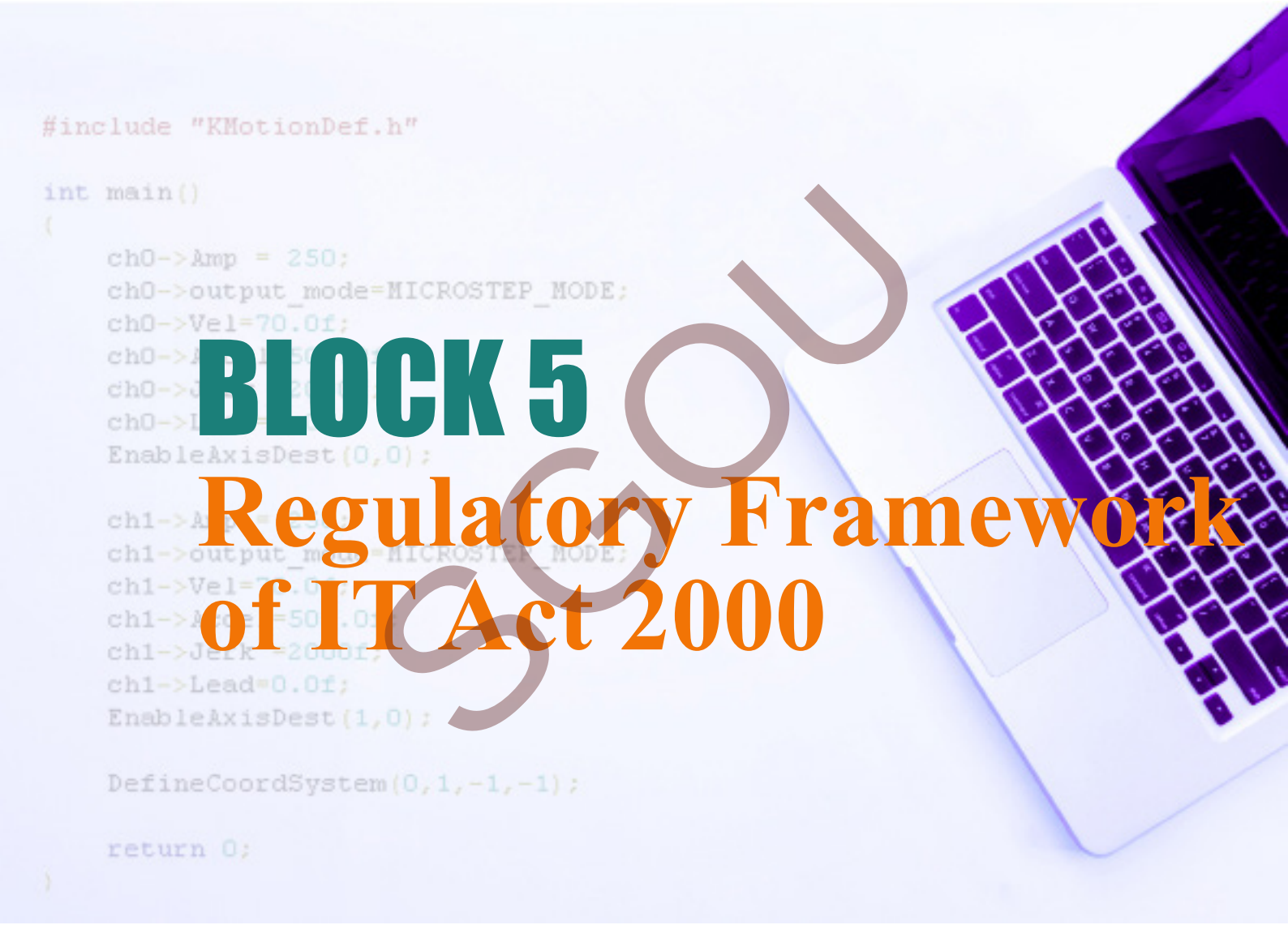
2. Holt, T. J., Bossler, A. M., & Seigfried Spellar, K. C. (2018). *Cybercrime and digital forensics: An introduction*. Routledge.

3. Kshetri, N. (2010). *The global cybercrime industry: Economic, institutional and strategic perspectives*. Springer.

4. Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

5. Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (3rd ed.). Sage Publications.

SGOU



BLOCK 5

Regulatory Framework of IT Act 2000

SGOU



UNIT 1 Legal Framework

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- familiarize the key concepts of the Information Technology Act, 2000 and its role in regulating digital activities
- describe the process of Digital Signature and E-Signature with suitable examples
- apply the concept of digital signatures in real-life scenarios such as online transactions and e-governance services
- analyze the differences between Digital Signature and E-Signature in terms of security, usage, and technology

Prerequisites

In today's world, most activities are done using computers and the internet. People use online systems for banking, shopping, communication, education, and government services. Because of this, it is very important to have proper laws to control and protect these digital activities. The IT Act, 2000 provides legal recognition to electronic records and digital signatures, making online transactions safe and valid. It also helps to prevent cyber crimes like hacking, fraud, and identity theft, which are increasing in the digital age.

This topic is important for learners because it helps them understand how to use technology in a safe and responsible way. It creates awareness about cyber security and legal rights in the digital world. It also prepares learners to use e-governance services confidently, such as online applications, tax filing, and digital payments. In a rapidly growing digital society like India, this knowledge is essential for both personal use and professional growth.

Keywords

Information Technology Act, 2000, Digital Signature, Electronic Signature (E-Signature), Cyber Law, Hash Function, Public Key Infrastructure (PKI), Cyber Crime, Digital Certificate

SGOU

Discussion

5.1.1 Introduction

In the present digital age, computers and the internet have become an essential part of daily life. Activities such as communication, banking, education, shopping, and governance are increasingly carried out in electronic form. However, traditional laws were designed mainly for paper-based transactions and were not suitable for dealing with electronic records and cyber-related issues. This created the need for a legal framework to regulate digital activities and ensure security in cyberspace.

To address these challenges, the Government of India enacted the Information Technology Act, 2000 (IT Act, 2000). This Act provides legal recognition to electronic records and digital signatures and establishes rules for secure electronic transactions. It also defines various cyber crimes and prescribes punishments for them, thereby promoting trust in digital systems.

Role of IT Act in e-governance and Digital India

- Provides legal support for e-governance services
- Enables online tax filing and digital records
- Supports e-tendering and online applications
- Promotes paperless administration
- Builds trust in digital systems
- Encourages secure online transactions

5.1.2 Information Technology Act, 2000

The legal foundation for e-governance is provided mainly through Chapter III of the Information Technology Act, 2000. Section 4 gives legal recognition to electronic records, Section 5 gives legal recognition to electronic signatures, Section 6 provides for the use of electronic records and electronic signatures in Government and its agencies, Section 7 deals with retention of electronic records, and Section 8 provides for publication of rules, regulations, orders, notifications and other matters in the Electronic Gazette. Section 6A also provides for delivery of services through service providers, supporting digital service-delivery models.

The Information Technology Act, 2000 is the primary law in India that governs cyber activities and electronic transactions. It came into force to give legal recognition to electronic records and digital signatures, thereby facilitating the growth of e-commerce and e-governance.

The Act applies to the whole of India. Under Section 75 of the Information Technology Act, 2000, it also applies to an offence or contravention committed outside India by any person, irrespective of nationality, if the act involves a computer, computer system or computer network located in India. It covers a wide range of areas including electronic records, digital authentication, cyber crimes, and the regulation of certifying authorities.

SGOU

One of the most significant contributions of the IT Act is the legal recognition of electronic records. Earlier, only paper-based documents were considered valid in legal proceedings. However, with this Act, electronic documents such as emails, digital contracts, and online transactions gained the same legal status as traditional documents.

Another important feature of the Act is the recognition of digital signatures as a valid method of authentication. This enabled individuals and organizations to securely sign electronic documents, ensuring authenticity and integrity.

The Act also promotes e-governance by allowing government departments to accept electronic filings, issue digital certificates, and maintain records in digital form. Services such as online tax filing, digital land records, and e-tendering are possible because of this legal support.

To regulate the use of digital signatures, the Act established the Controller of Certifying Authorities (CCA). The CCA supervises and licenses Certifying Authorities, which are responsible for issuing Digital Signature Certificates (DSCs) to users after verifying their identity.

The Information Technology (Amendment) Act, 2008 further strengthened the legal framework by introducing new concepts and provisions. One of the major additions was the recognition of electronic signatures (e-signatures) as an alternative to digital signatures.

The amendment also introduced stricter provisions related to data protection, privacy, identity theft, and cyber terrorism. It expanded the scope of cyber offences and increased penalties for various crimes committed in cyberspace.

5.1.2.1 Objectives of the IT Act, 2000

The main objectives of the Act are:

- To provide legal recognition for electronic records and digital signatures
- To facilitate electronic governance (e-Governance)
- To promote e-commerce and online transactions
- To prevent and control cyber crimes
- To ensure security and confidentiality of digital data

5.1.2.2 Cyber Offences under IT Act, 2000

- Unauthorized access (Hacking)
- Identity theft (misuse of personal data)
- Cyber fraud (online cheating, scams)
- Data theft
- Publishing obscene or harmful content

SGOU

- Cyber terrorism (threat to national security)
- Email spoofing and phishing

5.1.2.3 Penalties and Punishments

The Information Technology Act, 2000 provides different forms of liability and punishment depending on the nature of the offence. Some provisions provide for compensation or monetary penalties, while specified criminal offences provide for imprisonment, fine, or both.

The penalty framework has also changed over time. The Jan Vishwas (Amendment of Provisions) Act, 2023 amended several provisions of the IT Act with effect from 30 November 2023. Among other changes, it removed Section 66A and converted certain offences, including Section 72A, from imprisonment-based punishment to monetary penalties.

Therefore, learners should not treat the penalty framework as a simple rule that all minor offences receive only fines and all serious offences receive imprisonment. The applicable section, the facts of the case, and subsequent amendments must be considered when determining the current legal consequence.

- Imprisonment for serious crimes
- Strict punishment for cyber terrorism

5.1.3 Digital Signature (Section 3 of the IT Act)

A digital signature is a secure and reliable method used to authenticate electronic documents. It is based on cryptographic techniques and ensures that the message has not been altered during transmission and that it originates from a verified sender.

5.1.3.1 How Digital Signatures Work

When the IT Act was originally passed in 2000, it specifically recognized Digital Signatures as the sole method to authenticate an electronic record.

The IT Act mandates that Digital Signatures must use an Asymmetric Cryptosystem and a Hash Function.

- Asymmetric Cryptosystem: This involves a secure pair of keys: a Private Key and a Public Key.
    - The Private Key is kept secret by the signer and is used to create the digital signature.
    - The Public Key is shared openly and is used by the receiver to verify the signature.
- Hash Function: An algorithm that converts the document into a fixed-length string of characters (a hash value). If even a single comma in the document is changed, the hash value changes entirely, immediately alerting the receiver that the document was tampered with.

SGOU

The working of a digital signature involves a series of steps. Initially, a message or document is created by the sender. This message is then processed using a hash function, which converts it into a fixed-length code known as a hash value. The hash value is then processed using the sender's private key, creating the digital signature. This signature is attached to the message and sent to the receiver.

Upon receiving the message, the receiver decrypts the digital signature using the sender's public key to retrieve the original hash value. The receiver also generates a new hash value from the received message and compares it with the decrypted hash. If both values match, the authenticity and integrity of the message are confirmed.

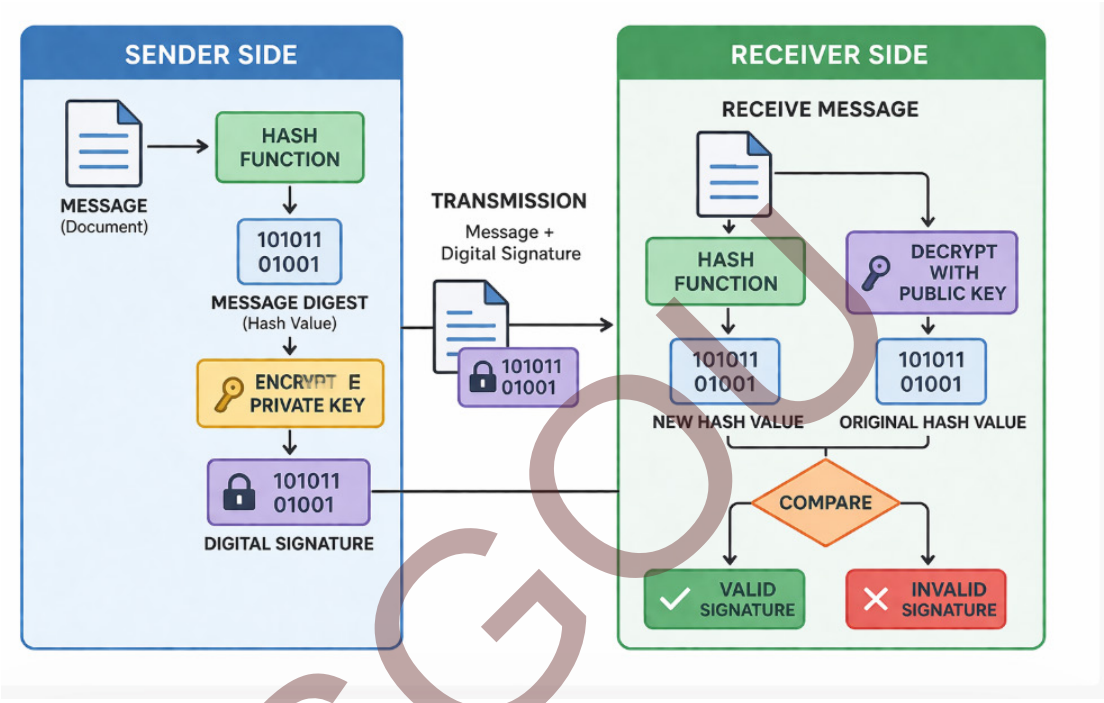


Fig 5.1.1: Digital Signature Process Diagram

The digital signature process begins at the sender's side, where the original message is first converted into a fixed-length hash value using a hash function. This hash value is then processed using the sender's private key to create the digital signature. The sender transmits both the original message and the digital signature to the receiver. At the receiver's side, the received message is again processed through the same hash function to generate a new hash value. Simultaneously, the digital signature is decrypted using the sender's public key to obtain the original hash value. Finally, the receiver compares the newly generated hash value with the decrypted hash value; if both match, the signature is considered valid and the message is authentic and unaltered, otherwise it is treated as invalid.

5.1.3.2 Advantages of Digital Signature

- Provides authentication (verifies identity of sender)
- Ensures data integrity (message cannot be altered)

SGOU

- Offers non-repudiation (sender cannot deny sending)
- Provides high security using encryption techniques
- Legally valid for official and financial transactions
- Reduces paperwork and supports paperless communication
- Enables faster processing of digital documents

5.1.4 Electronic Signature (E-Signature of the IT Act)

As technology evolved, it became clear that restricting authentication only to PKI-based Digital Signatures was too rigid. To make the law "technology-neutral," the government introduced the IT (Amendment) Act, 2008, which introduced the broader concept of Electronic Signatures (E-Signatures). An electronic signature, commonly known as e-signature, is a broader concept that includes any electronic method used to indicate acceptance or approval of a document. Unlike digital signatures, which rely strictly on cryptographic techniques, e-signatures can take various forms such as OTP-based authentication, biometric verification, or Aadhaar-based signing.

The Aadhaar-based e-signature system is widely used in India. In this method, the user uploads a document and provides their Aadhaar number. An OTP is sent to the registered mobile number, and upon successful verification, the document is electronically signed.

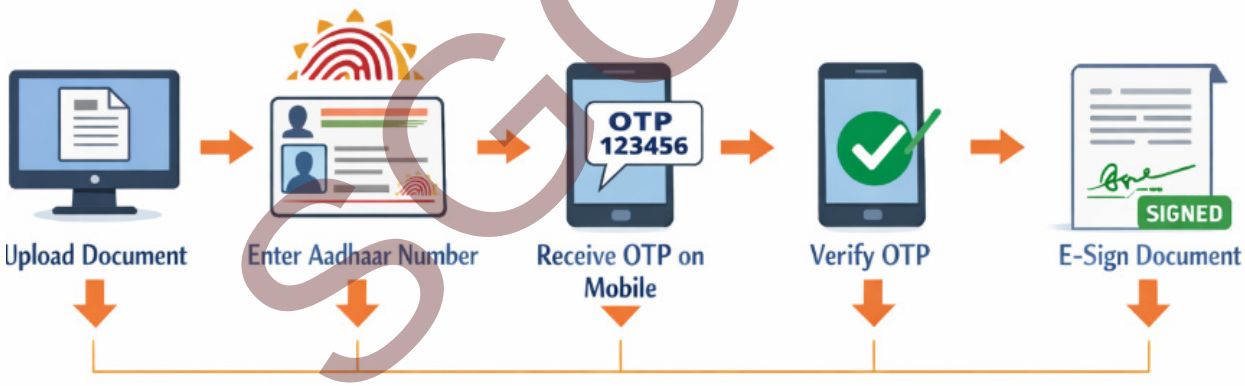


Fig 5.1.2: Aadhaar-based e-signature process

The image illustrates the Aadhaar-based E-Signature process in a clear and sequential manner using icons and directional arrows. It begins with the user uploading a document on a computer, followed by entering the Aadhaar number for identity verification. The process then shows a mobile phone receiving a One-Time Password (OTP), which the user must verify to authenticate their identity. Once the OTP is successfully verified, the system proceeds to apply the electronic signature to the document. The final step displays a digitally signed document marked as “SIGNED,” indicating completion of the process. The visual flow, supported by simple graphics and arrows, effectively represents how e-signatures enable secure, paperless, and quick authentication of digital documents.

SGOU

5.1.4.1 Advantages of E-Signature

- Easy to use and user-friendly
- Enables quick and paperless transactions
- Cost-effective (no printing or physical storage needed)
- Allows remote signing from anywhere
- Supports online services like banking and government forms
- Saves time and effort in document processing

Table 5.1.1: Difference between Digital Signature and E-Signature

Digital Signature	E-Signature (Electronic Signature)
Digital Signature uses cryptographic techniques based on Public Key Infrastructure.	E-Signature uses simple electronic methods such as OTP or biometric verification.
Digital Signature provides a very high level of security.	E-Signature provides a moderate level of security depending on the method used.
Digital Signature requires a Digital Signature Certificate issued by a Certifying Authority.	E-Signature usually does not require any certificate.
Digital Signature uses private and public keys for authentication.	E-Signature uses OTP, Aadhaar, or biometric authentication.
Digital Signature is more complex and time-consuming.	E-Signature is simple, fast, and user-friendly.
Digital Signature is mainly used for legal, financial, and government transactions.	E-Signature is used for general-purpose online transactions.
Digital Signature is relatively costly.	E-Signature is low-cost or free.

SGOU

Recap

- The Information Technology Act, 2000 provides legal recognition to electronic records and digital transactions.
- The Act supports e-commerce and e-governance by enabling online services.
- It applies to the whole of India and also to offences involving Indian computer systems outside India.
- The Act recognizes digital signatures as a valid method of authentication.
- The Controller of Certifying Authorities (CCA) regulates and issues Digital Signature Certificates.
- The IT (Amendment) Act, 2008 introduced e-signatures and strengthened cyber laws.
- A digital signature uses cryptographic techniques to ensure authentication, integrity, and non-repudiation.
- An e-signature is a simple electronic method such as OTP, Aadhaar, or biometric verification.
- The IT Act defines cyber offences like hacking, identity theft, cyber fraud, and cyber terrorism.
- The Act provides penalties such as fines and imprisonment to prevent cyber crimes.
- Digital signatures offer high security, while e-signatures are easy, fast, and suitable for everyday use.
- The IT Act promotes paperless communication and digital documentation.

SGOU

Objective Type Questions

1. Name the Act that provides legal recognition to electronic records and digital transactions in India.
2. Identify the year in which the Information Technology Act was enacted.
3. Expand the term IT Act.
4. Who regulates Digital Signature Certificates in India?
5. Expand the term CCA.

6. Identify the type of signature that uses cryptographic techniques for authentication.
7. Name the type of signature that uses OTP, Aadhaar, or biometric verification.
8. Define the process of converting a message into a fixed-length code.
9. Identify the key used by the sender to create a digital signature.
10. Name the term used for unauthorized access to a computer system.
11. Identify the Act that introduced the concept of e-signature in India.
12. Name the cyber crime that involves misuse of personal information such as passwords or Aadhaar details.

Answers to Objective Type Questions

1. IT Act
2. 2000
3. Information Technology Act
4. CCA
5. Controller of Certifying Authorities
6. Digital Signature
7. E-Signature
8. Hashing
9. Private Key
10. Hacking
11. Information Technology (Amendment) Act, 2008
12. Identity Theft

SGOU

Assignments

1. Explain the Information Technology Act, 2000 in detail
2. Describe the Digital Signature process with a neat diagram and explain its advantages.
3. Explain the concept of Electronic Signature (E-Signature) and describe the Aadhaar-based e-signature process.
4. Discuss the cyber offences under the IT Act, 2000 and explain the penalties and punishments provided for them.
5. Compare and analyze Digital Signature and E-Signature in terms of security, usability, and application. Which one is more suitable for different types of transactions and why?

Suggested Reading

1. Chander, A., & Sood, V. (2022). *Cyber Laws and IT Protection*. New Delhi: Academic Press.
2. Ministry of Electronics and Information Technology. (2022). *Guidelines for Electronic Signatures and Digital Authentication*. Government of India.
3. Government of India. (2000). *Information Technology Act, 2000*. New Delhi: Ministry of Law and Justice.
4. Government of India. (2008). *Information Technology (Amendment) Act, 2008*. New Delhi: Ministry of Law and Justice.
5. Singh, B. (2018). *Cyber Law and Information Technology*. New Delhi: PHI Learning.

SGOU

Reference

1. Stallings, W. (2023). *Cryptography and network security: Principles and practice* (8th ed.). Pearson.
2. Chander, A., & Sood, V. (2022). *Cyber laws and IT protection*. Academic Press.
3. Singh, B. (2018). *Cyber law and information technology*. PHI Learning.
4. https://www.indiacode.nic.in
5. https://www.meity.gov.in
6. https://cca.gov.in



UNIT 2 Electronic Records and Governance

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- explain the concept of electronic records and electronic evidence
- describe the features and types of electronic records in simple terms
- apply the concept of electronic evidence in real-life legal situations
- analyze the advantages and limitations of electronic records and e-governance
- differentiate between types of e-governance models such as G2C, G2B, G2G, and G2E

Prerequisites

Imagine a bank fraud case where a customer claims that money was withdrawn from their account without their knowledge. The bank checks transaction logs, CCTV footage, and email alerts to investigate the issue. All these are electronic records and electronic evidence. Without these digital records, it would be very difficult to identify the fraud and take legal action. The issue can be solved by properly maintaining and analyzing electronic records such as transaction logs and surveillance footage. These records act as reliable electronic evidence in identifying the person responsible for the fraud. Using secure systems, authentication methods, and legal provisions like Section 63, the evidence can be presented in court to ensure justice.

To effectively learn this topic, learners should have a basic understanding of computers and digital devices. They should be familiar with how data is created, stored, and processed in digital systems. Basic knowledge of the internet, emails, and online transactions is also important. Learners should have an awareness of cyber security concepts such as passwords, data protection, and safe internet usage. In addition, a simple understanding of legal systems and digital documentation will help learners grasp the concept of electronic evidence more easily.

Studying this topic helps learners understand how digital data is created, stored, and used in real-world situations. It gives knowledge about electronic records and their importance in organizations, businesses, and government systems. Learners also understand how electronic evidence is used in legal cases, which is highly relevant in

SGOU

today's digital world. Furthermore, it improves awareness about cyber security, data protection, and e-governance services, and helps learners develop practical knowledge for careers in IT, law, administration, and digital systems.

Keywords

Electronic Records, Electronic Evidence, e-governance, Encryption, Cyber security, Digital Signature, Section 63, ICT

Discussion

5.2.1 Electronic Record

Electronic records refer to any form of information that is created, stored, processed, or transmitted in digital format using electronic devices. Unlike traditional paper-based records, electronic records exist in intangible form and can be easily managed using computer systems. These records play a crucial role in modern organizations, as they enable efficient data storage, faster communication, and improved accessibility of information.

Electronic records are commonly stored in various digital environments such as computers, servers, cloud storage systems, and mobile devices. These storage systems allow users to access data anytime and from anywhere, making electronic records highly flexible and convenient for both personal and organizational use.

Electronic records exist in many forms depending on the type of data and its usage. Emails are one of the most common examples, used for communication in both personal and professional environments. Word documents and PDF files are widely used for storing textual information such as reports, letters, and official documents. Databases store structured data in an organized manner, which is useful for managing large volumes of information.

In addition, digital images and videos are also considered electronic records, especially in areas such as media, surveillance, and documentation. Transaction logs, which record activities such as financial transactions or system operations, are another important type of electronic record used for tracking and auditing purposes.

5.2.1.1 Features of Electronic Records

1. Easy Storage

Electronic records require significantly less physical space compared to traditional paper records. Large volumes of data can be stored in compact digital storage devices such as hard drives or cloud systems, reducing the need for physical storage infrastructure.

2. Quick Retrieval

One of the most important features of electronic records is the ability to retrieve

SGOU

information quickly. Advanced search tools and indexing techniques allow users to locate specific data within seconds, improving efficiency and productivity.

3. Cost-Effective

Electronic records help reduce costs associated with paper, printing, and physical storage. Organizations can save money by minimizing the use of paper and reducing maintenance costs related to physical record keeping.

4. Security

Electronic records can be protected using various security mechanisms such as passwords, encryption, and access control systems. These measures ensure that only authorized users can access sensitive information, thereby maintaining confidentiality and integrity.

5. Easy Sharing

Electronic records can be easily shared through networks such as the internet or internal communication systems. This enables fast communication and collaboration among users, regardless of their physical location.

5.2.1.2 Types of Electronic Records

1. Structured Records

Structured records are stored in a predefined format, usually in databases. These records are organized in tables with rows and columns, making them easy to process and analyze. Examples include customer databases and financial records.

2. Unstructured Records

Unstructured records do not follow a fixed format and include data such as emails, images, videos, and social media content. These records are more complex to manage and analyze due to their lack of structure.

3. Semi-Structured Records

Semi-structured records have some level of organization but do not follow a strict format like structured data. Examples include XML and JSON files, where data is stored with tags or labels that provide partial structure.

5.2.1.3 Advantages of Electronic Records

Electronic records offer several advantages that make them more efficient than traditional record-keeping methods. They provide faster access to information, allowing users to retrieve data instantly when needed. The accuracy of data is improved, as electronic systems reduce human errors associated with manual record keeping.

They also significantly reduce paperwork, making processes more environmentally friendly and efficient. Electronic records support easy backup and recovery, ensuring that data can be restored in case of system failure. Additionally, they enable better

SGOU

data management by organizing and maintaining large volumes of information in a systematic manner.

5.2.1.4 Limitations of Electronic Records

Despite their advantages, electronic records also have certain limitations. One major concern is security risks, as digital data can be vulnerable to hacking, unauthorized access, and data theft. Organizations must implement strong security measures to protect sensitive information.

Another limitation is the dependence on technology. Electronic records can only be accessed with the help of electronic devices and software, which may fail or become outdated. Data loss is also a significant risk, especially in cases of system crashes, hardware failures, or cyber-attacks.

Finally, managing electronic records requires technical expertise. Users must have the necessary skills and knowledge to operate digital systems effectively, which may require training and resources.

5.2.2 Electronic Evidence

Electronic evidence refers to any type of information that is created, stored, or transmitted in digital form and can be used as proof in a court of law. In the modern digital world, most human activities such as communication, financial transactions, and business operations are carried out electronically, making electronic evidence highly significant in legal proceedings.

Unlike traditional forms of evidence such as paper documents or physical objects, electronic evidence is intangible in nature. It exists in digital devices such as computers, laptops, mobile phones, servers, and cloud storage systems. Because of its digital nature, electronic evidence can be easily stored, copied, and transmitted across networks.

However, for electronic evidence to be accepted in a court of law, it must be properly collected, preserved, and authenticated. Any alteration or mishandling can affect its reliability and admissibility. Therefore, strict procedures and technical methods are followed to ensure the integrity and authenticity of electronic evidence.

5.2.2.1 Types of Electronic Evidence

Electronic evidence can exist in various forms depending on how the data is created and stored.

1. Emails

Emails are one of the most commonly used forms of electronic evidence. They are widely used in both personal and professional communication. Emails contain important details such as the sender's address, receiver's address, date, time, and message content. These details make emails reliable sources of evidence in cases related to fraud, business agreements, and communication disputes.

2. Digital Documents

Digital documents include files such as Word documents, PDF files, spreadsheets, and

SGOU

electronic contracts. These documents are commonly used in organizations to store official information. In legal cases, digital documents can be used to prove agreements, transactions, or official communications.

3. Multimedia Files

Multimedia files such as audio recordings, video recordings, CCTV footage, and digital images are also considered electronic evidence. These are especially useful in criminal investigations where visual or audio proof is required. For example, CCTV footage can help identify suspects and reconstruct events.

4. System Logs

System logs are records automatically generated by computer systems. They store information about system activities such as login attempts, file access, transactions, and system errors. These logs are very important in detecting unauthorized access, cyber attacks, and system misuse.

5. Social Media Data

Social media platforms generate a large amount of digital data, including messages, posts, comments, and chat histories. This data can be used as electronic evidence in cases involving cyberbullying, harassment, fraud, and other online crimes.

5.2.2.2 Characteristics of Electronic Evidence

1. Intangible Nature

Electronic evidence does not have a physical form and exists only in digital format within electronic devices like computers and mobile phones.

2. Easily Copyable

It can be copied or duplicated multiple times without any loss of quality, making it easy to store and share.

3. Prone to Tampering

Electronic data can be easily modified, altered, or deleted if proper security measures are not applied.

4. Requires Authentication

It must be verified using techniques like digital signatures, hash values, or certificates to ensure its originality.

5. Highly Sensitive

Electronic evidence is delicate and can be damaged or corrupted due to viruses, system failure, or improper handling.

6. Time-Stamped Information

Most electronic records contain date and time details, which help in tracking events accurately.

SGOU

7. Dependent on Technology

Accessing and analyzing electronic evidence requires proper hardware, software, and technical tools.

8. Large Storage Capacity

A large volume of data can be stored in small digital devices, making management efficient.

9. Easy Transmission

Electronic evidence can be quickly transferred over networks, emails, or cloud platforms.

10. Volatile Nature

Some data (like RAM data) is temporary and can be lost when the system is turned off.

5.2.2.3 Legal Aspects (India)

In India, electronic evidence is legally recognised under the Information Technology Act, 2000 and the Bharatiya Sakshya Adhiniyam, 2023 (BSA). The BSA came into force on 1 July 2024 and introduced the present statutory framework for admissibility of electronic records.

Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 deals with the admissibility of electronic records. It performs the role that Section 65B of the Indian Evidence Act, 1872 previously performed for electronic evidence, but it is not merely a renumbering. Section 63(4) requires a certificate in the prescribed Schedule when an electronic record is submitted under the section.

The certificate contains two parts. Part A identifies the electronic record and the relevant device or process and includes the hash value of the record. Part B contains the expert declaration relating to the electronic record. These requirements support the assessment of authenticity and integrity of electronic evidence.

In Pune Bar Association v. Union of India, decided by the Supreme Court on 22 May 2026, the Court upheld Section 63(4) and the Schedule. The Court also clarified that a person having appropriate expertise in computer science or cyber forensics may sign Part B when the court is satisfied about that expertise; it is not restricted only to an Examiner notified under Section 79A of the IT Act.

The change from the Indian Evidence Act to the BSA does not erase the relevance of Section 65B for every historical matter. The savings provision in Section 170(2) of the BSA preserves the Indian Evidence Act for specified applications, trials, inquiries, investigations, proceedings and appeals that were pending immediately before the BSA came into force. Thus, Section 63 is the current provision for proceedings governed by the BSA, while Section 65B may remain relevant to proceedings protected by the savings provision.

5.2.2.4 Challenges in Electronic Evidence

1. Electronic evidence can be easily tampered or modified, which affects its reliability.

SGOU

2. It is difficult to prove authenticity, as digital data can be copied many times.
3. There are privacy concerns, since personal data may be accessed during investigation.
4. Handling electronic evidence requires technical knowledge and skills.
5. There are legal complexities, as laws keep changing with new technologies.

5.2.3 Electronic Governance (e-governance)

Electronic Governance, commonly known as e-governance, refers to the use of information and communication technology (ICT) by the government to provide services, exchange information, and interact with citizens, businesses, and other government departments.

It aims to improve the efficiency, transparency, and accessibility of government services by using digital platforms instead of traditional manual processes.

5.2.3.1 Objectives of e-governance

1. To provide faster and efficient services to citizens.
2. To ensure transparency in government activities.
3. To reduce corruption by minimizing human intervention.
4. To improve accessibility of services anytime and anywhere.
5. To promote citizen participation in governance.

5.2.3.2 Features of e-governance

1. Digital Service Delivery

   Government services are provided online through websites and portals.

2. Transparency

   Information is openly available to the public, reducing corruption.

3. Accountability

   Government officials are more responsible due to digital tracking.

4. Efficiency

   Processes are faster and more accurate.

5. User-Friendly Access

   Citizens can easily access services through mobile apps and online systems.

5.2.3.3 Types of e-governance

1. G2C (Government to Citizen)

SGOU

G2C refers to the services provided directly by the government to citizens through digital platforms. These services include online certificate applications, bill payments, Aadhaar services, and other public services that make it easier for citizens to interact with the government.

2. G2B (Government to Business)

G2B involves the interaction between the government and business organizations. It includes services such as online tax filing, business registration, licensing, and regulatory compliance, which help businesses operate more efficiently.

3. G2G (Government to Government)

G2G refers to the communication and data sharing between different government departments and agencies. It helps in improving coordination, decision-making, and efficiency within the government system.

4. G2E (Government to Employee)

G2E involves services provided by the government to its employees through digital systems. These services include salary management, leave management, and internal communication, which improve administrative efficiency.

5.2.3.4 Advantages of e-governance

1. Provides Quick and Efficient Services

e-governance enables the government to deliver services quickly and efficiently through online platforms. Citizens can access services such as bill payments, applications, and certificates without delays.

2. Reduces Paperwork and Manual Effort

With the use of digital systems, e-governance minimizes the need for paper-based documentation. This reduces manual work, saves resources, and makes processes more organized.

3. Increases Transparency and Accountability

e-governance ensures that government processes are transparent, as information is available online. It also improves accountability because activities are recorded and can be monitored easily.

4. Saves Time and Cost

Both the government and citizens save time and money by using online services. There is no need for physical visits to offices, which reduces travel costs and waiting time.

5. Improves Public Satisfaction

By providing faster, easier, and more reliable services, e-governance increases the satisfaction of citizens. It enhances the overall experience of interacting with government systems.

SGOU

5.2.3.5 Challenges of e-governance

1. Digital Divide

One of the major challenges of e-governance is the digital divide, as not all citizens have access to the internet or modern technology. This creates inequality in accessing government services.

2. Security Issues

e-governance systems are vulnerable to cyber attacks and data breaches. Sensitive government and citizen data must be protected using strong security measures.

3. Lack of Awareness

Many people, especially in rural areas, are not aware of online government services. This limits the effective use of e-governance systems.

4. Technical Problems

System failures, server issues, and poor infrastructure can affect the smooth functioning of e-governance services. These problems may cause delays and inconvenience to users.

5. Resistance to Change

Some people are comfortable with traditional methods and may resist using digital platforms. This slows down the adoption of e-governance

Recap

- Electronic records are digital data stored and managed using electronic devices.
- They do not have a physical form and can be accessed anytime and anywhere.
- Examples include emails, documents, databases, images, and videos.
- Electronic records require less storage space and allow quick retrieval.
- They are cost-effective and can be easily shared through networks.
- They provide better accuracy and reduce paperwork.
- However, they depend on technology and may face security and data loss risks.
- Electronic evidence is digital information used as proof in legal cases.
- It is stored in devices like computers, mobiles, and servers.
- Examples include emails, digital documents, videos, system logs, and social media data.

SGOU

- It is intangible, easily copyable, and prone to tampering.
- It must be properly authenticated to be accepted in court.
- In India, it is governed by the Information Technology Act, 2000 and Indian Evidence Act.
- Section 63 defines conditions for admissibility of electronic evidence.
- Challenges include security risks, privacy issues, and technical complexity.
- e-governance is the use of ICT by the government to provide digital services.
- It improves efficiency, transparency, and accessibility of services.
- It provides faster services and reduces corruption.
- Types include G2C, G2B, G2G, and G2E interactions.
- It reduces paperwork and saves time and cost.
- It improves public satisfaction through better service delivery.
- Challenges include digital divide, security issues, lack of awareness, and technical problems.

Objective Type Questions

1. Who uses electronic records in organizations?
2. Where are electronic records commonly stored?
3. When is electronic evidence used in legal cases?
4. Why are electronic records preferred over paper records?
5. How can electronic records be protected from unauthorized access?
6. Who verifies the authenticity of electronic evidence?
7. Where is electronic evidence presented for legal decisions?
8. When can electronic data be lost easily?
9. Why is e-governance important for citizens?
10. How does e-governance improve transparency?
11. Who benefits from G2C services?
12. Where can citizens access e-governance services?

SGOU

Answers to Objective Type Questions

1. Employees
2. Computers
3. Court
4. Efficiency
5. Encryption
6. Expert
7. Court
8. Failure
9. Citizens
10. Technology
11. Citizens
12. Online

Assignments

1. Explain the concept of electronic records and its features in detail.
2. Describe the different types of electronic records with suitable examples.
3. Discuss the advantages and limitations of electronic records.
4. Explain the concept of electronic evidence and its importance in legal proceedings.
5. Describe the different types of electronic evidence with examples.
6. Explain the characteristics of electronic evidence in detail.
7. Discuss the legal aspects of electronic evidence in India with reference to Information Technology Act, 2000 and Indian Evidence Act.
8. Explain Section 63 and its importance in electronic evidence.
9. Discuss the challenges involved in handling electronic evidence.

SGOU

10. Explain the concept of e-governance and its objectives.

11. Describe the different types of e-governance with examples.

12. Discuss the advantages and challenges of e-governance.

Suggested Reading

1. Joshi, N. (2025). *Electronic evidence* (2nd ed.). Lawmann.

2. Kalra, K. (2025). *Law of electronic evidence* (3rd ed.). Vinod Publications.

3. Sharma, V. (2018). *Cyber law and information technology*. New Delhi: PHI Learning.

4. Government of India. (2000). *Information Technology Act, 2000*. New Delhi: Author.

5. Gupta, M. P. (2011). *E-governance in India: From vision to implementation*. New Delhi: Prentice Hall India.

Reference

1. Roy, N. R., Singh, A. P., Kumar, P., & Kaul, A. (Eds.). (2025). *Cyber security and digital forensics: Select proceedings of ReDCySec 2024*. Springer

2. https://www.indiacode.nic.in

3. https://www.meity.gov.in

4. https://cert-in.org.in

5. https://tdsat.gov.in

SGOU



UNIT 3 Regulatory Authorities

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- explain the key features and significance of the Information Technology Act, 2000 in regulating digital activities
- describe the roles and functions of the Controller of Certifying Authorities, and Telecom Disputes Settlement and Appellate Tribunal
- apply the concept of Digital Signature Certificates to demonstrate how secure electronic transactions are performed
- illustrate how Certifying Authorities verify identity and issue digital certificates in real-world scenarios
- analyze the relationship and coordination between CCA, CAs, and CAT in ensuring cyber security and legal compliance

Prerequisites

In today's digital world, consider a situation where a person performs an online banking transaction or submits an important document through an e-governance portal, but later discovers that their data has been altered or misused by an unauthorized person. This creates serious problems such as financial loss, identity theft, and lack of trust in digital systems. To solve such issues, a strong legal and regulatory framework is required. The Information Technology Act, 2000 provides this solution by giving legal recognition to electronic records and digital signatures. It ensures that digital transactions are secure, authentic, and legally valid. Regulatory authorities such as the Controller of Certifying Authorities, Certifying Authorities, and the Telecom Disputes Settlement and Appellate Tribunal work together to verify identities, prevent misuse, and resolve disputes, thereby creating a safe and trustworthy digital environment.

Studying this topic offers several advantages. It helps learners understand the legal framework governing digital activities and provides knowledge about cyber security and safe online practices. It explains how digital signatures ensure authenticity, integrity, and reliability in electronic transactions. The topic also creates awareness about cyber crimes and their prevention, while enhancing understanding of modern

SGOU

digital systems such as e-commerce and e-governance. Learners can easily relate the concepts to everyday activities like online banking, digital payments, and electronic communication. Moreover, it helps individuals protect themselves from cyber threats and understand government digital initiatives, making it both practically useful and academically valuable.

Keywords

Information Technology Act, 2000, Cyber Law, Digital Signature, Electronic Records, Controller of, Certifying Authorities (CCA), Certifying Authorities (CAs), Cyber Appellate Tribunal (CAT), Public Key Infrastructure (PKI), Digital Signature Certificate (DSC), Authentication, Cyber Security, Certificate Revocation List (CRL)

Discussion

5.3.1 Introduction

With the rapid growth of digital technologies, the world has witnessed a massive increase in digital transactions, e-commerce platforms, and online communication systems. Today, activities such as online banking, digital payments, e-filing of taxes, and electronic governance services have become an integral part of everyday life. However, this digital transformation also brings challenges related to security, authenticity, privacy, and legal validity.

To address these challenges, there is a strong need for legal regulation and governance in cyberspace. In India, the Information Technology Act, 2000 was enacted to provide a comprehensive legal framework for managing and regulating cyber activities. This Act gives legal recognition to electronic records and digital signatures, making them valid and enforceable in courts of law.

In addition to this, the Act plays a crucial role in:

- Preventing cyber crimes such as hacking, identity theft, and data breaches
- Promoting secure electronic transactions
- Supporting the growth of e-commerce and digital economy
- Facilitating efficient e-governance services

To effectively implement the provisions of this Act, several regulatory authorities have been established. These authorities are responsible for monitoring, controlling, and enforcing cyber laws in the country. They ensure that digital systems operate in a secure, reliable, and trustworthy environment.

The main objectives of these regulatory authorities include:

- Ensuring security of electronic transactions so that users can safely perform online activities

SGOU

- Maintaining the authenticity and integrity of digital signatures
- Preventing and controlling cyber crimes and unauthorized access
- Providing mechanisms for the resolution of cyber disputes

The key regulatory authorities established under the IT Act are:

- Controller of Certifying Authorities (CCA)
- Certifying Authorities (CAs)
- Telecom Disputes Settlement and Appellate Tribunal (TDSAT)

These authorities work together to create a strong legal and technical framework for cyber security and digital trust.

5.3.2 Controller of Certifying Authorities (CCA)

The Controller of Certifying Authorities (CCA) is the highest regulatory authority appointed by the Central Government under the IT Act. It plays a central role in the regulation and supervision of digital signature infrastructure in India.

The CCA is responsible for overseeing the activities of Certifying Authorities and ensuring that they function according to the rules and standards prescribed under the law. It acts as the "root of trust" in the Public Key Infrastructure (PKI), which is the backbone of secure digital communication.

In simple terms, the CCA ensures that:

- Digital certificates issued are reliable
- Electronic transactions are secure
- Identity verification mechanisms are trustworthy

Without the CCA, there would be no centralized authority to regulate and maintain trust in digital certification systems.

5.3.2.1 Appointment

The Controller of Certifying Authorities is appointed by the Central Government of India. The appointment is made to ensure proper implementation of the IT Act and effective regulation of cyber activities.

Key points regarding appointment:

- The CCA works under the supervision of the Ministry of Electronics and Information Technology (MeitY)
- The Controller may be supported by Deputy Controllers, Assistant Controllers, and other officials
- These officials help in carrying out administrative, technical, and regulatory functions

SGOU

The structured hierarchy ensures smooth functioning and efficient management of digital certification processes across the country.

5.3.2.2 Powers of the Controller

The Controller is vested with wide-ranging powers to regulate and control the functioning of digital certification systems. These powers ensure that all Certifying Authorities operate in a secure and lawful manner.

1. Licensing Powers

One of the most important powers of the Controller is to grant licenses to Certifying Authorities.

- Only licensed entities can issue Digital Signature Certificates (DSCs)
- The Controller evaluates the technical and financial capability of applicants
- If a Certifying Authority violates rules or fails to maintain standards, the Controller has the power to:
    - Suspend the license temporarily
    - Revoke the license permanently

This ensures that only trusted and competent organizations are allowed to operate as Certifying Authorities.

2. Regulatory Powers

The Controller has the authority to define rules and standards related to digital signatures and electronic records.

- Specifies technical standards for encryption and security
- Defines procedures for issuing and managing Digital Signature Certificates
- Establishes guidelines for maintaining confidentiality and data protection

These regulations help in maintaining uniformity and reliability across all Certifying Authorities.

3. Supervisory Powers

The Controller continuously monitors the activities of Certifying Authorities.

- Ensures compliance with provisions of the IT Act
- Conducts audits and inspections
- Verifies whether security practices are properly followed

This supervision helps in preventing misuse and maintaining the integrity of digital systems.

SGOU

4. Investigative Powers

The Controller also has the authority to investigate any violation of rules.

- Can access computers, networks, and data systems
- Can examine records and documents
- Can take action against non-compliant entities

These powers are essential for detecting fraud, misuse, or security breaches in digital certification processes.

5.3.2.3 Functions of the Controller

Apart from its powers, the Controller performs several important functions to ensure smooth functioning of the digital ecosystem.

- Certifies public keys of Certifying Authorities, thereby establishing a chain of trust
- Maintains a National Repository of Digital Certificates, which stores important certificate-related information
- Specifies security guidelines and standards for electronic records and systems
- Promotes the use of digital signatures in e-governance and online services
- Encourages adoption of secure digital practices across industries

These functions collectively strengthen the digital infrastructure of the country.

5.3.3 Certifying Authorities (CAs)

A Certifying Authority (CA) is an organization or entity that is officially licensed by the Controller of Certifying Authorities to issue Digital Signature Certificates (DSCs). These certificates are used to verify the identity of individuals, organizations, and systems involved in electronic transactions.

In the digital environment, where physical presence is absent, Certifying Authorities play a crucial role in ensuring that the identity of users is authentic, verified, and trustworthy. A Digital Signature Certificate issued by a CA acts like a digital identity card, confirming that the person or organization is genuine.

Certifying Authorities act as trusted third parties in electronic communication. They build trust between two unknown parties who are interacting over the internet.

The primary roles of Certifying Authorities include:

- Authentication of identity: They verify the identity of users before issuing certificates, ensuring that the person is who they claim to be.
- Issuance of digital certificates: They provide Digital Signature Certificates that are used to sign electronic documents securely.

SGOU

- Ensuring secure communication: By using encryption and digital signatures, they help maintain confidentiality, integrity, and authenticity of data.

In simple terms, Certifying Authorities ensure that online interactions are safe, reliable, and legally valid.

5.3.3.1 Functions of Certifying Authorities

Certifying Authorities perform several important functions to maintain the security and reliability of digital transactions.

1. Issuance of Digital Signature Certificates

One of the primary functions of a Certifying Authority is to issue Digital Signature Certificates to individuals and organizations.

- These certificates are used to digitally sign documents and transactions
- They ensure that the sender's identity is genuine
- They provide legal validity to electronic documents

2. Verification of Identity

Before issuing a certificate, the Certifying Authority verifies the identity of the applicant.

- This process may include checking documents such as Aadhaar, PAN card, or passport
- In some cases, biometric verification or video verification is also used
- This step ensures that certificates are issued only to legitimate users

3. Maintenance of Certificate Records

Certifying Authorities maintain detailed records of all certificates issued.

- They store information about certificate holders
- They maintain a Certificate Revocation List (CRL), which contains details of revoked certificates
- This helps users verify whether a certificate is valid or has been cancelled

4. Revocation and Suspension of Certificates

If a certificate is misused, compromised, or no longer required, the Certifying Authority has the power to:

- Revoke the certificate permanently, making it invalid
- Suspend the certificate temporarily, until further verification

This ensures that compromised certificates cannot be used for fraudulent activities.

SGOU

5.3.3.2 Duties of Certifying Authorities

Certifying Authorities must follow strict guidelines and responsibilities to maintain trust and security.

- They must follow all rules and regulations issued by the Controller
- They must ensure confidentiality of user data and protect sensitive information
- They must maintain a secure technical infrastructure to prevent hacking or misuse
- They must publish a Certificate Practice Statement (CPS), which explains their procedures and security policies

5.3.3.3 Examples of Certifying Authorities in India

Some well-known Certifying Authorities operating in India include:

- National Informatics Centre (NIC), which provides digital certificates for government services
- eMudhra, a leading provider of digital signature solutions
- Sify Technologies, which offers various IT and certification services

These organizations play a vital role in supporting secure digital transactions across the country.

5.3.3.4 Importance of Certifying Authorities

Certifying Authorities are essential for the functioning of modern digital systems.

- They enable secure e-commerce transactions, such as online payments and contracts
- They provide authentication and data integrity, ensuring that information is not altered
- They support e-governance services, such as online filing and digital documentation
- They help prevent fraud, impersonation, and cyber attacks

5.3.4 Telecom Disputes Settlement and Appellate Tribunal (TDSAT)

The Cyber Appellate Tribunal was established under Section 48 of the IT Act. In 2017, its appellate functions were transferred to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT). Therefore, learners may encounter the term Cyber Appellate Tribunal in older books and cases, but the present appellate forum is TDSAT.

SGOU

The Telecom Disputes Settlement and Appellate Tribunal (TDSAT) is a quasi-judicial body established under the provisions of the IT Act. Its main purpose is to hear appeals against decisions made by the Controller of Certifying Authorities or Adjudicating Officers.

It acts as a specialized forum for resolving disputes related to cyber laws, digital signatures, and electronic transactions. By providing a dedicated platform, it ensures that cyber-related cases are handled efficiently and effectively.

The Telecom Disputes Settlement and Appellate Tribunal is established by the Central Government of India.

- It functions similarly to a court but follows simplified procedures
- It is designed to handle cyber law cases quickly and efficiently
- It reduces delays compared to traditional court systems

5.3.4.1 Composition

TDSAT is headed by a Chairperson and has Members as provided under its governing law. In the context of the appellate jurisdiction transferred from the former Cyber Appellate Tribunal, learners should not use the old Presiding Officer structure as the current composition of the tribunal.

5.3.4.2 Jurisdiction and Powers

The Telecom Disputes Settlement and Appellate Tribunal has several important powers and responsibilities.

1. Appellate Authority

The Tribunal acts as an appellate body.

- It hears appeals against decisions made by the Controller or Adjudicating Officers
- It reviews cases and ensures fairness in decisions

2. Civil Court Powers

The Tribunal has powers similar to those of a civil court.

- It can summon witnesses
- It can require the production of documents
- It can examine evidence and records

These powers enable the Tribunal to conduct proper investigations and hearings.

3. Decision Making

After hearing both parties, the Tribunal gives its decision.

SGOU

- The decisions are legally binding
- The Tribunal ensures justice based on evidence and legal provisions
- It provides a fair opportunity for both sides to present their case

5.3.4.3 Importance of Telecom Disputes Settlement and Appellate Tribunal

The Telecom Disputes Settlement and Appellate Tribunal plays a vital role in the cyber law framework.

- It provides speedy justice in cyber-related disputes
- It reduces the burden on traditional courts
- It ensures proper enforcement of cyber laws
- It enhances trust in digital systems and legal processes

Without such a tribunal, resolving cyber disputes would be slow and inefficient.

5.3.5 Relationship Between the Authorities

Controller of Certifying Authorities (CCA) → licenses and regulates → Certifying Authorities (CAs) → issue Digital Signature Certificates (DSCs) → Subscribers

Controller / Adjudicating Officer → orders under the IT Act → TDSAT (Appellate Forum)

The Controller of Certifying Authorities, Certifying Authorities, Adjudicating Officers and Telecom Disputes Settlement and Appellate Tribunal work together in a coordinated manner to create a secure and trustworthy digital ecosystem.

- The Controller of Certifying Authorities acts as the regulatory and supervisory body. It ensures that all Certifying Authorities follow the rules and maintain security standards.
- The Certifying Authorities operate under the supervision of the Controller and are responsible for issuing Digital Signature Certificates and ensuring secure communication.
- The Telecom Disputes Settlement and Appellate Tribunal acts as a dispute resolution body. It handles appeals and ensures justice when conflicts arise.

Thus, each authority has a distinct role:

- The Controller regulates and supervises
- Certifying Authorities authenticate and issue certificates
- The Tribunal resolves disputes and ensures justice

SGOU

Together, they form a complete system that ensures:

- Security of digital transactions
- Trust in electronic communication
- Effective enforcement of cyber laws

This coordinated functioning is essential for the growth of e-commerce, e-governance, and digital society.

Recap

- The rapid growth of digital technologies has increased the need for security, privacy, and legal regulation in cyberspace.
- The Information Technology Act, 2000 provides a legal framework for electronic records and digital signatures in India.
- The Act promotes secure electronic transactions, e-commerce, and e-governance services.
- It also helps in preventing cyber crimes like hacking, identity theft, and data breaches.
- To implement the Act, three key authorities are established: **CCA, CAs, and CAT**.
- The Controller of Certifying Authorities (CCA) is the highest regulatory authority supervising digital certification systems.
- The CCA acts as the "root of trust" in Public Key Infrastructure (PKI).
- The CCA has powers such as licensing Certifying Authorities, regulation, supervision, and investigation.
- It also performs functions like maintaining digital certificate repositories and setting security standards.
- Certifying Authorities (CAs) are licensed entities that issue Digital Signature Certificates (DSCs).
- CAs ensure authentication, confidentiality, integrity, and secure communication in digital transactions.
- They perform functions such as identity verification, certificate issuance, record maintenance, and revocation of certificates.
- The Telecom Disputes Settlement and Appellate Tribunal (TDSAT) is a quasi-judicial body that handles appeals and cyber dispute resolution.

SGOU

- All three authorities work together:
  - **CCA** → Regulates and supervises
  - **CAs** → Authenticate and issue certificates
  - **CAT** → Resolves disputes and ensures justice

Objective Type Questions

1. In which year was the Information Technology Act, 2000 enacted?
2. What is the main objective of the IT Act, 2000?
3. Which authority is the highest regulatory body for digital signatures in India?
4. Who appoints the Controller of Certifying Authorities (CCA)?
5. Under which ministry does the CCA function?
6. In which system does the CCA act as the "root of trust"?
7. Who grants licenses to Certifying Authorities?
8. Name any one power of the Controller of Certifying Authorities.
9. What is the main role of Certifying Authorities (CAs)?
10. Who issues Digital Signature Certificates (DSCs)?
11. What is the purpose of a Digital Signature Certificate?
12. What process is performed before issuing a digital certificate?
13. What is the Certificate Revocation List (CRL)?
14. What type of body is the Telecom Disputes Settlement and Appellate Tribunal (TDSAT)?
15. What is the main function of the Telecom Disputes Settlement and Appellate Tribunal?
16. What is the primary objective of regulatory authorities in cyberspace?

SGOU

Answers to Objective Type Questions

1. 2000
2. To regulate cyber activities and provide legal recognition to electronic transactions
3. Controller of Certifying Authorities (CCA)
4. Central Government
5. Ministry of Electronics and Information Technology (MeitY)
6. Public Key Infrastructure (PKI)
7. Controller of Certifying Authorities (CCA)
8. Granting licenses / regulation / supervision / investigation (any one)
9. To issue Digital Signature Certificates and ensure secure transactions
10. Certifying Authorities (CAs)
11. Identity verification and secure digital signing
12. Identity verification
13. A list of revoked digital certificates
14. Quasi-judicial body
15. To hear appeals and resolve cyber disputes
16. To ensure security and trust in digital transactions

SGOU

Assignments

1. Explain the need and significance of the Information Technology Act, 2000 in the digital era.

2. Describe the role and importance of regulatory authorities under the IT Act.

3. Explain in detail the powers and functions of the Controller of Certifying Authorities (CCA).

4. Discuss the appointment and responsibilities of the Controller of Certifying Authorities.

5. Explain the concept and role of Certifying Authorities (CAs) in digital communication.

6. Describe the functions and duties of Certifying Authorities in detail.

7. Explain the process of issuing Digital Signature Certificates by Certifying Authorities.

8. Discuss the importance of Certifying Authorities in ensuring secure electronic transactions.

9. Explain the structure, powers, and functions of the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).

10. Discuss the role of the Telecom Disputes Settlement and Appellate Tribunal in hearing appeals under the IT Act.

11. Compare the roles of Controller of Certifying Authorities, Certifying Authorities, and Telecom Disputes Settlement and Appellate Tribunal.

12. Explain the relationship and coordination between the CCA, CAs, Adjudicating Officers and TDSAT.

13. Discuss how the IT Act supports e-governance and e-commerce in India.

14. Explain how digital signatures ensure security, authenticity, and integrity in electronic transactions.

SGOU

Suggested Reading

1. Gupta and Agrawal. (2025). *Cyber laws*. New Delhi: Premier Publishing Company

2. J. Hams, J. (2025). *Cyber law for India: Policies, regulations, and case studies*. Code Academy.

3. Chris Reed, C., & John Angel, J. (2018). *Computer law* (7th ed.). Oxford: Oxford University Press.

4. Vakul Sharma, V. (2015). *Information technology law and practice: Cyber laws and laws relating to e-commerce*. New Delhi: Universal Law Publishing.

5. Farooq Ahmad, F. (2015). *Cyber law in India: Law on internet*. New Delhi: Allahabad Law Agency.

6. Pavan Duggal, P. (2014). *Cyber law in India*. New Delhi: Wolters Kluwer India.

Reference

1. Pavan Duggal, P. (2025). *Cyber law* (3rd ed.). New Delhi: LexisNexis.

2. D. P. Mittal, D. P. (2025). *Law relating to information technology*. New Delhi: Commercial Law Publishers.

3. https://ndl.iitkgp.ac.in

4. https://www.edx.org

SGOU



UNIT 4 Cyber Law Applications and E-Commerce

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- understand the concept of data security and explain its importance in protecting digital information
- explain the features and types of e-contracts used in e-commerce systems
- apply data security techniques such as encryption and authentication in real-life digital transactions
- analyze the advantages and limitations of e-contracts in online business environments
- differentiate between data security, e-contracts, and e-forms based on their roles in e-commerce systems

Prerequisites

In today's digital world, consider a real-time situation where a customer purchases a product from an online shopping website. The customer enters personal details, an address, and credit card information to complete the transaction. However, due to weak security measures, a hacker intercepts this data and misuses it for fraudulent activities. This leads to financial loss, identity theft, and a loss of trust in online systems. This example clearly shows the risks involved in digital transactions and highlights the importance of data security, e-contracts, and e-forms in ensuring safe and reliable e-commerce operations. To solve this problem, strong data security measures such as encryption, authentication, and firewalls must be implemented to protect sensitive information.

The concepts of data security, e-contracts, and e-forms are essential for building a secure and trustworthy digital environment. They not only protect users from cyber risks but also ensure the smooth functioning of e-commerce and e-governance systems. Understanding these concepts enables learners to actively participate in the digital world with confidence and responsibility. Learners develop awareness of cyber security practices and learn how to protect personal and organizational data. They also understand the legal aspects of online transactions, which are essential in today's digital economy.

SGOU

Keywords

Data Security, E-Commerce, e-contracts, e-forms, Encryption, Authentication, Authorization, Cyber Law, Digital Signature, Cyber Security

Discussion

5.4.1 Introduction

In the modern digital era, the widespread use of the internet has fundamentally transformed the way individuals, businesses, and governments function. Everyday activities such as online shopping, digital banking, electronic communication, online education, and e-governance services have become an integral part of human life. This digital transformation has significantly contributed to the rapid growth of e-commerce, where commercial transactions are conducted electronically without the need for physical presence. Businesses can now reach global markets, consumers can purchase products and services with just a few clicks, and governments can deliver services efficiently through digital platforms. This shift has not only improved convenience and speed but also reduced operational costs and enhanced accessibility.

However, alongside these advantages, the expansion of digital technologies has introduced several critical challenges. Issues such as data theft, cyber fraud, unauthorized access, identity theft, phishing attacks, and lack of trust in online systems have become increasingly common. For instance, when a customer makes an online purchase, they are required to share sensitive information such as credit card details, personal identification data, and contact information. If this data is not adequately protected, it can be intercepted or misused by cybercriminals, leading to financial loss, privacy violations, and reputational damage. Such risks create hesitation among users and highlight the urgent need for robust security mechanisms and legal protection in the digital environment.

To address these challenges, cyber laws play a vital role in establishing a secure and trustworthy digital ecosystem. The Information Technology Act, 2000 serves as the primary legal framework in India for regulating electronic transactions and cyber activities. It provides legal recognition to electronic records, digital signatures, and online contracts, thereby ensuring that digital interactions are valid and enforceable in a court of law. The Act also defines penalties for cyber offenses, promotes secure communication practices, and supports the growth of e-commerce and digital governance. By creating a structured legal environment, it helps in building confidence among users and organizations engaging in online transactions.

This unit focuses on three major aspects that are essential for the functioning of secure e-commerce systems: Data Security, e-contracts, and e-forms. Data security ensures that information is protected from unauthorized access and misuse, maintaining confidentiality, integrity, and availability. e-contracts facilitate legally binding agreements in electronic form, enabling seamless business transactions without

SGOU

physical documentation. e-forms simplify data collection and processing in digital formats, improving efficiency in both business and government operations. Together, these components form the backbone of a secure, efficient, and reliable e-commerce ecosystem, ensuring that digital transactions are not only convenient but also safe and legally protected.

5.4.2 Data Security

Data security refers to the process of protecting digital information from unauthorized access, corruption, misuse, or theft throughout its life cycle. In today's digital environment, vast amounts of data are generated, stored, and transmitted across networks, making it highly vulnerable to cyber threats. Data security ensures that sensitive information such as personal details, financial records, business data, and confidential communications remain protected from unauthorized users. It focuses on maintaining confidentiality, integrity, and availability of data so that only authorized individuals can access and use it appropriately. In simple terms, data security can be understood as protecting data from misuse and ensuring that it is accessed only by the right person at the right time, thereby preserving trust and reliability in digital systems.

Data security plays a critical role in the success and sustainability of e-commerce systems. In online transactions, customers are required to share sensitive information such as credit card numbers, bank details, addresses, and personal identification data. At the same time, businesses store large volumes of confidential data including customer databases, transaction histories, and proprietary information. Since e-commerce involves continuous exchange of sensitive information over the internet, ensuring its protection becomes essential.

The importance of data security in e-commerce lies in its ability to protect customer privacy, prevent financial fraud, and maintain the confidentiality of business operations. It builds trust between customers and businesses, encouraging more users to engage in online transactions. Moreover, strong data security practices ensure compliance with legal regulations such as the Information Technology Act, 2000, thereby avoiding legal penalties. It also safeguards the reputation of organizations, as data breaches can severely damage public trust and result in financial losses. Thus, data security is not only a technical requirement but also a strategic necessity for the growth of digital commerce.

5.4.2.1 Types of Data Security

Data security can be classified into different types based on the level at which protection is applied. Each type plays a significant role in ensuring overall system security.

1. Physical Security

Physical security refers to the protection of hardware devices and infrastructure such as servers, computers, storage devices, and data centers from physical damage, theft, or unauthorized access. It includes measures like surveillance cameras, biometric access controls, security guards, and restricted entry to server rooms. Without proper physical security, attackers may gain direct access to systems and steal or damage data. For example, if a server containing sensitive customer information is stolen or tampered

SGOU

with, it can lead to serious data breaches. Therefore, physical security forms the first line of defense in protecting digital systems.

2. Network Security

Network security focuses on protecting data while it is being transmitted across communication networks such as the internet or private networks. Since data travels through multiple channels, it is vulnerable to interception by unauthorized users. Network security uses technologies such as firewalls, intrusion detection systems, encryption protocols (like SSL/TLS), and secure routers to prevent unauthorized access and data leakage. It ensures that data sent from one point to another remains confidential and intact. For example, when users perform online banking transactions, network security mechanisms ensure that their financial data is safely transmitted without being intercepted by hackers.

3. Application Security

Application security involves protecting software applications from threats and vulnerabilities that could be exploited by attackers. Applications such as web portals, mobile apps, and e-commerce platforms often handle sensitive user data, making them prime targets for cyber attacks. Security measures include secure coding practices, regular updates, patch management, and testing for vulnerabilities such as SQL injection, cross-site scripting (XSS), and malware attacks. Proper application security ensures that users can safely interact with software systems without risking data exposure or system compromise. It also helps maintain the reliability and trustworthiness of digital services.

4. Cloud Security

Cloud security refers to the protection of data stored in cloud computing environments, where information is stored on remote servers instead of local devices. With the increasing use of cloud services for data storage and business operations, ensuring cloud security has become essential. It includes measures such as data encryption, secure access controls, identity management, and regular monitoring of cloud systems. Cloud security ensures that data is protected from unauthorized access, data loss, and cyber attacks even when stored remotely. For example, companies using cloud storage must ensure that only authorized users can access their data and that proper backup systems are in place to prevent data loss.

5.4.2.2 Principles of Data Security

Data security is based on three fundamental principles that ensure the protection and proper management of information in digital systems. These principles form the foundation for designing secure systems and are essential for maintaining trust in electronic environments.

1. Confidentiality

Confidentiality ensures that data is accessible only to authorized users and is protected from unauthorized disclosure. It focuses on preventing sensitive information from being exposed to individuals who do not have permission to access it. This is achieved

SGOU

through techniques such as encryption, passwords, and access control mechanisms. For example, personal data such as bank details or passwords should only be visible to the rightful user. Maintaining confidentiality helps protect privacy and prevents misuse of information.

2. Integrity

Integrity ensures that data is accurate, complete, and not altered in an unauthorized manner. It protects data from being modified, deleted, or corrupted either intentionally or accidentally. Maintaining integrity is important because incorrect or manipulated data can lead to wrong decisions and serious consequences. Techniques such as hashing, validation checks, and digital signatures are used to ensure data integrity. For example, in financial systems, transaction details must remain unchanged to ensure correctness and reliability.

3. Availability

Availability ensures that data and systems are accessible to authorized users whenever required. It focuses on providing continuous and reliable access to information without unnecessary delays or interruptions. This is especially important for systems such as e-commerce websites and online banking, which need to operate 24/7. Measures such as backups, redundancy, and regular system maintenance are used to ensure availability. Without availability, even secure data becomes useless if users cannot access it when needed.

These three principles - confidentiality, integrity, and availability - are collectively known as the CIA Triad, and they form the core foundation of data security.

5.4.2.3 Data Security Techniques

Several techniques are used to ensure data security and protect information from cyber threats. These techniques work together to provide multiple layers of protection.

1. Encryption

Encryption is a technique that converts readable data into an unreadable format using algorithms and keys. This ensures that even if the data is intercepted, it cannot be understood by unauthorized users. Only users with the correct decryption key can access the original data. Encryption is widely used in online transactions, emails, and secure communications. It plays a crucial role in maintaining confidentiality of sensitive information.

2. Authentication

Authentication is the process of verifying the identity of users before granting access to a system. It ensures that only legitimate users can access data and resources. Common methods include passwords, PINs, biometric verification, and multi-factor authentication. This process helps prevent unauthorized users from gaining access to sensitive information. Strong authentication mechanisms enhance overall system security.

SGOU

3. Authorization

Authorization determines the level of access granted to an authenticated user. It ensures that users can only access the data and resources that they are permitted to use. Different users may have different levels of access based on their roles and responsibilities. For example, an employee may have limited access, while an administrator may have full access. Authorization helps in preventing misuse of data and ensures controlled access.

4. Firewalls

Firewalls are security systems that monitor and control incoming and outgoing network traffic. They act as a barrier between trusted internal networks and untrusted external networks, such as the internet. Firewalls block unauthorized access while allowing legitimate communication. They play a crucial role in protecting systems from hackers and cyber attacks. Proper firewall configuration is essential for maintaining network security.

5. Antivirus Software

Antivirus software is used to detect, prevent, and remove malicious software such as viruses, worms, and spyware. It continuously scans the system for threats and provides real-time protection against cyber attacks. Regular updates are necessary to ensure protection against new and evolving threats. Antivirus software helps maintain the health and security of computer systems and prevents data loss or damage.

5.4.2.4 Challenges in Data Security

1. Rapid growth of cyber attacks

The number of cyber attacks is increasing rapidly due to the widespread use of digital technologies. Attackers are using more advanced and sophisticated methods, making it difficult to detect and prevent such threats effectively.

2. Lack of user awareness

Many users are not aware of basic cyber security practices such as identifying phishing emails or using secure websites. This lack of awareness makes them vulnerable to cyber attacks and increases the chances of data breaches.

3. Weak passwords

Users often create simple or commonly used passwords, which are easy for attackers to guess or crack. Reusing the same password across multiple platforms further increases the risk of unauthorized access.

4. Insider threats

Insider threats arise when employees or authorized users misuse their access privileges. These threats can be intentional or accidental and are difficult to detect because insiders already have system access.

5. Advanced hacking techniques

SGOU

Hackers continuously develop new and complex techniques such as ransomware and zero-day attacks. These advanced methods can bypass traditional security systems, making data protection more challenging.

5.4.2.5 Legal Framework for Data Security

- Data security in e-commerce is not only a technical issue but also a legal responsibility. Section 43 of the IT Act provides for compensation in specified cases involving unauthorised access, downloading or copying of data, introduction of a virus or contaminant, disruption of a computer resource and related acts.

- Section 43A deals with compensation where a body corporate is negligent in implementing and maintaining reasonable security practices and procedures while handling sensitive personal data or information. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 provide the associated framework.

- Section 72A addresses disclosure of information in breach of a lawful contract. Following the Jan Vishwas (Amendment of Provisions) Act, 2023, Section 72A provides for a monetary penalty that may extend to twenty-five lakh rupees for the specified disclosure rather than the earlier imprisonment-based punishment.

- Section 70B establishes CERT-In as the national agency for cyber security incident response. The Directions issued on 28 April 2022 require covered entities to report specified cyber security incidents within the prescribed six-hour period and to maintain logs for 180 days, subject to the applicable requirements.

- The Digital Personal Data Protection Act, 2023 introduces a new framework for processing digital personal data. The Digital Personal Data Protection Rules, 2025 were notified on 13 November 2025, and commencement is phased. Section 44(2), which provides for the omission of Section 43A, is part of the eighteen-month commencement phase. Therefore, the DPDP framework should be presented as the transition from the earlier Section 43A and SPDI framework rather than as an already completed replacement.

5.4.3 e-contracts (Electronic Contracts)

Section 10A of the Information Technology Act, 2000 provides the specific statutory basis for the validity of contracts formed through electronic means. It states that a contract is not unenforceable merely because proposals, acceptances, revocations or other matters were expressed through electronic records or electronic means. The essential requirements of the contract itself continue to be governed by the Indian Contract Act, 1872.

The IT Act also contains exclusions in Section 1(4) read with the First Schedule. These include certain documents and transactions such as negotiable instruments other than cheques, powers of attorney, trusts, wills and contracts for the sale or conveyance of

SGOU

immovable property. Therefore, learners should not assume that every type of legal document can be completed electronically merely because electronic contracts are generally recognised.

An electronic contract, commonly known as an e-contract, is a legally binding agreement created and executed in electronic form without the need for physical paper or face-to-face interaction. These contracts are formed using digital communication methods such as emails, websites, mobile applications, or other online platforms.

In simple terms, an e-contract is an agreement between two or more parties that is created, communicated, and signed electronically. The Information Technology Act, 2000 provides legal recognition to such contracts, making them valid and enforceable in courts of law.

5.4.3.1 Features of e-contracts

E-contracts have several unique features that distinguish them from traditional paper-based contracts:

- They are created and executed in electronic form
- They do not require physical presence of parties
- They involve digital signatures or electronic consent
- They enable fast and efficient transactions
- They are stored and maintained digitally
- They can be accessed and verified anytime and anywhere

5.4.3.2 Types of e-contracts

E-contracts can be classified into different types based on how they are formed and accepted:

1. Click-Wrap Agreements

These contracts require users to click on an "I Agree" button before proceeding. They are commonly used in software installations and online services. Users must explicitly accept the terms and conditions.

2. Browse-Wrap Agreements

In these contracts, the terms and conditions are available on a website, and users are assumed to accept them by simply using the website. No explicit consent is required.

3. Shrink-Wrap Agreements

These agreements are associated with packaged software. The terms are included inside the product packaging, and the user accepts them by opening or using the product.

5.4.3.3 Essential Elements of e-contracts

Like traditional contracts, e-contracts must satisfy certain legal requirements:

SGOU

1. Offer – One party makes a clear proposal to another party expressing willingness to enter into a contract under specific terms and conditions.

2. Acceptance – The other party agrees to the terms of the offer without making any changes, thereby indicating consent to the agreement.

3. Consideration – There must be an exchange of something valuable, such as money, goods, or services, between the parties involved in the contract.

4. Intention to create legal relations – Both parties must intend that the agreement will be legally binding and enforceable in a court of law.

5. Free consent – The agreement must be made voluntarily without any coercion, fraud, misrepresentation, or undue influence.

6. Lawful object – The purpose of the contract must be legal and should not be against any law or public policy.

These elements ensure that e-contracts are valid, reliable, and legally enforceable.

5.4.3.4 Formation of e-contracts

The formation of an e-contract follows a similar process to traditional contracts but occurs electronically:

1. The seller displays products or services on a website (invitation to offer) – The display generally constitutes an invitation to potential buyers to make an offer, subject to the applicable terms and conditions.

2. The buyer selects the product and places an order (offer) – The buyer chooses the desired product or service and places an order, thereby making an offer to purchase.

3. The seller accepts the order – The seller accepts the buyer's offer according to the applicable terms. Payment then provides the consideration for the transaction.

4. Confirmation is sent via email or notification – After successful payment, the system sends a confirmation message or email, indicating that the contract has been formed.

This entire process happens digitally, making transactions quick, convenient, and efficient.

5.4.3.5 Advantages of e-contracts

E-contracts offer several advantages:

1. Speed and convenience – Contracts can be created and completed instantly without the need for physical meetings or paperwork.

SGOU

2. Cost-effective – E-contracts reduce costs by eliminating the need for paper, printing, and physical storage.

3. Global reach – Parties from different parts of the world can easily enter into contracts without geographical barriers.

4. Easy storage and retrieval – Digital records can be stored securely and accessed easily whenever required.

5. Environment-friendly – E-contracts reduce the use of paper, thereby supporting eco-friendly practices.

These advantages make e-contracts highly popular in e-commerce and business transactions.

5.4.3.6 Limitations of e-contracts

Despite their benefits, e-contracts have some limitations:

1. Lack of awareness among users – Many users are not fully aware of how e-contracts work, which may lead to misunderstandings or misuse.

2. Difficulty in verifying identity in some cases – It can be challenging to confirm the true identity of parties without strong authentication methods.

3. Risk of cyber fraud and hacking – Electronic contracts are vulnerable to cyber attacks, which may compromise their security and authenticity.

4. Legal issues in cross-border transactions – Different countries have different laws, which may create complications in enforcing e-contracts internationally.

5. Dependence on internet and technology – E-contracts require reliable internet connectivity and technical systems, and any failure may disrupt the process.

5.4.4 e-forms (Electronic Forms)

E-forms receive legal recognition as electronic records through Section 4 of the Information Technology Act, 2000. The provision gives legal recognition to information in electronic form where the law requires information to be in writing or printed form, subject to the conditions specified by the Act and the applicable law.

An electronic form, commonly known as an e-form, is a digital version of a traditional paper form that is used to collect, process, and store information electronically. In the modern digital environment, e-forms have become widely used across various online platforms such as websites, mobile applications, and e-governance portals, enabling users to submit information without the need for physical paperwork. These forms allow users to enter their details digitally and submit them instantly through the internet, making the process faster, more efficient, and convenient. Moreover, e-forms are legally recognized under the Information Technology Act, 2000, which ensures that the information submitted through them is valid and acceptable for official and legal purposes.

SGOU

A real-time example of e-forms can be seen when a student applies for an examination through an online university portal. In this process, the student enters personal and academic details into an electronic form provided on the website. The system automatically checks and validates the entered information to ensure accuracy and completeness before submission. Once the form is successfully submitted, the student receives a confirmation message or email as proof of submission. The submitted data is then stored digitally and processed by the institution for further actions such as registration and scheduling. This example clearly shows how e-forms make the process faster, more efficient, and paperless.

5.4.4.1 Features of e-forms

1. E-forms are paperless, as they eliminate the need for physical documents and manual filing.

2. They provide real-time data submission, allowing users to send information instantly.

3. E-forms support data validation, ensuring that correct and complete information is entered before submission.

4. They offer easy accessibility, as users can fill and submit forms from anywhere using the internet.

5. E-forms allow secure data storage, protecting information from loss or damage.

5.4.4.2 Types of e-forms

1. Simple e-forms – These forms are used to collect basic information such as name, email, and contact details. Example: A website contact form where users enter their name, email address, and message to get in touch with a company.

2. Interactive e-forms – These forms include features such as drop-down lists, checkboxes, and dynamic fields to improve user interaction. Example: An online shopping checkout form where users select options like delivery address, payment method, and product preferences using drop-down menus and checkboxes.

3. Secure e-forms – These forms are used for sensitive data and include security features such as encryption and authentication. Example: An online banking form where users enter account details, passwords, or OTPs for fund transfer or login purposes.

4. Government e-forms – These forms are used in e-governance services such as tax filing, registration, and application submissions. Example: An online income tax filing form or a passport application form submitted through a government portal.

SGOU

5.4.4.3 Advantages of e-forms

1. Time-saving – E-forms reduce the time required for filling, submitting, and processing information.

2. Cost-effective – They eliminate expenses related to paper, printing, and storage.

3. Accuracy – Built-in validation reduces errors and ensures correct data entry.

4. Convenience – Users can fill and submit forms anytime and from anywhere.

5. Efficient data management – Information can be stored, retrieved, and processed easily in digital format.

5.4.4.4 Limitations of e-forms

1. Dependence on technology – E-forms require internet access and electronic devices for usage.

2. Security risks – Sensitive data may be exposed if proper security measures are not implemented.

3. Technical issues – System errors or server failures may interrupt the submission process.

4. Lack of digital literacy – Some users may find it difficult to use e-forms due to limited technical knowledge.

5. Data privacy concerns – Improper handling of data may lead to privacy violations.

5.4.4.5 Applications of e-forms

1. E-forms are widely used in e-governance for services such as tax filing, license applications, and public service requests.

2. They are used in education systems for student registration, examinations, and feedback collection.

3. Businesses use e-forms for customer registration, surveys, and order processing.

4. Banks and financial institutions use e-forms for account opening, loan applications, and KYC processes.

5. Healthcare systems use e-forms for patient registration and medical records management.

SGOU

5.4.5 Comparison of Data Security, e-contracts, and e-forms

Table 5.4.1: Roles of Data Security, e-contracts, and e-forms

Aspect	Data Security	e-contracts	e-forms
Nature	Protection process and control framework	Electronic agreement	Digital information-collection instrument
Main Purpose	Protect confidentiality, integrity and availability	Create and evidence contractual relationships	Collect and submit information electronically
Legal basis	Sections 43, 43A, 70B and related rules	Section 10A and applicable contract law	Section 4 for legal recognition of electronic records
Example	Encryption and access control	Online purchase agreement	Online application form
Key Function	Protects confidentiality, integrity, and availability of data	Ensures agreement between parties with legal recognition	Collects and manages user information digitally
Examples	Encryption, firewalls, authentication	Online purchase agreement, click-wrap agreement	Online application forms, registration forms
Legal Aspect	Prevents cyber crimes and data breaches	Recognized under Information Technology Act, 2000	Accepted for official and legal submissions
Role in E-Commerce	Protects user and transaction data	Facilitates online agreements and transactions	Helps in collecting customer details and processing orders

SGOU

Recap

- The rapid growth of digital technologies has transformed daily activities such as shopping, banking, and communication into online processes.
- E-commerce enables businesses and consumers to perform transactions electronically without physical interaction.
- However, digital systems face challenges such as data theft, cyber fraud, and unauthorized access.
- Cyber laws play an important role in ensuring security and trust in digital transactions.
- The Information Technology Act, 2000 provides legal recognition to electronic records, digital signatures, and online contracts.
- Data security refers to protecting digital information from unauthorized access, misuse, or theft.
- It ensures confidentiality, integrity, and availability of data, forming the CIA Triad.
- Different types of data security include physical, network, application, and cloud security.
- Techniques such as encryption, authentication, authorization, firewalls, and antivirus software help protect data.
- Despite these measures, challenges like cyber attacks, weak passwords, and lack of awareness still exist.
- E-contracts are legally binding agreements created and executed in electronic form.
- They include essential elements such as offer, acceptance, consideration, free consent, and lawful object.
- E-contracts provide advantages like speed, cost-effectiveness, and global accessibility but also face issues like cyber risks and legal complexities.
- E-forms are digital forms used to collect, process, and store information electronically.
- They are widely used in e-governance, education, business, banking, and healthcare systems.
- Data security, e-contracts, and e-forms together form the foundation of a secure and efficient e-commerce ecosystem.

SGOU

Objective Type Questions

1. Identify the term used for protection of digital information from unauthorized access.
2. State the principle that ensures data is accessible only to authorized users.
3. Mention the principle that ensures data remains accurate and unaltered.
4. Specify the principle that ensures data is available whenever required.
5. Give the term for the unreadable form of data produced after encryption.
6. Identify the process used to verify the identity of a user.
7. Name the mechanism that determines user access rights.
8. Specify the type of security used to protect data during transmission over networks.
9. Define the term used for an electronic agreement between two parties.
10. Identify the element of a contract that indicates agreement to an offer.
11. Name the type of e-contract that requires users to click “I Agree”.
12. Give the term for a digital form used to collect and submit information electronically.
13. Identify the type of e-form designed to handle sensitive data securely.
14. Name the software used to detect and remove malicious programs.

SGOU

Answers to Objective Type Questions

1. Data Security
2. Confidentiality
3. Integrity
4. Availability
5. Ciphertext
6. Authentication
7. Authorization

8. Network Security
9. e-contract
10. Acceptance
11. Click-wrap
12. e-form
13. Secure E-Form
14. Antivirus

Assignments

1. Explain the concept of data security and discuss its types, principles, techniques, and challenges in detail.
2. Describe e-contracts and explain their features, types, formation process, advantages, and limitations.
3. Discuss the concept of e-forms, including their features, types, advantages, limitations, and applications in various fields.
4. Compare data security, e-contracts, and e-forms, and explain their role in ensuring a secure and efficient e-commerce environment.
5. Analyze how data security techniques such as encryption, authentication, and firewalls help in preventing cyber threats in e-commerce systems.
6. Examine the advantages and limitations of e-contracts and evaluate their effectiveness in ensuring secure and legally valid online transactions.

Suggested Reading

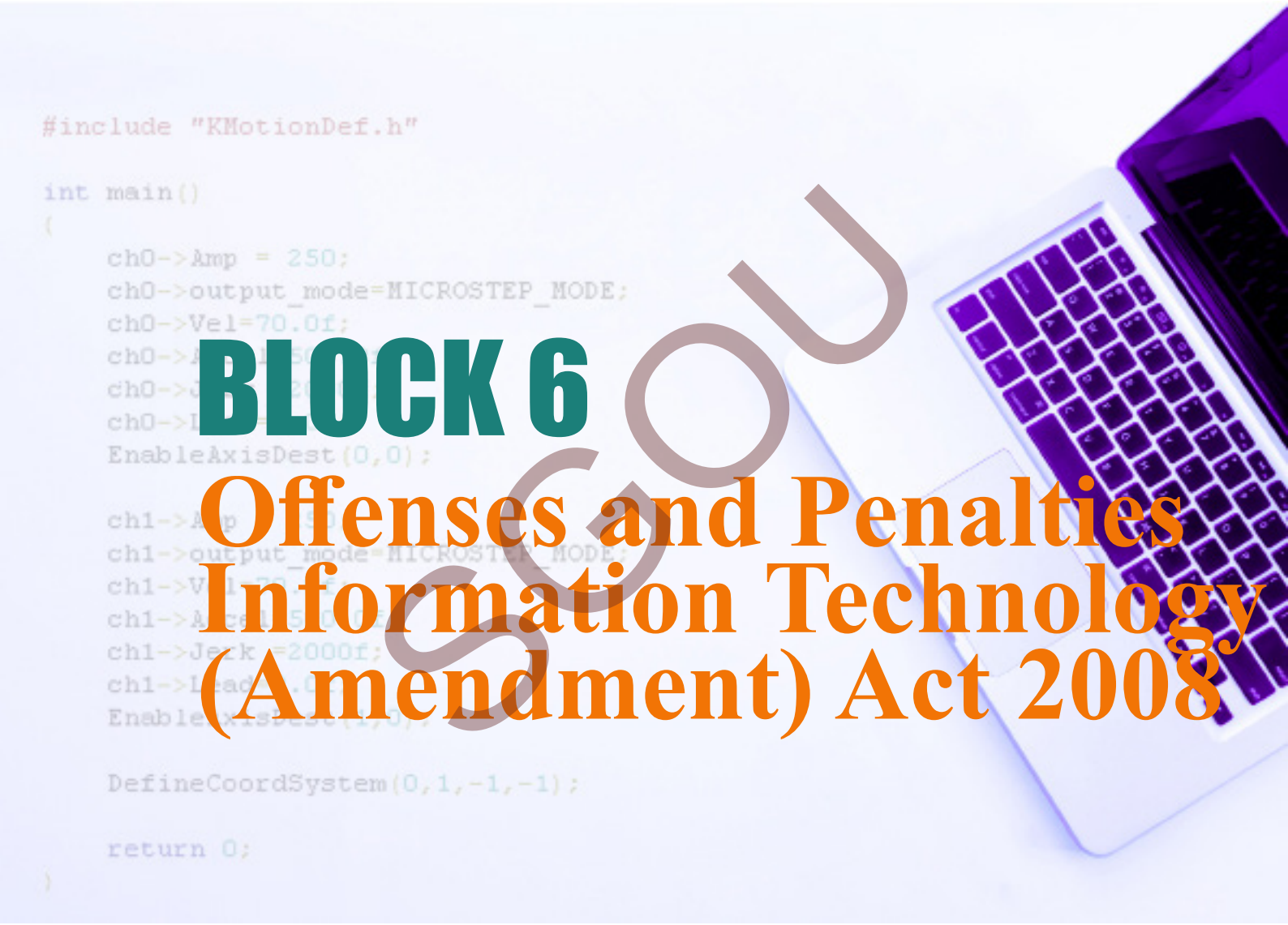
1. Duggal, P. (2025). *Cyber Law* (3rd ed.). LexisNexis.
2. Tiwari, G. (2014). *Understanding Laws: Cyber Laws and Cyber Crimes*. LexisNexis.
3. Ryder, R. D. (2011). *Guide to Cyber Laws*. Wadhwa & Company.

SGOU

Reference

1. Kosseff, J. (2025). Cyber security Law (4th ed.). John Wiley & Sons.
2. Craig, B. (2013). *Cyberlaw: The Law of the Internet and Information Technology*. Pearson Education.
3. Seth, K. (2012). *Computers, Internet and New Technology Laws*. LexisNexis.
4. https://www.cyberlaws.ne
5. https://www.indiacode.nic.in
6. https://www.meity.gov.in
7. https://cert-in.org.in
8. https://tdsat.gov.in

SGOU



BLOCK 6

Offenses and Penalties Information Technology (Amendment) Act 2008

SGOU

UNIT 1 Overview of Cyber Law and Jurisdiction

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- define the concept of cyber law and cyberspace
- list the need, importance, and objectives of cyber law in the digital environment
- explain the scope and applicability of cyber law in regulating online activities
- describe the legal framework governing cyberspace in India
- explain the concept of jurisdiction in cyberspace, identify the types and challenges of cyber jurisdiction

Prerequisites

A basic understanding of computers, the internet, and digital communication helps in understanding the concepts related to cyberspace and cyber law. Knowledge of how people use online platforms such as email services, websites, and social media explains how communication takes place through interconnected networks. For example, sending a message through *Gmail* involves the exchange of digital information through cyberspace.



SGOU

Familiarity with common online activities such as online banking, e-commerce, and digital payments also supports the understanding of cyber law concepts. These activities involve electronic transactions and digital records that require legal regulation and protection. For example, purchasing products through *Amazon* involves online payment systems and electronic contracts.

A general idea about legal rules and regulations in society also supports the understanding of how laws are applied in the digital environment. Just as traditional laws regulate activities in the physical world, cyber law governs activities carried out through computers and networks. For example, unauthorized access to a computer system or stealing digital data can be punished under the Information Technology Act, 2000 in India.

Keywords

Cyberspace, Information Technology Act, Cyber Jurisdiction, Applicability, Legal Framework.

Discussion

6.1.1 Introduction to Cyber Law

Cyberspace refers to the virtual environment created by interconnected computer networks, the internet, and digital communication systems where people interact, exchange information, and perform various online activities. It includes websites, online platforms, databases, and communication networks that enable global connectivity. For example, when a person sends an email, makes an online payment, or shops through an e-commerce website, these activities occur within cyberspace. Thus, cyberspace forms the digital world where individuals, organizations, and governments communicate and conduct transactions.

As cyberspace expanded, various online activities such as communication, financial transactions, data sharing, and online services increased rapidly. However, this growth also led to issues like hacking, identity theft, online fraud, and misuse of digital information. Since traditional laws were not fully capable of addressing crimes occurring in the digital environment, there arose a need for specific legal rules to regulate activities in cyberspace. This necessity created the foundation for cyber law, which helps maintain order, security, and accountability in the online world.

Cyber law refers to the set of legal rules and regulations that govern activities in cyberspace, including internet usage, digital transactions, cybercrimes, and protection of data and privacy. It ensures that individuals and organizations use digital technologies responsibly and legally. For example, laws that punish hacking, protect personal data, and regulate online banking transactions fall under cyber law. The concept of cyberspace itself gained recognition in the early 1980s when the term "cyberspace" first appeared in the science fiction works of *William Gibson*, particularly in his novel *Neuromancer*,

SGOU

which described a virtual digital world created by computer networks. Over time, the rapid growth of the internet transformed cyberspace from a fictional idea into a real global digital environment, leading to the development of cyber law to regulate it.

6.1.1.1 Need and Importance of Cyber Law

With the expansion of digital communication and online services, cyber law has become essential to regulate activities and protect users in cyberspace.

Need for Cyber Law

The rapid growth of the internet and digital technologies has significantly increased online activities such as communication, banking, e-commerce, and data sharing. Along with these benefits, cyberspace has also become vulnerable to various cybercrimes such as hacking, identity theft, online fraud, and data breaches. Therefore, cyber law is required to regulate activities in the digital environment, protect users, and ensure responsible use of technology. The need for cyber law arises due to several reasons:

- prevent cybercrimes
- give legal recognition to online transactions
- protect personal data and privacy
- ensure accountability

Importance of Cyber Law

Cyber law is important for ensuring safety, reliability, and proper conduct in the digital environment. It helps regulate online activities and control cybercrimes by taking legal action against offenders. Cyber law also encourages the development of digital services such as e-commerce, e-governance, and online banking by giving legal support to electronic transactions. In addition, it protects the rights of individuals and organizations by safeguarding data, privacy, and intellectual property. Therefore, cyber law plays a vital role in promoting the secure and responsible use of information technology in today's digital society.

6.1.2 Objectives of Cyber Law

Cyber law aims to establish a legal framework that governs activities carried out through computers, networks, and the internet. It focuses on regulating the use of digital technologies while ensuring security, fairness, and accountability in cyberspace. As online communication, digital transactions, and data sharing continue to expand, cyber law plays an important role in protecting users and maintaining trust in the digital environment. The major objectives of cyber law (Fig 6.1.1) include the following:

a. to prevent and control cybercrimes such as hacking, phishing, and online fraud.

b. to provide legal recognition to electronic records, digital signatures, and online transactions.

c. to protect personal data and ensure the privacy of individuals in the digital space.

SGOU

d. to safeguard intellectual property rights related to digital content and software.

e. to promote secure and reliable e-commerce and online services.

f. to ensure accountability and legal responsibility for individuals and organizations using information technology.



Fig 6.1.1: Objectives of Cyber Law

6.1.2.1 Scope of Cyber Law in the Digital Environment

Cyber law covers a wide range of activities and legal issues related to the use of computers, networks, and the internet. It regulates digital interactions and ensures security, legality, and proper conduct in the online environment. Some key points are:

- regulation of cybercrimes such as hacking, phishing, identity theft, and online fraud.
- legal recognition of electronic transactions including e-contracts and digital signatures.
- protection of personal data and privacy of individuals in digital platforms.
- safeguarding intellectual property rights related to software, digital content, and online publications.
- regulation of e-commerce activities and online business transactions.
- governance of internet usage and digital communication such as emails and social media.
- cybersecurity and protection of computer systems and networks from unauthorized access.
- legal control over online content and digital information sharing.

SGOU

6.1.3 Applicability of Cyber Law

In India, cyber law is mainly governed by the *Information Technology Act, 2000*, which provides legal recognition to electronic transactions and regulates activities in cyberspace. The Act applies to the whole country and also covers offences committed outside India if they involve a computer, computer system, or network located in India. It plays a significant role in supporting e-governance, e-commerce, and controlling cybercrimes.

Key Applicability of Cyber Law (IT Act, 2000)

- **Scope:** Applies to activities involving computers, computer systems, and computer networks.
- **Territorial Jurisdiction:** Applicable throughout India.
- **Extra-territorial Jurisdiction:** Covers cyber offences committed outside India if they involve a computer or network located in India.
- **E-Commerce and E-Governance:** Provides legal recognition to electronic records, digital signatures, and e-contracts.
- **Cybercrimes:** Addresses offences such as hacking, data theft, phishing, identity theft, and online fraud.

Key Exclusions (Non-Applicability)

The IT Act does not apply to certain legal documents, meaning their electronic form is not legally recognized under the Act:

- Promissory notes
- Trust deeds
- Power of attorney
- Will or testamentary documents
- Contracts related to the sale or transfer of immovable property

SGOU

6.1.3.1 Legal Framework Governing Cyberspace

The legal framework governing cyberspace refers to the set of laws, regulations, and policies that control and regulate activities carried out through computers, networks, and the internet. These laws are designed to ensure security, protect users, regulate online transactions, and prevent cybercrimes in the digital environment. In India, cyberspace is mainly regulated through specific legislation, rules, and regulatory authorities that manage digital activities and maintain cyber security.

Key components of the legal framework governing cyberspace include:

- **Information Technology Act, 2000:** The primary law that regulates electronic transactions, digital signatures, e-governance, and cybercrimes in India.

- **Information Technology (Amendment) Act, 2008:** Strengthens the IT Act by introducing provisions related to data protection, cyber terrorism, and identity theft.
- **Cybercrime Laws and Penal Provisions:** Certain cyber offences are also addressed under the Bharatiya Nyaya Sanhita (BNS), 2023, the Digital Personal Data Protection Act, 2023, and the updated IT Intermediary Guidelines and Digital Media Ethics Code Amendment Rules, 2026.
- **Data Protection and Privacy Regulations:** Laws and guidelines that protect personal and organizational data in digital systems.
- **Intellectual Property Laws:** Protect digital content, software, and online publications through copyright and related laws.
- **Regulatory Authorities and Agencies:** Government bodies responsible for monitoring cyber activities, handling cybercrime complaints, and enforcing cyber laws.

Together, these laws and regulations form a structured legal system that governs activities in cyberspace and ensures the secure and responsible use of information technology.

6.1.4 Jurisdiction in Cyberspace

Jurisdiction in cyberspace refers to the legal authority of a court or government to apply and enforce laws over activities that occur in the digital environment. Since the internet allows communication and transactions across national borders, determining which country's laws apply to a particular online activity can be challenging. Cyber jurisdiction helps identify the appropriate legal authority responsible for handling disputes, crimes, or legal matters that arise from online activities.

In cyberspace, jurisdiction may depend on factors such as the location of the user, the place where the computer system or server is located, or the country where the impact of the online activity occurs. Different countries have their own cyber laws to regulate online behavior and protect digital resources. In India, cyber offences and online transactions are mainly governed by the *Information Technology Act, 2000*, which also provides provisions for handling cybercrimes that involve computers or networks located within the country.

Thus, jurisdiction in cyberspace plays an important role in ensuring that cyber laws can be applied effectively, even when digital activities cross geographical and national boundaries.

6.1.4.1 Types of Jurisdiction in Cyber Law

Cyber jurisdiction refers to the authority of courts to hear and decide cases related to activities carried out in cyberspace. Since internet activities often cross geographical boundaries, determining the appropriate jurisdiction can be complex. Problems regarding cyber jurisdiction usually arise in different types of cases depending on whether the issue occurs within a country or across national borders.

SGOU

1. Cyber Jurisdiction in National Cases

Cyber jurisdiction in national cases refers to situations where a cyber activity or offence occurs within the boundaries of a single country and is handled by the courts of that country. These cases may involve disputes or crimes committed through computers, networks, or the internet within the same legal territory.

- **Cyber jurisdiction in civil cases:** Civil cyber cases involve disputes between individuals or organizations related to online activities.

  For example, a dispute between an online seller and buyer over a failed e-commerce transaction, or a case of copyright infringement on a website.

- **Cyber jurisdiction in criminal cases:** Criminal cyber cases involve offences where a person commits a cybercrime that violates criminal law.

  For example, hacking into a company's computer system, spreading malware, or committing online fraud within the country.

2. Cyber Jurisdiction in International Cases

International cyber jurisdiction arises when a cyber activity involves more than one country. In such cases, determining which country's court has the authority to handle the case becomes difficult because the offender, victim, and computer systems may be located in different countries. For example, a hacker located in another country illegally accessing a bank server located in India or committing online fraud targeting Indian users.

6.1.4.2 Challenges of Cyber Jurisdiction

The borderless nature of the internet makes it difficult to determine which country or legal authority has the power to handle cyber-related disputes and crimes. As online activities often involve multiple locations and jurisdictions, several challenges arise in applying and enforcing cyber laws effectively.

Major challenges of cyber jurisdiction include:

- **Borderless nature of the Internet:** Cyberspace does not follow geographical boundaries, making it difficult to identify the exact location where a cyber activity or offence occurred.

- **Difficulty in identifying the offender:** Cybercriminals often hide their identity using anonymous accounts, fake profiles, or virtual networks, making it challenging to trace the actual person responsible.

- **Multiple jurisdictions involved:** In many cyber cases, the offender, victim, and server may be located in different countries, creating confusion about which country's laws should apply.

- **Differences in national cyber laws:** Different countries have different legal frameworks for cybercrime, which may lead to conflicts or gaps in enforcement.

SGOU

- **Problems in evidence collection:** Digital evidence may be stored in different locations or countries, making it difficult for authorities to access and collect it legally.
- **Lack of international cooperation:** Effective investigation of cybercrimes often requires cooperation between countries, but differences in laws and procedures can delay the legal process.

Cyber law refers to the legal rules that regulate activities carried out through computers, networks, and the internet. It is necessary to prevent cybercrimes, protect data and privacy, and provide legal recognition to electronic transactions and digital communication. The scope of cyber law covers areas such as cybersecurity, e-commerce, data protection, online communication, and intellectual property rights. In India, cyberspace activities are mainly regulated by the Information Technology Act 2000, which provides legal support for electronic records and digital transactions. Cyber jurisdiction determines the authority of courts to handle cyber-related cases, although the borderless nature of the internet creates several challenges in enforcing cyber laws.

Recap

- Cyber law refers to the legal rules that regulate activities carried out through computers, networks, and the internet.
- Cyberspace is the virtual environment where digital communication and online transactions take place.
- The growth of the internet has increased the need for cyber law to control misuse of digital technologies.
- Cyber law helps prevent cybercrimes such as hacking, phishing, identity theft, and online fraud.
- It provides legal recognition to electronic transactions like e-commerce, e-contracts, and digital signatures.
- Cyber law also protects personal data and privacy of individuals in the digital environment.
- One objective of cyber law is to ensure accountability and responsible use of information technology.
- The scope of cyber law covers areas such as cybersecurity, digital communication, e-commerce, and intellectual property rights.
- Cyber law also regulates online content, digital information sharing, and internet usage.
- In India, cyberspace activities are mainly governed by the Information Technology Act, 2000.

SGOU

- The legal framework of cyberspace includes laws, regulations, and authorities responsible for cyber security and cybercrime control.
- Jurisdiction in cyberspace refers to the authority of courts to deal with cyber-related disputes and offences.
- Cyber jurisdiction may apply to civil cases such as online business disputes.
- It also applies to criminal cases involving cyber offences like hacking and data theft.
- The borderless nature of the internet creates challenges in cyber jurisdiction such as identifying offenders and determining the correct legal authority.

Objective Type Questions

1. What is the virtual environment created by interconnected computer networks called?
2. Which law primarily governs cyber activities in India?
3. What term refers to crimes committed using computers and the internet?
4. What is the legal recognition given to online agreements called?
5. What type of signature is used to authenticate electronic documents?
6. What is unauthorized access to a computer system commonly called?
7. What term refers to the authority of a court to hear a cyber case?
8. What type of jurisdiction deals with disputes between individuals or organizations online?
9. What type of jurisdiction deals with offences like hacking and fraud?
10. What is the illegal act of stealing personal information online called?
11. What term refers to protecting creative digital works such as software and content?
12. What is the process of buying and selling goods through the internet called?
13. What term refers to government services provided through digital platforms?
14. What type of evidence is collected from computers or electronic devices in cyber cases?
15. What term describes the global digital network that connects computers worldwide?

SGOU

Answers to Objective Type Questions

1. Cyberspace
2. IT Act
3. Cybercrime
4. E Contract
5. Digital Signature
6. Hacking
7. Jurisdiction
8. Civil
9. Criminal
10. Identity Theft
11. Copyright
12. E commerce
13. E governance
14. Digital Evidence
15. Internet

Assignments

1. Explain the concept of cyber law and discuss the need and importance of cyber law in the digital society.
2. Describe the objectives and scope of cyber law in the digital environment with suitable examples.
3. Explain the applicability of cyber law in India and discuss the legal framework governing cyberspace with reference to the Information Technology Act, 2000.
4. Discuss the concept of jurisdiction in cyberspace and explain the types of cyber jurisdiction and the challenges involved in enforcing cyber laws.

SGOU

Suggested Reading

1. Legal Bites – Cyber Law Notes and Study Material https://www.legalbites.in/library-cyber-laws
2. Cyber Law India – Cyber Law Resources and Legal Information https://www.cyberlawindia.com/
3. Cyber Talk India – Cyber Laws Basic https://www.cybertalkindia.com/cyber-laws-basic/
4. Centre for Research and Governance on Cyber Law (CRGCL) https://crgcl.com/resources/
5. eGyanKosh – Introduction to Cyber Law and IT Act in India http://egyankosh.ac.in/handle/123456789/56074

Reference

1. Information Technology Law and Practice: Cyber Laws and Laws Relating to E-Commerce Sharma, V., & Sharma, S. (2025). *Information technology law and practice: Cyber laws and laws relating to e-commerce* (9th ed.). LexisNexis.
2. Cyber Law Duggal, P. (2023). *Cyber law: An exhaustive section-wise commentary on the Information Technology Act*. LexisNexis.
3. Information Technology and Cyber Law Malik, K. P. (2025). *Information technology and cyber law* (3rd ed.). Allahabad Law Agency.
4. Information Technology Law (Cyber Laws) Myneni, S. R. (2024). *Information technology law (Cyber laws)* (5th ed.). Asia Law House.
5. Cyber Security and Cyber Laws Jain, N., & Menon, R. (2020). *Cyber security and cyber laws*. Wiley India.

SGOU



UNIT 2 Cyber Crimes and Legal Penalties

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- define the concept of cyber crimes and legal penalties in the digital environment
- identify different types of cyber crimes covered under various sections of the Information Technology Act
- list the relevant legal sections related to common cyber offences
- explain the penalties, punishments, and fines associated with different cyber crimes
- describe the importance of cyber laws in preventing cyber offences and ensuring digital security

Prerequisites

A basic understanding of computers, the internet, and digital communication systems is important for understanding cyber crimes and legal penalties. Knowledge of how people use online platforms such as email, social media, and online banking helps explain how cyber offences occur in the digital environment. For example, receiving a fake email requesting bank account details or login credentials is a common situation related to online fraud.

Familiarity with basic cybersecurity concepts and common online threats is also helpful. Terms such as hacking, phishing, malware, and data privacy provide a foundation for understanding different types of cyber offences. For example, when someone illegally accesses another person's social media account and changes the password without permission, it is an example of hacking and identity theft.

Basic awareness of laws and regulations related to digital activities is another important prerequisite. Online actions are also governed by legal rules, and certain activities may lead to legal consequences. For example, creating a fake online profile to cheat someone or sharing obscene content on the internet can result in penalties under the Information Technology Act, 2000.

SGOU



Keywords

Legal Framework, Ethical Hackers, Cyber Safety, Legal Sections, Penalties

Discussion

6.2.1 Introduction to Cyber Crimes

Imagine receiving a message that appears to be from your bank asking you to verify your account details. Trusting the message, you enter your login credentials only to later discover that your money has been stolen. This is a common example of a cybercrime known as phishing, where criminals use digital platforms to deceive individuals and gain unauthorized access to sensitive information. Such incidents highlight how technology, while beneficial, can also be misused for illegal activities.

Cybercrime refers to any unlawful act that is carried out using computers, digital devices, or the internet. These crimes may target individuals, organizations, or governments and often involve the theft, manipulation, or destruction of data. Examples include hacking, identity theft, online fraud, cyberstalking, and spreading malicious software. As technology continues to advance, the scope and complexity of cybercrimes are also increasing.

The meaning of cybercrime extends beyond just illegal activities involving computers. It includes any offense where a computer, network, or digital device acts as a tool, target, or medium of the crime. In some cases, computers are used to commit traditional crimes like fraud or harassment, while in others, they are the primary target, such as in hacking or denial-of-service attacks. Thus, cybercrime is a broad term that covers a wide range of digital offenses.

The term "*cybercrime*" has evolved alongside the rise of the internet and digital technology. While the concept of using technology for criminal purposes is not new, the

SGOU

specific term gained popularity in the late 20th century as computers became integral to everyday life. The first recorded cybercrime dates back to 1820, illustrating that the intersection of technology and crime has a long history.

With the rapid growth of the internet in the late 20th and early 21st centuries, cybercrime has become a major global concern. Increased connectivity, online transactions, and digital communication have created more opportunities for cybercriminals to exploit vulnerabilities. As a result, governments and organizations worldwide have developed laws and security measures to combat cyber threats, making awareness and understanding of cybercrime essential in today's digital age.

6.2.2 Classification of Cyber Crimes

Classification of cyber crimes refers to the systematic grouping of different types of cyber offences based on their target, nature, and impact. This classification helps in better understanding cyber threats and enables legal authorities to apply appropriate laws and penalties. Generally, cyber crimes are classified into four major categories: crimes against individuals, property, organizations, and society or government.

1. **Crimes against individuals:** These are cyber crimes that directly affect a person's privacy, reputation, or financial security. The main objective is to harm or exploit an individual using digital means. Examples include identity theft, cyberstalking, online harassment, phishing, and email spoofing. For instance, creating a fake social media profile to defame someone or stealing personal banking details through fraudulent emails falls under this category.

2. **Crimes against property:** These crimes target digital or intellectual property such as data, software, and digital assets. The intention is usually to damage, steal, or misuse property. Examples include hacking, spreading malware or viruses, data theft, and software piracy. For example, illegally accessing a company's database and stealing confidential information or distributing pirated software online are crimes against property.

3. **Crimes against organizations:** These cyber crimes are committed against companies, institutions, or organizations to disrupt their operations or steal sensitive information. Examples include unauthorized access to corporate systems, denial-of-service (DoS) attacks, ransomware attacks, and data breaches. For instance, hackers attacking a company's website and making it unavailable to users is a common organizational cybercrime.

4. **Crimes against society and government:** These are serious cyber offences that impact public order, national security, or government operations. Examples include cyber terrorism, online propaganda, spreading fake news, and hacking government websites. For example, attacking a government database or spreading misinformation to create panic among the public are considered crimes against society and government.

In conclusion, classifying cyber crimes helps in understanding the wide range of digital offences and their impact on different sectors. It also plays a crucial role in developing effective prevention strategies and enforcing cyber laws.

SGOU

6.2.3 Legal Framework for Cyber Crimes in India

India has developed a structured legal framework to address the growing challenges of cyber crimes. With the rapid expansion of digital technologies and online transactions, there was a need for specific laws to regulate cyberspace and ensure security. The legal framework mainly consists of the Information Technology Act, 2000 and the Indian Penal Code, along with other supporting regulations and amendments. These laws define cyber offences, prescribe penalties, and provide mechanisms for investigation and enforcement.

6.2.3.1 Overview of the Information Technology Act, 2000

The Information Technology Act, 2000 is the primary legislation governing cyber activities in India. It was enacted to provide legal recognition to electronic records, digital signatures, and online transactions, thereby facilitating e-commerce and e-governance. The Act also defines various cyber offences such as hacking, identity theft, cyber terrorism, and publishing obscene content, along with their respective punishments and penalties.

The Act includes important provisions like Section 43 (penalties for damage to computer systems), Section 66 (computer-related offences), Section 66C (identity theft), Section 66D (cheating by personation), and Section 67 (publishing or transmitting obscene material). Amendments to the Act, especially in 2008, strengthened its provisions by addressing emerging cyber threats and enhancing penalties. Overall, the Act serves as the backbone of cyber law enforcement in India.

6.2.3.2 Role of the Indian Penal Code in Cyber Offences

While the Information Technology Act, 2000 specifically deals with cyber crimes, the Indian Penal Code also plays a significant role in addressing offences that involve digital elements. Traditional crimes such as cheating, fraud, defamation, criminal intimidation, and forgery are covered under the IPC, even when they are committed through online platforms.

For example, online cheating can be punished under Section 420 of the IPC, while cyber defamation is addressed under Section 499. Similarly, sending threatening messages through digital means can fall under criminal intimidation provisions. Thus, the IPC complements the IT Act by covering areas that are not explicitly mentioned in cyber laws.

In conclusion, the combined application of the Information Technology Act, 2000 and the Indian Penal Code ensures a comprehensive legal approach to tackling cyber crimes in India, helping maintain law and order in the digital environment.

6.2.3.3 Types of Cybercriminals

Cybercriminals are individuals or groups who use computers and digital technologies to perform illegal or unethical activities. They vary based on their skills, intentions, and methods. Understanding these types (Fig 6.2.1) helps in identifying threats and improving cybersecurity measures.

SGOU

1. **White Hat Hackers (Ethical Hackers):** White hat hackers are authorized professionals who use their skills to identify and fix security vulnerabilities in systems. They work legally for organizations to strengthen cybersecurity.

   ***Example**:* A cybersecurity expert hired by a company to test its website for weaknesses and prevent hacking attacks.

2. **Black Hat Hackers:** Black hat hackers are malicious individuals who exploit system vulnerabilities for personal gain, financial benefit, or to cause damage. Their actions are illegal.

   Example: A hacker breaking into a bank's database to steal customer account details and transfer money.

3. **Grey Hat Hackers:** Grey hat hackers fall between white and black hat hackers. They may access systems without permission but usually do not have harmful intentions. However, their actions are still considered illegal.

   Example: A hacker finding a security flaw in a website and informing the company after accessing it without authorization, sometimes expecting a reward.

4. **Script Kiddies (Amateur Hackers):** These are inexperienced individuals who use existing hacking tools created by others. They often lack deep technical knowledge and act for fun or curiosity.

   Example: A student using free software to temporarily crash a website.

5. **Organized Cybercriminal Groups:** These are professional groups involved in large-scale cybercrimes for financial gain. They operate like businesses with planned attacks.

   Example: A group launching ransomware attacks on companies and demanding payment to restore data.

6. **Insiders (Internal Threats):** Insiders are individuals within an organization who misuse their access to harm the system or steal data.

   Example: An employee leaking confidential company information to competitors.

7. **Hacktivists:** Hacktivists carry out cyber attacks to promote political or social causes. Their goal is not money but spreading a message or protest.

   Example: Defacing a government website to protest against a policy.

8. **Cyber Terrorists:** Cyber terrorists use digital attacks to create fear and disrupt national security or critical infrastructure.

   Example: Attacking a country's power grid or communication systems.

SGOU



Fig 6.2.1: Types of Cybercriminals

9. **State-Sponsored Hackers:** These hackers are supported by governments to conduct cyber espionage or attacks on other nations.

   Example: Stealing confidential military or strategic data from another country.

10. **Identity Thieves and Online Fraudsters:** These criminals specialize in stealing personal and financial information for fraud.

    Example: Sending fake emails (phishing) to trick users into revealing bank passwords.

Cybercriminals range from ethical professionals to highly dangerous attackers. Categories like white, grey, and black hat hackers highlight the difference between ethical, unethical, and illegal activities. Understanding these types is essential for developing effective cybersecurity strategies and legal controls.

6.2.4 Various Cyber Crimes and Relevant Legal Sections

Cybercrime refers to illegal activities carried out using computers, digital devices, or the internet, which can harm individuals, organizations, and governments. With the

rapid growth of technology and online communication, different forms of cybercrimes such as hacking, identity theft, online fraud, cyberstalking, and data breaches have become increasingly common. These crimes not only cause financial losses but also threaten privacy, security, and trust in digital systems. To combat such offences, various laws and legal provisions have been established to regulate online activities and punish offenders. Understanding the different types of cybercrimes and the relevant legal sections helps individuals become aware of their rights and responsibilities in the digital environment.

1. Hacking and Unauthorized Access (Sections 43 and 66)

Hacking refers to gaining unauthorized access to a computer system, network, or data without the permission of the owner. Under Section 43 of the Information Technology Act, 2000, any person who accesses, downloads, copies, or damages data from a computer system without authorization is liable to pay compensation for the damage caused. When such actions are carried out with dishonest or fraudulent intention, Section 66 treats it as a criminal offence. The offender may face imprisonment and a fine for illegally accessing or damaging computer resources.

2. Identity Theft (Section 66C)

Identity theft occurs when a person fraudulently uses another individual's personal information such as passwords, digital signatures, or identification details without consent. Section 66C of the Information Technology Act, 2000 specifically deals with identity theft in the digital environment. Cybercriminals may misuse such information to access bank accounts, social media accounts, or other online services. The law prescribes punishment including imprisonment and monetary fines for such offences.

3. Cheating by Personation (Section 66D)

Cheating by personation refers to pretending to be someone else through electronic communication in order to deceive or defraud others. According to Section 66D of the Information Technology Act, 2000, this crime commonly occurs through fake emails, fraudulent websites, or impersonating individuals on social media platforms. The intention is usually to obtain money, personal data, or other benefits from victims. Individuals found guilty of this offence may face imprisonment along with a fine.

4. Cyber Terrorism (Section 66F)

Cyber terrorism involves the use of computer systems or networks to threaten national security, public safety, or the sovereignty of a country. Section 66F of the Information Technology Act, 2000 defines cyber terrorism as acts such as attacking critical information infrastructure, accessing sensitive government data, or causing large-scale disruptions through cyber attacks. These activities can create fear and instability in society. Due to the seriousness of the crime, cyber terrorism is punishable with severe penalties, including life imprisonment.

5. Publishing Obscene Content (Section 67)

Publishing or transmitting obscene material through electronic media is punishable

SGOU

under Section 67 of the Information Technology Act, 2000. This includes sharing obscene images, videos, or messages through websites, emails, or social networking platforms. Such content is considered harmful to public morality and social values. The law provides penalties including imprisonment and fines for individuals who create, publish, or distribute obscene material online.

6. Data Theft and Privacy Violations (Sections 43 and 72)

Data theft refers to the unauthorized access, copying, or misuse of confidential or personal information stored in computer systems. Section 43 of the Information Technology Act addresses unauthorized extraction or use of data, while Section 72 deals with breaches of confidentiality and privacy. Section 72 applies particularly to individuals who disclose personal information obtained during their professional duties without permission. Such actions can harm individuals and organizations, and offenders may face legal penalties.

7. Phishing and Online Fraud (Sections 66C and 66D)

Phishing and online fraud involve deceiving individuals into revealing sensitive information such as passwords, bank details, or OTPs through fake emails, messages, or websites. Cybercriminals often impersonate trusted institutions like banks or companies to gain the victim's trust. These crimes fall under Sections 66C and 66D of the Information Technology Act, 2000, which address identity theft and cheating by personation. The law imposes strict punishments to prevent financial fraud and protect online users.

The table 6.2.1 below shows some common types of cyber crimes along with the relevant sections of the Information Technology Act, 2000 and their simple description.

Table 6.2.1: Cyber Crimes and Legal Sections

Cyber Crime	Section	Description
Hacking and Unauthorized Access	Section 43, 66	Accessing or damaging a computer system or data without the owner's permission.
Identity Theft	Section 66C	Using another person's password, digital signature, or personal details without permission.
Cheating by Personation	Section 66D	Pretending to be another person online to cheat or deceive someone.
Cyber Terrorism	Section 66F	Using computers or networks to threaten national security or create fear in society.
Publishing Obscene Content	Section 67	Sharing or publishing obscene images, videos, or messages online.
Data Theft and Privacy Violations	Section 43, 72	Stealing or misusing confidential data and breaking privacy rules.
Phishing and Online Fraud	Section 66C, 66D	Tricking people through fake emails or websites to steal personal or bank information.

SGOU

Understanding different cyber crimes and their related legal sections helps individuals become more aware of digital threats and their legal consequences. These laws play an important role in protecting users, maintaining cybersecurity, and ensuring responsible use of technology.

6.2.5 Penalties, Punishments, and Fines

Penalties, punishments, and fines are important legal measures used to control and prevent cyber crimes. These legal consequences are defined under the Information Technology Act, 2000 and other relevant laws to ensure that offenders are held responsible for their actions. Depending on the seriousness of the offence, the punishment may include imprisonment, monetary fines, or both. Such legal provisions help protect individuals, organizations, and governments from cyber threats. They also promote responsible and lawful use of digital technologies.

Imprisonment Provisions

Imprisonment provisions are legal punishments that involve sending offenders to jail for committing cyber crimes. Under the Information Technology Act, 2000, serious offences such as hacking, identity theft, cyber fraud, and cyber terrorism may lead to imprisonment for a specified period. The length of imprisonment depends on the severity and impact of the crime. These provisions act as a strong deterrent against committing cyber offences.

Monetary Penalties and Compensation

Monetary penalties refer to fines imposed on individuals who commit cyber offences. In some cases, offenders may also be required to pay compensation to the victims for the damage or financial loss caused. These penalties are specified under different sections of the Information Technology Act, 2000. Monetary punishments help ensure that victims receive some form of justice and recovery for their losses.

Civil vs Criminal Liability

Civil liability and criminal liability are two types of legal responsibilities related to cyber crimes. Civil liability usually involves paying compensation for damages caused to another person or organization. Criminal liability, on the other hand, involves punishment such as imprisonment or fines imposed by the court for committing a crime. Both forms of liability help enforce laws and ensure accountability in the digital environment.

6.2.5.1 Penalties, Punishments, and Fines related to Cyber Crimes

The penalties, punishments, and fines related to the various cyber crimes discussed above are explained below.

1. **Hacking and Unauthorized Access (Sections 43, 66):** Hacking or unauthorized access to a computer system is punishable under the Information Technology Act, 2000. Section 43 provides for compensation for damages caused due to unauthorized access, downloading, or disruption of computer

SGOU

systems. If the act is done with dishonest or fraudulent intention, Section 66 applies, which provides punishment of imprisonment up to three years or a fine up to ₹5 lakh, or both.

2. **Identity Theft (Section 66C):** Identity theft involves the fraudulent use of another person's electronic identity such as passwords, digital signatures, or personal identification details. According to Section 66C of the Information Technology Act, 2000, offenders committing identity theft can be punished with imprisonment up to three years and a fine up to ₹1 lakh.

3. **Cheating by Personation (Section 66D):** Cheating by personation refers to impersonating someone else through electronic communication in order to cheat or deceive another person. Section 66D of the Information Technology Act, 2000 states that individuals found guilty of this offence may face imprisonment up to three years along with a fine up to ₹1 lakh.

4. **Cyber Terrorism (Section 66F):** Cyber terrorism is considered one of the most serious cyber offences as it threatens national security and public safety. Under Section 66F of the Information Technology Act, 2000, individuals involved in cyber terrorism activities such as attacking critical information infrastructure may be punished with imprisonment for life.

5. **Publishing Obscene Content (Section 67):** Publishing or transmitting obscene material in electronic form is punishable under Section 67 of the Information Technology Act, 2000. For the first offence, the punishment may include imprisonment up to three years and a fine up to ₹5 lakh. For subsequent offences, the punishment may extend to imprisonment up to five years and a fine up to ₹10 lakh.

6. **Data Theft and Privacy Violations (Sections 43, 72):** Data theft and violation of privacy are punishable offences under the Information Technology Act, 2000. Section 43 provides compensation for unauthorized access or misuse of data, while Section 72 deals with breach of confidentiality and privacy. The punishment under Section 72 may include imprisonment up to two years or a fine up to ₹1 lakh, or both.

7. **Phishing and Online Fraud (Sections 66C, 66D):** Phishing and online fraud involve deceiving individuals to obtain sensitive information such as bank details or passwords. These offences are covered under Sections 66C and 66D of the Information Technology Act, 2000. Offenders may face imprisonment up to three years and a fine up to ₹1 lakh for such fraudulent activities.

The table 6.2.2 below depicted penalties, punishments, and fines related to the various cyber crimes.

SGOU

Table 6.2.2: Penalties, punishments, and fines related to the various cyber crimes

Cyber Crime	Relevant Section(s)	Penalties / Punishment / Fine
Hacking and Unauthorized Access	Section 43, 66	Compensation for damages under Section 43. Under Section 66, imprisonment up to 3 years or fine up to ₹5 lakh, or both.
Identity Theft	Section 66C	Imprisonment up to 3 years and fine up to ₹1 lakh.
Cheating by Personation	Section 66D	Imprisonment up to 3 years and fine up to ₹1 lakh.
Cyber Terrorism	Section 66F	Imprisonment for life.
Publishing Obscene Content	Section 67	*First offence:* Imprisonment up to 3 years and fine up to ₹5 lakh. *Subsequent offences:* Imprisonment up to 5 years and fine up to ₹10 lakh.
Data Theft and Privacy Violations	Section 43, 72	Compensation for damages under Section 43. Under Section 72, imprisonment up to 2 years or fine up to ₹1 lakh, or both.
Phishing and Online Fraud	Section 66C, 66D	Imprisonment up to 3 years and fine up to ₹1 lakh.

6.2.6 Cyber Crime Investigation and Enforcement

Cyber crime investigation and enforcement involve the process of identifying, examining, and taking legal action against individuals who commit cyber offences. Law enforcement agencies use specialized tools, technologies, and legal procedures to track cybercriminals and collect evidence. Investigations often include analyzing computer systems, networks, and digital records to find proof of illegal activities. Effective enforcement of cyber laws helps ensure justice and strengthens cybersecurity.

Role of Cyber Cells and Law Enforcement Agencies

Cyber cells are specialized units within law enforcement agencies that deal specifically with cyber crimes. These units investigate cases such as hacking, online fraud, identity theft, and cyber harassment. They work with digital experts and use advanced technologies to trace cybercriminals and gather evidence. Cyber cells also assist victims in reporting crimes and take necessary legal actions against offenders.

Digital Evidence and Forensic Procedures

Digital evidence refers to information stored or transmitted in electronic form that can be used during cyber crime investigations. Examples include emails, log files, digital

SGOU

documents, and data from computers or mobile devices. Forensic procedures involve collecting, preserving, analyzing, and presenting this digital evidence in a legally acceptable manner. Digital forensics helps investigators identify the source of cyber attacks and support legal proceedings in court.

6.2.7 Challenges in Cyber Law Enforcement

Cyber law enforcement faces several challenges due to the complex and rapidly evolving nature of digital technologies. Cyber crimes often occur across different networks and locations, making investigation and legal action difficult. Law enforcement agencies must continuously update their knowledge, skills, and tools to effectively deal with emerging cyber threats. Overcoming these challenges is essential for ensuring the effective implementation of cyber laws and protecting users in the digital environment.

1. **Jurisdiction issues:** Jurisdiction issues arise when cyber crimes involve individuals, computer systems, or servers located in different countries or regions. Since the internet operates globally, it becomes difficult to determine which country's legal authority should handle the case. This creates complications in investigation, evidence collection, and prosecution of offenders. International cooperation between governments and law enforcement agencies is often required to address such cases.

2. **Rapid technological changes:** Technology is advancing at a very fast pace, and cybercriminals constantly develop new techniques to exploit digital systems. This rapid change makes it difficult for existing laws and enforcement mechanisms to keep up with emerging threats. Law enforcement agencies must regularly upgrade their technical knowledge and investigative tools. Continuous training and technological support are therefore necessary for effective cyber crime investigation.

3. **Lack of awareness:** Lack of awareness among internet users is another major challenge in cyber law enforcement. Many people are not fully aware of cyber laws, online risks, or the procedures for reporting cyber crimes. As a result, victims may fail to take preventive measures or may delay reporting incidents. Increasing public awareness and cybersecurity education can help reduce cyber offences and improve law enforcement efforts.

4. **Difficulty in identifying cybercriminals:** Identifying cybercriminals can be very challenging because offenders often hide their identities using fake accounts, encrypted communication, or anonymous networks. They may also operate from different locations or countries, making it harder to trace them. This anonymity complicates the process of tracking and collecting evidence against offenders. Advanced investigation techniques and digital forensic tools are required to identify and catch cybercriminals.

6.2.8 Preventive Measures and Cyber Safety

Preventive measures and cyber safety practices are essential for protecting individuals, organizations, and digital systems from cyber threats. By following proper security

SGOU

practices and being aware of online risks, users can reduce the chances of becoming victims of cyber crimes. Cyber safety involves adopting responsible online behavior, using secure technologies, and regularly updating security systems. Both individuals and institutions play an important role in maintaining a safe and secure digital environment.

1. **Individual precautions:** Individuals can protect themselves from cyber threats by following basic online safety practices. These include using strong and unique passwords, avoiding sharing personal information online, and being cautious about suspicious emails or links. Regularly updating software and installing antivirus programs can also help prevent cyber attacks. Being aware of common cyber fraud techniques such as phishing is important for personal cybersecurity.

2. **Organizational security practices:** Organizations must implement strong cybersecurity measures to protect their data and systems from cyber attacks. This includes using firewalls, encryption, secure networks, and regular security audits. Employee training programs can help staff understand cyber risks and follow safe digital practices. Proper data backup and access control systems also help prevent data breaches and unauthorized access.

3. **Government initiatives:** Governments play a key role in promoting cyber safety by creating laws, policies, and awareness programs. They establish specialized cyber security agencies and cyber cells to investigate and prevent cyber crimes. Governments also conduct public awareness campaigns and provide guidelines for safe internet usage. Such initiatives help strengthen national cybersecurity and protect citizens from digital threats.

4. **Cybersecurity awareness and education:** Cybersecurity awareness and education are important for building a safe digital society. Educational institutions, organizations, and government bodies conduct training programs, workshops, and campaigns to educate people about cyber risks and safety practices. These programs help individuals understand how to protect their personal data and recognize cyber threats. Increasing awareness plays a vital role in reducing cyber crimes.

In conclusion, cyber crimes have become a major concern with the rapid growth of digital technologies and internet usage. Different types of cyber offences are addressed under various sections of the Information Technology Act, 2000, which specify the corresponding penalties, punishments, and fines. These legal provisions aim to deter cybercriminal activities and ensure justice for victims. Awareness of these laws helps individuals understand the legal consequences of cyber offences and promotes responsible digital behavior. Strengthening cyber law enforcement and public awareness is essential for maintaining a safe and secure cyberspace.

SGOU

Recap

- Cyber crime refers to illegal activities carried out using computers, networks, or the internet.
- The rapid growth of digital technology has increased the number of cyber crimes worldwide.
- In India, cyber crimes are mainly addressed under the Information Technology Act, 2000.
- Hacking involves unauthorized access to computer systems or networks.
- Unauthorized access and damage to computer resources are covered under Section 43.
- Section 66 deals with computer-related offences including hacking.
- Identity theft occurs when someone uses another person's digital identity without permission.
- Identity theft is punishable under Section 66C of the IT Act.
- Cheating by personation in online environments is covered under Section 66D.
- Cyber terrorism refers to the use of computers or networks to threaten national security and is addressed under Section 66F.
- Publishing or transmitting obscene content online is punishable under Section 67.
- Phishing is a cyber fraud technique used to obtain sensitive information such as passwords and banking details.
- Data theft and privacy violations involve the unauthorized use or disclosure of personal or organizational data.
- Cyber crimes can lead to serious legal consequences including imprisonment and fines.
- Some cyber offences may also require offenders to pay compensation to victims.
- Cyber crimes can involve both civil liability and criminal liability.
- Digital evidence plays an important role in investigating cyber offences.
- Cyber cells and law enforcement agencies handle cyber crime investigations.
- Challenges in cyber law enforcement include jurisdiction issues and rapid technological changes.
- Awareness of cyber laws helps promote safe and responsible use of digital technologies.

SGOU

Objective Type Questions

1. What type of crime is committed using computers and the internet?
2. Which Act in India mainly deals with cyber crimes?
3. Under which section is identity theft punished in the IT Act?
4. Which section deals with cheating by personation in cyber space?
5. What is the illegal access to a computer system called?
6. Which section of the IT Act deals with cyber terrorism?
7. Which section punishes publishing obscene content online?
8. What is the act of sending fake emails to obtain personal information called?
9. What term refers to stealing confidential digital information?
10. What type of evidence collected from computers is used in cyber crime investigations?
11. Which government units handle cyber crime complaints in many cities?
12. What term describes legal responsibility that results in punishment like imprisonment?
13. What term describes legal responsibility involving compensation or damages?
14. What issue arises when a cyber crime involves different countries?
15. What is the malicious software used to damage computer systems called?

SGOU

Answers to Objective Type Questions

1. Cyber crime
2. IT Act
3. 66C
4. 66D
5. Hacking
6. 66F

7. 67
8. Phishing
9. Data theft
10. Digital evidence
11. Cyber cells
12. Criminal
13. Civil
14. Jurisdiction
15. Malware

Assignments

1. Explain various types of cyber crimes with suitable examples and discuss the relevant sections under the Information Technology Act, 2000.
2. Discuss the penalties, punishments, and fines imposed for different cyber crimes under the provisions of the Information Technology Act, 2000.
3. Explain the process of cyber crime investigation, including the role of cyber cells, law enforcement agencies, and digital forensic procedures.
4. Examine the major challenges in cyber law enforcement and discuss possible preventive measures and cyber safety practices to reduce cyber crimes.

Suggested Reading

1. Cyber Crime and Cyber Law in India: An Analysis of the Information Technology Act, 2000 https://www.legalserviceindia.com/Legal-Articles/cyber-crime-and-cyber-law-in-india-an-analysis-of-the-information-technology-act-2000/ (Legal Service India)
2. Cyber Crimes in India: A Legal Analysis with Reference to the Information Technology Act, 2000 https://www.legalserviceindia.com/Legal-Articles/cyber-crimes-in-india-a-legal-analysis-with-special-reference-to-the-information-technology-act-2000-bns-2023-and-bnss-2023/ (Legal Service India)

SGOU

3. Cyber Crimes and Provisions under the Information Technology Act https://thelaw.institute/business-law-as-applicable-to-co-operative-i/cyber-crimes-information-technology-act-2002/ (The Law Institute)

4. Cyber Crime and Legal Frameworks in India https://www.apnilaw.com/criminal/cyber-crime/cyber-crime-and-legal-frameworks-in-india/ (Apni Law)

5. Overview of Cyber Laws in India (PDF Resource) https://caaa.in/Image/cyber%20laws%20overview.pdf (Caaa)

Reference

1. Rastogi, A. (2024). *Cyber law: Law of information technology and the internet*. LexisNexis.

2. Kumar, S., & Kaur, G. (2024). *Cyber crimes & laws* (3rd rev. ed.). Marsden Law Book.

3. Tripathi, P. K., & Tiwari, N. K. (2024). *Cyber security*. S. K. Kataria & Sons.

4. Gupta, S., Agrawal, B., & Deoghare, M. V. (2022). *Cyber laws: With comprehensive coverage of information technology law, e-commerce, e-crimes, cyber crime investigation, and data protection*. Premier Publishing Company.

5. Goswami, A. K., & Gautam, R. (2022). *Cyber crime, regulations and security: Contemporary issues and challenges*. The Law Brigade Publishers.

SGOU



UNIT 3 Penal Provisions for Cyber Offenses

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- explain the concept of cyber offenses and their impact on individuals and organizations
- describe the different types of cyber crimes such as phishing, spam, malware, hacking, trespass, and cyber stalking
- summarize the legal framework and penal provisions related to various cyber offenses
- interpret the importance of cyber laws in ensuring digital security and protecting user data
- discuss the preventive measures and legal consequences associated with cyber crimes

Prerequisites

A basic understanding of computers, internet technologies, and digital communication is essential before studying this unit on penal provisions for cyber offenses. Familiarity with concepts such as computer networks, email systems, web browsing, and online transactions is important. Knowledge of how data is stored, transmitted, and accessed in digital systems helps in understanding how cyber crimes occur. For example, understanding how login credentials function makes it easier to comprehend how phishing attacks deceive users into sharing sensitive information.

In addition, awareness of fundamental cyber security principles is necessary. Concepts such as strong passwords, authentication methods, data privacy, and safe internet usage provide a foundation for identifying and preventing cyber threats. For example, understanding the role of antivirus software and firewalls helps in recognizing how systems are protected against viruses, worms, and other malicious programs.

A basic idea of legal and ethical aspects related to technology also supports better understanding of this unit. Knowledge of digital rights, responsible use of online platforms, and the importance of data protection helps in appreciating the need for cyber laws and

SGOU

penal provisions. For example, awareness of privacy rights highlights why unauthorized access or cyber stalking is considered a punishable offense under cyber law.



Keywords

Hacking, Phishing, Identity Theft, Malware, Cyber Stalking

Discussion

6.3.1 Introduction to Penal Provisions for Cyber Offenses

The rapid growth of information and communication technologies has significantly transformed the way individuals, businesses, and governments interact and exchange information. Along with the benefits of digital connectivity, there has also been a rise in cyber offenses such as hacking, phishing, identity theft, malware distribution, and online harassment. These offenses exploit vulnerabilities in computer systems, networks, and digital platforms, causing financial loss, privacy violations, and disruption of services. As cyber crimes continue to evolve with technological advancements, it has become essential to establish legal mechanisms that regulate and penalize such unlawful activities.

Penal provisions for cyber offenses refer to the legal rules and regulations that define cyber crimes and prescribe punishments, penalties, and corrective measures for offenders. These provisions aim to protect digital information, ensure secure use of technology, and maintain trust in electronic transactions. Various countries have introduced specific cyber laws and amendments to existing criminal laws to address cyber threats. Such legal frameworks provide guidelines for identifying cyber crimes, prosecuting offenders, and safeguarding individuals and organizations from digital threats.

SGOU

Meaning of Cyber Offenses

Cyber offenses are unlawful acts committed using computers, digital devices, or communication networks such as the internet. These offenses involve unauthorized access, manipulation, theft, or destruction of digital information and computer systems. Cyber offenses may target individuals, organizations, or government institutions and can include activities such as phishing, hacking, spreading viruses, cyber stalking, identity theft, and online fraud.

In simple terms, a cyber offense occurs when a computer system or network is used either as a tool to commit a crime or as the target of the crime itself. With the increasing dependence on digital technologies, cyber offenses have become more complex and widespread, requiring specialized laws and enforcement mechanisms to address them effectively.

Need for legal control of Cyber Crimes

The growing use of the internet and digital technologies has made societies more vulnerable to cyber threats. Cyber criminals can operate across borders, often remaining anonymous and exploiting weaknesses in computer systems. Without proper legal control, such activities may lead to serious consequences such as financial fraud, theft of confidential information, damage to digital infrastructure, and violation of privacy rights. Therefore, legal regulation is necessary to control and deter cyber crimes.

Legal control of cyber crimes helps in establishing accountability and ensuring that offenders are punished according to the severity of their actions. It also provides a framework for investigating cyber incidents, collecting digital evidence, and prosecuting criminals in a court of law. Furthermore, legal measures promote responsible use of technology and encourage organizations to adopt security practices that protect data and digital resources.

Overview of Cyber Laws and Penal Provisions

Cyber laws refer to the set of legal principles and regulations that govern activities conducted in cyberspace. These laws address issues related to electronic communication, digital transactions, data protection, privacy, intellectual property, and cyber crimes. Penal provisions within cyber laws specify the punishments, fines, and penalties imposed on individuals who engage in illegal activities involving computer systems and networks.

In many countries, specific legislation has been enacted to deal with cyber crimes. For example, laws may include provisions for offenses such as unauthorized access to computer systems, data theft, identity fraud, spreading malicious software, and online harassment. Penal provisions serve as a deterrent by clearly defining the consequences of cyber offenses and ensuring that offenders are held legally responsible for their actions.

Role of Information Technology Laws in Cyber Crime Prevention

Information Technology (IT) laws play a vital role in preventing and controlling cyber crimes by providing a structured legal framework for regulating digital activities. These

SGOU

laws define various cyber offenses, establish procedures for investigation, and prescribe appropriate penalties for violations. They also support law enforcement agencies in tracking cyber criminals and taking legal action against them.

In addition to punishment, IT laws promote preventive measures by encouraging organizations and individuals to adopt secure digital practices. They also help in protecting electronic records, digital signatures, and online transactions, thereby strengthening trust in digital systems. Through effective implementation and awareness of IT laws, governments can reduce cyber threats and create a safer digital environment for users.

6.3.2 Legal Framework for Cyber Crime Penalties

The expansion of digital technologies has created new opportunities for communication, commerce, and information exchange. However, it has also increased the risk of cyber crimes that threaten data security, privacy, and digital infrastructure. To address these challenges, governments have developed legal frameworks that define cyber offenses and prescribe appropriate penalties for individuals who misuse computer systems and networks. These legal frameworks aim to maintain order in cyberspace and ensure that digital activities are conducted responsibly.

A legal framework for cyber crime penalties consists of laws, regulations, enforcement mechanisms, and judicial procedures designed to identify, investigate, and punish cyber offenders. It provides clarity regarding the types of cyber offenses, the rights of victims, and the responsibilities of organizations handling digital information. Through well-defined penal provisions, authorities can take action against cyber criminals and deter others from engaging in unlawful digital activities.

Cyber Laws and Regulatory Authorities

Cyber laws are specialized legal provisions that regulate activities occurring in the digital environment. These laws address issues such as unauthorized access to computer systems, data theft, cyber fraud, identity theft, online harassment, and the distribution of malicious software. In many countries, cyber laws form part of a broader legal structure that includes criminal law, data protection regulations, and electronic commerce legislation.

Regulatory authorities play a significant role in enforcing these laws and maintaining cyber security. Government agencies, cyber crime investigation units, and specialized regulatory bodies monitor cyber activities, investigate complaints, and ensure compliance with legal standards. These authorities also collaborate with law enforcement agencies and international organizations to track cyber criminals who operate across borders. Their efforts contribute to effective regulation and help strengthen trust in digital technologies.

Importance of Penal Provisions in Cyber Security

Penal provisions form an essential component of cyber security laws because they establish the consequences for unlawful digital activities. By clearly defining punishments for cyber offenses, these provisions discourage individuals from engaging

SGOU

in activities that threaten the integrity, confidentiality, and availability of information systems. The presence of legal penalties acts as a deterrent and encourages responsible behavior among users of digital technologies.

Another important function of penal provisions is to provide justice for victims of cyber crimes. Individuals and organizations that suffer financial losses, data breaches, or reputational damage due to cyber attacks can seek legal remedies through established legal procedures. Penal provisions also strengthen the accountability of organizations responsible for safeguarding digital data, thereby promoting a culture of security awareness and compliance with cyber security standards.

Punishments, Fines, and Legal consequences for Cyber Offenders

Punishments and fines are imposed on cyber offenders based on the severity and nature of the offense committed. Legal consequences may include imprisonment, monetary penalties, or both, depending on the extent of damage caused by the cyber crime. For example, unauthorized access to computer systems, data manipulation, or distribution of malicious software may result in significant penalties under cyber laws. These measures are intended to discourage individuals from exploiting digital platforms for illegal purposes.

In addition to criminal penalties, cyber offenders may also face civil liabilities and administrative actions. Organizations responsible for data breaches or security negligence may be required to compensate affected parties or implement corrective measures. Legal consequences may also include restrictions on the use of digital systems, seizure of equipment used in the crime, or disqualification from certain professional activities. Such comprehensive penalties ensure that cyber crimes are addressed effectively and reinforce the importance of maintaining a secure and trustworthy digital environment.

6.3.3 Penal Provisions for Phishing

The widespread use of digital communication platforms such as email, social media, and online banking has increased the risk of fraudulent activities in cyberspace. Among these threats, phishing has become one of the most common forms of cyber crime targeting individuals and organizations. Cyber criminals often attempt to deceive users into revealing sensitive information such as passwords, credit card details, or personal identification data. These attacks are usually carried out by impersonating trusted institutions or legitimate service providers.

To address the growing threat of phishing, cyber laws include penal provisions that define such activities as criminal offenses and prescribe appropriate punishments for offenders. Legal frameworks recognize phishing as a form of online fraud and identity theft because it involves the misuse of digital communication tools to obtain confidential information unlawfully. Penal provisions aim to discourage these fraudulent practices and protect users from financial and personal data losses.

Definition and concept of Phishing

Phishing (Fig 6.3.1) is a cyber crime in which attackers attempt to obtain sensitive information from individuals by pretending to be trustworthy entities in electronic

SGOU

communications. The term originates from the idea of "fishing," where cyber criminals cast deceptive messages in the hope that victims will disclose valuable information. These messages often appear to come from banks, government agencies, or well-known companies.

The primary objective of phishing is to manipulate victims into providing confidential data such as login credentials, bank account numbers, or personal identification details. Once the information is obtained, attackers may use it to conduct financial fraud, identity theft, or unauthorized transactions. Phishing attacks rely heavily on social engineering techniques that exploit human trust rather than technical system vulnerabilities.



Fig 6.3.1: Illustration of phishing

Methods and Techniques used in Phishing Attacks

Phishing attacks are conducted using various techniques designed to deceive users into believing that the communication is legitimate. One of the most common methods is email phishing, where attackers send fraudulent emails that mimic official messages from banks, online services, or financial institutions. These emails often contain links directing users to fake websites that resemble legitimate platforms.

Another technique is spear phishing, which targets specific individuals or organizations using personalized messages. Attackers may collect information about their targets to make the communication appear authentic. In addition, smishing (phishing through SMS) and vishing (voice phishing through phone calls) are increasingly used to trick victims into revealing confidential information. Deepfake phishing is an advanced social engineering attack where cybercriminals use artificial intelligence to generate

synthetic audio, video, or images. These methods exploit trust and urgency, prompting users to act quickly without verifying the authenticity of the request.

Legal Sections and Punishments for Phishing

Phishing is considered a criminal offense under various cyber laws because it involves deception, unauthorized access to information, and financial fraud. Legal provisions often classify phishing under offenses related to identity theft, cheating by impersonation, and unauthorized use of computer resources. Offenders involved in phishing activities may face imprisonment, monetary fines, or both, depending on the severity of the crime and the damage caused.

In addition to general cyber crime provisions, laws related to electronic fraud and data protection may also apply to phishing cases. Authorities may investigate phishing incidents using digital evidence such as email records, website logs, and communication data. Legal punishment not only penalizes offenders but also serves as a deterrent to prevent similar fraudulent activities in the digital environment.

Preventive Measures against Phishing

Preventing phishing attacks requires awareness, cautious online behavior, and the use of appropriate security practices. Users should verify the authenticity of emails, messages, or websites before providing sensitive information. It is advisable to avoid clicking on suspicious links and to check website addresses carefully to ensure that they belong to legitimate organizations.

Organizations can also reduce phishing risks by implementing strong authentication mechanisms, secure email filtering systems, and regular cyber security training for employees. The use of updated antivirus software, firewalls, and secure communication protocols further strengthens protection against phishing attempts. By combining technological safeguards with user awareness, individuals and institutions can significantly reduce the chances of falling victim to phishing attacks.

6.3.4 Penal Provisions for Spam

With the increasing use of email and online communication platforms, spam has become a widespread problem in the digital environment. Spam refers to the practice of sending unsolicited messages in large quantities through electronic communication systems. These messages are often distributed without the consent of recipients and may promote advertisements, fraudulent schemes, or malicious links. Excessive spam can disrupt communication systems, consume network resources, and expose users to security threats.

To address this issue, cyber laws include penal provisions that regulate the misuse of electronic communication channels. Legal measures are designed to prevent individuals and organizations from sending unsolicited messages that may cause inconvenience, fraud, or harm to recipients. By establishing penalties and regulatory guidelines, authorities aim to reduce spam activities and maintain the reliability of digital communication systems.

SGOU

Meaning and Types of Spam

Spam (Fig 6.3.2) refers to unwanted electronic messages that are sent in bulk to a large number of recipients through digital communication platforms such as email, messaging services, and social media networks. These messages are typically distributed automatically using specialized software programs that target numerous users simultaneously. Spam messages may contain promotional content, misleading information, or links directing users to malicious websites.

Different types of spam exist depending on the medium used for communication. Email spam is the most common form and usually involves advertisements or fraudulent offers. Other forms include messaging spam, where unwanted messages are sent through instant messaging platforms, and SMS spam, which involves unsolicited text messages sent to mobile devices. Social media spam also occurs when automated accounts distribute repetitive promotional content across social networking platforms.

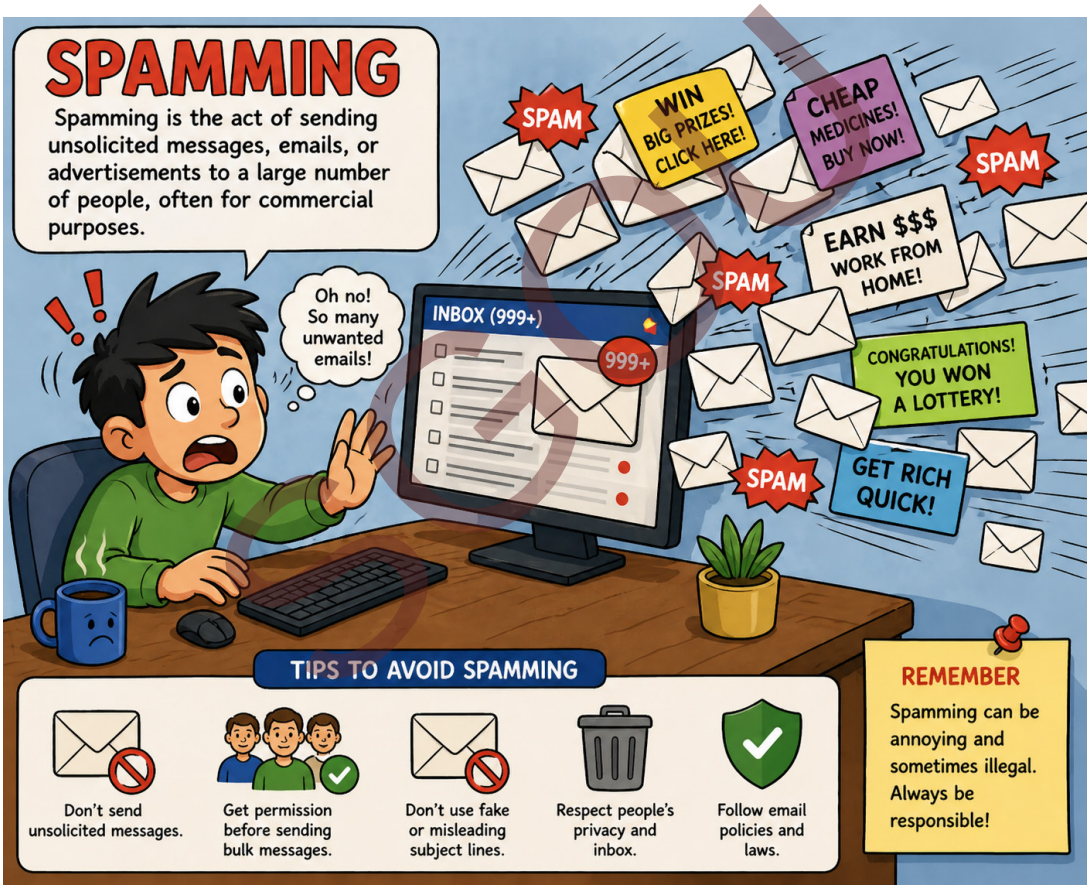


Fig 6.3.2: Illustration of spamming

Impact of Spam on Individuals and Organizations

Spam can create several problems for both individuals and organizations. For individual users, unsolicited messages can be annoying and may increase the risk of exposure to scams, phishing attempts, or malicious software. Many spam messages attempt to trick

recipients into revealing personal information or clicking on harmful links, which can lead to identity theft or financial losses.

Organizations also face challenges due to the presence of spam in their communication systems. Large volumes of unwanted messages can consume storage space, reduce network efficiency, and affect employee productivity. In addition, spam campaigns may damage the reputation of businesses if their names are falsely used in fraudulent communications. Consequently, managing spam effectively is essential for maintaining secure and efficient digital communication environments.

Legal Actions and Penalties for Spamming

Legal systems in many countries have introduced regulations to control the misuse of electronic messaging services. Spamming may be treated as an offense when individuals or organizations send unsolicited messages that violate privacy rights, promote fraudulent activities, or distribute harmful content. Cyber laws and electronic communication regulations often specify restrictions on bulk messaging and require senders to obtain consent from recipients.

Individuals who engage in unlawful spamming may face legal consequences such as monetary penalties, fines, or restrictions on their digital activities. In cases where spam messages are linked to fraud, phishing, or malware distribution, more severe criminal charges may be applied. Law enforcement authorities can investigate such activities using digital evidence, including message logs, server records, and communication data, to identify and prosecute offenders.

Measures to Control Spam

Controlling spam requires both technological solutions and responsible user behavior. Email service providers and communication platforms use spam filters, content scanning systems, and blacklisting techniques to detect and block unwanted messages. These technologies analyze message patterns and sender information to prevent spam from reaching users' inboxes.

Users can also take preventive steps by avoiding the disclosure of their email addresses on unsecured websites and by carefully reviewing the authenticity of online messages. Organizations often implement security policies, employee awareness programs, and advanced filtering systems to reduce spam-related risks. By combining regulatory enforcement with technical safeguards and user awareness, the negative effects of spam can be significantly minimized in digital communication systems.

6.3.5 Penal Provisions for Virus, Worms, and Malware

The increasing reliance on computer systems and internet-based technologies has made digital environments vulnerable to various forms of malicious software. Cyber attackers often develop and distribute harmful programs to damage computer systems, steal information, or disrupt network operations. Among the most common threats are computer viruses, worms, and other forms of malware that can spread rapidly across digital networks. These malicious programs can compromise data integrity, affect system performance, and create serious security risks for individuals and organizations.

SGOU

To combat such threats, cyber laws include penal provisions that prohibit the creation, distribution, and use of malicious software. Legal frameworks recognize these activities as cyber offenses because they intentionally harm computer systems and digital infrastructure. Governments enforce strict penalties against individuals who develop or spread malicious programs in order to discourage cyber attacks and protect digital resources.

Computer Virus- Meaning and Characteristics

A computer virus is a type of malicious software designed to replicate itself and infect computer systems by attaching to legitimate files or programs. When an infected program is executed, the virus becomes active and begins spreading to other files or systems within the network. Viruses can alter, delete, or corrupt data and may cause significant damage to software and hardware resources.

Computer viruses exhibit several distinctive characteristics. They are capable of self-replication, which allows them to multiply rapidly once they enter a system. Many viruses also remain hidden within files until the infected program is executed, making them difficult to detect in the early stages. In addition, viruses may contain harmful instructions that disrupt system operations, display unwanted messages, or compromise confidential information stored in the computer.

Worms and their impact on Computer Systems

A worm is another form of malicious program that spreads automatically through computer networks without requiring user interaction. Unlike viruses, worms do not need to attach themselves to existing files or programs in order to propagate. Instead, they exploit vulnerabilities in operating systems or network protocols to replicate and transmit themselves to other connected devices.

The presence of worms in a network can cause serious disruptions to computer systems and communication infrastructures. Because worms replicate rapidly, they can consume large amounts of network bandwidth and system resources, leading to slow performance or system failures. In some cases, worms may also install additional malicious components such as spyware or backdoors that allow attackers to gain unauthorized access to infected systems.

Malware and its different types

Malware is a broad term used to describe any software intentionally designed to harm computer systems, networks, or users. It includes various types of malicious programs that perform unauthorized activities such as stealing information, monitoring user behavior, or damaging system files. Cyber criminals develop malware to gain financial benefits, collect sensitive data, or disrupt digital operations.

There are several categories of malware that target computer systems in different ways. Trojans disguise themselves as legitimate software but secretly perform harmful actions once installed. Spyware collects personal or confidential information without the user's knowledge. Ransomware blocks access to computer systems or files until a payment

SGOU

is made to the attacker. Adware displays unwanted advertisements and may track user activity. Each type of malware presents unique security challenges and requires appropriate protective measures.

Legal Provisions and Penalties for creating or distributing Malware

The development and distribution of malicious software are considered serious cyber offenses under many legal systems. Cyber laws include provisions that prohibit individuals from intentionally introducing harmful programs into computer networks or causing damage to digital resources. These legal rules classify the creation and dissemination of viruses, worms, and malware as acts of unauthorized interference with computer systems.

Individuals found guilty of developing or spreading malware may face severe legal consequences. Penalties may include imprisonment, financial fines, or both, depending on the extent of damage caused by the malicious activity. In cases where malware attacks lead to significant financial loss, disruption of services, or theft of sensitive data, courts may impose stricter punishments. These legal provisions are designed to deter cyber criminals and ensure the protection of digital infrastructure and information systems.

6.3.6 Penal Provisions for Hacking

The expansion of digital technologies and networked systems has increased the risk of unauthorized access to computer resources. Hacking is one of the most widely recognized cyber offenses that threatens the confidentiality, integrity, and availability of information systems. Cyber attackers attempt to bypass security mechanisms in order to gain control over computer networks, databases, or online services. Such activities can lead to data theft, service disruption, financial loss, and exposure of confidential information.

To address these threats, cyber laws include specific penal provisions that classify hacking as a criminal offense. Legal frameworks prohibit unauthorized access to computer systems and prescribe punishments for individuals who intentionally interfere with digital resources. These provisions aim to protect electronic data, maintain system security, and discourage unlawful intrusion into computer networks.

Meaning and concept of Hacking

Hacking (Fig 6.3.3) refers to the act of gaining unauthorized access to a computer system, network, or digital device by bypassing security controls. Individuals who perform such activities are known as hackers. The main objective of hacking is often to obtain sensitive information, manipulate data, or disrupt system operations.

The concept of hacking originally referred to the exploration and modification of computer systems for learning or experimentation. However, in the context of cyber crime, the term is commonly associated with illegal activities carried out with malicious intent. Unauthorized intrusion into computer systems is considered a violation of cyber laws because it compromises data security and the privacy of individuals or organizations.

SGOU



Fig 6.3.3: Illustration of hacking

Types of Hacking Attacks

Hacking attacks can take different forms depending on the techniques used by attackers and the targets they aim to exploit. One common type is password hacking, where attackers attempt to guess or crack user passwords to gain access to protected systems. This method often involves automated tools that test multiple password combinations rapidly.

Another form is network hacking, which involves intercepting or manipulating network traffic to obtain confidential information. Website hacking is also frequently observed, where attackers modify website content or gain administrative control over web servers. Additionally, email hacking occurs when unauthorized individuals access email accounts to read or misuse private communications. Each of these attacks can result in significant security risks for users and organizations.

Legal Sections and Punishments for Hacking

Hacking is treated as a punishable offense under various cyber laws because it involves unauthorized access to computer systems and potential damage to digital information. Legal provisions typically define hacking as an act that interferes with the functioning of computer networks, alters stored data, or allows unauthorized control over digital systems.

Individuals found guilty of hacking may face legal penalties such as imprisonment, monetary fines, or a combination of both. The severity of the punishment depends on the extent of damage caused, the intention behind the attack, and the value of the

SGOU

affected information. In situations where hacking leads to financial fraud, identity theft, or large-scale disruption of services, courts may impose stricter penalties in accordance with cyber crime legislation.

Preventive measures against Hacking

Preventing hacking requires the implementation of strong security practices and technological safeguards. One of the most effective measures is the use of strong passwords combined with multi-factor authentication to protect user accounts and sensitive data. Regular software updates and security patches also help eliminate vulnerabilities that attackers might exploit.

Organizations can further strengthen their defenses by deploying firewalls, intrusion detection systems, and network monitoring tools. Conducting security audits and vulnerability assessments helps identify weaknesses in digital infrastructure. In addition, educating users about safe online behavior and cyber security awareness reduces the risk of accidental exposure to hacking attempts. These preventive strategies play a vital role in protecting computer systems and maintaining a secure digital environment.

6.3.7 Penal Provisions for Cyber Trespass

The increasing use of computers and networked systems has made digital environments susceptible to unauthorized entry and misuse. Cyber trespass is a form of cyber offense in which an individual intentionally gains access to a computer system, network, or digital resource without permission from the authorized owner. Such activities can interfere with the normal functioning of systems and may expose confidential data to unauthorized users. As organizations increasingly rely on digital platforms to store and process sensitive information, protecting these systems from unauthorized intrusion has become essential.

Cyber laws include penal provisions to address the issue of cyber trespass and to ensure that individuals who violate digital boundaries are held legally accountable. These provisions define unauthorized access as an offense and establish penalties for those who intentionally interfere with computer systems or attempt to obtain restricted information. Legal regulation helps safeguard digital infrastructure and encourages responsible use of technological resources.

Meaning of Cyber Trespass

Cyber trespass refers to the act of entering or accessing a computer system, network, or online resource without proper authorization. It is similar to physical trespassing, where an individual enters someone else's property without permission. In the digital environment, this offense occurs when a person bypasses security controls to access files, databases, or network services that are intended to be restricted.

This form of cyber offense may involve viewing confidential information, copying data, or simply exploring a system without the consent of the owner. Even when no direct damage occurs, unauthorized entry into digital systems is considered a violation of privacy and security. Cyber trespass undermines trust in digital systems and may create opportunities for more serious cyber crimes.

SGOU

Unauthorized Access and System Intrusion

Unauthorized access occurs when an individual gains entry into a computer system or network without legitimate authorization. Attackers may exploit software vulnerabilities, weak passwords, or misconfigured security settings to enter restricted digital environments. Such intrusions can compromise sensitive data and disrupt the normal operation of information systems.

System intrusion may also involve the installation of malicious tools that allow attackers to monitor activities, copy confidential files, or maintain continued access to the network. These actions can result in data breaches, unauthorized modification of information, and potential damage to digital resources. Therefore, preventing unauthorized access is an essential aspect of maintaining cyber security in both personal and organizational environments.

Legal Consequences and Penalties for Cyber Trespass

Cyber trespass is recognized as a punishable offense under many cyber laws because it violates the security and privacy of digital systems. While 'cyber trespass' is primarily recognized as a theoretical common-law concept, the legal framework in India specifically addresses and penalizes such activities as 'unauthorized access' under Section 43 of the Information Technology Act. Legal provisions typically classify unauthorized access to computer resources as a cyber crime, even if the offender does not cause visible damage to the system. The law considers the act itself to be an infringement of digital rights and security.

Individuals found guilty of cyber trespass may face penalties such as monetary fines, imprisonment, or other legal sanctions depending on the severity of the offense. In situations where unauthorized access leads to data theft, system damage, or financial loss, stricter punishments may be imposed by the courts. These legal consequences are designed to discourage unauthorized intrusion and to protect the integrity of computer systems and digital information.

6.3.8 Penal Provisions for Cyber Stalking

The growth of online communication platforms has created new opportunities for interaction, but it has also introduced risks related to harassment and misuse of digital technologies. Cyber stalking is a serious cyber offense in which an individual repeatedly uses electronic communication to threaten, harass, or intimidate another person. Such activities often occur through social media platforms, emails, messaging services, or other online communication channels. Victims of cyber stalking may experience emotional distress, fear, and invasion of privacy due to persistent unwanted contact.

To address these concerns, legal systems have introduced penal provisions that classify cyber stalking as a punishable offense. These laws aim to protect individuals from online harassment and ensure that offenders who misuse digital platforms are held accountable. By establishing clear legal penalties, cyber laws contribute to creating a safer digital environment and promote responsible behavior in online communication.

SGOU

Meaning and Nature of Cyber Stalking

Cyber stalking refers to the repeated use of digital technologies to monitor, threaten, harass, or intimidate another individual without their consent. It involves persistent unwanted communication or surveillance conducted through online platforms. Unlike traditional stalking, cyber stalking occurs in virtual spaces and may involve anonymous or disguised identities.

The nature of cyber stalking often includes actions such as sending threatening messages, spreading false information about the victim, or continuously tracking an individual's online activities. These behaviors can cause psychological stress and may interfere with the victim's personal and professional life. Because cyber stalking can occur at any time and across multiple digital platforms, it poses a significant challenge for maintaining online safety.

Methods used in Cyber Stalking

Cyber stalkers use a variety of techniques to target their victims through digital communication channels. One common method involves sending repeated emails, messages, or comments that contain threats, abusive language, or unwanted personal attention. These messages may be delivered through social networking sites, messaging applications, or email services.

Another approach includes monitoring a victim's online activities by tracking their social media posts, online profiles, or digital interactions. In some cases, cyber stalkers may create fake accounts to impersonate the victim or to spread misleading information. They may also attempt to collect personal details about the victim and misuse this information to cause embarrassment or fear. These actions demonstrate how digital tools can be misused to harass individuals in cyberspace.

Legal Provisions and Punishments for Cyber Stalking

Cyber stalking is recognized as a criminal offense under various cyber laws and legal provisions related to online harassment and privacy protection. Legal frameworks prohibit the repeated use of digital communication tools to intimidate or threaten another individual. Authorities treat such behavior as a violation of personal rights and online safety.

Individuals found guilty of cyber stalking may face legal consequences such as imprisonment, monetary fines, or both, depending on the seriousness of the offense. In cases where threats or harassment lead to severe emotional distress or damage to reputation, courts may impose stricter penalties. Law enforcement agencies may also investigate digital evidence such as emails, chat records, and social media activity to identify and prosecute offenders.

Protection Measures for Victims

Protecting victims of cyber stalking requires a combination of technological safeguards and legal support. Individuals should avoid sharing excessive personal information on public online platforms and review privacy settings on social media accounts to limit

SGOU

access to personal details. Blocking suspicious accounts and reporting abusive behavior to platform administrators are important steps in reducing unwanted contact.

Victims can also seek assistance from cyber crime authorities or legal agencies that handle online harassment cases. Preserving digital evidence such as threatening messages, screenshots, or communication records is useful for filing complaints and initiating legal action. Awareness programs and support systems further help individuals understand their rights and respond effectively to cyber stalking incidents, thereby strengthening personal safety in the digital environment.

6.3.9 Challenges in enforcing Cyber Crime Laws

The enforcement of cyber crime laws presents several difficulties due to the complex and evolving nature of digital technologies. Unlike traditional crimes that occur within clearly defined physical boundaries, cyber crimes often take place in virtual environments where offenders can operate anonymously and across multiple locations. This makes investigation and legal action more complicated for law enforcement agencies. As cyber threats continue to grow in scale and sophistication, authorities must constantly adapt their strategies to address new forms of digital misconduct.

Another challenge in enforcing cyber laws is the need for specialized technical knowledge and advanced investigative tools. Cyber crime investigations often require digital forensics, data analysis, and cooperation among different organizations. Limited resources, lack of trained personnel, and insufficient awareness about cyber regulations may further complicate the process of detecting and prosecuting offenders. Therefore, strengthening legal frameworks and enhancing technological capabilities are essential for effective cyber law enforcement.

Difficulty in identifying Cyber Criminals

One of the major obstacles in combating cyber crime is the difficulty in identifying the individuals responsible for illegal online activities. Cyber criminals frequently use techniques such as anonymous accounts, encrypted communication, and proxy servers to conceal their identities. These methods allow offenders to hide their real location and personal information while carrying out cyber attacks.

Additionally, attackers may route their activities through multiple networks and devices, making it difficult to trace the origin of the crime. Investigators must analyze digital evidence such as IP addresses, server logs, and communication records to identify potential suspects. The process can be time-consuming and technically complex, which often delays legal proceedings against cyber offenders.

Jurisdictional issues in Cyber Crimes

Cyber crimes often cross national boundaries, creating jurisdictional challenges for law enforcement agencies. An offender may operate from one country while targeting victims or computer systems located in another region. In such situations, determining which legal system has the authority to investigate and prosecute the crime becomes complicated.

SGOU

Different countries have varying cyber laws, legal procedures, and levels of technological capability, which can hinder cooperation during investigations. Obtaining digital evidence from foreign servers or service providers may require international agreements or mutual legal assistance treaties. Effective collaboration among governments and international organizations is therefore necessary to address cyber crimes that involve multiple jurisdictions.

Rapid Technological Changes

The continuous development of digital technologies presents another challenge in enforcing cyber crime laws. New technologies, software platforms, and communication tools are introduced frequently, creating opportunities for cyber criminals to exploit emerging vulnerabilities. Legal systems often struggle to keep pace with these rapid technological advancements.

Cyber criminals may adopt advanced techniques such as sophisticated malware, encryption tools, and automated attack systems to avoid detection. As a result, law enforcement agencies must regularly update their technical skills and investigative methods. Policymakers also need to revise cyber laws and regulatory frameworks to ensure that they remain effective in addressing new types of digital offenses and security threats.

In conclusion, this unit has examined the various penal provisions related to cyber offenses, including phishing, spam, viruses, worms, malware, hacking, cyber trespass, and cyber stalking, highlighting how each poses significant risks to digital security and user safety. The discussion emphasized the importance of legal frameworks in defining these offenses, prescribing punishments, and ensuring accountability for misuse of information technology. It also underscored the need for preventive measures, user awareness, and technological safeguards to complement legal enforcement. As cyber threats continue to evolve, a balanced approach combining strong laws, effective implementation, and responsible digital practices is essential for maintaining a secure and trustworthy cyberspace.

SGOU

Recap

- Cyber offenses are illegal activities carried out using computers and digital networks.
- Penal provisions define punishments and legal actions against cyber criminals.
- Cyber laws aim to protect data, privacy, and digital infrastructure.
- Phishing involves deceiving users to obtain sensitive information fraudulently.
- Phishing attacks often use fake emails, websites, or messages.
- Spam refers to unsolicited bulk messages sent through electronic communication.
- Spamming can lead to fraud, system overload, and reduced productivity.
- Computer viruses are malicious programs that replicate and infect files.
- Worms spread automatically across networks without user interaction.
- Malware includes harmful software such as spyware, ransomware, and trojans.
- Creating or distributing malware is a punishable cyber offense.
- Hacking involves unauthorized access to computer systems or networks.
- Hackers may steal, modify, or destroy sensitive data.
- Cyber trespass refers to unauthorized entry into digital systems.
- Even without damage, unauthorized access is considered illegal.
- Cyber stalking involves repeated online harassment or monitoring of individuals.
- Victims of cyber stalking may suffer emotional and psychological distress.
- Legal provisions impose fines, imprisonment, or both depending on the offense.
- Preventive measures include strong passwords, security tools, and user awareness.
- Effective cyber security requires a combination of legal enforcement and safe digital practices.

SGOU

Objective Type Questions

1. What type of crime is committed using computers and networks?
2. What is the term for fraudulent attempts to obtain sensitive information online?
3. What do we call unsolicited bulk electronic messages?
4. Which malicious program attaches itself to files and spreads?
5. What type of malware spreads without user action?
6. What is the general term for harmful software?
7. What is unauthorized access to a computer system called?
8. What is the act of entering a system without permission known as?
9. What is repeated online harassment called?
10. What is the legal punishment for cyber crimes broadly referred to as?
11. What technique uses fake emails to trick users?
12. What type of malware demands payment to restore access?
13. What is stealing personal data online called?
14. What is the use of fake identity in cyber crime called?
15. What is the main goal of cyber laws?

SGOU

Answers to Objective Type Questions

1. Cybercrime
2. Phishing
3. Spam
4. Virus
5. Worm
6. Malware
7. Hacking

8. Trespass
9. Stalking
10. Penalty
11. Phishing
12. Ransomware
13. Theft
14. Impersonation
15. Security

Assignments

1. Explain the concept of cyber offenses and discuss the penal provisions related to phishing, spam, and malware in detail.
2. Describe different types of cyber crimes such as hacking, cyber trespass, and cyber stalking, along with their legal consequences and punishments.
3. Examine the role of cyber laws in preventing cyber crimes and analyze the importance of penal provisions in ensuring cyber security.
4. Discuss various preventive measures against cyber offenses and evaluate the challenges in enforcing cyber crime laws in the modern digital environment.

Suggested Reading

1. W3Schools Cyber Security Tutorial https://www.w3schools.com/cybersecurity/
2. Simplilearn Cyber Crime Course https://www.simplilearn.com/free-cybercrime-course-for-beginners-skillup
3. Cybert.io Cybersecurity Resources https://cybert.io/careers/resources/
4. Cybersecurity Education Resources https://www.cybersecurityeducation.org/resources/
5. A to Z Cyber Help for Society https://atozcyber.co.in/

SGOU

Reference

1. Casey, E. (2019). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press.

2. Kurose, J. F., & Ross, K. W. (2021). *Computer networking: A top-down approach* (8th ed.). Pearson.

3. Maiwald, E. (2020). *Fundamentals of network security* (3rd ed.). McGraw-Hill Education.

4. Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to computer forensics and investigations* (6th ed.). Cengage Learning.

5. Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.

SGOU



UNIT 4 Human Rights in Cyberspace

Learning Outcomes

Upon the completion of this unit, the learner will be able to:

- define human rights in cyberspace
- list types of online privacy and cyber threats
- explain the link between cybersecurity and human rights
- describe intellectual property rights in the digital world
- outline the role of cyber laws and governance

Prerequisites

A basic understanding of digital technologies and internet usage is essential before studying human rights in cyberspace. Familiarity with how online platforms, websites, and digital communication tools function helps in recognizing how personal data is shared and used. Knowledge of common terms such as data, networks, cybersecurity, and online services provides a foundation for understanding digital environments. For example, awareness of how social media platforms store user information makes it easier to understand privacy concerns.



Understanding fundamental human rights in cyberspace is also important. Concepts such as the right to privacy, freedom of expression, and equality form the basis for analyzing how these rights apply in online spaces. Basic awareness of legal systems

SGOU

and rules helps in understanding how laws protect individuals in both physical and digital environments. For example, knowing that personal information should not be shared without consent helps in understanding data protection laws.

In addition, familiarity with common online risks and ethical practices supports better understanding of the unit. Knowledge of cyber threats such as hacking, identity theft, and online fraud helps in linking cybersecurity with human rights protection. Awareness of responsible online behavior, such as respecting digital content ownership and avoiding misuse of information, is also important. For example, understanding that copying digital content without permission is wrong helps in learning about intellectual property rights in cyberspace.

Keywords

Digital Privacy, Cybersecurity, Human Rights, Intellectual Property, Cyber Governance, GDPR.

Discussion

6.4.1 Introduction

Human rights in cyberspace refer to the application of fundamental rights such as freedom of expression, privacy, access to information, and equality, within digital environments. As the internet and digital technologies have become integral to communication, commerce, education, and governance, the protection of these rights has extended beyond physical boundaries into virtual spaces. Cyberspace enables global interaction, but it also introduces risks like surveillance, data misuse, cybercrime, and digital exclusion. Ensuring human rights online requires balancing individual freedoms with security, accountability, and technological advancement. Governments, international bodies, and private organizations all play crucial roles in safeguarding these rights while maintaining an open and secure digital ecosystem.

Meaning and Scope of Cyberspace

Cyberspace is the virtual environment created by interconnected computer systems, networks, and digital devices where communication and data exchange take place. It includes the internet, cloud systems, social media platforms, online services, and digital communication channels. The scope of cyberspace is vast and constantly expanding, covering activities such as online banking, e-learning, e-commerce, digital governance, and social interaction. It is not limited by geographical boundaries, allowing users from different parts of the world to interact instantly. Cyberspace also supports emerging technologies like artificial intelligence, the Internet of Things (IoT), and big data systems. Its wide scope makes it a critical domain for economic growth, social development, and the exercise of human rights, while also presenting challenges related to security, privacy, and regulation.

SGOU

Evolution of Digital Rights

Digital rights have developed alongside the growth of information and communication technologies. In the early stages of the internet, the focus was mainly on access to information and freedom of expression. As digital platforms expanded, concerns about privacy, data protection, and online identity became more significant. The rise of social media and digital services led to increased awareness of issues such as surveillance, data breaches, and misuse of personal information. Legal frameworks and international efforts, such as the General Data Protection Regulation, have been introduced to protect user data and ensure accountability. Today, digital rights encompass a broader range of protections, including the right to be forgotten, digital security, and equal access to technology. The evolution continues as new technologies raise fresh ethical and legal challenges in the digital age.

Importance of Human Rights in the Digital Era

Human rights remain essential in the digital age because online spaces have become central to everyday life, influencing communication, education, employment, and governance. Protecting these rights ensures that individuals can express opinions freely, access information without discrimination, and participate in digital society with dignity. Safeguarding privacy is crucial as vast amounts of personal data are collected, stored, and processed through digital platforms. Equal access to technology helps reduce the digital divide and promotes inclusive development across different social groups. Strong human rights protections also build trust in digital systems, encouraging innovation, economic growth, and responsible use of technology. Upholding these principles creates a balanced environment where technological progress supports human well-being rather than undermining it.

Challenges in Protecting Rights Online

Protecting human rights in the digital environment is complex due to technological advancements, global connectivity, and varying legal systems.

1. **Rapid Technological Change:** New innovations develop quickly, leaving laws and policies struggling to keep pace with emerging digital issues.

2. **Cybercrime and Security Threats:** Hacking, phishing, and identity theft expose individuals to financial loss and personal harm.

3. **Data Privacy Concerns:** Extensive collection and processing of personal data increase the chances of misuse and unauthorized access.

4. **Misinformation and Harmful Content:** False information and offensive material spread rapidly, influencing public opinion and social harmony.

5. **Lack of Digital Literacy:** Limited awareness about online safety makes users more vulnerable to exploitation and fraud.

6. **Balancing Security and Freedom:** Efforts to strengthen security may sometimes restrict basic freedoms such as privacy and expression.

SGOU

6.4.2 Right to Privacy

The right to privacy is a fundamental human right that protects individuals from unauthorized access, collection, and misuse of their personal information. In the digital era, this right has become increasingly important as people share large amounts of data through online platforms, communication tools, and digital services. Privacy ensures that individuals have control over their personal details, online activities, and digital identities. It also supports dignity, freedom of expression, and personal security by preventing unwanted intrusion. Governments and organizations are expected to adopt laws and practices that safeguard user data and respect individual privacy in cyberspace.

Concept of Privacy in the Digital World

Privacy in the digital world refers to the ability of individuals to control how their personal information is collected, used, stored, and shared online. It includes protection of sensitive data such as personal identification details, financial information, browsing history, and communication records. Digital privacy also involves the right to remain anonymous, the ability to choose what information is made public, and protection against surveillance or tracking. With the growth of social media, cloud computing, and online services, maintaining privacy has become more challenging. Strong security measures, user awareness, and effective regulations are essential to ensure that personal data is handled responsibly and securely.

6.4.2.1 Types of Online Privacy

Online privacy can be understood through different categories based on the type of information being protected and how it is used in digital environments (Fig 6.4.1).

1. Data Privacy

Data privacy refers to the protection of personal and sensitive information stored or processed online. This includes details such as names, addresses, financial records, health information, and browsing history. Individuals should have control over how their data is collected, used, and shared by organizations. Proper safeguards like encryption and secure storage help prevent unauthorized access and data breaches.

2. Communication Privacy

Communication privacy focuses on protecting the confidentiality of digital interactions. It ensures that emails, messages, voice calls, and video conversations remain secure from interception or unauthorized monitoring. Technologies such as end-to-end encryption are used to keep communication private and accessible only to the intended participants.

3. Identity Privacy

Identity privacy involves safeguarding personal identity in the digital space. It includes protection against identity theft, impersonation, and misuse of personal credentials. Maintaining strong passwords, using multi-factor authentication, and limiting the sharing of personal details online are important measures to protect digital identity.

SGOU

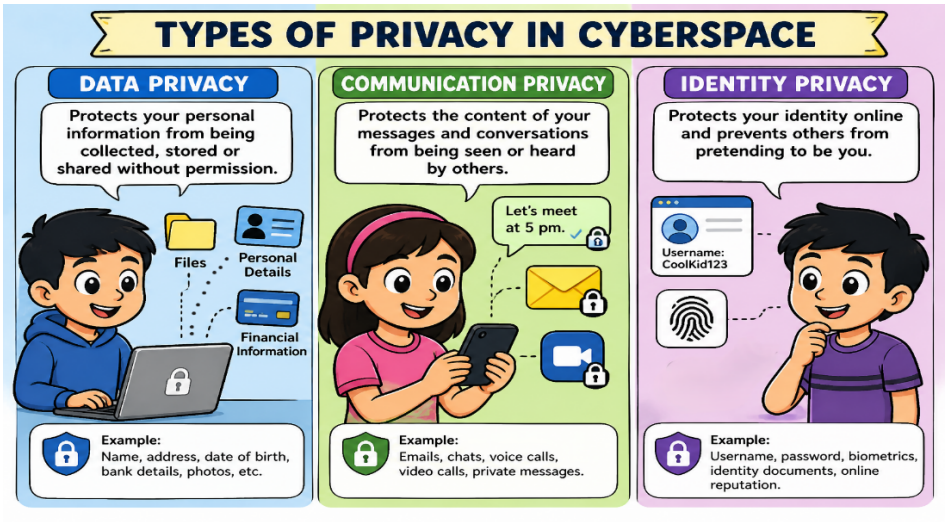


Fig 6.4.1: Types of online privacy

Protecting data, communication, and identity privacy is essential for ensuring safety, trust, and individual freedom in the digital world.

6.4.2.2 Threats to Privacy

Privacy in the digital environment is constantly at risk due to various technological and organizational practices that expose personal information.

1. Surveillance

Surveillance refers to the monitoring of individuals' online activities by governments, organizations, or other entities. This may include tracking browsing behavior, monitoring communications, or collecting metadata. Excessive surveillance can violate personal freedom and discourage individuals from expressing their views openly.

2. Data Breaches

Data breaches occur when unauthorized individuals gain access to confidential or sensitive information stored in digital systems. This can result from weak security measures, hacking, or system vulnerabilities. Breaches may expose personal data such as passwords, financial details, and private records, leading to identity theft and financial loss.

3. Tracking

Tracking involves the collection of user data based on online behavior, such as websites visited, search history, and interactions. It is often used by companies for advertising and personalization purposes. However, continuous tracking without consent can invade privacy and create detailed user profiles without the individual's knowledge.

Surveillance, data breaches, and tracking pose significant challenges to privacy, making it essential to implement strong security measures and ethical data practices in the digital space.

SGOU

6.4.2.3 Legal Frameworks for Privacy Protection

Legal frameworks for privacy protection are designed to safeguard personal data, regulate its collection and use, and ensure accountability among organizations handling such information. These frameworks establish rules for data processing, define the rights of individuals, and impose obligations on governments and private entities. With the rapid growth of digital technologies, strong privacy laws have become essential to protect individuals from misuse of their personal information and to promote trust in digital systems.

1. General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is one of the most comprehensive data protection laws in the world, implemented by the European Union in 2018. It applies to all organizations that process the personal data of individuals within the EU, regardless of where the organization is located.

GDPR is based on key principles such as lawfulness, fairness, transparency, data minimization, accuracy, storage limitation, and accountability. It gives individuals strong rights over their personal data, including the right to access their data, correct inaccuracies, request deletion (right to be forgotten), restrict processing, and obtain data portability.

Organizations are required to obtain clear consent before collecting data, ensure data security through appropriate technical measures, and report data breaches within a specified time. Heavy penalties are imposed for non-compliance, making GDPR a strict and influential regulation. It has also inspired many other countries to strengthen their own privacy laws.

2. IT Laws and Privacy Regulations

Various countries have enacted Information Technology (IT) laws and privacy regulations to address data protection issues within their jurisdictions. In India, the Information Technology Act, 2000 provides a legal framework for electronic governance, cybersecurity, and protection of sensitive information.

Under this law, provisions related to data protection include penalties for unauthorized access, data theft, and damage to computer systems. Additional rules, such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, define how organizations should handle sensitive personal data like financial details, health records, and passwords.

India has also introduced the Digital Personal Data Protection Act, 2023, which focuses specifically on protecting personal data. This law emphasizes consent-based data processing, rights of individuals to access and correct their data, and responsibilities of data handlers to ensure security and transparency.

Globally, many countries have adopted similar regulations to address privacy concerns, reflecting the growing importance of data protection in the digital age.

Legal frameworks such as GDPR and national IT laws play a crucial role in protecting

SGOU

privacy by establishing clear rules, empowering individuals, and ensuring that organizations handle personal data responsibly in cyberspace.

6.4.2.4 Privacy vs Security Debate

The privacy vs security debate focuses on the balance between protecting individual personal information and ensuring safety through monitoring and control measures in the digital environment.

Privacy emphasizes the right of individuals to keep their personal data, communications, and online activities free from unauthorized access or surveillance. It supports freedom of expression, autonomy, and dignity by allowing people to control their own information. Strong privacy protections limit how much data governments and organizations can collect and use.

Security, on the other hand, involves measures taken to protect individuals, systems, and nations from threats such as cyberattacks, terrorism, and criminal activities. Governments and organizations often use surveillance, data collection, and monitoring tools to detect and prevent such threats. These practices can enhance safety but may also reduce personal privacy.

The conflict arises because increased security measures often require access to personal data, which can lead to intrusion into private lives. For example, monitoring online communications may help prevent cybercrime but can also expose sensitive personal information. Similarly, data collection for security purposes may be misused if not properly regulated.

Achieving a balance between privacy and security requires clear laws, transparency, and accountability. Measures such as limited data collection, strong encryption, judicial oversight, and informed consent can help ensure that security efforts do not unnecessarily violate individual rights.

In conclusion, the privacy vs security debate highlights the need to protect both individual freedoms and collective safety by adopting balanced and responsible approaches in the digital world.

6.4.3 Cybersecurity and Human Rights

Cybersecurity and human rights are closely connected in the digital age, as the protection of digital systems directly affects the safety and freedoms of individuals. Cybersecurity involves safeguarding networks, devices, and data from unauthorized access, attacks, and damage, while human rights ensure dignity, privacy, freedom of expression, and access to information. Effective cybersecurity measures help protect individuals from cyber threats such as hacking, identity theft, and online harassment, thereby supporting their fundamental rights. At the same time, excessive security practices like mass surveillance or intrusive data collection can restrict personal freedoms and violate privacy. Therefore, a balanced approach is necessary to ensure that efforts to secure digital environments also respect and uphold human rights principles.

Definition of Cybersecurity

Cybersecurity refers to the practice of protecting computer systems, networks,

SGOU

applications, and data from unauthorized access, attacks, damage, or disruption. It involves the use of technologies, policies, and procedures to ensure the confidentiality, integrity, and availability of information. Cybersecurity measures include firewalls, encryption, authentication mechanisms, and intrusion detection systems. Its primary goal is to safeguard digital infrastructure and prevent cyber threats such as hacking, malware, and data breaches.

Relationship between Cybersecurity and Human Rights

Cybersecurity and human rights are interconnected because the protection of digital systems directly influences the protection of individual freedoms. Strong security measures help protect rights such as privacy, freedom of expression, and access to information by preventing cybercrime and unauthorized data access. At the same time, certain cybersecurity practices, such as surveillance and data monitoring, can impact these rights if not properly regulated. Ensuring this relationship remains balanced requires adopting security measures that protect individuals without unnecessarily limiting their fundamental rights in the digital environment.

6.4.3.1 Cyber threats and their impact on rights

Cyber threats are malicious activities carried out in digital environments that can harm individuals, organizations, and societies. These threats not only affect systems and data but also directly impact fundamental human rights such as privacy, security, dignity, and freedom of expression. As reliance on digital platforms increases, the consequences of cyber threats on individual rights have become more serious and widespread (Fig 6.4.2).

1. Cybercrime

Cybercrime refers to illegal activities conducted using computers, networks, or the internet. Examples include hacking, phishing, financial fraud, malware attacks, and unauthorized access to systems. Cybercrime can violate the right to privacy by exposing personal data and the right to security by causing financial and psychological harm. It may also restrict access to essential services when systems are disrupted. Victims often face loss of trust in digital platforms, which can limit their participation in online activities.

2. Identity Theft

Identity theft occurs when someone illegally obtains and uses another person's personal information, such as passwords, bank details, or identification numbers, without permission. This information is often used for financial fraud or impersonation. Identity theft directly violates the right to privacy and can damage an individual's reputation and financial stability. Victims may experience long-term consequences, including legal complications and emotional distress. It also undermines confidence in digital identity systems and online transactions.

3. Online Harassment

Online harassment involves abusive behavior conducted through digital platforms,

SGOU

including threats, bullying, hate speech, and stalking. It can occur on social media, messaging apps, or other online forums. This threat affects the right to dignity, equality, and freedom of expression, as victims may feel unsafe or discouraged from participating in online spaces. Continuous harassment can lead to psychological harm, stress, and social isolation. In severe cases, it can silence individuals and restrict their ability to express opinions freely.

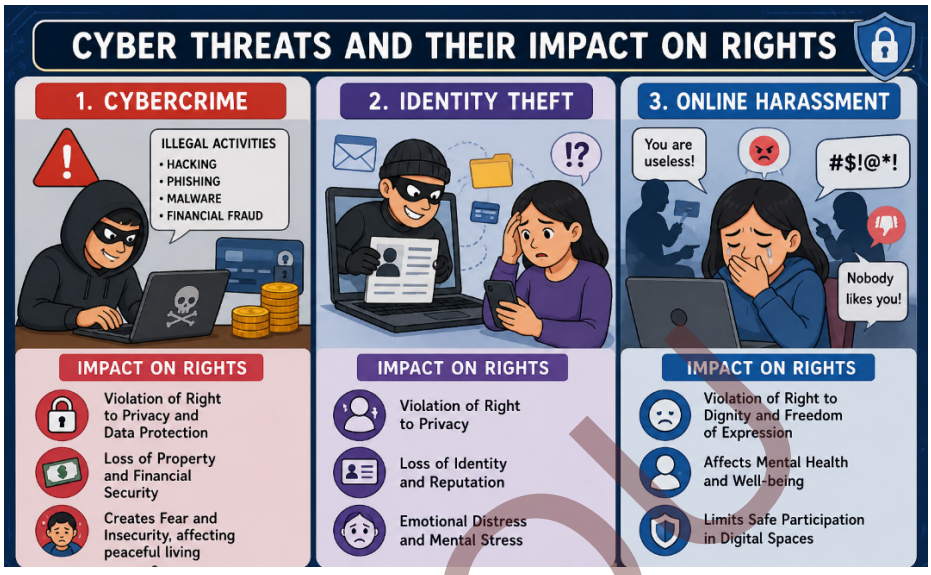


Fig 6.4.2: Cyber threats and their impact on rights

Cyber threats such as cybercrime, identity theft, and online harassment pose significant risks to fundamental human rights, making it essential to implement strong security measures, legal protections, and user awareness to ensure a safe and respectful digital environment.

6.4.3.2 Role of Governments and Organizations in Cybersecurity

Governments and organizations play a crucial role in ensuring cybersecurity by creating policies, implementing safeguards, and promoting safe digital practices. Governments are responsible for developing cyber laws, national security strategies, and regulatory frameworks that protect critical infrastructure and citizens' data. They also establish agencies to monitor threats, respond to cyber incidents, and coordinate with international bodies to combat global cybercrime. Public awareness programs and digital literacy initiatives are promoted to help individuals understand online risks and safe practices.

Organizations, including private companies and institutions, are responsible for securing their systems and protecting user data. They implement security measures such as encryption, firewalls, and access controls to prevent unauthorized access. Regular security audits, employee training, and incident response plans help reduce vulnerabilities. Organizations must also follow legal requirements and ethical standards to ensure transparency and accountability in handling data. Collaboration between governments and organizations strengthens overall cybersecurity and helps create a safer digital environment.

SGOU

6.4.3.3 Ethical Issues in Cybersecurity Practices

Cybersecurity practices often raise ethical concerns related to privacy, fairness, and accountability. One major issue is the use of surveillance and monitoring tools, which may help detect threats but can also invade individual privacy if used excessively. The collection and storage of large amounts of personal data create risks of misuse and unauthorized access. Ethical concerns also arise in decisions about how much information should be shared, who has access to it, and how long it should be retained.

Another issue involves the balance between security and individual rights, where strict security measures may limit freedom of expression or restrict access to information. The use of artificial intelligence in cybersecurity can introduce bias or unfair decision-making if not properly managed. Additionally, ethical dilemmas may occur when organizations choose between disclosing vulnerabilities and protecting their reputation. Ensuring ethical cybersecurity requires transparency, respect for user rights, responsible data handling, and adherence to legal and professional standards.

Effective cybersecurity depends not only on technical measures but also on responsible governance and ethical practices that protect both systems and human rights in the digital world.

6.4.4 Intellectual Property Rights in Cyberspace

Intellectual Property Rights (IPR) in cyberspace refer to the legal protections given to creators and owners of digital content, ideas, and innovations in the online environment. With the rapid growth of the internet, digital platforms have made it easier to create, share, and distribute content such as music, software, videos, literature, and designs. While this has encouraged creativity and innovation, it has also increased the risk of unauthorized copying, piracy, and misuse of original work. IPR in cyberspace ensures that creators receive recognition and economic benefits for their work while preventing illegal use or duplication. It also helps maintain fairness, encourages innovation, and supports the growth of digital industries.

Meaning of Intellectual Property (IP)

Intellectual Property (IP) refers to creations of the human mind that have commercial and legal value. These creations include inventions, literary and artistic works, symbols, names, images, and designs used in business and creative fields. Unlike physical property, intellectual property is intangible, meaning it cannot be touched but can be owned and protected by law. IP rights give creators exclusive control over the use of their creations for a certain period, allowing them to benefit financially and gain recognition. These rights also encourage innovation and creativity by ensuring that original ideas are not used or copied without permission.

6.4.4.1 Types of IPR in Digital Environment

Intellectual Property Rights in the digital environment protect various forms of creative and innovative work shared through online platforms (Fig 6.4.3).

SGOU

1. Copyright

Copyright protects original literary, artistic, and creative works such as books, music, films, software, and digital content. It gives the creator exclusive rights to reproduce, distribute, display, or modify their work. In the digital space, copyright helps prevent unauthorized copying, downloading, and sharing of content, ensuring that creators receive recognition and financial benefits.

2. Trademarks

Trademarks protect symbols, logos, names, slogans, or designs that distinguish a brand or business from others. In cyberspace, trademarks are important for maintaining brand identity and preventing misuse or imitation of well-known brands online. They help consumers identify genuine products and services and protect businesses from unfair competition.

3. Patents

Patents provide legal protection for new inventions, technological innovations, and processes. They give inventors exclusive rights to use, produce, or sell their invention for a specified period. In the digital environment, patents are often related to software, algorithms, and technological systems, encouraging innovation while preventing unauthorized use of new inventions.

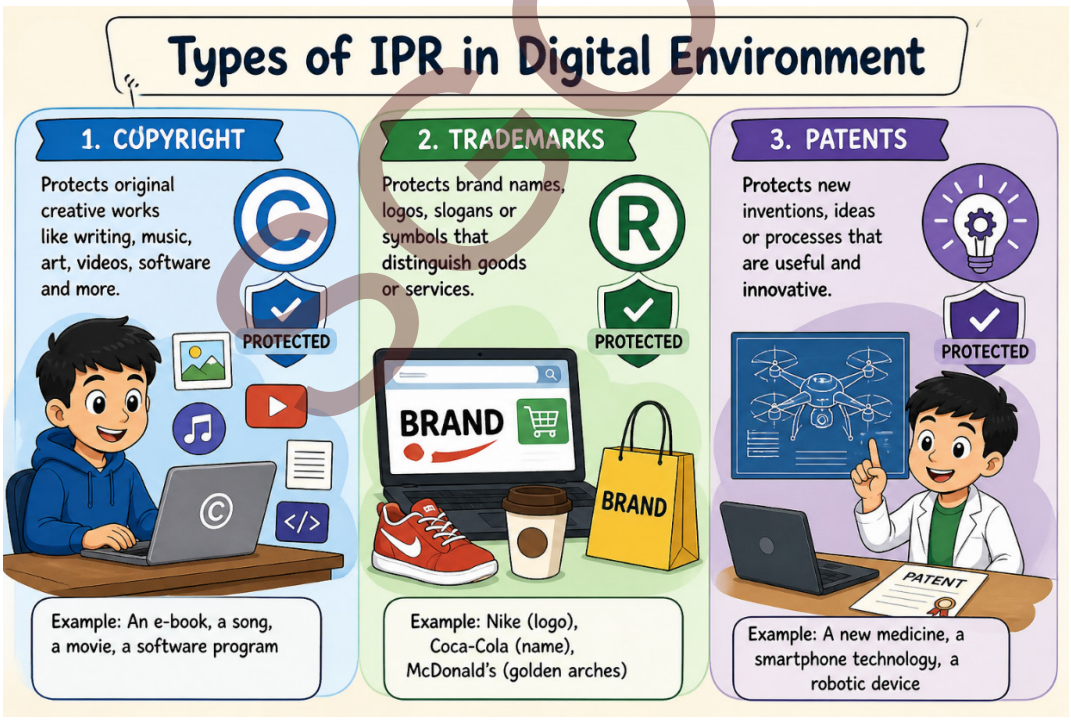


Fig 6.4.3: Types of IPR in Digital Environment

Copyright, trademarks, and patents play a vital role in protecting intellectual property in cyberspace, ensuring that creators and innovators are rewarded for their work while promoting fair use and innovation.

6.4.4.2 Challenges of IPR in Cyberspace

Protecting Intellectual Property Rights (IPR) in cyberspace is difficult due to the ease of copying, storing, and distributing digital content across global networks.

1. Piracy

Piracy refers to the unauthorized copying, downloading, or distribution of copyrighted material such as movies, music, software, e-books, and games. Digital platforms make it easy to duplicate content without quality loss, leading to widespread illegal sharing. Piracy reduces the income of creators and industries, discourages innovation, and violates the rights of content owners. It also creates challenges for enforcement because pirated content can be distributed quickly across multiple platforms and regions.

2. Digital Content Sharing

Digital content sharing involves the distribution of media and information through online platforms, sometimes without proper authorization. While sharing promotes accessibility and collaboration, it can also lead to infringement of intellectual property rights when content is shared without the creator's consent. Social media, file-sharing websites, and cloud services make it easy to distribute copyrighted material widely. This creates difficulty in tracking ownership, controlling usage, and ensuring fair compensation for creators.

Piracy and unauthorized digital content sharing pose major challenges to IPR in cyberspace, requiring stronger legal measures, technological solutions, and user awareness to protect intellectual property effectively.

6.4.4.3 Protection Mechanisms for Digital Content

Protecting digital content is essential to ensure that creators retain control over their work and receive proper recognition and compensation. Various legal, technical, and organizational mechanisms are used to prevent unauthorized access, copying, and distribution of digital materials.

1. **Copyright Laws:** Copyright laws provide legal protection to creators by granting exclusive rights over the use, reproduction, and distribution of their work. These laws allow creators to take legal action against unauthorized use or infringement.

2. **Digital Rights Management (DRM):** Digital Rights Management refers to technologies used to control access to digital content. DRM systems restrict copying, sharing, or modifying content without permission, ensuring that only authorized users can access it.

3. **Encryption:** Encryption protects digital content by converting it into a secure format that can only be accessed with a proper key. It is widely used to safeguard data during storage and transmission.

4. **Watermarking and Fingerprinting:** Digital watermarking involves

SGOU

embedding hidden information into content to identify ownership. Finger printing assigns a unique identity to each copy of the content, helping trace unauthorized distribution.

5. **Licensing and Agreements:** Licensing allows creators to specify how their content can be used by others. Terms and conditions clearly define permissions, restrictions, and payment requirements for usage.

6. **Access Control Mechanisms:** Access control systems limit who can view, download, or modify digital content. Methods such as passwords, authentication, and user permissions help prevent unauthorized access.

7. **Monitoring and Enforcement:** Regular monitoring of digital platforms helps detect unauthorized use of content. Legal enforcement actions, such as takedown notices and penalties, are used to address violations.

A combination of legal frameworks, technological tools, and proper enforcement is necessary to effectively protect digital content and uphold intellectual property rights in cyberspace.

6.4.4.4 Role of International Organizations

International organizations play a vital role in protecting intellectual property rights (IPR) across countries by creating common standards, promoting cooperation, and ensuring effective enforcement. Since cyberspace is global in nature, no single country can fully address IPR issues alone. These organizations help harmonize laws, provide guidance to governments, and support dispute resolution. They also raise awareness about the importance of protecting intellectual property and encourage innovation by ensuring that creators' rights are respected worldwide.

World Intellectual Property Organization (WIPO)

The World Intellectual Property Organization (WIPO) is a specialized agency of the United Nations responsible for promoting the protection of intellectual property globally. It develops international treaties and agreements that help standardize IPR laws across member countries, making it easier to protect digital content beyond national boundaries.

WIPO provides a platform for cooperation among countries to address challenges such as online piracy, copyright infringement, and digital content misuse. It also offers dispute resolution services, helping parties settle intellectual property conflicts without lengthy legal procedures. In addition, WIPO supports capacity-building programs by assisting countries in developing effective IP systems and policies.

The organization plays an important role in adapting intellectual property laws to the digital environment by addressing emerging issues related to the internet, software, and digital media. Through awareness programs and global initiatives, WIPO encourages respect for intellectual property and promotes creativity and innovation in the digital age.

SGOU

International organizations like WIPO are essential for ensuring consistent and effective protection of intellectual property rights in cyberspace through global cooperation and standardized legal frameworks.

6.4.5 Regulation and Governance in Cyberspace

Regulation and governance in cyberspace refer to the system of laws, policies, rules, and institutions that guide the use of digital technologies and online platforms. As cyberspace has become an essential part of modern life, proper governance is necessary to ensure security, protect user rights, and maintain order in the digital environment. It involves the participation of governments, private organizations, and international bodies to create a balanced framework that supports innovation while preventing misuse. Effective regulation helps address issues such as cybercrime, data protection, intellectual property violations, and online safety.

Need for Cyber Laws and Governance

Cyber laws and governance are essential to regulate activities in the digital world and ensure a safe and secure online environment. They provide legal recognition to electronic transactions, making digital communication and e-commerce reliable and trustworthy. These laws help prevent and control cybercrimes such as hacking, fraud, identity theft, and data breaches by defining offenses and prescribing penalties.

They also play a crucial role in protecting fundamental rights like privacy and freedom of expression by setting limits on data collection and surveillance. Cyber laws establish responsibilities for organizations to handle user data securely and transparently. Governance frameworks ensure coordination among different stakeholders, including governments, businesses, and users, to address global cyber challenges effectively.

In addition, cyber laws help resolve disputes related to online activities and provide mechanisms for enforcement across digital platforms. They support the growth of the digital economy by building trust among users and encouraging safe participation in online services.

The need for cyber laws and governance arises from the increasing dependence on digital systems, making it necessary to maintain security, protect rights, and ensure responsible use of cyberspace.

6.4.5.1 National Cyber Laws and Policies

National cyber laws and policies are legal frameworks established by individual countries to regulate activities in cyberspace, ensure cybersecurity, and protect the rights of users. These laws provide guidelines for the use of digital technologies, define cyber offenses, and prescribe penalties for violations. They also aim to secure critical infrastructure, promote safe online practices, and support the growth of the digital economy.

In India, the Information Technology Act, 2000 serves as the primary legislation governing cyber activities. It provides legal recognition to electronic records and digital signatures, enabling secure online transactions. The Act also addresses cybercrimes such as hacking, data theft, identity fraud, and unauthorized access to computer systems, along with penalties for offenders.

SGOU

To strengthen data protection, India introduced the Digital Personal Data Protection Act, 2023, which focuses on safeguarding personal data. This law emphasizes consent-based data processing, rights of individuals to access and correct their data, and obligations of organizations to ensure data security and transparency.

National policies such as cybersecurity strategies outline the country's approach to preventing cyber threats, protecting infrastructure, and improving incident response capabilities. These policies also promote awareness, capacity building, and cooperation between government agencies and private sectors.

In conclusion, national cyber laws and policies are essential for maintaining security, protecting user rights, and ensuring the responsible use of digital technologies within a country's jurisdiction.

6.4.5.2 International Cyber Governance Frameworks

International cyber governance frameworks are systems of rules, agreements, and cooperative mechanisms developed by countries and global organizations to manage activities in cyberspace. Since the internet operates beyond national borders, these frameworks help create common standards for cybersecurity, data protection, digital rights, and responsible state behavior. They promote collaboration, reduce conflicts, and ensure that cyberspace remains secure, open, and accessible for all users.

One important framework is the Budapest Convention on Cybercrime, which is the first international treaty aimed at combating cybercrime. It provides guidelines for criminalizing cyber offenses, improving investigative procedures, and enhancing cooperation among countries in handling cyber incidents.

Another key initiative is led by the United Nations, which promotes responsible state behavior in cyberspace through discussions and guidelines developed by groups such as the UN Group of Governmental Experts (GGE). These efforts focus on maintaining peace, security, and respect for human rights in the digital domain.

Organizations like the International Telecommunication Union (ITU) also contribute by setting technical standards, improving global connectivity, and supporting cybersecurity capacity-building across countries.

These frameworks address issues such as cross-border cybercrime, data protection, digital trade, and internet governance. They encourage information sharing, joint response to cyber threats, and the development of consistent legal approaches.

International cyber governance frameworks are essential for managing the global nature of cyberspace by promoting cooperation, standardization, and the protection of rights and security across nations.

6.4.5.3 Role of Governments, Private Sector, and Civil Society

Effective governance of cyberspace depends on the coordinated efforts of governments, private organizations, and civil society, each contributing distinct responsibilities to ensure security, protect rights, and promote responsible digital use.

SGOU

1. Role of Governments

Governments are responsible for creating and enforcing cyber laws, policies, and regulations that ensure security and protect citizens' rights. They establish national cybersecurity strategies, regulate data protection, and define legal consequences for cyber offenses. Public institutions also develop infrastructure for cyber defense, respond to incidents, and cooperate with other countries to address cross-border threats. Awareness programs and digital literacy initiatives are promoted to help citizens use technology safely.

2. Role of Private Sector

The private sector, including technology companies, internet service providers, and online platforms, plays a major role in maintaining cybersecurity. These organizations design and manage digital systems, making them responsible for implementing strong security measures such as encryption, access controls, and regular system updates. They also ensure the protection of user data, comply with legal requirements, and maintain transparency in their operations. Innovation by the private sector contributes to the development of advanced security technologies and safer digital services.

3. Role of Civil Society

Civil society includes non-governmental organizations, advocacy groups, and individual users who contribute to promoting digital rights and accountability. These groups raise awareness about issues such as privacy, freedom of expression, and digital inclusion. They monitor the actions of governments and corporations, advocate for fair policies, and support victims of cyber violations. Civil society also plays a key role in educating users and encouraging ethical behavior in online spaces.

Collaboration among governments, the private sector, and civil society is essential to create a secure, inclusive, and rights-respecting cyberspace that benefits all users.

6.4.5.4 Issues in Global Cyber Governance

Managing cyberspace at a global level involves several challenges due to its borderless nature and the diversity of legal systems across countries.

1. Jurisdiction

Jurisdiction refers to the authority of a country to apply its laws and take legal action in cyberspace. Since online activities often cross national boundaries, it becomes difficult to determine which country's laws should apply to a particular issue. For example, a cybercrime may be committed in one country, target victims in another, and involve servers located elsewhere. This creates confusion and delays in legal proceedings. Differences in legal standards and priorities among countries further complicate cooperation and decision-making.

2. Enforcement Challenges

Enforcement challenges arise when it is difficult to implement and uphold cyber laws

SGOU

effectively across different regions. Even when laws exist, identifying offenders, collecting digital evidence, and prosecuting crimes can be complex due to anonymity and technological barriers. Lack of coordination between countries and limited resources in some regions weaken enforcement efforts. Additionally, rapid technological changes make it hard for law enforcement agencies to keep up with new types of cyber threats.

3. Lack of Uniform Laws and Standards

Different countries follow different legal frameworks, policies, and cybersecurity standards, leading to inconsistencies in how cyberspace is regulated. This lack of uniformity creates confusion for global organizations and makes cooperation between nations more difficult. It also allows cybercriminals to exploit weaker legal systems and operate from regions with less strict regulations.

4. Data Privacy and Sovereignty Concerns

Countries have varying approaches to data protection and control over data generated within their borders. Data sovereignty refers to the idea that data is subject to the laws of the country where it is stored or processed. Conflicts arise when data flows across borders, as nations may have different rules regarding access, storage, and sharing. These differences can impact user privacy, international trade, and cooperation in cybersecurity efforts.

Issues such as jurisdiction conflicts, enforcement difficulties, lack of uniform laws, and data sovereignty concerns make global cyber governance complex and challenging, highlighting the need for stronger international cooperation, harmonized regulations, and effective coordination among nations.

6.4.5.5 Future Trends in Cyber Regulation

Cyber regulation is continuously evolving to address new challenges arising from rapid technological advancements and increasing digital dependence. Future trends focus on strengthening security, protecting user rights, and ensuring responsible use of emerging technologies.

1. **Stronger Data Protection Laws:** Countries are expected to introduce more comprehensive data protection regulations to enhance user privacy and ensure better control over personal information.

2. **Regulation of Artificial Intelligence (AI):** Governments are likely to develop policies to regulate artificial intelligence, ensuring transparency, fairness, and accountability in automated decision-making systems.

3. **Cross-Border Cooperation:** International collaboration will increase to address cybercrime and data protection issues that extend beyond national boundaries, leading to more unified global frameworks.

4. **Focus on Cybersecurity Standards:** Standardized cybersecurity practices and guidelines will be developed to improve the protection of digital infrastructure across industries.

SGOU

5. **Platform Accountability:** Digital platforms and social media companies will face stricter regulations to control harmful content, misinformation, and misuse of user data.

6. **Protection of Digital Rights:** Greater emphasis will be placed on safeguarding fundamental rights such as privacy, freedom of expression, and access to information in the digital environment.

7. **Regulation of Emerging Technologies:** Technologies such as blockchain, Internet of Things (IoT), and cloud computing will require new regulatory approaches to manage risks and ensure secure usage.

Future cyber regulation will aim to create a balanced digital ecosystem that promotes innovation while ensuring security, accountability, and protection of human rights.

In conclusion, human rights in cyberspace represent a critical intersection between law, technology, and society, where traditional rights are reinterpreted in the digital environment. The right to privacy ensures control over personal information and protects individuals from excessive surveillance and data misuse. Cybersecurity strengthens the protection of these rights by securing digital infrastructure and reducing vulnerabilities that can lead to rights violations. Intellectual Property Rights encourage innovation and creativity by safeguarding digital content while maintaining a balance between protection and access. Meanwhile, regulation and governance provide the necessary legal and ethical framework to manage cyberspace responsibly and fairly. Overall, the unit highlights that protecting human rights online requires continuous cooperation between individuals, governments, and technology systems to ensure a safe, fair, and inclusive digital world.

Recap

- Human rights apply equally in cyberspace as in the physical world.
- Digital platforms influence privacy, freedom of expression, and access to information.
- The right to privacy protects personal data and online activities.
- Online privacy includes protection of data, communication, and identity.
- Data breaches and surveillance pose major threats to privacy.
- Tracking and profiling can lead to misuse of personal information.
- Cybersecurity protects systems, networks, and digital data.
- Cybersecurity helps safeguard human rights such as privacy and safety.
- Excessive surveillance can violate fundamental rights.
- Cyber threats include cybercrime, identity theft, and online harassment.

SGOU

- Cybercrime can cause financial loss and security risks.
- Identity theft involves unauthorized use of personal information.
- Online harassment affects dignity and freedom of expression.
- Intellectual Property Rights protect digital creations and innovations.
- Copyright, trademarks, and patents are major types of IPR.
- Piracy and unauthorized sharing challenge intellectual property protection.
- Digital content is protected through DRM, encryption, and licensing.
- Cyber laws regulate online activities and ensure user protection.
- Global cyber governance faces issues like jurisdiction and enforcement.
- Cooperation among governments, organizations, and society ensures effective cyber governance.

Objective Type Questions

1. What is the main focus of human rights in cyberspace?
2. Which right protects personal data online?
3. What type of privacy protects emails and messages?
4. What is unauthorized access to data called?
5. Which threat involves monitoring online activities?
6. What does cybersecurity primarily protect?
7. Which cyber threat involves stealing personal identity?
8. What type of harassment occurs on digital platforms?
9. What does IPR stand for?
10. Which IPR protects creative works like music and films?
11. Which IPR protects logos and brand names?
12. What is illegal copying of digital content called?
13. What is the act of collecting user data based on online behavior called?
14. Which law provides data protection in the EU?

SGOU

15. Which Indian law governs cyber activities?
16. What is the main aim of cyber laws?
17. What issue arises due to different laws in different countries?
18. What does jurisdiction mean in cyberspace?
19. Who plays a role in cyber governance along with governments?
20. Which organization promotes global intellectual property protection?

Answers to Objective Type Questions

1. Protection of human rights in digital environments
2. Right to Privacy
3. Communication Privacy
4. Hacking
5. Surveillance
6. Systems, networks, and data
7. Identity Theft
8. Online Harassment
9. Intellectual Property Rights
10. Copyright
11. Trademark
12. Piracy
13. Tracking
14. General Data Protection Regulation (GDPR)
15. Information Technology Act, 2000
16. To regulate and secure online activities
17. Jurisdiction issues
18. Legal authority of a country in cyberspace
19. Private sector and civil society
20. World Intellectual Property Organization (WIPO)

SGOU

Assignments

1. Explain the concept of human rights in cyberspace and discuss its importance in the digital age.
2. Describe the right to privacy in the online environment and analyze the major threats to digital privacy.
3. Examine the relationship between cybersecurity and human rights with suitable examples.
4. Discuss Intellectual Property Rights in cyberspace and explain the challenges faced in protecting digital content.
5. Analyze the role of cyber laws and global governance in regulating cyberspace, highlighting key issues and challenges.

Suggested Reading

1. CYRILLA Global Digital Rights Law https://cyrilla.org/en/
2. Centre for Research and Governance on Cyber Law https://crgcl.com/resources/
3. Centre for Internet and Society https://cis-india.org/
4. Council of Europe Internet Governance Portal https://www.coe.int/en/web/portal/council-of-europe-and-internet
5. Digital Constitutionalism Network https://digitalconstitutionalism.org/

SGOU

Reference

1. Kaur, G., Dalei, N. N., & Mahapatra, S. K. (Eds.). (2024). Cybersecurity, law, and economics: The case of India. Routledge.
2. Myneni, S. R. (2024). Information technology law (5th ed.). Asia Law House.
3. Rastogi, A. (2024). Cyber law: Law of information technology and internet. LexisNexis.
4. Rattan, J. (2024). Cyber laws, information technology and artificial intelligence (10th ed.). Bharat Law House.
5. Duggal, P. (2023). Textbook on cyber law (2nd ed.). Universal LexisNexis.

SREENARAYANAGURU OPEN UNIVERSITY

QP CODE: …… Reg. No : .....

Name : …….....

Model Question Paper- set-I

End Semester Examination

BACHELOR OF COMPUTER APPLICATIONS

B21CA13DE: CYBER CRIME

(CBCS - UG)

2023-24 Admission Onwards

Time: 3 Hours Max Marks: 70

Section A

Answer any 10 questions. Each carries one mark (10×1= 10)

1. What is a cyber attack?
2. What is email spoofing?
3. What is online grooming?
4. Which malware demands payment from users?
5. What is unauthorized copying of software called?
6. Which ATM fraud copies card data using an unauthorized reader placed at the card slot?
7. What is the first phase of a cyber-attack?
8. What is the process of obtaining higher-level privileges called?
9. Which phase in cyber attack involves removing evidence of an attack?
10. What are Botnets?
11. Write about Virus.
12. Name the mechanism that determines user access rights.
13. Name the term used for unauthorized access to a computer system.
14. What is cyber trespass?
15. Which organization promotes global intellectual property protection?

Section B

Answer any 5 questions. Each carries two marks (5x2=10)

16. What is a malware attack? Mention one example of malware
17. What is cyber-defamation? Mention one example
18. What is software piracy? Mention its effects and prevention methods.

SGOU

19. What is a trademark?
20. Define lateral movement.
21. Distinguish between footprinting and enumeration.
22. What is a Remote Access Trojan (RAT)?
23. Write any for targets of Banking and Financial Fraud.
24. What are the advantages of using E-Signatures?
25. List and explain the two types of electronic records.
26. How does a computer virus spread from one file or system to another?

Section C

Answer any 5 questions. Each carries four marks (5x4=20)

27. Explain Man-in-the-Middle (MitM) attacks and describe how such attacks can affect communication
28. Differentiate between phishing, spear phishing, and whaling
29. Explain how a backdoor works and discuss its different types.
30. Explain the salami attack, its effects, and prevention methods.
31. Explain the role of reconnaissance and scanning in a cyber-attack.
32. Describe privilege escalation and explain its major types.
33. Explain about Ransomware and its types.
34. Write about 4 Characteristics of Nation State Attacks.
35. Explain the differences between a Digital Signature and an E-Signature.
36. Explain the classification of cyber crimes.

Section D

Answer any 2 questions. Each carries fifteen mark (2×15= 30)

37. Explain major cyber threats to individuals, women and children, and government systems
38. What is malware? Explain its different types, effects, and prevention methods in detail.
39. Explain the complete phases of a cyber-attack.
40. Analyze the different types of computer worms based on their propagation methods. Explain the characteristics, working mechanisms, and effects of each type with suitable examples.

SGOU

SREENARAYANAGURU OPEN UNIVERSITY

QP CODE: …… Reg. No : .....

Name : …….....

Model Question Paper- set-II

End Semester Examination

BACHELOR OF COMPUTER APPLICATIONS

B21CA13DE: CYBER CRIME

(CBCS - UG)

2023-24 - Admission Onwards

Time: 3 Hours Max Marks: 70

Section A

Answer any 10 questions. Each carries one mark (10x1=10)

1. Name any one type of internal attack.
2. What is phishing?
3. What is cyber terrorism?
4. What is the full form of DDoS?
5. Which attack creates an unusually large compressed file that expands to consume excessive system resources?
6. Which fraud uses fake messages or websites to steal sensitive information?
7. What type of attack does not directly alter the target system?
8. What technique attempts to obtain stored authentication credentials?
9. Which phase involves gathering information about a target?
10. What is Spyware?
11. What is Cryptojacking?
12. Define the term used for an electronic agreement between two parties.
13. What is the main role of Certifying Authorities (CAs)?
14. What is meant by cyber jurisdiction?
15. What is repeated online harassment called?

Section B

Answer any 5 questions. Each carries two marks (5×2= 10)

16. What is a password attack? Mention any one common method used in password attacks.
17. Mention any two types of cyber attacks that can target government networks

SGOU

18. Differentiate between a virus and a worm.
19. What is jackpotting?
20. What is enumeration in cybersecurity?
21. What is exfiltration? Give one example of information that may be exfiltrated.
22. Write about any four examples of Packet Sniffers.
23. Write about Spear Phishing.
24. What are the main objectives of the IT Act, 2000?
25. State two major functions of the Controller in a digital ecosystem.
26. What are the challenges of Intellectual Property Rights (IPR) in cyberspace?

Section C

Answer any 5 questions. Each carries four marks (5×4= 20)

27. Explain Denial-of-Service (DoS) attacks and describe their major effects on a target system
28. Explain website defacement and discuss its major effects on government websites
29. Write about intruder attacks.
30. Write about ATM-related cybercrime.
31. Describe lateral movement and explain how attackers move between compromised systems.
32. Describe the major activities involved in covering tracks after a cyber-attack.
33. How RATs Work?
34. Write about types of Keyloggers.
35. Describe the Digital Signature process with a neat diagram and explain its advantages.
36. Describe different types of cyber crimes?

Section D

Answer any 2 questions. Each carries fifteen mark (2x15=30)

37. Explain phishing and its different forms with examples and preventive measures
38. Explain the different types of crimes related to social media.
39. Discuss the techniques used to obtain and retain unauthorized access to systems.
40. Explain about different types of Remote Attack Methods.

SGOU

സർവ്വകലാശാലാഗീതം

വിദ്യയാൽ സ്വതന്ത്രരാകണം
വിശ്വപൗരരായി മാറണം
ഗ്രഹപ്രസാദമായ് വിളങ്ങണം
ഗുരുപ്രകാശമേ നയിക്കണേ

കൂരിരുട്ടിൽ നിന്നു ഞങ്ങളെ
സൂര്യവീഥിയിൽ തെളിക്കണം
സ്നേഹദീപ്തിയായ് വിളങ്ങണം
നീതിവൈജയന്തി പാറണം

ശാസ്ത്രവ്യാപ്തിയെന്നുമേകണം
ജാതിഭേദമാകെ മാറണം
ബോധരശ്മിയിൽ തിളങ്ങുവാൻ
ജ്ഞാനകേന്ദ്രമേ ജ്വലിക്കണേ

കുരീപ്പുഴ ശ്രീകുമാർ

SGOU

SREENARAYANAGURU OPEN UNIVERSITY

Regional Centres

Kozhikode
Govt. Arts and Science College
Meenchantha, Kozhikode,
Kerala, Pin: 673002
Ph: 04952920228
email: rckdirector@sgou.ac.in

Thalassery
Govt. Brennen College
Dharmadam, Thalassery,
Kannur, Pin: 670106
Ph: 04902990494
email: rctdirector@sgou.ac.in

Tripunithura
Govt. College
Tripunithura, Ernakulam,
Kerala, Pin: 682301
Ph: 04842927436
email: rcedirector@sgou.ac.in

Pattambi
Sree Neelakanta Govt. Sanskrit College
Pattambi, Palakkad,
Kerala, Pin: 679303
Ph: 04662912009
email: rcpdirector@sgou.ac.in

SAY NO TO RAGGING

BEFORE YOU EVEN THINK OF RAGGING



Humiliation

Blacklisting

Ruined Career

Download

ANTI RAGGING

App

Don't just stand and watch. Stop Ragging! Show Character

Visit UGC Website i.e. www.ugc.Ac.in & www antinaging.in to UGC Anti Ragging regulations.

Ministry of Education
Government of India

Are You Being Ragged ?

विश्वविद्यालय अनुदान आयोग
University Grants Commission
quality higher education for all

DON'T LET IT BE TOO LATE

SAY NO TO DRUGS

LOVE YOURSELF AND ALWAYS BE HEALTHY



SREENARAYANAGURU OPEN UNIVERSITY

The State University for Education, Training and Research in Blended Format, Kerala

SGOU

Cyber Crime

COURSE CODE: B21CA13DE

SGOU











Sreenarayanaguru Open University
Kollam, Kerala Pin- 691601, email: info@sgou.ac.in, www.sgou.ac.in Ph: +91 474 2966841

ISBN 978-81-903304-4-2

9 788190 330442