Computer Security and Privacy

By Kajol Ramtel

Computer Security and Controls

- Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your computer system.
- Computer security refers to measures and controls that ensure the confidentiality, integrity and availability of the information processed and stored by a computer.

Computer Security

- **Confidentiality** is ensuring that information is available only to the intended audience
- **Integrity** is protecting information from being modified by unauthorized parties
- **Availability** is making data and information available to the users when they need them.

Unauthorized Access

- Unauthorized access refers to the act of gaining entry to a computer system, network, or data without explicit permission from the owner or administrator. It is considered a breach of security and can lead to unauthorized actions, such as stealing sensitive information, disrupting services, or causing damage to the system. Unauthorized access can occur through various means, including exploiting software vulnerabilities, using stolen credentials, or bypassing security measures.

Authorized Use

- Authorized use refers to the legitimate and permitted access to a computer system, network, or data by authorized users who have been granted appropriate permissions or privileges. Authorized users are typically employees, contractors, or individuals who have been granted access rights based on their roles and responsibilities within an organization. Authorized use involves adhering to security policies, following established procedures, and using resources in accordance with acceptable use guidelines.

Protecting against unauthorized access and unauthorized use

- **Strong Password Policy:-**
  - Enforce best practices for user passwords—force users to select long passwords including letters, numbers and special characters, and change passwords frequently. Educate users to avoid using terms that can be guessed in a brute force attack, inform them about routine password updating, and to tell them to avoid sharing passwords across systems.
- **Two Factor authentication and multi- factor authentication:-**
  - Credentials based on user names, passwords, answers to security questions, etc. are known more generally as knowledge-based security factors. Knowledge-based factors are an important authentication method, but they are inherently weak and easy to compromise.
  - One of the best ways to prevent unauthorized access in your organization is to supplement knowledge-based factors with additional authentication methods:

Protecting against unauthorized access and unauthorized use

- Possession factors — authentication via objects possessed by the user. For example, a mobile phone, a security token or a physical card.
- Inherence factors — authentication via something the user is or has. This includes biometric authentication using fingerprints, iris scans or voice recognition.

- **Physical Security Practices:-**
  - Train users to always lock devices when walking away from their desks, and to avoid writing down passwords or leaving sensitive documents in the open. Have a clear policy about locking office doors and ensure only authorized parties can enter sensitive areas of your physical facility.

Protecting against unauthorized access and unauthorized use

- **Monitoring User Activity:-**
  - It is crucial to monitor what is happening with user accounts, to detect anomalous activity such as multiple login attempts, login at unusual hours, or login by users to systems or data they don't usually access. There are several strategies for monitoring users and accounts:
    - Log analysis — security analysts can gain visibility into logs of sensitive enterprise systems and uncover suspicious activity
    - Rule-based alerts — security tools can alert security staff to suspicious activity patterns, such as multiple login attempts or incorrect login to sensitive systems
    - Behavioral analytics — User and Event Behavioral Analytics (UEBA) monitors users and systems, establishes a baseline of normal activity, and detects any behavior that represents an anomaly and may be malicious.

Protecting against unauthorized access and unauthorized use

- **Implement least privilege and zero-trust**
  - Instead of giving all users unlimited access to your systems, minimize their privileges. Take a "least privilege" approach where you only grant permission based on a user's needs. This way, if someone gains access to your network with one user's credentials, they have a limited reach and can't do as much damage.
  - Whitelisting is tempting, but because nothing is infallible, it's not always a safe option. That's why organizations should implement a zero-trust approach. Assume that everything attempting to access your network is a potential attack.

Computer Sabotage

- Computer sabotage refers to the deliberate act of causing harm, disruption, or damage to computer systems, networks, or data. It encompasses various malicious activities aimed at compromising the integrity, availability, or confidentiality of digital assets. Computer sabotage can be carried out by individuals, groups, or organizations with malicious intent, and it may have various motives.

Computer Crime

- Computer crime is an act performed by a knowledgeable computer user, sometimes called a "hacker," who illegally browses or steals a company's or individual's private information. Sometimes, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.
- Criminal activities that are carried out using computers, networks, or digital devices as tools or targets.

Questions

- Explain some of the protection against computer sabotage.
- List and explain different computer crimes in today's date.

Software piracy

Software piracy refers to the unauthorized use, reproduction, distribution, or sale of software protected by copyright laws.

It involves obtaining software without proper authorization or licensing from the copyright holder, often through illegal means such as downloading pirated copies from the internet, sharing unauthorized copies with others.

Types of Software piracy

1. Softlifting:

The most common type of piracy, softlifting, (also called softloading), means sharing a program with someone who is not authorized by the license agreement to use it. A common form of softlifting involves purchasing a single licensed copy of software and then loading the software onto several computers, in violation of licensing terms. On college campuses, it is rare to find a software program that has not been softloaded. People regularly lend programs to their roommates and friends, either not realizing it's wrong, or not thinking that it's a big deal. Softlifting is common in both businesses and homes.

2. End user piracy:

This occurs when individuals or businesses use unauthorized copies of software without the appropriate licenses. It includes activities such as installing software on multiple computers with a single license, using cracked or keygen versions of software, or sharing licensed software with others who are not entitled to use it.

Types of Software piracy

3. Counterfeiting

Counterfeiting means producing fake copies of a software, making it look authentic. This involves providing the box, CDs, and manuals, all designed to look as much like the original product as possible. Microsoft products are the ones most commonly counterfeited, because of their widespread use. Counterfeit software is often sold at a fraction of the legitimate price, making it an attractive option for those seeking cheaper alternatives.

4. Internet Piracy

Internet piracy involves the unauthorized distribution of software over the internet. This includes websites, forums, or online platforms that offer illegal downloads of software, serial keys, or activation codes. Peer-to-peer file-sharing networks and torrent sites are common avenues for internet piracy.

Types of Software piracy

5. Hard-disk loading

Hard-disk loading occurs when computer manufacturers or retailers install unauthorized copies of software on computers before selling them to customers. This practice often involves pre-installing pirated software on computers to make them more attractive to buyers, but it violates software licensing agreements and copyright laws.

Anti piracy

Anti-piracy refers to measures, strategies, and initiatives aimed at preventing, combating, and reducing software piracy and unauthorized use of intellectual property rights.

These efforts involve various stakeholders, including governments, law enforcement agencies, industry associations, software developers, and content creators.

Computer Virus

A computer virus is a type of malware that, when executed, replicates itself by modifying other computer programs and inserting its own code into those programs.

Computer virus will have adverse effects on the device it resides.

It can be discovered through the common signs of performance loss including:-

- A computer running slower than usual.
- Unwanted pop-ups.
- Unexpected closing and self execution of programs.
- System crashes and computer closing down itself.
- Changes to the system’s homepage. etc

Characteristics of Computer Virus

Self-Replication: A computer virus can replicate itself and spread to other files or systems through various means, such as email attachments, infected removable media, or network connections.

Destructive Payload: Viruses may have a payload designed to cause harm to the infected system, such as corrupting files, deleting data, or disrupting system operations.

Stealth Mechanisms: Some viruses employ stealth techniques to evade detection by antivirus software or system administrators. This may include polymorphic code, encryption, or rootkit capabilities.

Propagation Methods: Viruses can spread through different propagation methods, including email spam campaigns, drive-by downloads, social engineering tactics, or exploiting software vulnerabilities.

Activation Triggers: Viruses may be programmed to activate under specific conditions or triggers, such as a particular date, system event, or user action.

Types of Computer Virus

1. File Infector Viruses: These viruses attach themselves to executable files and infect them. When an infected file is executed, the virus code is activated and may spread to other files on the system.

2. Boot Sector Viruses: Boot sector viruses infect the master boot record (MBR) or boot sector of storage devices, such as hard drives or USB drives. They are activated when the infected device is booted, allowing the virus to control the boot process and spread to other devices.

3. Macro Viruses: Macro viruses infect documents or templates that support macros, such as Microsoft Word or Excel files. They exploit the macro scripting capabilities to execute malicious code when the infected document is opened.

Note : A macro refers to a sequence of instructions or commands that are grouped together as a single command to perform a specific task or automate a series of tasks.

Types of Computer Virus

4.Polymorphic Viruses: Polymorphic viruses use encryption or obfuscation techniques (making hard to understand) to change their appearance and evade detection by antivirus software. They generate new variants of themselves with each infection, making it challenging to detect and remove them.

5.Resident Viruses: Resident viruses embed themselves in system memory and can execute malicious code whenever the infected system is running. They may intercept system calls or manipulate system functions to avoid detection.

Worms

A worm is a type of malware that is designed to replicate itself and spread across computer networks, typically without requiring user interaction.

Unlike viruses, worms do not need to attach themselves to existing files or programs to propagate, and they can spread independently by exploiting vulnerabilities in network protocols or software applications.

Spyware

Spyware is a type of malicious software (malware) designed to secretly collect sensitive information from a user's computer or device without their knowledge or consent.

It often operates covertly in the background, monitoring user activity, capturing keystrokes, logging browsing habits, and harvesting personal or confidential data.

Questions

- Explain about the effects of software piracy. Explain some approaches to anti piracy.
- Explain the differences between worms and viruses.
- Explain some of the protection against computer sabotage.
- List and explain different computer crimes in today's date.

Ethical Issues In Computer

Ethical issues in computer science and technology are numerous and diverse, encompassing various aspects of privacy, security, accessibility, fairness, and more.

Some common ethical issues in computer science include:

- **Cyber crime**
- **Software Piracy**
- **Unauthorized Access**
- **Hacking**
- **Use of computers to commit fraud**
- **Sabotage in the form of viruses**
- **Making false claims using computers**

Cyber Law

Cyber law, also known as cybercrime law or internet law, encompasses the legal frameworks and regulations governing online activities, digital transactions, and cybersecurity.

It addresses various legal issues arising in cyberspace, including but not limited to the following:

Data Protection and Privacy: Cyber law includes regulations concerning the collection, storage, processing, and sharing of personal data online. It aims to protect individuals' privacy rights and ensure that organizations handle personal information responsibly.

Cybersecurity: Cyber law encompasses regulations and laws aimed at safeguarding computer systems, networks, and data from unauthorized access, cyber attacks, and other security threats. It may include provisions for mandatory security measures, incident reporting requirements, and penalties for cybercriminal activities.

Cyber Law

Intellectual Property Rights: Cyber law governs the protection of intellectual property rights in the digital realm, including copyright, trademarks, patents, and trade secrets. It addresses issues such as online piracy, digital rights management, and infringement of intellectual property online.

Electronic Transactions: Cyber law provides legal recognition and validity to electronic transactions, contracts, and signatures conducted over the internet. It establishes rules and standards for electronic commerce, electronic contracts, and electronic signatures to facilitate online transactions.

Cybercrime: Cyber law defines and prohibits various forms of cybercrime, including hacking, phishing, identity theft, online fraud, cyber stalking, and cyberbullying. It outlines legal measures and penalties for individuals and organizations involved in illegal online activities.

Freedom of Expression and Speech: Cyber law addresses issues related to freedom of expression and speech online, including regulations governing online content, hate speech, defamation, and censorship. It balances the right to free speech with the need to protect individuals from harm and maintain a safe online environment.

Cyber Law

Jurisdiction and Enforcement: Cyber law deals with jurisdictional issues and enforcement mechanisms concerning online crimes and disputes. It determines which laws apply to cross-border cybercrimes and establishes procedures for international cooperation and extradition in cybercrime investigations.

Regulatory Compliance: Cyber law imposes obligations and responsibilities on businesses, organizations, and individuals to comply with legal requirements related to cybersecurity, data protection, and online conduct. It may require entities to implement security measures, data protection policies, and incident response plans to ensure regulatory compliance.

Network Security

Network security refers to the practice of safeguarding computer networks from unauthorized access, misuse, modification, or disruption. It involves implementing measures and protocols to protect the confidentiality, integrity, and availability of data and resources within a network. Network security aims to prevent unauthorized users or attackers from gaining access to sensitive information, exploiting vulnerabilities, or causing damage to network infrastructure and systems.

Key components of network security include:

Access Control: Access control mechanisms regulate and manage user access to network resources based on their identity, role, and permissions. This includes authentication (verifying the identity of users), authorization (granting appropriate access privileges), and accounting (tracking user activities).

Firewalls: Firewalls are security devices or software applications that monitor and control incoming and outgoing network traffic based on predefined security rules. They act as barriers between trusted internal networks and untrusted external networks (such as the internet), filtering traffic to block potential threats and unauthorized access attempts.

Network Security

Intrusion Detection and Prevention Systems (IDPS): IDPS are security systems that monitor network traffic for signs of suspicious or malicious activity. They analyze network packets and log data to detect and respond to security threats, such as intrusion attempts, malware infections, and denial-of-service attacks.

Encryption: Encryption involves encoding data into an unreadable format using cryptographic algorithms, making it unintelligible to unauthorized users or attackers. Encrypted communication channels, such as Virtual Private Networks (VPNs) and Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocols, protect data privacy and confidentiality during transmission over insecure networks.

Vulnerability Management: Vulnerability management processes identify, assess, and mitigate security vulnerabilities within network infrastructure, devices, and applications. This includes regularly scanning networks for known vulnerabilities, patching or updating software to address security flaws, and implementing security best practices to reduce the risk of exploitation.

Network Security

Security Monitoring and Logging: Security monitoring tools and logging mechanisms collect and analyze network activity logs, event data, and security alerts to detect and investigate security incidents in real-time. This includes monitoring network traffic, system logs, and user activities for indicators of compromise or abnormal.

Firewall

A firewall is a network security device or software application that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Its primary function is to establish a barrier between a trusted internal network and untrusted external networks, such as the internet, to prevent unauthorized access, data breaches, and cyberattacks.

Types of firewall:-

- Hardware firewall
- Software firewall

Firewall

Hardware firewall:

A hardware firewall is a physical device that is typically installed at the perimeter of a network, such as between the internal network and the internet connection.

It operates at the network level (Layer 3 or above) of the OSI model and filters traffic based on predefined rules and policies.

Hardware firewalls are standalone appliances or devices specifically designed for network security, such as routers, switches, or dedicated firewall appliances.

They provide centralized network security management and offer high-performance filtering capabilities, making them suitable for protecting entire networks or large-scale deployments.

Hardware firewalls offer protection for all devices connected to the network, including computers, servers, and IoT devices.

Firewall

Software firewall:

A software firewall is a program or application installed on individual computers or devices to control inbound and outbound network traffic.

It operates at the host level (Layer 7) of the OSI model and monitors traffic based on application-specific rules and policies.

Software firewalls are installed directly on the operating system of a device and run as background processes or services, providing protection at the endpoint level.

They offer flexibility and customization options, allowing users to define specific rules for each application or service running on the device.

Software firewalls are commonly included as built-in security features in modern operating systems, such as Windows Firewall for Windows-based systems and iptables/firewalld for Linux-based systems.

They are particularly useful for protecting individual devices, such as laptops, desktops, and mobile devices, especially when connected to untrusted networks or public Wi-Fi hotspots.

Data and Message Security

Data and message security refer to the protection of data and messages from unauthorized access, interception, tampering, and theft. It involves implementing various security measures to ensure the confidentiality, integrity, and availability of sensitive information.

Encryption

Encryption is the process of converting plaintext (readable data) into ciphertext (unreadable data) using an algorithm and a cryptographic key. The ciphertext appears as random and meaningless characters, making it unintelligible to anyone without the corresponding decryption key. Encryption can be applied to various forms of data, including text, files, emails, and network traffic.

There are two primary types of encryption:

Symmetric Encryption: In symmetric encryption, the same key is used for both encryption and decryption. The sender and receiver must share the secret key securely before communication begins. Examples of symmetric encryption algorithms include AES (Advanced Encryption Standard) and DES (Data Encryption Standard).

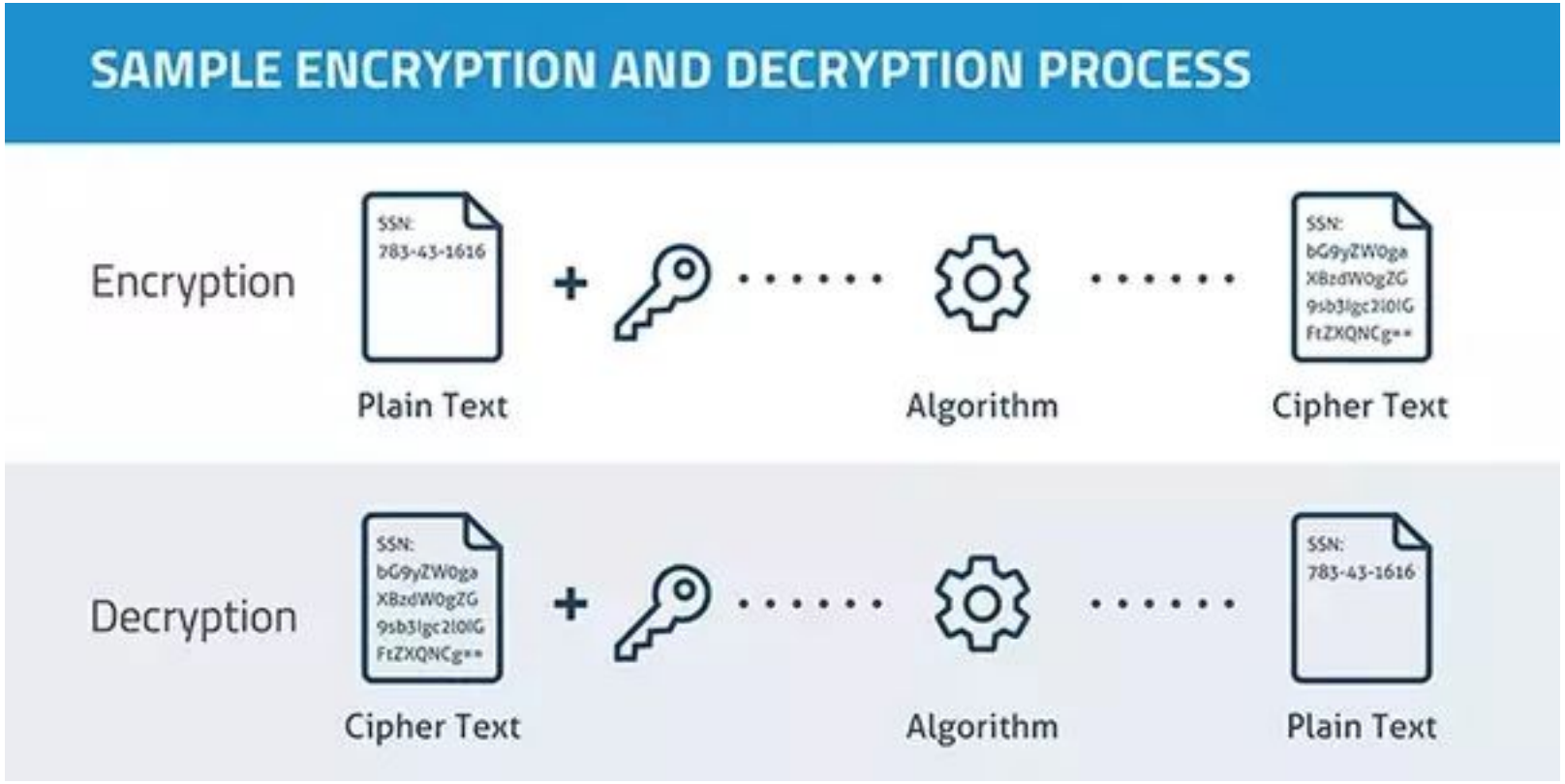
Asymmetric Encryption (Public-key Encryption): Asymmetric encryption uses a pair of keys - a public key for encryption and a private key for decryption. The public key is widely distributed and used by anyone to encrypt messages, while the private key is kept secret and used by the intended recipient to decrypt the messages. RSA (Rivest-Shamir-Adleman) is a common asymmetric encryption algorithm.

Decryption

Decryption is the process of converting cipher text back into plaintext using the appropriate decryption key. The decryption key must match the encryption key used to encrypt the data. In symmetric encryption, the same key is used for both encryption and decryption, while in asymmetric encryption, the private key is used for decryption.

The decryption process reverses the encryption process, applying the decryption algorithm to the cipher text with the correct key to recover the original plaintext. Once decrypted, the data becomes readable and usable again.

Encryption and Decryption process



Question

Explain some ethical issues in computer.

Explain the Encryption and Decryption process.