MUSLIM ASSOCIATION
COLLEGE OF ARTS & SCIENCE
Panavoor,Thiruvananthapuram

CYBER SECURITY

Sixth Semester B.Sc Computer Science

Study Material under the Syllabus of University of Kerala

2024

By
Prasanth B
Assistant Professor
Muslim Association College of Arts & Science

MUSLIM ASSOCIATION COLLEGE OF ARTS AND SCIENCE

Panavoor,Thiruvananthapuram,Kerala

(*Affiliated to the University of Kerala***)**

Department of Computer Science

CS1643 : CYBER SECURITY

Name : ……………………………………………………………………………………………

Candidate Code: …………………………………………………………………………….

CS1643 : CYBER SECURITY

SYLLABUS

Module I: Introduction to Information Systems: components, categories, types, individuals involved, steps in developing information systems, Information Assurance, security challenges, need for cyber security, **Information Security Risk analysis:** use and benefits of risk analysis, risk analysis model, risk assessment, risk equation, risk management, trusted computing.

Module II: Cyber Security Threats and vulnerabilities: types of threats, attacks, malwares, firewalls, hacking, network and services attack, IDPS, honeypots , cryptography and cryptanalysis, network behaviour analysis**, Intrusion Detection Systems:** Types and components of IDS- Network based, Host Based, Hybrid IDS, wireless IDPS

Module III: Security policies: needs and uses**,** policy development, types of security policies, steps in policy review process, **Security Standards**- ISO, Intellectual property rights, patents, trademarks, copyrights, software licensing, e-contracts, Cyber laws in India.. **Security and Law:-** Regulations in India- IT Act 2000/2008, Cyber Crime- cyber law, Indian Copyright Act, Indian Contract Act , Consumer Protection Act, Future Trends –The Law of Convergence.

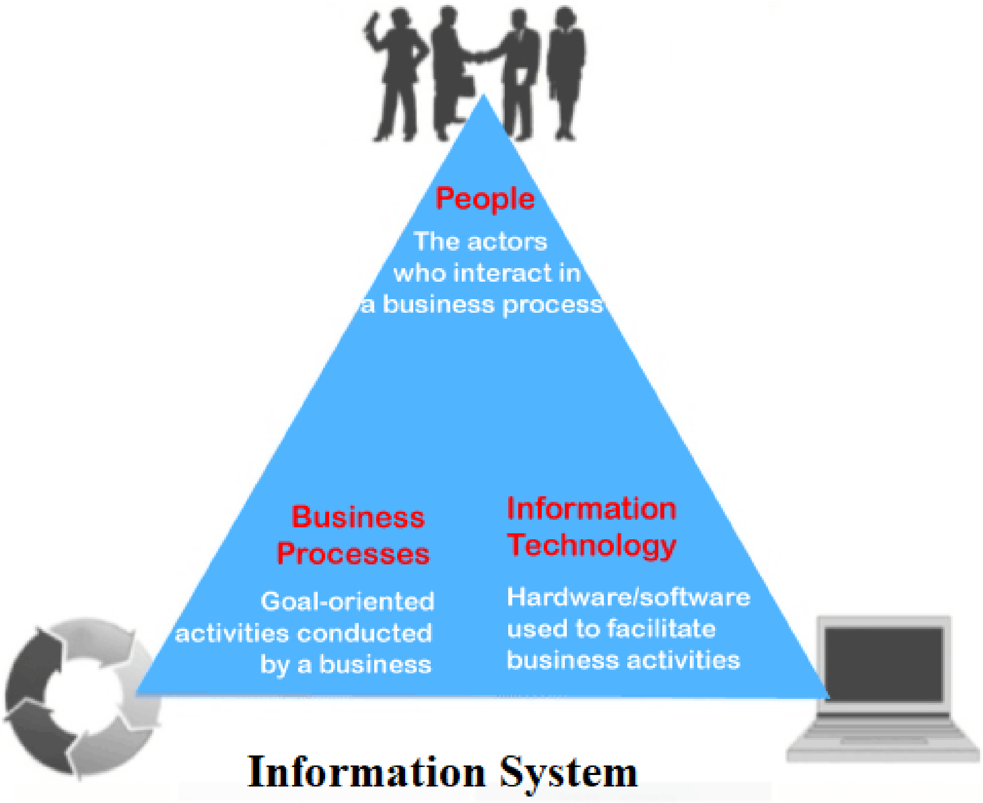
Module IV: Cybercrimes and cyber ethics: cyber space, cyber crimes-nature and scope of cyber crimes**,** types and categories of cybercrimes, penalty for cybercrimes under IT Act, digital foot prints, cyber forensics, Cyber ethics- concerns and responsibilities.

MODULE I

Introduction to Information Systems: components, categories, types, individuals involved, steps in developing information systems, Information Assurance, security challenges, need for cyber security, **Information Security Risk analysis:** use and benefits of risk analysis, risk analysis model, risk assessment, risk equation, risk management, trusted computing.

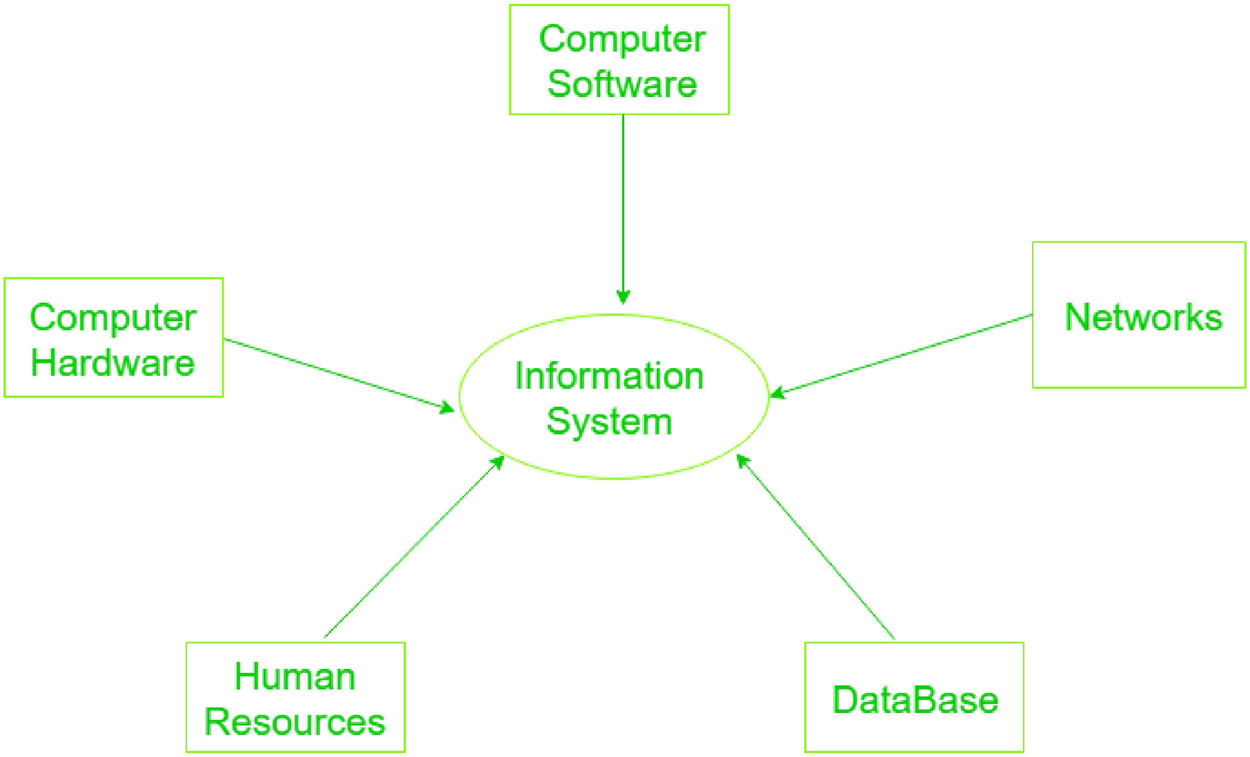
Introduction to Information Systems

- Information systems are a set of interconnected elements working together to collect, process, store, and distribute information to help coordination, visualization in an organization, analysis, and decision-making.
- "Information system is set of people, information technology, and business process in order to achieve a business objective."
- The Information system can be defined as a collection of software, hardware, and telecommunications network that people develop and use to gather, create, and distribute useful data, mainly in organizational settings.
- In other words, an information system means a collection of interrelated components which work together to gather, process, store, and break down the information to help decision making



Components of Information System

Information Systems (IS) consist of several interconnected components that work together to collect, process, store, and disseminate information. These components typically include:



1.Computer Hardware

- Physical equipment used for input, output and processing.
- The hardware structure depends upon the type and size of the organization.
- It consists of an input and an output device, operating system, processor, and media devices. This also includes computer peripheral devices.

2. Computer Software:

- The programs/ application program used to control and coordinate the hardware components.
- It is used for analysing and processing of the data.
- These programs include a set of instruction used for processing information.
- Software is further classified into 3 types: System Software,Application Software and Procedures

3.Databases:

- Data are the raw facts and figures that are unorganized that are later processed to generate information.
- Softwares are used for organizing and serving data to the user, managing physical storage of media and virtual resources.
- As the hardware can't work without software the same as software needs data for processing.
- Data are managed using Database management system.
  Database software is used for efficient access for required data, and to manage knowledge bases.

4. Network:

- Networks resources refer to the telecommunication networks like the intranet, extranet and the internet.
- These resources facilitate the flow of information in the organization.
- Networks consists of both the physical devices such as networks cards, routers, hubs and cables and software such as operating systems, web servers, data servers and application servers.
- Networks include communication media, and Network Support.

5. Human Resources (People):

- It is associated with the manpower required to run and manage the system.
- People are the end user of the information system,
- End-user use information produced for their own purpose,
- The main purpose of the information system is to benefit the end user.
- The end user can be accountants, engineers, salespersons, customers, clerks, or managers etc.
- People are also responsible to develop and operate information systems. They include systems analysts, computer operators, programmers, and other clerical IS personnel, and managerial techniques.

Categories of Information System

Information System is categorized into three

1.Organizational

2.Management

3.Technology

1.ORGANIZATIONAL:

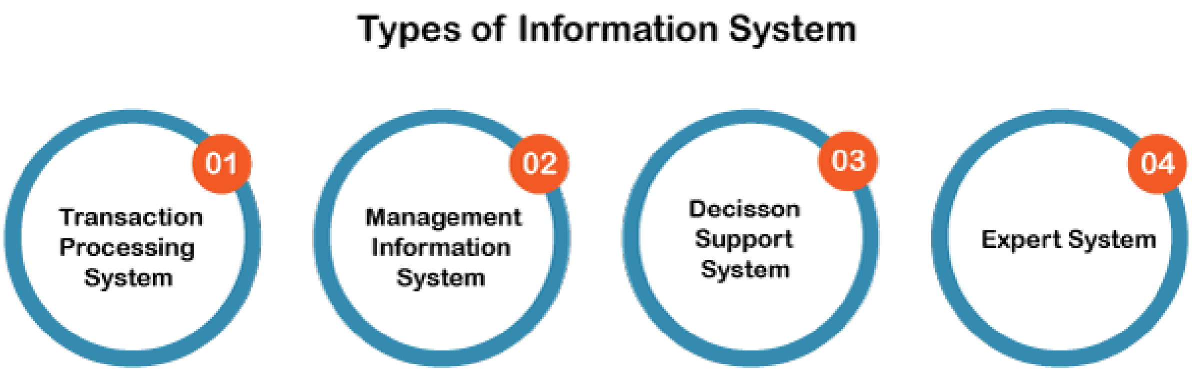
- It is the information System which works for a particular organization.
- Information system are part of organization.
- Information system will have the standard operating procedure and culture of an organization embedded within them.
- This involves :a)Functional specialties b)Business processes c)Culture d)Political interest groups

2.MANAGEMENT :

- Managers perceive business challenges in the environment.
- Information systems supply tools and information needed by the managers to allocate,coordinate and monitor their work, make decision,create new products and services and make long range strategic decision.

3.TECHNOLOGY:

- Management uses technology to carry out their functions.
- It consists of – computer hardware/software, data management technology, networking/telecom technology.
- Its one of the many tools managers use to cope with the change.


Types of Information System
01
Transaction Processing System
02
Management Information System
03
Decisson Support System
04
Expert System

Information is dived into four types

1. Transaction Processing System (TPS)
2. Management Information System (MIS)
3. Decision Support System (DSS)
4. Experts System(ES)

1. Transaction Processing System (TPS):

- The term "transaction processing system" refers to an information system that processes data are originating from business transactions.
- The primary purpose of a transaction processing system is to offer transactions to update records and produce reports required for storekeeping.
- Online Transaction Processing and Batching Processing are the methods which we used to complete the transaction.
- Examples of transaction processing systems are Stock control systems, Payroll systems, Bill systems.

2. Management Information System (MIS):

- The purpose of a management information system is to transform comparatively raw data accessible through using Transaction Processing System into a summarized and aggregated form for managers, generally in the form of a report. Operational supervisors and middle management are likely to use the reports.

- In MIS, there are various kinds of reports generated. Few reports are a kind of summary report, ad-hoc reports, exception report, and on-demand report.
- Examples of Management Information System are Human resource management system and Sales management systems.

3. Decision Support System (DSS)

- Another type of information system is a decision support system. It is interactive, which offers information, data manipulation tools, and models to support decision-making in a semi-structured and unstructured scenario.
- This type of information system includes tools and techniques to help gather relevant information and examine options, and substitutes, the end-user being more elaborate in making DSS than MIS.
- ***Examples of Decision Support System:*** Bank loan management systems, financial planning systems.

4. Experts System

- The expert system contains expertise which is helpful for a manager in ***identifying problems*** or in ***problem-solving.*** The principles of artificial intelligence research are used to develop these kinds of information systems.
- This type of information system is a knowledge-based system. It acts as an expert consultant to users by utilizing its knowledge of a specific area.
- There are some components of expert systems such as Knowledgebase and software modules. These modules make inferences based on knowledge and provide answers to a user's query.

Individuals Involved in Information System

Information systems involve various individuals who play different roles in designing, developing, managing, and using them. The following are the people involved in the working of Information System

1. **System Analysts:** They analyze the information needs of an organization, design systems to meet those needs, and translate requirements into technical specifications.
2. **Developers/Programmers:** These individuals write, test, and maintain the code that makes up the information systems. They can specialize in various programming languages and technologies.
3. **Database Administrators (DBAs):** They manage and maintain databases, ensuring data integrity, security, and availability. They also handle backup, recovery, and performance tuning.
4. **Network Administrators:** Responsible for the configuration, management, and maintenance of an organization's networks, ensuring connectivity and security.
5. **IT Managers:** Oversee the planning, implementation, and maintenance of information systems within an organization. They often make strategic decisions regarding technology use.
6. **Security Analysts:** Focus on protecting information systems from cyber threats, implementing security measures, and responding to security incidents.
7. **End Users:** These are the people who interact with the information system, using it to perform their tasks within the organization. They provide feedback and insights for system improvement.
8. **Quality Assurance/Testers:** They ensure that the information system functions correctly by testing it thoroughly, identifying bugs, and verifying that it meets requirements.
9. **System Architects:** Design the overall structure of an information system, ensuring that different components work together efficiently and effectively.
10. **Vendor/Supplier Representatives:** Work with organizations to provide and support specific software or hardware solutions.

Steps In Developing Information Systems

Developing an information system involves several steps that help in designing, building, testing, and deploying a functional and efficient system. Here's an overview of the typical steps in the development process:

1.Identifying Needs and Planning:

- Understand the requirements of the system and the needs of end-users.
- Define the scope, objectives, and constraints of the project.
- Create a project plan outlining tasks, timelines, resources, and budget.

2.Analysis:

- Gather detailed requirements through interviews, surveys, and analysis of existing systems.
- Document functional and non-functional requirements (e.g., features, performance, security).

3.Design:

- Create a system design based on gathered requirements.
- Architectural design: Define the structure, components, and interfaces of the system.
- Database design: Design the structure and relationships of the database.
- User interface design: Develop the user interface based on user needs.

4.Development:

- Write code based on the design specifications.
- Develop and integrate different system components (frontend, backend, database).
- Perform unit testing to identify and fix bugs in individual modules.

5.Testing:

- Conduct various tests to ensure the system meets requirements.
- System testing: Test the integrated system as a whole to validate functionality.
- User acceptance testing (UAT): Involve end-users to validate the system against their needs.
- Perform quality assurance to ensure the system is reliable and secure.

6.Deployment:

- Prepare the system for deployment in the production environment.
- Install the system and configure it to operate within the organization.
- Conduct training for end-users and support staff.

7.Maintenance and Evaluation:

- Provide ongoing support and maintenance to address issues and updates.
- Gather feedback from users and stakeholders for system improvement.
- Evaluate system performance and make enhancements or upgrades as needed.

Information Assurance (IA)

- Information Assurance (IA) refers to the measures and practices implemented to protect and manage information and information systems.
- Its primary focus is on ensuring the confidentiality, integrity, authenticity, availability, and reliability of information and the systems that store, process, or transmit it.
- IA encompasses a wide range of strategies, policies, technologies, and practices to safeguard sensitive data and the systems that handle it.

Information Assurance Model :

The Assurance Model is multidimensional model based on four dimensions :

1.**Information States**

Information is referred to as interpretation of data which can be found in three states stored, processed, or transmitted.

2.**Security Services**

It is fundamental pillar of the model which provides security to system and consists of five services namely availability, integrity, confidentiality, authentication, and non-repudiation.

3.**Security Countermeasures**

This dimension has functionalities to save system from immediate vulnerability by accounting for technology, policy & practice, and people.

4.Time

This dimension can be viewed in many ways. At any given time data may be available offline or online, information and system might be in flux thus, introducing risk of unauthorized access. Therefore, in every phase of System Development Cycle, every aspect of Information Assurance model must be well defined and well implemented in order to minimize risk of unauthorized access.

Security challenges

Security challenges in information systems are diverse and continuously evolving due to technological advancements and increasingly sophisticated cyber threats. Some of the prominent security challenges include:

1. **Cyber Threats and Attacks:** Constantly evolving cyber threats such as malware, ransomware, phishing attacks, and zero-day exploits pose significant risks to information systems. These threats can lead to data breaches, unauthorized access, or system disruptions.
2. **Data Breaches and Data Loss:** Breaches resulting from vulnerabilities or human error can lead to the exposure of sensitive information, including personal, financial, or proprietary data. Such breaches can damage an organization's reputation and result in legal and financial consequences.
3. **Insider Threats:** Malicious actions or unintentional errors by insiders (employees, contractors, or partners) can compromise information security. This could involve data theft, unauthorized access, or the introduction of malware.
4. **Inadequate Access Controls:** Weak or misconfigured access controls can lead to unauthorized access to systems and data. This includes weak passwords, insufficient user authentication, and improper authorization levels.
5. **Lack of Patch Management:** Failure to promptly apply security patches and updates can leave systems vulnerable to known vulnerabilities that attackers can exploit.
6. **Cloud Security Risks:** As more organizations adopt cloud services, ensuring the security of data stored and processed in the cloud becomes critical. Issues like misconfigured cloud settings, data breaches, and lack of visibility into security controls are common challenges.

7. **Mobile Device Security:** The proliferation of mobile devices introduces security risks, including device theft, data loss, insecure Wi-Fi connections, and vulnerable mobile apps.
8. **Complexity of IT Environments:** Managing security in complex IT environments with diverse systems, interconnected networks, and third-party integrations poses challenges in ensuring consistent and comprehensive security measures.
9. **Compliance and Regulations:** Meeting various compliance standards and regulations (e.g., GDPR, HIPAA, PCI DSS) can be challenging due to their complexities and the need for continuous adherence to specific security requirements.
10. **Security Awareness and Training:** Human error remains a significant factor in security breaches. Insufficient security awareness among employees and inadequate training on security best practices can increase the risk of successful attacks.

Need for Cyber Security

Cybersecurity is essential due to the increasingly interconnected and digital nature of our world. Several critical reasons highlight the need for robust cybersecurity measures:

1. **Protection of Sensitive Data:** Cybersecurity safeguards sensitive information, including personal, financial, and proprietary data, from unauthorized access, theft, or manipulation. This protection is crucial to maintaining individuals' privacy and securing valuable assets for organizations.

2. **Prevention of Data Breaches:** Cybersecurity measures help prevent data breaches that can lead to significant financial losses, reputational damage, and legal implications. Breaches often result in the exposure of confidential information, impacting individuals, businesses, and even governments.

3. **Mitigation of Cyber Attacks:** Cyber attacks, such as malware, ransomware, phishing, and DDoS attacks, pose serious threats to individuals, businesses, and critical

infrastructure. Effective cybersecurity measures help detect, prevent, and respond to these attacks, minimizing their impact.

4. **Safeguarding Infrastructure and Services:** Critical infrastructure, including energy, transportation, healthcare, and financial systems, relies heavily on digital systems. Cybersecurity protects these systems from disruptions that could have far-reaching consequences on public safety and essential services.

5. **Preservation of Trust and Confidence**: In today's digital economy, trust is paramount. Strong cybersecurity practices build trust among customers, partners, and stakeholders, enhancing relationships and maintaining confidence in an organization's ability to protect sensitive information.

Information Security Risk analysis

- Risk analysis refers to the review of risks associated with the particular action or event.
- The risk analysis is applied to information technology, projects, security issues and any other event where risks may be analysed based on a quantitative and qualitative basis.
- The analysis of risk should be occurred on a regular basis and be updated to identify new potential threats.
- The strategic risk analysis helps to minimize the future risk probability and damage.

Benefits of risk analysis

Every organization needs to understand about the risks associated with their information systems to effectively and efficiently protect their IT assets. Risk analysis can help an organization to improve their security in many ways. These are:

- Concerning financial and organizational impacts, it identifies, rate and compares the overall impact of risks related to the organization.

- It helps to identify gaps in information security and determine the next steps to eliminate the risks of security.
- It can also enhance the communication and decision-making processes related to information security.
- It improves security policies and procedures as well as develop cost-effective methods for implementing information security policies and procedures.
- It increases employee awareness about risks and security measures during the risk analysis process and understands the financial impacts of potential security risks.

Risk Analysis Model

The risk analysis model consist of the following steps.

1. **Asset Identification:** Identify and inventory the organization's information assets, including data, systems, hardware, software, networks, and facilities. Understanding what needs protection is fundamental to the risk analysis process.

2. **Threat Identification:** Identify potential threats that could exploit vulnerabilities and harm the identified assets. This includes considering various threat sources such as hackers, malware, insider threats, natural disasters, etc.

3. **Vulnerability Assessment:** Determine the weaknesses or vulnerabilities within the systems, processes, or controls that could be exploited by threats. This involves assessing the security controls in place and identifying gaps or weaknesses.

4. **Risk Assessment:** Evaluate the likelihood and potential impact of identified threats exploiting vulnerabilities. Assess the level of risk associated with each threat by considering the probability of occurrence and the impact it would have on the organization.

5. **Risk Quantification and Prioritization:** Assign a value or score to each identified risk, considering factors such as likelihood, impact, and any existing controls. Prioritize risks based on their severity to focus on the most critical ones that require immediate attention.

6. **Risk Mitigation and Treatment:** Develop and implement strategies to manage, mitigate, or eliminate identified risks. This may involve implementing security controls, transferring risks through insurance, avoiding certain risks by changing processes, or accepting residual risks if they are within acceptable limits.

7. **Monitoring and Review:** Continuously monitor the effectiveness of implemented controls and reassess risks periodically. Information security is dynamic, and new threats and vulnerabilities may emerge, requiring ongoing risk analysis and adjustments to the risk management strategy.

Risk Assessment

Risk assessment is a systematic process of identifying, evaluating, and prioritizing potential risks or uncertainties that could affect an organization, project, process, or activity. It involves analyzing both the likelihood of an event occurring and the potential impact it might have if it does occur.

The key steps in a risk assessment typically include:

1. **Identification:** Recognizing and understanding potential risks that could arise.
2. **Analysis:** Evaluating the probability of each risk occurring and assessing its potential impact.
3. **Assessment:** Prioritizing risks based on their likelihood and potential impact.
4. **Mitigation:** Developing strategies to minimize, control, or eliminate the identified risks.
5. **Monitoring and Review:** Continuously assessing and revisiting the risk assessment process to account for changes and updates.

Risk Equation

The goal of using risk equations is to prioritize and focus resources on mitigating the most significant risks to an organization's information assets. Risk equation helps in understanding and quantifying risk in information security.The following is the risk equation

Risk=Threat × Vulnerability × Impact

1. **Threat:** This refers to any potential danger or harm that could exploit a vulnerability in a system or asset. It could be a malicious attacker, a natural disaster, human error, etc.
2. **Vulnerability:** This signifies weaknesses or gaps in security measures that could be exploited by a threat. It could be outdated software, misconfigured systems, lack of encryption, etc.
3. **Impact:** This denotes the potential damage or harm that could result if a threat exploits a vulnerability. Impact could range from financial losses, reputational damage, loss of data confidentiality or integrity, legal consequences, and more.

Risk Management

Risk management in cyber security involves identifying, assessing, and mitigating potential threats and vulnerabilities to protect digital assets, information, and systems from cyber attacks. The process involves several key steps:

1. **Asset Identification:** Identifying and cataloging digital assets, including hardware, software, data, and systems, to understand what needs protection.
2. **Threat Identification:** Recognizing potential cyber threats such as malware, phishing attacks, insider threats, or denial-of-service attacks that could target the organization's assets.
3. **Vulnerability Assessment:** Evaluating weaknesses or vulnerabilities in systems or processes that could be exploited by cyber threats. This involves assessing the security posture of systems, networks, and applications.
4. **Risk Analysis:** Assessing the likelihood of threats exploiting vulnerabilities and the potential impact of such incidents on the organization. This step often involves quantitative and qualitative analysis to prioritize risks.

5. **Risk Mitigation:** Developing and implementing strategies to manage, reduce, or eliminate identified risks. This might involve deploying security controls, encryption, access controls, employee training, incident response plans, and regular security updates.
6. **Monitoring and Response:** Continuously monitoring systems for potential threats and vulnerabilities. Establishing response plans to react swiftly and effectively to cyber incidents, minimizing their impact and restoring normal operations.
7. **Compliance and Governance:** Ensuring that cybersecurity measures align with regulatory requirements and industry best practices. This includes maintaining standards, policies, and procedures to manage risks effectively.

Trusted Computing

- Trusted Computing refers to a set of technologies and standards aimed at creating a more secure computing environment by ensuring the integrity, confidentiality, and authenticity of computer systems and their operations.
- The fundamental goal is to establish trust in the computing infrastructure, protecting against various threats such as malware, unauthorized access, and tampering.
- The Trusted Computing Group (TCG), an industry consortium, has developed and promoted standards and specifications for Trusted Computing.
- Key components and concepts associated with Trusted Computing include:

1. **Trusted Platform Module (TPM):** A hardware-based security chip that provides a secure storage area for cryptographic keys, measurements of system integrity, and secure execution of operations. TPM is used to store sensitive information, verify system integrity, and support secure boot processes.
2. **Secure Boot:** A process that ensures the integrity of the boot sequence by verifying the authenticity of each component before allowing the operating system to load. It prevents unauthorized or malicious software from executing during the boot-up process.

3. **Remote Attestation:** A feature that allows a computing device to prove its current state and configuration to another party. This enables verification of the system's integrity and security posture remotely.
4. **Sealed Storage:** The ability to encrypt and protect sensitive data in a way that ties it to specific system configurations, ensuring that it remains secure and inaccessible if transferred or accessed on unauthorized systems.
5. **Trusted Execution Environment (TEE):** A secure and isolated area within a computing device where sensitive operations can be executed with guarantees of confidentiality and integrity. Examples include Intel SGX (Software Guard Extensions) and ARM TrustZone.

***************** END OF MODULE 1 *****************

MODULE II

Cyber Security Threats and vulnerabilities: types of threats, attacks, malwares, firewalls, hacking, network and services attack, IDPS, honeypots , cryptography and cryptanalysis, network behaviour analysis**, Intrusion Detection Systems:** Types and components of IDS-Network based, Host Based, Hybrid IDS, wireless IDPS

Cyber Security Threats and Vulnerabilities

What is Cyber security threats .?

Cyber security threats refer to potential risks and dangers in the digital world that can compromise the confidentiality, integrity, or availability of information systems, networks, and data. These threats can come in various forms, each with its own methods and goals.

Types of Cyber Security Threads

1. **Malware:**
   Software designed to harm, access, or disrupt a computer, network, or device. It includes viruses, worms, trojans, ransomware, spyware, and adware.
2. **Phishing:**
   Deceptive attempts to obtain sensitive information (passwords, financial data) by pretending to be a trustworthy entity via email, phone, or messaging.
3. **Man-in-the-Middle (MitM) Attacks:**
   Hackers intercept and possibly alter communication between two parties without their knowledge. This can occur in various forms, like session hijacking or DNS spoofing.
4. **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks:**
   Overwhelm a system, server, or network with excessive traffic, rendering it unavailable to its intended users.
5. **Zero-day Exploits:**
   Exploiting software vulnerabilities unknown to the developer or vendor, leaving no time for a fix before exploitation.
6. **IoT Vulnerabilities:**
   Weak security measures in Internet of Things (IoT) devices, making them susceptible to attacks that compromise networks or access sensitive information.
7. **Ransomware:**
   Malware that encrypts data, denying access until a ransom is paid.
8. **Supply Chain Attacks:**
   Target vulnerabilities in a supply chain to gain access to a primary target, often by compromising a vendor or supplier.

9. **Cryptojacking:**

   Illegally using someone else's computer to mine cryptocurrency without their knowledge.

10. **Password Attacks:**

    Trying to obtain passwords by various methods, including brute force attacks, dictionary attacks, or password spraying.

Cyber security attacks

Cyber security attacks are malicious actions aimed at exploiting vulnerabilities in digital systems, networks, or devices to compromise data, disrupt operations, or gain unauthorized access. These attacks come in various forms, targeting different aspects of digital infrastructure.

Some common types of cyber attacks include:

1. **Malware Attacks:** Malicious software (viruses, worms, trojans, ransomware) designed to infiltrate systems, steal data, or cause damage.

2. **Phishing Attacks:** Deceptive attempts to trick individuals into revealing sensitive information (like passwords or financial details) via emails, texts, or messages, often impersonating trusted entities.

3. **Man-in-the-Middle (MitM) Attacks:** Interception and alteration of communication between two parties, allowing attackers to eavesdrop or manipulate data without detection.

4. **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks:** Overloading servers or networks with excessive traffic to disrupt services and make them inaccessible to legitimate users.

5. **Ransomware Attacks:** Encrypting data on systems or networks, denying access until a ransom is paid to the attacker.

6. **SQL Injection Attacks:** Exploiting vulnerabilities in web applications' databases by injecting malicious SQL code, enabling unauthorized access or data manipulation.

7. **Zero-Day Exploits:** Exploiting unknown vulnerabilities in software or hardware before developers can patch or fix them.

8. **Credential Stuffing:** Using previously stolen usernames and passwords to gain unauthorized access to other accounts, exploiting the habit of people using the same credentials across multiple platforms.

9. **IoT-Based Attacks:** Targeting vulnerabilities in Internet of Things (IoT) devices to compromise networks or launch attacks.

10. **Supply Chain Attacks:** Compromising software or hardware at the manufacturing or distribution level to gain access to broader networks.

Malware

- Any malicious software intended to harm or exploit any programmable device, service, or network is referred to as malware.
- Cybercriminals typically use it to extract data they can use against victims to their advantage in order to profit financially.
- Financial information, medical records, personal emails, and passwords are just a few examples of the types of information that could be compromised.
- Malware is short for malicious software and refers to any software that is designed to cause harm to computer systems, networks, or users.

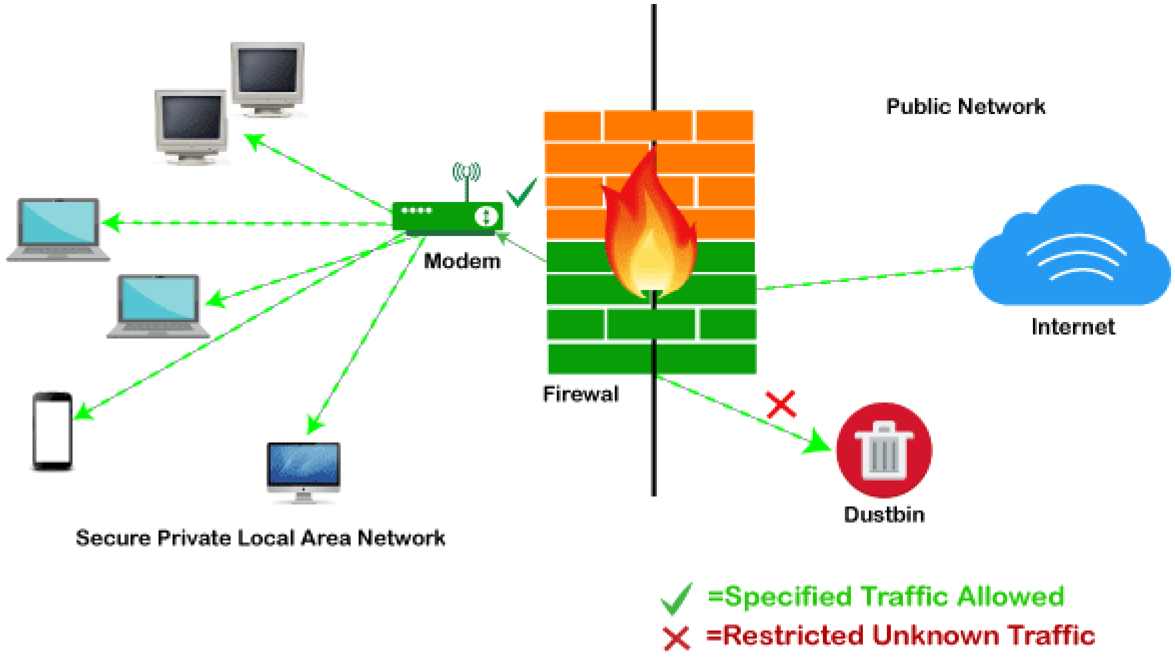
Types of Malware

1. **Viruses –** A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.

2. **Worms –** Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.
3. **Trojan horse –** A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, and audio files.
4. **Ransomware** – Ransomware grasps a computer system or the data it contains until the victim makes a payment. Ransomware encrypts data in the computer with a key that is unknown to the user. The user has to pay a ransom (price) to the criminals to retrieve data. Once the amount is paid the victim can resume using his/her system
5. **Adware** – It displays unwanted ads and pop-ups on the computer. It comes along with software downloads and packages. It generates revenue for the software distributer by displaying ads.
6. **Spyware** – Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.
7. **Logic Bombs –** A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens. Once triggered, a logic bomb implements a malicious code that causes harm to a computer.
8. **Rootkits –** A rootkit modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly. Most rootkits take advantage of software vulnerabilities to modify system files.
9. **Keyloggers –** Keylogger records everything the user types on his/her computer system to obtain passwords and other sensitive information and send them to the source of the keylogging program.

Firewall

- A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules.
- It acts as a barrier between internal private networks and external sources (such as the public Internet).
- The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks.
- A firewall is a cyber security tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.


Public Network
Modem
Internet
Firewal
Dustbin
Secure Private Local Area Network
✓ =Specified Traffic Allowed
✗ =Restricted Unknown Traffic

How does a firewall work?

A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.

Typically, firewalls intercept network traffic at a computer's entry point, known as a port. Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on pre-defined security rules. Incoming traffic is allowed only through trusted IP addresses, or sources.

Functions of Firewall

Firewalls have become so powerful, and include a variety of functions and capabilities with built-in features:

- Network Threat Prevention
- Application and Identity-Based Control
- Hybrid Cloud Support
- Scalable Performance
- Network Traffic Management and Control
- Access Validation
- Record and Report on Events

Hacking

- An effort to attack a computer system or a private network inside a computer is known as hacking.
- Simply, it is unauthorized access to or control of computer network security systems with the intention of committing a crime.
- Hacking is the process of finding some security holes in a computer system or network in order to gain access to personal or corporate information.
- One example of computer hacking is the use of a password cracking technique to gain access to a computer system.

- The process of gaining illegal access to a computer system, or a group of computer systems, is known as hacking.
- This is accomplished by cracking the passwords and codes that grant access to systems.
- Cracking is the term used to describe the process of obtaining a password or code.
- The hacker is the individual who performs the hacking.

Following are some of the things that can be hacked:

- Single systems
- Email account
- A group of systems
- LAN network
- A website
- Social media sites, etc.

Types of Hackers

Computer hackers are unauthorized users who gain access to computers in order to steal, alter, or delete data, generally by installing malicious software without your knowledge or agreement.

1.Black Hat Hackers: These are the stereotypical "bad" hackers who exploit vulnerabilities for malicious purposes. They may engage in activities like stealing data, spreading malware, conducting cyber-attacks for personal gain, or causing harm to individuals or organizations.

2.White Hat Hackers: Also known as ethical hackers or penetration testers, they use their skills to identify and fix security vulnerabilities. White hat hackers work legally and ethically, often employed by organizations to strengthen their cybersecurity defenses.

3.Grey Hat Hackers: This category falls in between black hat and white hat hackers. They might break into systems without authorization but not necessarily with malicious intent. Grey hat hackers may discover vulnerabilities and inform the affected parties without causing damage.

Network and Service Attacks

Network and service attacks refer to various methods used to compromise the availability, integrity, or confidentiality of computer networks and services. These attacks aim to disrupt normal operations, steal data, or gain unauthorized access.

Here are some common types:

1. **Denial-of-Service (DoS) Attack:** Overwhelms a system or network with excessive traffic, making it unavailable to legitimate users. This can be achieved by flooding the target with traffic or exploiting vulnerabilities to consume resources.
2. **Distributed Denial-of-Service (DDoS) Attack:** Similar to DoS but conducted from multiple sources, making it harder to mitigate. Botnets, networks of compromised devices, are often used to launch coordinated DDoS attacks.
3. **Man-in-the-Middle (MitM) Attack:** Intercepting communication between two parties, allowing the attacker to eavesdrop, alter, or inject data without the knowledge of the communicating parties.
4. **Packet Sniffing:** Monitoring and capturing data packets transmitted over a network, potentially exposing sensitive information like passwords or financial details.
5. **DNS Spoofing/Cache Poisoning:** Manipulating the Domain Name System (DNS) to redirect traffic from legitimate websites to malicious ones, leading users to fake sites or compromising their data.
6. **Zero-Day Exploits:** Exploiting unknown vulnerabilities in software or systems before they are patched or fixed by developers.
7. **Botnet Attacks:** Using networks of compromised devices (bots) to carry out coordinated attacks, such as spamming, DDoS, or distributing malware.

Intrusion Detection and Prevention Systems(IDPS)

IDPS stands for Intrusion Detection and Prevention Systems, crucial components of network security. These systems are designed to monitor network traffic, detect potential security threats or unauthorized activities, and take action to prevent or mitigate these threats in real-time.

There are two primary components within IDPS:

1.Intrusion Detection System (IDS): IDS monitors network traffic, looking for suspicious patterns or activities that could indicate a security breach or unauthorized access. It works by analyzing network packets, logs, and other data sources to identify known attack signatures or anomalous behavior. When it detects a potential threat, it generates alerts or notifications for further investigation by security personnel.

2.Intrusion Prevention System (IPS): IPS goes a step further than IDS by actively blocking or preventing identified threats or malicious activities. It not only detects potential security breaches but also takes automated actions to stop or mitigate the impact of these threats. IPS can include features like packet filtering, blocking specific types of traffic, or reconfiguring network devices to defend against attacks in real-time.

IDPS solutions can be network-based (monitoring and protecting network traffic), host-based (focused on individual devices or hosts), or hybrid systems that combine both approaches for comprehensive security coverage.

The key functions and benefits of IDPS include:

1. **Threat Detection:** Identifying suspicious patterns, anomalies, or known attack signatures within network traffic.
2. **Real-time Monitoring:** Constantly monitoring network activity to detect and respond to threats as they occur.

3. **Incident Response:** Providing immediate alerts and responses to potential security incidents, allowing for rapid mitigation.
4. **Policy Enforcement:** Enforcing security policies and rules to ensure compliance and prevent unauthorized access or activities.
5. **Adaptive Protection:** Adapting to new threats by updating databases, signatures, or behavior analysis techniques.

Honeypots

Honeypots are a type of cybersecurity mechanism used to detect, deflect, or study attempts at unauthorized use of information systems. They are essentially decoy systems or resources intentionally designed to attract attackers, allowing security professionals to observe and analyze their tactics, techniques, and methods.

Types of Honeypots:

1.Production Honeypots: These are deployed within a network to mimic real systems and services. They help detect and deflect attacks away from critical systems by attracting attackers to these decoys.

2.Research Honeypots: These are used for studying attackers' behaviors and methods. They are often placed on the internet to observe and analyze a wide range of attacks.

Purposes of Honeypots:

1.Detection: Honeypots can identify unauthorized access attempts or unusual activities that might not be detected by traditional security measures.

2.Deterrence: By diverting attackers' attention away from actual critical systems, honeypots can act as a deterrent, making the real systems less likely targets.

3.Response and Analysis: Security professionals can study attackers' behavior, techniques, and methods without risking the compromise of actual critical systems. This information helps in understanding emerging threats and improving cyber security measures.

Cryptography

- "Crypto" indicates "hidden," and "graphy" indicates "writing," respectively.
- Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it
- Cryptography is the art and science of encoding and decoding information in a secure way to ensure secure communication.
- It involves techniques for converting plaintext (readable data) into ciphertext (encoded data) and vice versa.
- Encryption and decryption are fundamental processes in cryptography used to secure and protect information.

Encryption:

- This is the process of converting plaintext (normal, readable data) into ciphertext (encoded, unreadable data) using an algorithm and a key.
- The goal is to make the data unreadable to anyone who doesn't possess the correct key. There are two main types of encryption

Decryption:

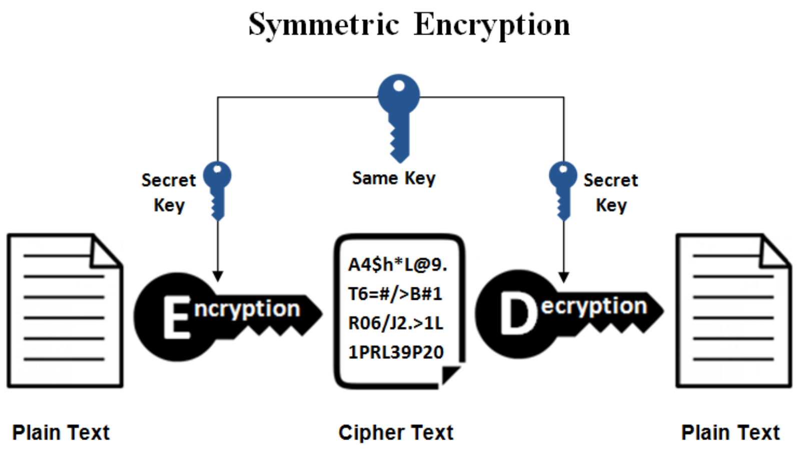
- Decryption is the reverse process of encryption.
- It involves converting the ciphertext back into plaintext using the appropriate decryption algorithm and key.
- For symmetric encryption, the same key used for encryption is also used for decryption.
- For asymmetric encryption, the recipient uses their private key to decrypt data encrypted with their public key.

Types of Cryptography: In general there are three types Of cryptography:

1. Symmetric Key Cryptography
2. Asymmetric Key Cryptography
3. Hash Functions

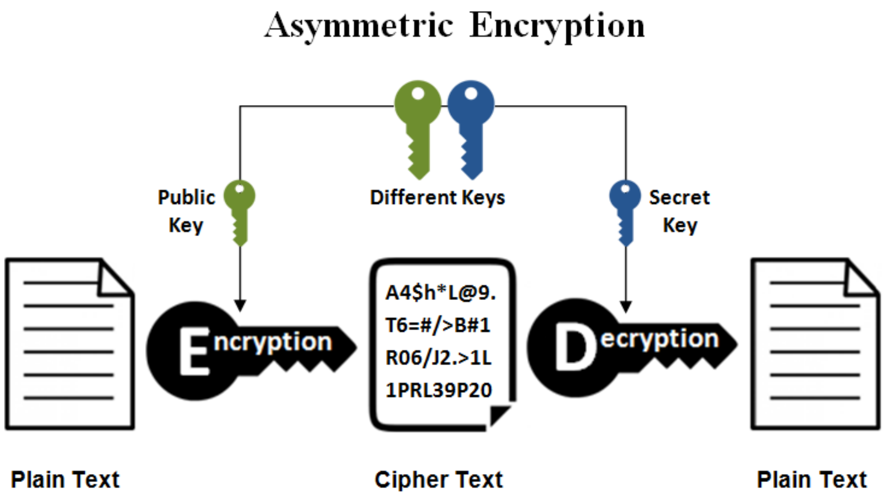
1.Symmetric Key Cryptography:

- It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages.
- Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner.
- The most popular symmetric key cryptography system are Data Encryption System(DES) and Advanced Encryption System(AES).



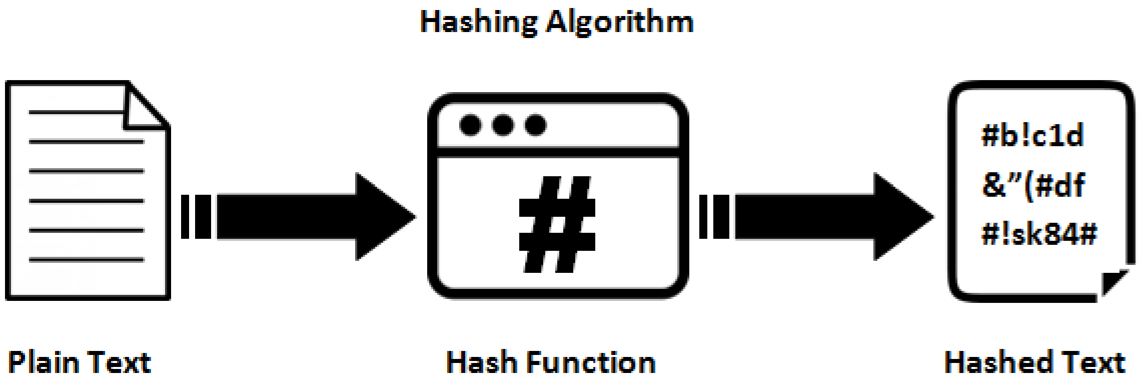
2.Asymmetric Key Cryptography:

- Under this system a pair of keys is used to encrypt and decrypt information.
- A receiver's public key is used for encryption and a receiver's private key is used for decryption. Public key and Private Key are different.
- Even if the public key is known by everyone the intended receiver can only decode it because he alone know his private key.
- The most popular asymmetric key cryptography algorithm is RSA algorithm



3.Hash Functions:

- There is no usage of any key in this algorithm.
- A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered.
- Many operating systems use hash functions to encrypt passwords.



Cryptanalysis

Cryptanalysis is the study of analyzing and breaking encryption and cryptographic systems. Its primary goal is to uncover weaknesses or vulnerabilities in cryptographic algorithms, protocols, or implementations to decrypt encrypted data without having access to the proper key.

There are various approaches to cryptanalysis:

1. **Brute Force Attack:** This method involves trying all possible keys until the correct one is found. It's typically impractical for strong encryption algorithms due to the vast number of possible keys.
2. **Known-plaintext Attack:** In this approach, the attacker has access to some plaintext-ciphertext pairs. By analyzing these pairs, they attempt to deduce the key or other weaknesses in the encryption system.
3. **Chosen-plaintext Attack:** Here, the attacker can choose and encrypt specific plaintexts and observe the corresponding ciphertexts. This method helps deduce information about the encryption algorithm or the key.
4. **Frequency Analysis:** This technique involves analyzing the frequency of characters or patterns in the ciphertext to infer information about the plaintext. For example, in simple substitution ciphers, certain letters or combinations of letters might appear with different frequencies than in normal language.
5. **Side-Channel Attacks:** These attacks focus on exploiting weaknesses not in the encryption algorithm itself, but in its implementation or the system around it. For instance, timing information, power consumption, electromagnetic radiation, or other physical properties of the system might leak information about the encryption key.

Network Behavior Analysis(NBA)

- Network Behavior Analysis (NBA) is a cybersecurity approach that focuses on monitoring and analyzing network traffic patterns and behaviors to identify and respond to potential security threats and anomalies.
- Instead of relying solely on signature-based detection (matching against known patterns of attacks), NBA looks at the broader behavior of network traffic, devices, and users

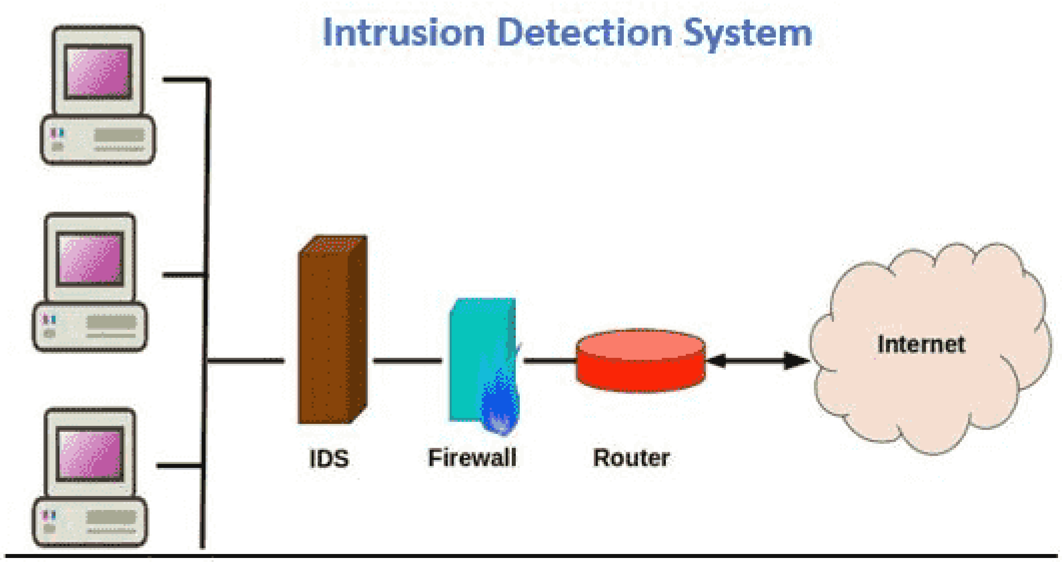
It involves analyzing various parameters, such as:

1. **Traffic Patterns:** Examining normal patterns of data transfer, communication protocols used, and typical traffic volumes.
2. **Device Behavior:** Monitoring the behavior of devices on the network, such as endpoints, servers, and IoT devices, to detect unusual activities.
3. **User Activity:** Observing user behavior and access patterns to detect any abnormal or suspicious actions.
4. **Anomaly Detection:** Identifying deviations from established baselines or normal behaviors, which might indicate potential security threats like malware infections, data,unauthorized access..

Intrusion Detection Systems

- A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed.
- It is software that checks a network or system for malicious activities or policy violations.
- Each illegal activity or violation is often recorded either centrally using a software or notified to an administration.
- IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders.

- The intrusion detector learning task is to build a predictive model (i.e. a classifier) capable of distinguishing between ‘bad connections’ (intrusion/attacks) and ‘good (normal) connections’.



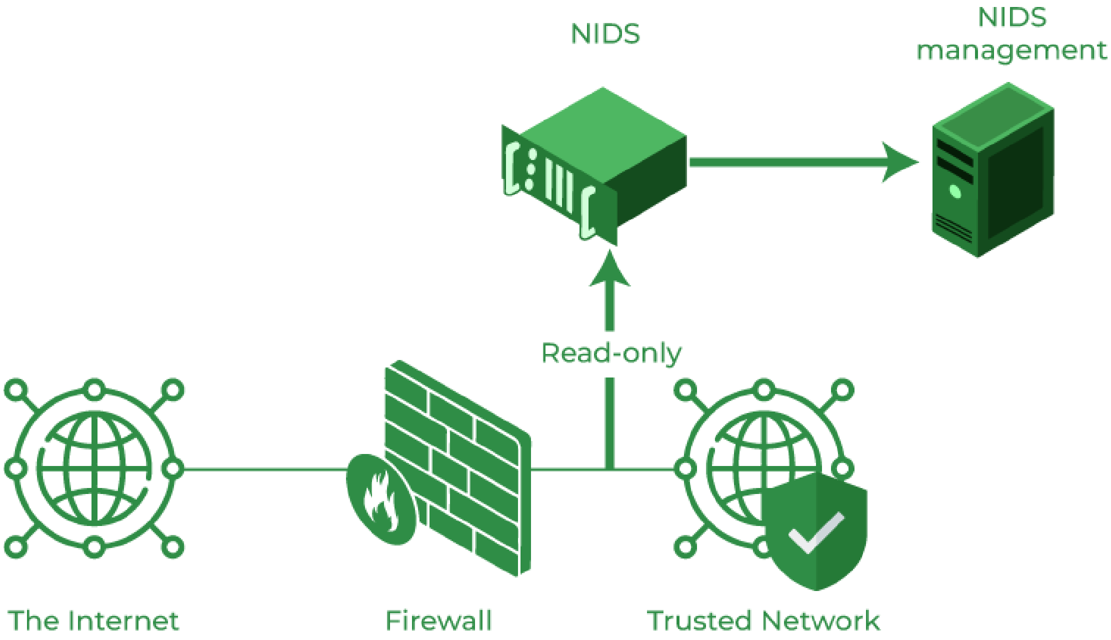
Types of Intrusion Detection System

IDS are classified into 5 types:

1. Network Intrusion Detection System (NIDS)
2. Host Intrusion Detection System (HIDS):
3. Protocol-based Intrusion Detection System (PIDS
4. Application Protocol-based Intrusion Detection System (APIDS
5. Hybrid Intrusion Detection System
6. Wireless Intrusion Detection System (WIDS)

1.Network Intrusion Detection System (NIDS):

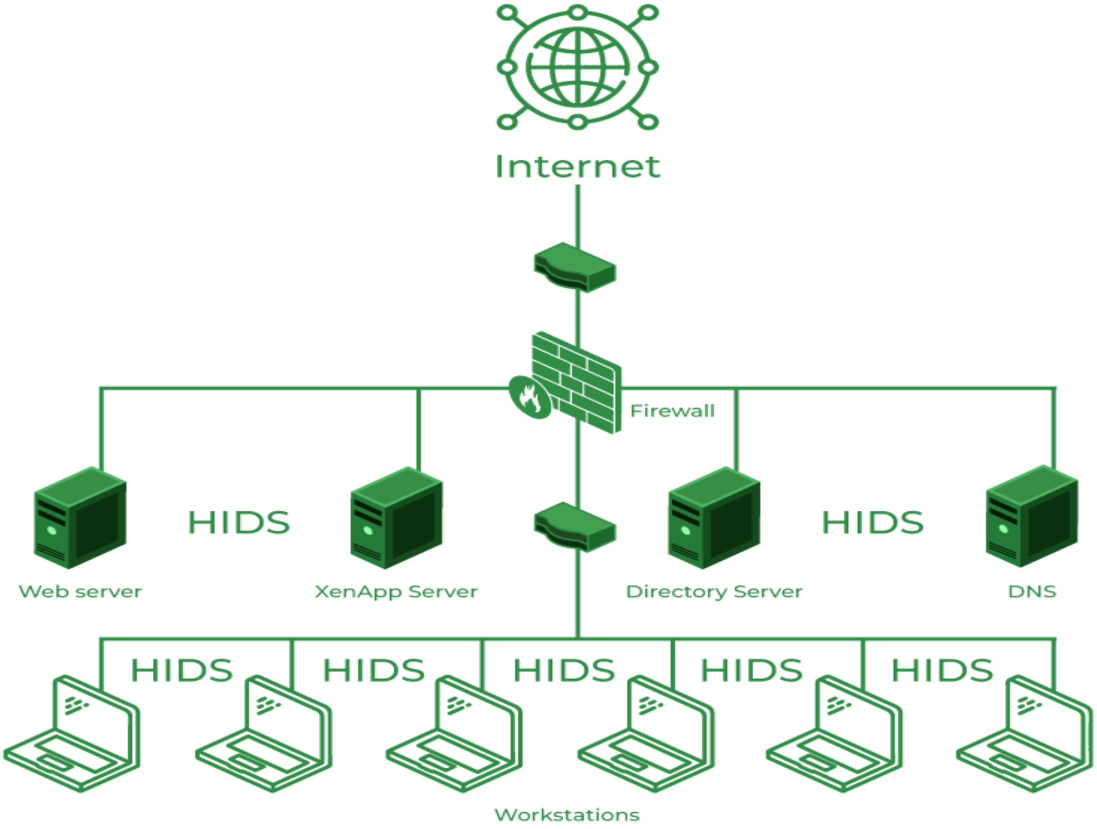
- Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network.
- It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks.
- Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator.
- An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.



2.Host Intrusion Detection System (HIDS):

- Host intrusion detection systems (HIDS) run on independent hosts or devices on the network.
- A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected.

- It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate.
- An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.



3.Protocol-based Intrusion Detection System (PIDS):

- Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server.
- It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accepting the related HTTP protocol.
- As HTTPS is unencrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

4.Application Protocol-based Intrusion Detection System (APIDS):

- An application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers.
- It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols.
- For example, this would monitor the SQL protocol explicitly to the middleware as it transacts with the database in the web server.

5.Hybrid Intrusion Detection System:

- Hybrid intrusion detection system is made by the combination of two or more approaches to the intrusion detection system.
- In the hybrid intrusion detection system, the host agent or system data is combined with network information to develop a complete view of the network system.
- The hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

6.Wireless IDS

- Wireless Intrusion Detection and Prevention Systems (WIDPS) are specialized security solutions designed to monitor and protect wireless networks from potential security threats and intrusions.
- These systems are specifically tailored to address the unique vulnerabilities and risks associated with wireless communication protocols.
- Wireless networks introduce unique security challenges due to their inherent nature of broadcasting data over the air.
- WIDPS play a crucial role in safeguarding these networks by monitoring and protecting against various threats, including rogue access points, unauthorized access attempts, denial-of-service attacks, and other wireless-specific vulnerabilities.

Components of Intrusion Detection System

1. **Sensors**: These components are responsible for collecting data related to network traffic, system events, logs, or user activities. Sensors can be network-based (NIDS) or host-based (HIDS) and gather information from various sources within the network or system.
2. **Analytical Engine:** This core component processes the data collected by sensors. It applies various methods such as signature-based detection, anomaly detection, or behavior analysis to identify potential security threats or intrusions.
3. **Alerting Mechanism:** When the analytical engine detects suspicious activities or anomalies, it triggers alerts or notifications. This mechanism notifies security administrators or personnel, enabling them to investigate and respond to potential threats promptly.
4. **Event Logs and Databases:** IDS systems maintain detailed logs and databases of security-related events, alerts, and detected incidents. These logs provide a historical record for analysis, reporting, and forensic purposes.
5. **User Interface:** The user interface provides a graphical or command-line interface for security analysts or administrators to interact with the IDS. It allows for monitoring, configuration, analysis of alerts, and investigation of security incidents.

***************** END OF MODULE 2 *****************

MODULE III

Security policies: needs and uses**,** policy development, types of security policies, steps in policy review process, **Security Standards**- ISO, Intellectual property rights, patents, trademarks, copyrights, software licensing, e-contracts, Cyber laws in India.. **Security and Law:-**Regulations in India- IT Act 2000/2008, Cyber Crime- cyber law, Indian Copyright Act, Indian Contract Act , Consumer Protection Act, Future Trends –The Law of Convergence.

Security Policies

- Security policies are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information.
- It is a written document in the organization which is responsible for how to protect the organizations from threats and how to handles them when they will occur.
- A security policy also considered to be a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.

Need of Security Policies

1) It increases efficiency.

- The best thing about having a policy is being able to increase the level of consistency which saves time, money and resources.
- The policy should inform the employees about their individual duties, and telling them what they can do and what they cannot do with the organization sensitive information.

2) It upholds discipline and accountability

- When any human mistake will occur, and system security is compromised, then the security policy of the organization will back up any disciplinary action and also supporting a case in a court of law.
- The organization policies act as a contract which proves that an organization has taken steps to protect its intellectual property, as well as its customers and clients.

3) It can make or break a business deal

- It is not necessary for companies to provide a copy of their information security policy to other vendors during a business deal that involves the transference of their sensitive information.
- It is true in a case of bigger businesses which ensures their own security interests are protected when dealing with smaller businesses which have less high-end security systems in place.

4) It helps to educate employees on security literacy

- A well-written security policy can also be seen as an educational document which informs the readers about their importance of responsibility in protecting the organization sensitive data.
- It involves on choosing the right passwords, to providing guidelines for file transfers and data storage which increases employee's overall awareness of security and how it can be strengthened.

Uses of Cyber Security Polices

1. **Risk Management:** Cyber security policies help identify and assess potential risks to an organization's systems and data. They outline procedures to mitigate these risks, such as implementing firewalls, encryption, or regular software updates.
2. **Compliance and Regulations:** Many industries have specific regulations (like GDPR, HIPAA, etc.) that require adherence to certain cybersecurity standards. Policies ensure that the organization complies with these regulations, avoiding penalties and legal issues.
3. **Employee Guidelines:** Policies establish rules and best practices for employees regarding the use of company devices, networks, and data. This includes guidelines on password management, acceptable use of resources, and how to handle sensitive information.

4. **Security Awareness and Training:** Policies often include provisions for ongoing education and training programs to keep employees informed about emerging threats and how to respond to them effectively.
5. **Regular Auditing and Updates:** Policies need to evolve with the changing threat landscape and technology. Regular audits ensure that security measures are up to date and effective against the latest threats.

Types of Cyber Security Polices

There are some important cyber security policies recommendations describe below-

1. Virus and Spyware Protection policy: This policy provides the following protection:

- It helps to detect, removes, and repairs the side effects of viruses and security risks by using signatures.
- It helps to detect the threats in the files which the users try to download by using reputation data from Download Insight.
- It helps to detect the applications that exhibit suspicious behaviour by using SONAR heuristics and reputation data.

2. Firewall Policy :This policy provides the following protection:

- It blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
- It detects the attacks by cybercriminals.
- It removes the unwanted sources of network traffic.

3. Intrusion Prevention policy

- This policy automatically detects and blocks the network attacks and browser attacks. It also protects applications from vulnerabilities.
- It checks the contents of one or more data packages and detects malware which is coming through legal ways.

4. LiveUpdate policy

- This policy can be categorized into two types one is LiveUpdate Content policy, and another is LiveUpdate Setting Policy.
- The LiveUpdate policy contains the setting which determines when and how client computers download the content updates from LiveUpdate.
- We can define the computer that clients contact to check for updates and schedule when and how often clients computer check for updates.

5. Application and Device Control

- This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system.
- The device control policy applies to both Windows and Mac computers whereas application control policy can be applied only to Windows clients.

6. Exceptions policy

This policy provides the ability to exclude applications and processes from detection by the virus and spyware scans.

7. Host Integrity policy

- This policy provides the ability to define, enforce, and restore the security of client computers to keep enterprise networks and data secure.
- We use this policy to ensure that the client's computers who access our network are protected and compliant with companies? securities policies.
- This policy requires that the client system must have installed antivirus.

Steps in Policy Review Process

The review process for cyber security policies involves several steps to ensure they remain effective and aligned with the evolving threat landscape and organizational needs. Here's an overview of the steps typically involved:

1.Initiation and Planning:

- Identify the need for a policy review, triggered by factors like changes in regulations, technology, or recent security incidents.
- Formulate a review team or designate responsible individuals to oversee the process.
- Establish a timeline and scope for the review.

2.Gather Information:

- Collect existing cybersecurity policies, procedures, and related documentation.
- Review incident reports, security assessments, and compliance requirements to identify gaps or areas for improvement.

3.Risk Assessment:

- Conduct a thorough risk assessment to understand current threats and vulnerabilities faced by the organization.
- Analyze potential impacts of these risks on the organization's assets, operations, and reputation.

4.Policy Analysis:

- Evaluate the existing policy against current best practices, industry standards, and regulatory requirements.
- Identify areas where the policy might be outdated, unclear, or lacking in coverage.

5.Drafting and Revision:

- Update the policy language, incorporating new security measures, guidelines, and controls as per identified needs.
- Ensure the policy aligns with the organization's goals, culture, and risk tolerance.
- Seek feedback from relevant stakeholders and subject matter experts for input and revisions.

6.Approval and Implementation:

- Obtain approval from management or the appropriate governing body for the revised policy.
- Develop an implementation plan, including communication strategies, training, and awareness programs for employees.

7.Monitoring and Review:

- Implement the revised policy and monitor its effectiveness.
- Establish metrics and key performance indicators (KPIs) to measure compliance and the impact of the updated policy.
- Schedule periodic reviews, possibly annually or bi-annually, to ensure the policy remains relevant and effective.

8.Documentation and Communication:

- Document all changes made during the review process.
- Communicate the updated policy to all relevant stakeholders and ensure they understand their roles and responsibilities.

9.Continuous Improvement:

- Establish a feedback mechanism to continuously gather insights from security incidents, audits, or employee suggestions for further policy improvements.
- Incorporate lessons learned and best practices into future policy revisions.

Security Standards

- To make cybersecurity measures explicit, the written norms are required. These norms are known as cybersecurity standards: the generic sets of prescriptions for an ideal execution of certain measures.
- The standards may involve methods, guidelines, reference frameworks, etc.
- It ensures efficiency of security, facilitates integration and interoperability, enables meaningful comparison of measures, reduces complexity, and provide the structure for new developments.
- The goal of security standards is to improve the security of information technology (IT) systems, networks, and critical infrastructures.
- The Well-Written cybersecurity standards enable consistency among product developers and serve as a reliable standard for purchasing security products.
- Security standards are generally provided for all organizations regardless of their size or the industry and sector in which they operate.

The following are Cyber Security Standerds

1.ISO

- ISO stands for International Organization for Standardization.
- These standards provide a world-class specification for products, services and computers, to ensure quality, safety and efficiency.
- ISO standard is officially established On 23 February 1947.
- It is an independent, non-governmental international organization. Today, it has a membership of 162 national standards bodies and 784 technical committees and subcommittees to take care of standards development.
- ISO has published over 22336 International Standards and its related documents which covers almost every industry, from information technology, to food safety, to agriculture and healthcare.

ISO 27000 Series

It is the family of information security standards which is developed by the International Organization for Standardization and the International Electrotechnical Commission to provide a globally recognized framework for best information security management. It helps the organization to keep their information assets secure such as employee details, financial information, and intellectual property.

The ISO 27000 series can be categorized into many types. They are-

ISO 27001- This standard allows us to prove the clients and stakeholders of any organization to managing the best security of their confidential data and information.

ISO 27000- This standard provides an explanation of terminologies used in ISO 27001.

ISO 27002- This standard provides guidelines for organizational information security standards and information security management practices.

ISO 27005- This standard supports the general concepts specified in 27001. It is designed to provide the guidelines for implementation of information security based on a risk management approach.

ISO 27032- It is the international Standard which focuses explicitly on cybersecurity. This Standard includes guidelines for protecting the information beyond the borders of an organization such as in collaborations, partnerships or other information sharing arrangements with clients and suppliers.

2. Intellectual property rights (IPR)

- Intellectual property rights is a right that allow creators, or owners of patents, trademarks or copyrighted works to benefit from their own plans, ideas, or other intangible assets or investment in a creation.

- These IPR rights are outlined in the Article 27 of the Universal Declaration of Human Rights.
- It provides for the right to benefit from the protection of moral and material interests resulting from authorship of scientific, literary or artistic productions.
- These property rights allow the holder to exercise a monopoly on the use of the item for a specified period.

3. Patent

- Patent is a law that deals with new inventions.
- Traditional patent law protect tangible scientific inventions, such as circuit boards, heating coils, car engines, or zippers.
- As time increases patent law have been used to protect a broader variety of inventions such as business practices, coding algorithms, or genetically modified organisms.
- It is the right to exclude others from making, using, selling, importing, inducing others to infringe, and offering a product specially adapted for practice of the patent.
- Patents protect inventions or discoveries, granting the inventor exclusive rights to use, make, or sell their invention for a limited period (usually 20 years). They cover processes, machines, compositions of matter, or improvements on existing inventions.

In general, a patent is a right that can be granted if an invention is:

- Not a natural object or process
- New
- Useful
- Not obvious.

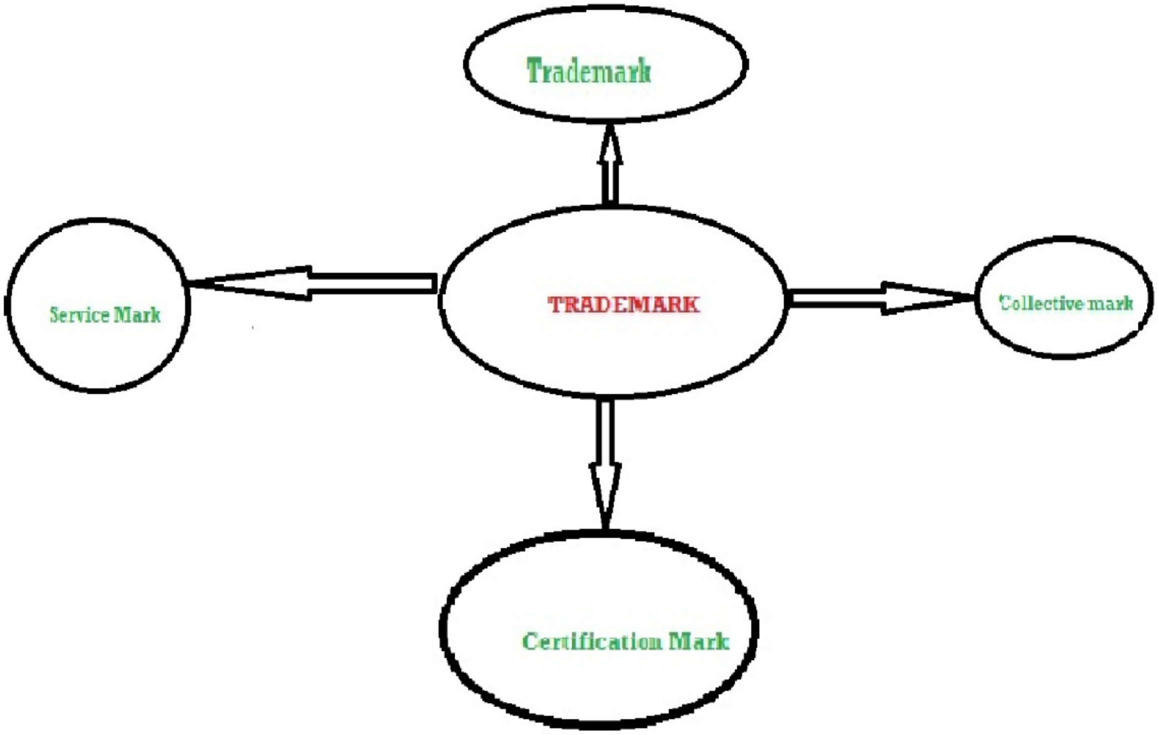
4.Trad mark

A trademark is a distinctive sign, symbol, logo, word, phrase, or a combination of these elements that identifies and distinguishes the products or services of one party from those of others in the market.

It essentially serves as a badge of origin, signaling to consumers the source of the goods or services and representing the quality and reputation associated with that source.

Types of Trademarks:

Trademarks can be classified into 4 types:



1. **Trademark –**

   It is a mark which includes any word, name, symbol, or any combination which is used in commerce to identify and differentiate the products of a manufacturer from products of others. In short, Trademark is a brand name.

2. **Service Mark –**

   It is a mark which includes any word, name, symbol, or any combination which is used in commerce to identify and differentiate the services provided by one provider from services provided by others. It is used in service business.

3. **Certification Mark –**

   It is a mark which includes any word, name, symbol, or any combination which is used in commerce by other persons with owner's consent and certifies them regional, material, mode of manufacture, or other characteristics of owner's goods .

4. **Collective Mark –**

   It is a mark which includes any word, name, symbol, or any combination which is used in commerce by members of an association or group or organization.

5 copyright

- A copyright is a kind of intellectual property that grants its owner the sole authority to reproduce, display, transmit, modify, and perform creative work, frequently for a limited period.
- Creative work can be in a literature form, an art form, or an education form.
- The purpose of copyrights is to safeguard the first innovative representation of a concept.
- It aids in protecting authors against others copying their works without their approval for profit. In short, a copyright is a "Right to Copy" only granted to the real author.

Types of Copyrights in India

Copyrights promote an atmosphere that encourages creativity by protecting the rights of the original authors of works. The copyrights act applies to a variety of works. The copyrights available in India are listed below:

1. Literary works

Works that include original or distinct literary production fall under this category. Scripts, novels, biographies, research papers, technical books, and algorithms are examples of literary works.

2. Dramatic works

It is another type of literary work. It covers play preparation, entertainment show, drama, choreography etc. The cinematic movie is not considered in the dramatic work.

3. Artistic works

The "Copyright Act of 1957 "protects artistic works such as paintings, moulds, photographs, buildings, schematics, etchings, cartoons, plans, and casts for sculptures, graphics, drawings etc.

4. Cinematographic films

Cinematographic films typically contain all previously-recorded visual and moving-image works. It is work that combines a visual recording with sound recordings.

5. Sound recording

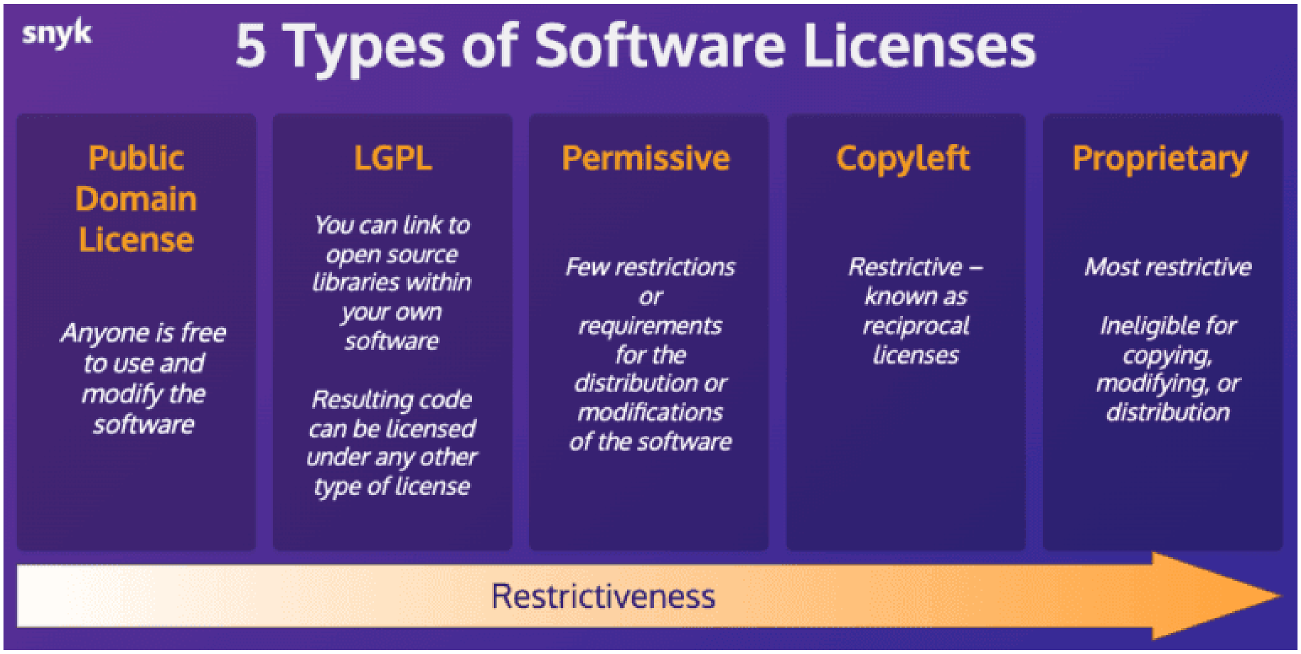
Audio recording on any storage medium qualifies as a sound recording. Its examples are songs with or without music, a podcast, or recorded audio.

6.Software Licensing

- Software licensing in cybersecurity refers to the legal agreement between the software provider (licensor) and the user (licensee) that outlines the terms and conditions for the use of specific cybersecurity software.
- These licenses dictate how the software can be used, distributed, modified, and whether the user needs to pay for its use.
- In simple terms, a software license establishes rules of use and outlines any restrictions that may apply.
- A software license key is a combination of numbers and/or letters that authorizes the use of software.
- This unique code is used to verify a purchaser's right to install software and makes it available for use, so long as the license key has not already been used.

Types of software licenses

There are five main software license categories or types used to cover different kinds of software and various business arrangements.



snyk

5 Types of Software Licenses

Public Domain License
Anyone is free to use and modify the software

LGPL
You can link to open source libraries within your own software
Resulting code can be licensed under any other type of license

Permissive
Few restrictions or requirements for the distribution or modifications of the software

Copyleft
Restrictive – known as reciprocal licenses

Proprietary
Most restrictive
Ineligible for copying, modifying, or distribution

Restrictiveness

5 types of software licenses

1. Public Domain License

- When software is defined as being in the public domain, anyone is free to use and modify the software without restrictions. This is a "permissive" license that allows adopting the code into applications or projects and reusing the software as desired.
- Public domain software may not always adhere to best coding practices or may not be up to standards of secure software that the application requires.
- Software that does not fall under specific licensing terms is not always public domain code. Be sure the software is truly public domain before copying, reusing, or distributing it.

2. GNU/LGPL – GNU Lesser General Public License (LGPL)

- Under an LGPL license, developers have rights to link to open source libraries within their own software.
- Resulting code can be licensed under any other type of license – even proprietary – when projects are compiled or linked to include an LGPL-licensed library.
- The caveat is that if any part of the library is copied into the code or modified, the terms of the original LGPL license will apply to the developed code that used the library.

3. Permissive

- This type of license is one of the most common and popular among open-source software licenses.
- Under a permissive license – also referred to as "**Apache**" or "**BSD** style" – there are few restrictions or requirements for the distribution or modifications of the software. Another variation of a permissive software license is the "MIT" license.
- Variants in permissive licenses include differences in requirements for preserving license notices and copyrights for the software, as well as how the software may be used (commercial or private), trademark requirements, and other stipulations.

4. Copyleft

- This license's terms are restrictive – known as reciprocal licenses. Under the terms of a copyleft license, the licensed code may be modified or distributed as part of a software project if the new code is distributed under the same software license.
- This means that if the code included in the software product was specified to be for "personal use only," the new product being distributed must carry that same designation/restriction.
- Since the original software included with the new project allowed modifications and distribution, this may not be the best license for software developers because the resulting code must also carry the copyleft license type – including the availability of the source code.

5. Proprietary

- These software licenses make the software ineligible for copying, modifying, or distribution. This is the most restrictive type of software license, protecting the developer or owner from unauthorized use of the software.

E-contracts

- E-contracts, short for electronic contracts, refer to agreements or contracts created, negotiated, and signed electronically, typically through digital means without physical paperwork.
- In the context of cybersecurity, e-contracts involve the use of digital technology to facilitate contract creation, execution, and storage while ensuring security and authenticity throughout the process.
- E-contracts offer efficiency, speed, and convenience in managing agreements, but their security is of paramount importance.

- It Ensuring that proper cybersecurity measures are in place throughout the lifecycle of e-contracts is crucial to prevent unauthorized access, tampering, or disputes, and to uphold the validity and enforceability of these digital agreements.

- An electronic contract is an agreement formulated online. The parties interact with one another in a digital format, rather than in-person or over the phone.

Essential Elements of E-Contracts

- **Offer:** A specific offer from one party to the other to perform some service or pay for some good.
- **Acceptance:** An acceptance from the other party agreeing to the terms of the offer.
- **Promise:** A promise to do the action that has been accepted, such as payment for certain goods.
- **Consideration:** Something of value given by one party to the other in exchange for goods or services. For example, $5,000 for office supplies.
- **Capacity:** Whether or not the signers understand the terms being agreed to.
- **Legality:** The contract matter itself is legal.

Cyber laws in India

In India, cyber laws encompass a range of regulations and statutes aimed at addressing various aspects of cybersecurity, data protection, electronic transactions, and online activities.

Some key cyber laws in India include:

1. **Information Technology Act, 2000 (IT Act):** This is the primary legislation governing cyber activities in India. It defines legal provisions related to electronic governance, digital signatures, data protection, and cybercrimes. Sections of the IT Act deal with offenses such as hacking, data theft, identity theft, cyber terrorism, and online fraud.
2. **The Information Technology (Intermediaries Guidelines) Rules, 2011:** These rules lay down guidelines and due diligence to be observed by intermediaries, including social media platforms and online service providers, concerning the content hosted on their platforms.

3. **The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016:** This act regulates the use of Aadhaar, a biometric identification system used for various government services. It addresses data protection and the use of Aadhaar information.
4. **The Payment and Settlement Systems Act, 2007:** This act provides the legal framework for payment systems in India, including electronic fund transfers, digital payments, and the regulation of payment system operators.
5. **Data Protection Bill:** India has been working on a comprehensive data protection bill aimed at regulating the processing of personal data and ensuring the privacy of individuals. As of now, the bill is under review and might bring significant changes once enacted.

The Information Technology Act 200/2008

- The Information Technology Act, 2000 also Known as an **IT Act** is an act proposed by the Indian Parliament reported on 17th October 2000.
- This Information Technology Act is based on the United Nations Model law on Electronic Commerce 1996 (UNCITRAL Model) which was suggested by the General Assembly of United Nations by a resolution dated on 30th January, 1997.
- It is the most important law in India dealing with Cybercrime and E-Commerce.
- The main objective of this act is to carry lawful and trustworthy electronic, digital and online transactions and alleviate or reduce cybercrimes.
- The IT Act has 13 chapters and 94 sections.
- The last four sections that starts from ‘section 91 – section 94’, deals with the revisions to the Indian Penal Code 1860.

The IT Act, 2000 has two schedules:

- **First Schedule –**

  Deals with documents to which the Act shall not apply.
- **Second Schedule –**

  Deals with electronic signature or electronic authentication method.

The offences and the punishments in IT Act 2000 :

The offences and the punishments that falls under the IT Act, 2000 are as follows :-

1. Tampering with the computer source documents.
2. Directions of Controller to a subscriber to extend facilities to decrypt information.
3. Publishing of information which is obscene in electronic form.
4. Penalty for breach of confidentiality and privacy.
5. Hacking for malicious purposes.
6. Penalty for publishing Digital Signature Certificate false in certain particulars.
7. Penalty for misrepresentation.
8. Confiscation.
9. Power to investigate offences.
10. Protected System.
11. Penalties for confiscation not to interfere with other punishments.
12. Act to apply for offence or contravention committed outside India.
13. Publication for fraud purposes.
14. Power of Controller to give directions.

Sections and Punishments under Information Technology Act, 2000 are as follows :

SECTION	PUNISHMENT
Section 43	This section of IT Act, 2000 states that any act of destroying, altering or stealing computer system/network or deleting data with malicious intentions without authorization from owner of the computer is liable for the payment to be made to owner as compensation for damages.
Section 43A	This section of IT Act, 2000 states that any corporate body dealing with sensitive information that fails to implement reasonable security practices causing loss of other person will also liable as convict for compensation to the affected party.

Section 66	Hacking of a Computer System with malicious intentions like fraud will be punished with 3 years imprisonment or the fine of Rs.5,00,000 or both.
Section 66 B, C, D	Fraud or dishonesty using or transmitting information or identity theft is punishable with 3 years imprisonment or Rs. 1,00,000 fine or both.
Section 66 E	This Section is for Violation of privacy by transmitting image of private area is punishable with 3 years imprisonment or 2,00,000 fine or both.
Section 66 F	This Section is on Cyber Terrorism affecting unity, integrity, security, sovereignty of India through digital medium is liable for life imprisonment.
Section 67	This section states publishing obscene information or pornography or transmission of obscene content in public is liable for imprisonment up to 5 years or fine of Rs. 10,00,000 or both.

Cyber Crimes

Cybercrime refers to criminal activities carried out using digital technology or the internet. These offenses involve the use of computers, networks, or electronic devices to commit illegal acts, often targeting individuals, organizations, or governments.

The following are cyber Crimes

1. **Hacking:** Unauthorized access into computer systems, networks, or devices to steal data, disrupt operations, or cause damage.
2. **Malware Attacks:** Spreading malicious software (viruses, ransomware, spyware) to compromise systems, steal information, or extort money.
3. **Phishing and Social Engineering:** Deceptive techniques to trick individuals into revealing sensitive information such as passwords, credit card details, or personal data.
4. **Identity Theft:** Stealing personal information to impersonate someone for financial gain, access to services, or commit fraudulent activities.
5. **Online Fraud:** Various fraudulent schemes conducted online, including investment scams, lottery scams, and fake websites to deceive victims for monetary gain.

6. **Cyberbullying:** Harassment, intimidation, or defamation using digital platforms to harm or harass individuals.
7. **Distributed Denial of Service (DDoS) Attacks:** Overloading servers or networks with excessive traffic to disrupt services or websites, rendering them inaccessible to legitimate users.
8. **Child Exploitation:** Online exploitation of children for pornography, grooming, or trafficking purposes.
9. **Data Breaches:** Unauthorized access to and theft of sensitive information from databases or systems, leading to the exposure of personal or confidential data.

Cyber law

Cyber law refers to the legal framework that governs cyberspace, encompassing various aspects of digital technology, internet usage, electronic communications, and online activities. It includes laws, regulations, statutes, and legal principles that address the rights, responsibilities, and liabilities of individuals, organizations, and governments in the digital realm.

Cyber law covers a wide range of areas

1.Cybercrimes: Laws defining and regulating offenses committed using computers, networks, or digital devices. These laws address hacking, data breaches, identity theft, online fraud, cyberbullying, and other illegal activities in cyberspace.

2.Data Protection and Privacy: Laws and regulations governing the collection, storage, processing, and sharing of personal and sensitive information. They establish guidelines for safeguarding individuals' privacy rights and impose obligations on organizations handling personal data.

3.Electronic Transactions and Digital Signatures: Legal provisions that recognize electronic documents, digital signatures, and online contracts as legally valid and enforceable, promoting the use of digital transactions.

4.Intellectual Property Rights: Laws protecting intellectual property in the digital environment, covering copyright, patents, trademarks, and trade secrets. These laws address issues related to digital content, piracy, plagiarism, and infringement online.

5.Cybersecurity and Network Security: Legal frameworks related to cybersecurity measures, data security, and protection against cyber threats. They mandate security practices, incident reporting, and measures to prevent cyber attacks.

6.Online Freedom of Expression and Internet Governance: Laws concerning freedom of speech, censorship, regulation of content, and policies governing internet governance at national and international levels.

7.Regulation of Online Commerce: Laws governing e-commerce, digital contracts, consumer protection, and electronic payments to ensure fair and secure online transactions.

Indian Copyright Act

The Indian Copyright Act is a legislation that governs copyright law in India. Enacted in 1957, it has undergone several amendments to align with international standards, technological advancements, and evolving creative practices. The Act grants legal protection to original works of authorship and provides creators with exclusive rights to their creations.

<u>Scope of Protection:</u>

1.Original Works: The Act protects original literary, dramatic, musical, and artistic works, as well as cinematographic films and sound recordings. This includes books, poems, plays, music compositions, paintings, sculptures, movies, and recordings.

2.Exclusive Rights: Copyright holders are granted exclusive rights to reproduce, distribute, display, perform, and create derivative works based on their original creations.

Duration of Protection:

Term of Copyright: Generally, the duration of copyright protection lasts for the lifetime of the author plus 60 years after their death. For anonymous works, pseudonymous works, or works of joint authorship, protection extends to 60 years from the year of publication.

Rights of Copyright Holders:

1.Moral Rights: Authors have moral rights, including the right to claim authorship of the work and the right to prevent distortion or mutilation of the work.

2.Economic Rights: Copyright holders have economic rights allowing them to control the commercial exploitation of their works.

Indian Contract Act

The Indian Contract Act, 1872, is a key legislation that governs contracts and agreements in India. It outlines the legal framework for creating and enforcing contracts, defining the rights, duties, and obligations of parties involved in contractual relationships. Here are the key components and provisions of the Indian Contract Act:

Contract: The Act defines a contract as an agreement enforceable by law. It requires that an agreement must have lawful consideration, lawful object, and must not be expressly declared void by law.

Essentials of Valid Contracts:

Offer and Acceptance: A contract begins with an offer by one party and its acceptance by the other, creating mutual consent among the parties.

Lawful Consideration and Object: Consideration (something of value exchanged between parties) and object (purpose or thing to be done) must be lawful for a contract to be valid.

Capacity to Contract: Parties entering into a contract must have the legal capacity to do so. Minors, individuals of unsound mind, and those disqualified by law cannot enter into contracts.

Types of Contracts:

1. **Express and Implied Contracts:** Contracts can be express (stated verbally or in writing) or implied (inferred from actions or circumstances).
2. **Void, Voidable, and Valid Contracts:** Contracts can be void (lacking legal effect from the beginning), voidable (capable of being voided by one party), or valid (fully enforceable).

Performance and Discharge of Contracts:

1. **Performance:** Parties are required to fulfill their contractual obligations as agreed upon in the contract.
2. **Discharge:** Contracts are discharged by performance, agreement, impossibility of performance, breach, or operation of law.

The Consumer Protection Act (CPA)

The Consumer Protection Act (CPA) in India is a crucial legislation aimed at safeguarding consumers' interests, rights, and welfare. Enacted in 1986 and subsequently amended in 2019, the CPA provides a legal framework for addressing consumer grievances, ensuring fair and transparent dealings in the marketplace, and promoting consumer rights.

Objectives and Scope:

1. **Consumer Rights:** The Act identifies and protects the rights of consumers, including the right to safety, right to information, right to choose, right to be heard, right to seek redressal, and right to consumer education.

2. **Consumer Councils:** The Act establishes consumer protection councils at the national, state, and district levels to promote and protect consumers' interests.

Consumer Disputes Redressal Mechanism:

The Act sets up various consumer forums – District Consumer Disputes Redressal Forum, State Consumer Disputes Redressal Commission, and National Consumer Disputes Redressal Commission – for handling consumer complaints based on the value of goods or services and jurisdiction.

Consumer Rights and Responsibilities:

1. **Right to Information:** Consumers have the right to obtain accurate and detailed information about goods and services, including their quality, quantity, pricing, and safety.
2. **Right to Redressal:** Consumers can seek compensation or redressal for unfair trade practices, defective products, deficient services, or unfair treatment.

Law of Convergence

The Law of Convergence in cyber law refers to the intersection and integration of various legal disciplines that deal with the challenges posed by rapidly evolving technologies and their impact on society, commerce, and governance. It signifies the merging or convergence of traditional legal frameworks with laws governing digital technologies, communication, and information systems.

In essence, the Law of Convergence signifies the necessity for legal systems to adapt and evolve, considering the convergence of technological, social, economic, and legal aspects in the digital era. It seeks to establish a cohesive legal framework that effectively regulates and governs the complexities arising from the integration of technology into various facets of modern life.

The following are main field of evolution

Protection of Intellectual Property: Laws governing copyrights, trademarks, patents, and trade secrets in the digital environment are part of the Law of Convergence. They aim to protect creators' rights and encourage innovation while considering the challenges posed by digital reproduction and dissemination.

Global Dimension: Due to the borderless nature of the internet and digital technologies, the Law of Convergence emphasizes international cooperation, harmonization of laws, and global governance frameworks to address cross-border legal issues related to cyberspace.

***************** END OF MODULE 3 *****************

MODULE IV

Cybercrimes and cyber ethics: cyber space, cyber crimes-nature and scope of cyber crimes**,** types and categories of cybercrimes, penalty for cybercrimes under IT Act, digital foot prints, cyber forensics, Cyber ethics- concerns and responsibilities.

Cyber Space

- Cyberspace is a virtual network of computers that facilitates communication across the world.
- It's a digital world that allows people to access information and communicate over computer networks without physically moving.
- The best way to define Cyberspace is the virtual and dynamic space created by the machine clones.
- According to the Cyberspace definition, it is a web consisting of consumer computers, electronics and communication networks by which the consumer is connected to the world.
- Cyberspace mainly refers to the computer which is a virtual network and is a medium electronically designed to help online communications to occur.
- This facilitates easy and accessible communications to occur across the world.
- The whole Cyberspace is composed of large computer networks which have many sub-networks. These follow the TCP or IP protocol.
- Cyberspace is that space in which users share information, interact with each other; engage in discussions or social media platforms, and many other activities.

Cyber Crimes

Cybercrime refers to criminal activities carried out using digital technology or the internet. These offenses involve the use of computers, networks, or electronic devices to commit illegal acts, often targeting individuals, organizations, or governments.

Nature and Scope of Cyber Crimes

- The nature and scope of cybercrime have grown immensely with the evolution of technology and the pervasive presence of the internet.
- Cybercrime refers to criminal activities that are carried out using computers or over the internet. Its nature is diverse and constantly evolving, encompassing various illegal activities facilitated by technology.
- Cybercrime is Transnational in nature. These crimes are committed without being physically present at the crime location. These crimes are committed in the impalpable world of computer networks.
- To commit such crimes the only thing a person needs is a computer which is connected with the internet.
- With the advent of lightning fast internet, the time needed for committing the cybercrime is decreasing.
- The cyberspace, being a boundaryless world has become a playground of the perpetrators where they commit crimes and remain conspicuously absent from the site of crime.
- It is an Open challenge to the law which derives its lifeblood from physical proofs and evidence.
- In crimes relating to cyber space there is nothing sort of physical footprints, tangible traces or objects to track cyber criminals down.
- Cybercrimes possess huge amount complications when it comes to investigation.

Scope of Cyber Crimes

- Cyber Crime is when an individual intentionally uses information technology to produce destructive and harmful effects on the tangible and/or intangible property of others.
- It has no national boundaries and is usually a term for criminal activities involving a computer or a network as a tool or a target.

Cybercrime can be basically categorized into three parts:

1. Cyber Crimes against persons
2. Cyber Crimes against property
3. Cyber Crimes against government.

Types of Cyber Crime

1. **Hacking:** Unauthorized access into computer systems, networks, or devices to steal data, disrupt operations, or cause damage.
2. **Malware Attacks:** Spreading malicious software (viruses, ransomware, spyware) to compromise systems, steal information, or extort money.
3. **Phishing and Social Engineering:** Deceptive techniques to trick individuals into revealing sensitive information such as passwords, credit card details, or personal data.
4. **Identity Theft:** Stealing personal information to impersonate someone for financial gain, access to services, or commit fraudulent activities.
5. **Online Fraud:** Various fraudulent schemes conducted online, including investment scams, lottery scams, and fake websites to deceive victims for monetary gain.
6. **Cyberbullying:** Harassment, intimidation, or defamation using digital platforms to harm or harass individuals.
7. **Distributed Denial of Service (DDoS) Attacks:** Overloading servers or networks with excessive traffic to disrupt services or websites, rendering them inaccessible to legitimate users.
8. **Child Exploitation:** Online exploitation of children for pornography, grooming, or trafficking purposes.
9. **Data Breaches:** Unauthorized access to and theft of sensitive information from databases or systems, leading to the exposure of personal or confidential data.

Penalty for cybercrimes under IT Act

The following table shows the offence and penalties against all the mentioned sections of the I.T. Act −

Section	Offence	Punishment
65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs 2 lakhs
66	Computer Related Offences	Imprisonment up to 3 years or fine up to Rs 5 lakhs
66-A	Sending offensive messages through Communication service, etc...	Imprisonment up to 3 years and fine
66-B	Dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years and/or fine up to Rs. 1 lakh
66-C	Identity Theft	Imprisonment of either description up to 3 years and/or fine up to Rs. 1 lakh
66-D	Cheating by Personation by using computer resource	Imprisonment of either description up to 3 years and /or fine up to Rs. 1 lakh
66-E	Violation of Privacy	Imprisonment up to 3 years and /or fine up to Rs. 2 lakh
66-F	Cyber Terrorism	Imprisonment extend to imprisonment for Life
67	Publishing or transmitting obscene material in electronic form	On first Conviction, imprisonment up to 3 years and/or fine up to Rs. 5 lakh On Subsequent Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh
67-A	Publishing or transmitting of material containing sexually explicit act, etc... in	On first Conviction imprisonment up to 5 years and/or fine up to Rs. 10

	electronic form	lakh On Subsequent Conviction imprisonment up to 7 years and/or fine up to Rs. 10 lakh
67-B	Publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form	On first Conviction imprisonment of either description up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment of either description up to 7 years and/or fine up to Rs. 10 lakh
67-C	Intermediary intentionally or knowingly contravening the directions about Preservation and retention of information	Imprisonment up to 3 years and fine
68	Failure to comply with the directions given by Controller	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh
69	Failure to assist the agency referred to in sub section (3) in regard interception or monitoring or decryption of any information through any computer resource	Imprisonment up to 7 years and fine
69-A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource	Imprisonment up to 7 years and fine
69-B	Intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) in regard monitor and collect traffic data or information through any computer resource for cybersecurity	Imprisonment up to 3 years and fine
70	Any person who secures access or attempts	Imprisonment of either description up

	to secure access to the protected system in contravention of provision of Sec. 70	to 10 years and fine
70-B	Indian Computer Emergency Response Team to serve as national agency for incident response. Any service provider, intermediaries, data centres, etc., who fails to prove the information called for or comply with the direction issued by the ICERT.	Imprisonment up to 1 year and/or fine up to Rs. 1 lakh
71	Misrepresentation to the Controller to the Certifying Authority	Imprisonment up to 2 years and/ or fine up to Rs. 1 lakh.
72	Breach of Confidentiality and privacy	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh.
72-A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years and/or fine up to Rs. 5 lakh.
73	Publishing electronic Signature Certificate false in certain particulars	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh
74	Publication for fraudulent purpose	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh

Digital Footprint

- Anyone who uses and browses the Internet has a digital footprint.
- A digital footprint is commonly based on how an individual contributes data to the internet through websites and other sources of medium.
- Any kind of online activity like sending emails, submitting your personal information to websites, social media interactions leaves a digital footprint on a device.
- All the data which is accessed is being stored recorded and even tracked. In other words, your digital identity can be easily discredited and is at risk.

Types of Digital Footprints :

Digital Footprint usually falls into two categories, based on how the information is acquired:-

1.Active Digital footprint –

- An “Active Digital Footprint” is formed when your data should be submitted for accessing an internet service deliberately.
- For example, to send an email where the data is exchanged in either way.
- To submit an online examination application form, to access any e-governance services. In all such cases, an active digital footprint is formed which is unavoidable.
- This data resides in the data servers for years or more.

2.Passive Digital footprint –

- If you are accidentally accessing data or accessing a website directly or indirectly then a “Passive Digital Footprint” can be observed.
- Whenever we are browsing a website, the IP address of your device is recorded by the respective web-server.
- These details are enough to track your precise Geo-location data and ISP and retrieve much more information.
- A simple Google search, online shopping activities, search engine histories or even just visiting a website leaves a passive digital footprint beside.
- Irrespective of the IP address or the device you are accessing from, a passive digital footprint cannot be avoided.

Cyber Forensics

Cyber forensics is a process of extracting data as proof for a crime (that involves electronic devices) while following proper investigation rules to nab the culprit by presenting the evidence to the court. Cyber forensics is also known as computer forensics. The main aim of cyber forensics is to maintain the thread of evidence and documentation to find out who did the crime digitally. Cyber forensics can do the following:

- It can recover deleted files, chat logs, emails, etc
- It can also get deleted SMS, Phone calls.
- It can get recorded audio of phone conversations.
- It can determine which user used which system and for how much time.
- It can identify which user ran which program.

The Process Involved in Cyber Forensics

1. Obtaining a digital copy of the system that is being or is required to be inspected.
2. Authenticating and verifying the reproduction.
3. Recovering deleted files (using Autopsy Tool).
4. Using keywords to find the information you need.
5. Establishing a technical report.

Types of computer forensics

There are multiple types of computer forensics depending on the field in which digital investigation is needed. The fields are:

- **Network forensics:** This involves monitoring and analyzing the network traffic to and from the criminal’s network. The tools used here are network intrusion detection systems and other automated tools.
- **Email forensics:** In this type of forensics, the experts check the email of the criminal and recover deleted email threads to extract out crucial information related to the case.

- **Malware forensics:** This branch of forensics involves hacking related crimes. Here, the forensics expert examines the malware, trojans to identify the hacker involved behind this.
- **Memory forensics:** This branch of forensics deals with collecting data from the memory(like cache, RAM, etc.) in raw and then retrieve information from that data.
- **Mobile Phone forensics:** This branch of forensics generally deals with mobile phones. They examine and analyze data from the mobile phone.
- **Database forensics:** This branch of forensics examines and analyzes the data from databases and their related metadata.
- **Disk forensics:** This branch of forensics extracts data from storage media by searching modified, active, or deleted files.

Cyberethics

- Cyberethics is a branch of computer technology behavior that defines the best practices that must be adopted by a user when he uses the computer system.
- It refers to the basic ethics and etiquette that must be followed while using a computer system.
- Ethics, in general, refers to propagating good behavior, similarly by cyber ethics we refer to propagating good behavior online that is not harsh or rude.
- Cyberethics governs rules that individuals must be polite and responsible when they use the internet.
- Cyberethics aim to protect the moral, financial, social behavior of individuals.
- Cyberethics engages the users to use the internet safely and use technology responsibly and sensibly.
- Cyberethics empathizes the behavior that must be adopted while using cyber technology.

Cyber Ethics Concerns the following

1.Cyber Bullying:

- Cyberbullying is a form of bullying carried out via internet technology such as social media where individuals are mocked on their physical appearance, lifestyle, preferences, etc.
- The teenage generation or say youngsters are the major victims of this form of cyber ethic breach.
- Cyberbullying affects the emotional ethics of individuals and can cause mental disturbance to individuals.

2.Hacking:

- Stealing a user's personal or organizational information without authorized permission is not considered a good practice.
- It is one of the riskiest cyber breaches to data leak. Data leak includes passing of sensitive information such as passwords, bank details of the user to a third-party user who is not authorized to access the information.

3.Copywriting:

- Claiming of another individual as one's own is another type of cyber ethic breach that must be eradicated.
- Never engage in copywriting another person's content or document and claim as it is your own.
- It leads to a serious problem called plagiarism, which is a punishable offense and considered a legal crime.
- It is always advisable to follow general cyberethics, while using the internet or say any kind of technology.
- A proper code of conduct must be followed while using cyber technology.
- Cyberethics if not used wisely can lead to serious situations.
- Social and legal laws are defined to use cyber technology wisely. In extreme cases, legal action can be taken if there is a violation of cyber ethics.

Responsibilities of Cyber Ethics

Respect for Privacy: Safeguarding the privacy of oneself and others by not intruding into personal information, avoiding unauthorized access to private data, and respecting boundaries in digital communications.

Security Practices: Acting responsibly to ensure the security of digital systems, including using strong passwords, keeping software updated, and being cautious with sharing sensitive information.

Responsible Online Behavior: Behaving ethically in online interactions, which includes avoiding cyberbullying, harassment, spreading false information, or engaging in illegal activities.

Respect for Intellectual Property: Respecting copyrights, trademarks, and intellectual property rights by not plagiarizing content, respecting licensing agreements, and giving credit where it's due.

Ethical Use of Technology: Using technology in a manner that benefits society while considering the potential ethical implications of its use, such as in artificial intelligence, surveillance, or data collection.

Compliance with Laws and Regulations: Abiding by legal frameworks and regulations related to cyber activities, including data protection laws, cybersecurity standards, and internet regulations.

***************** END OF MODULE 4 *****************