IT 231
Foundation of Information Technology

Unit 9

Computer Security and Privacy

Computer Security

Protection of computer systems and information from harm, theft and unauthorized use.

Process of preventing and detecting unauthorized use of computer system.

Computer Security (Data and message security) can be achieved by three phenomenon: ***Confidentiality, Integrity and Availability.***

Three Pillars of Information security

Confidentiality : Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts.

Integrity : involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle.

Availability : Information should be consistently and readily accessible for authorized parties.

Security Control Mechanism

Security controls are parameters implemented to protect various forms of data and infrastructure important to an organization.

There are several types of security control that can be implemented to protect hardware, software, networks and data.

Any type of safeguard or countermeasure used to avoid, detect, counteract, or minimize security risks to physical property, information, computer system or other assets is considered a security control

Security Control Mechanism

Physical Security Controls : locks, guards, access control cards, biometric access, surveillance camera, IDS

Digital Security Controls : Password, 2FA,firewalls, Antivirus, Authorization and privileges mechanism

Cybersecurity Controls : Threat Protection mechanism, Firewall Security,

Unauthorized Access and Unauthorized Use

Unauthorized use of computer or network by connecting to it and then logging in as a legitimate user.

Unauthorized use refers to the illegal use of computer or computer's data without having privileged to it.

Authentication and Authorization can be use to protect against unauthorized access and unauthorized use.

Authentication Techniques

(Protecting against unauthorized Access)

- **Password Based Authentication**
- **Multi-Factor Authentication**
- **Certificate Based Authentication**
- **Biometric Authentication**
  - **Facial Recognition**
  - **Fingerprint Scanners**
  - **Speaker Recognition**
  - **Retina Scanners (Eye Scanning)**

Authorization

- Authorization is a security mechanism to determine access levels or user/client privileges related to system resources including files, services, computer programs, data and application features.
- This is the process of granting or denying access to a network resource which allows the user access to various resources based on the user's identity.

Computer Sabotage and protection

The input, alteration, erasure or suppression of computer data or computer programs, or interference with computer systems, with the intent to hinder the functioning of a computer or a telecommunication system.

Computer sabotage involves deliberate attacks intended to disable computers or networks for the purpose of disrupting commerce, education and recreation for personal gain, committing spying, or facilitating criminal conspiracies, such as drug and human trafficking.

Protection

Protection from computer sabotage means the taking proactive measures to guard hardware and software.

- Keep OS and Software up-to date.
- Use of Anti-Virus and firewall and keep it up-to date
- Use strong password and authentication mechanism.
- Beware of spam mail and attachment.
- Do not surfing around the untrusted web links.
- Take action about suspicious request. Etc.

Computer Crime

It is an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individual's private information.

In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.

Type of Computer Crime

- Child Pornography
- Cyber Terrorism
- Cyberbully or Cyber Stalking
- DoS Attack
- Fraud
- Identity Theft
- Intellectual Property Theft
- Phishing
- Spamming
- Creating Malware
- Spoofing
- Unauthorized Access

Software Piracy

- **Soft lifting:** Soft lifting is the act of purchasing a single copy of software and then downloading it onto more than one computer, despite agreement terms stating the software must only be downloaded once.
- **Software counterfeiting :** producing fake copies of a software, making it look authentic.
- **OEM unbundling (original equipment manufacturer):** (OEM unbundling) involves dissembling the major components of the bundled software that usually accompanies OEM hardware.

Software Piracy

- **Hard disk loading :** System builders purchase a legal copy of software, but then reproduce, copy or install the software onto computer hard disks. Then, a computer is sold with the hard disk containing the pre-installed software.
- **Renting :** Renting involves someone renting out a copy of software for temporary use, without the permission of the copyright holder.

Anti Piracy

- **Piracy:** the (illegal) mass sharing or distribution of copyrighted material such as music, films etc.
- **Anti piracy Law:** a law which makes the copying and distribution of copyrighted material (music, films etc.) illegal

Computer Virus

- type of malicious software, or malware, that spreads between computers and causes damage to data and software.
- Computer viruses aim to disrupt systems, cause major operational issues, and result in data loss and leakage.
- Viruses replicate by creating their own files on an infected system, attaching themselves to a legitimate program, infecting a computer's boot process or infecting user documents.

Computer Virus

- virus can be spread when a user opens an email attachment, runs an executable file, visits an infected website or views an infected website advertisement
- Once a virus has infected the host, it can infect other system software or resources, modify or disable core functions or applications, and copy, delete or encrypt data.

Worms

Worms are self-replicate from one computer to another without human activation after breaching a system. Typically, a worm spreads across a network through your Internet or LAN (Local Area Network) connection.

It consumes system resources such as memory and bandwidth and made the system slow in speed to such an extent that it stops responding.

Worms

- Hampering computer performance by slowing down it
- Automatic opening and running of programs
- Sending of emails without your knowledge
- Affected the performance of web browser
- Error messages concerning to system and operating system

Trojan Horse

- A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.
- Trojan Horse does not replicate itself like virus and worms.
- It is a hidden piece of code which steal the important information of user.

Common Trojan

- **Backdoor Trojan**
- **Distributed Denial of Service (DDoS) attack Trojan**
- **Rootkit Trojan**
- **Downloader Trojan**

Spyware

A type of malware that infects your PC or mobile device and gathers information about you, including the sites you visit, the things you download, your usernames and passwords, payment information, and the emails you send and receive.

Usually , Spy doesn't kill the system, it is running in background without realizing it and listen to the system users (key logging, email attachment, password etc.)

Ransomware

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.

More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.

Ethical Issues in Computer

Ethics deals with placing a "value" on acts according to whether they are "good" or "bad".

- Set of moral principles that regulate the use of computers.
- Ethical issues are guidelines for the morally acceptable use of computers in our society.
- **Four Primary Computer Ethics Issues**

i. **Privacy**
ii. **Accuracy**
iii. **Property**
iv. **Access**

The Ten Commandments

1) Thou shalt not use a computer to harm other people:
2) Thou shalt not interfere with other people's computer work:
3) Thou shalt not snoop around in other people's files:
4) Thou shalt not use a computer to steal:
5) Thou shalt not use a computer to bear false witness:

The Ten Commandments

6) Thou shalt not use or copy software for which you have not paid:
7) Thou shalt not use other people's computer resources without authorization:
8) Thou shalt not appropriate other people's intellectual output:
9) Thou shalt think about the social consequences of the program you write:
10) Thou shalt use a computer in ways that show consideration and respect:

Network Security

- Network security is the protection of the underlying networking infrastructure from unauthorized access, misuse, or theft.
- It involves creating a secure infrastructure for devices, applications, users, and applications to work in a secure manner.

How does network security work?

- Network security combines multiple layers of defenses at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats.

Network security

Firewalls: A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Intrusion prevention systems: An intrusion prevention system (IPS) scans network traffic to actively block attacks. Secure IPS appliances do this by correlating huge amounts of global threat intelligence to not only block malicious activity but also track the progression of suspect files and malware across the network to prevent the spread of outbreaks and reinfection.

Hardware vs Software Firewall

- **A software firewall** is a special type of computer software that runs on a computer/server. Its main purpose is to protect your computer/server from outside attempts to control or gain access and depending on your choice of a software firewall.
- It is physical piece of equipment planned to perform firewall duties. A hardware firewall can be a computer or a dedicated piece of equipment which serve as a firewall.

Data & Message Security

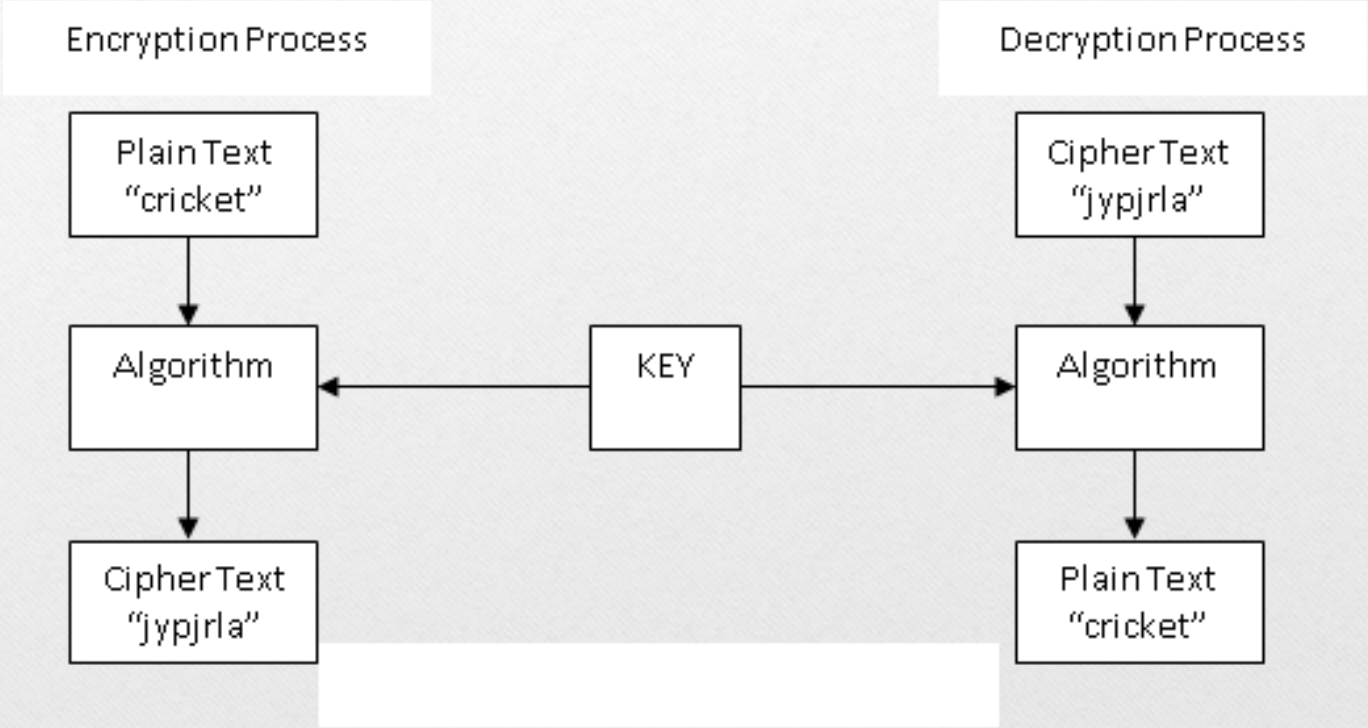
Encryption: It is the process of converting plain text into cipher text.

Encryption is the process by which a readable message is converted to an unreadable form to prevent unauthorized parties from reading it.

Decryption is the process of converting an encrypted message back to its original (readable) format.

The original message is called the **plain text message**. The encrypted message is called the **cipher text message**.

Data & Message Security



End of Chapter 9