Computer Security

Computer security refers to the protection of data and information (stored or being transferred), computer programs, credentials and computer hardware from intended harm, theft, unauthorized access or unintended accident/natural disaster etc.

Two types of computer security: i) Information security (InfoSec) ii) Hardware security

Information Security (InfoSec)

The Information security is protection of print, electronic, or any other form of confidential and sensitive programs, data and information from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.

Major (CIA) principles of Information Security

a) **C**onfidentiality: - Only authorized users can access the programs, data resources and information.

b) **I**ntegrity: - Only authorized users should be able to modify programs and data when needed.

c) **A**vailability: - Data and programs should be available to users when needed.

1.0 Security Threats

Computer security threats can potentially harm computer program, data and information. It could be physical such as someone stealing a computer that contains vital data or could be non-physical such as a cyber-attack.

Possible Security Threats

1.1 Malicious code (Malware)

- A code developed by cyber attackers, designed to cause extensive damage to data and systems or to gain unauthorized access to a network.
- Includes computer viruses, worms, Trojan horses and spyware.
- Perform a variety of different functions such as stealing, encrypting or deleting sensitive data, altering or hijacking (taking control) core computing functions and monitoring users computer activity without their permission.

Types of malware

a) A **virus** can execute itself and spread by infecting other programs or files.

b) A **worm** can self-replicate without a host program and typically spreads without any human interaction.

c) A **Trojan horse** is designed to appear as a legitimate (valid) program in order to gain access to a system. Once activated follows installation then executes their malicious functions.

d) **Spyware** is made to collect data and information on the user's device and observe their activity without their knowledge.

How can we protect a system from infection?

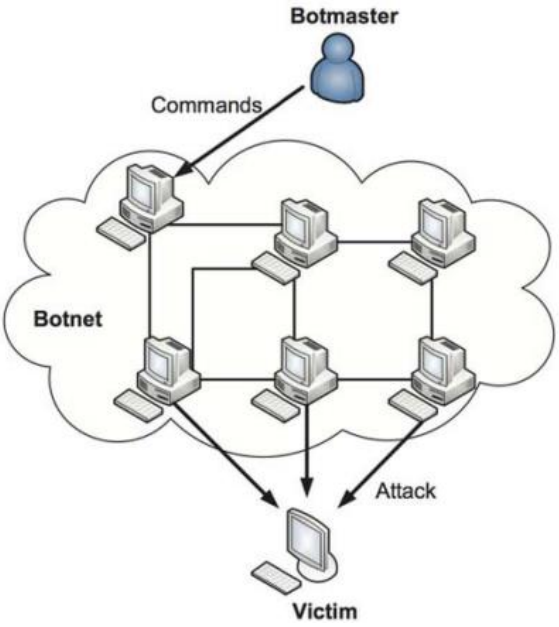
a) Use of firewall and antivirus software provides protection against cyber threats.

b) Do not download or open untrusted email attachments and links as these may carry harmful malware. Check with link scanners for safety before opening it.

c) Regularly back up your data and information into the cloud or to an external hard drive.

1.2. Phishing: Phishing attempts to obtain sensitive information like usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing, SMS or instant messaging.

1.3. Botnet: A botnet is a logical collection of Internet-connected devices such as computers, smartphones or internet of things (IoT) devices whose security has been breached and control is given away to a third party (Bot master). It commands through communication channels formed by standards-based network protocols, such as Hypertext Transfer Protocol (HTTP.



1.4. Rootkit: A rootkit is a malicious code (kit) that hides in system area provides continued Administrator's (root) privileged access to a computer while actively hiding its presence.

1.5. Key logger: Key logger is hardware or software for recording the keys pressed on a keyboard secretly. The person using the keyboard does not know that their actions are being monitored.

1.6. Hacker: A computer hacker is any skilled computer expert who uses his/her technical knowledge to overcome a problem. There are several types of Hacker, including White hats, Black hats and Grey hats hackers.

1.7. Drive-by attack: Drive-by download attacks are a common method of spreading malware. Hackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages. A drive-by download can take advantage of an app, operating system or web browser that contains security flaws due to unsuccessful updates or lack of updates. We need to keep our browsers and operating systems up to date and avoid websites that might contain malicious code.

2.0 Security mechanisms for data, information and software

A mechanism that is designed to detect, prevent, or recover from a security attack.
It includes:

- **Authentication Systems**
- **Firewalls**
- **Cryptography**
- **Antivirus Software**
- **Backup System**

2.1 Authentication System

Authentication is the process of verifying the identity of a person or device. Authentication system makes sure that only authorized user enters the system and access the information.

Types of Authentication

i) **Password** ii) **Biometric**

Password

A password is set of secret characters used to authenticate access to a digital system. It secures the data and programs by protecting from unauthorized access.

Any four criteria for strong password are:

a) Do not keep a password which can be easily guessed such as date of birth, nickname, etc.

b) Do not keep word as password that is currently popular.

c) Keep a password with mixture of alphabet and numbers which is difficult to guess.

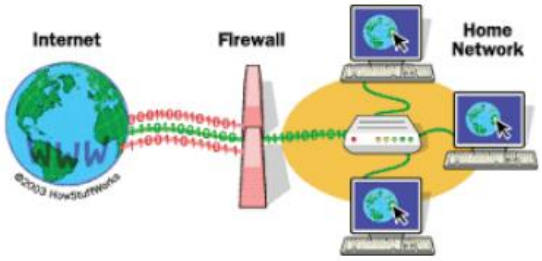
d) Keep changing your password regularly.

Biometric

Biometrics are unique human characteristics that can be used to digitally identify a person and grant access to systems, devices or data. For examples, fingerprints, face detection, retina matching and voice recognition.

2.2 Firewall

Firewall is a network security systems, either hardware or software that monitors and filters all incoming and outgoing network traffic based on security policies.



2.3 Cryptography

Cryptography is a technique of securing communications so that only the sender and intended receiver can understand it and process it.

- The prefix "crypt" means "hidden" and suffix graphy means "writing".
- A message sent over the network is transformed into an unrecognizable encrypted message known as data encryption. At the receiving end, the received message is converted to its original form known as decryption.
- Cryptography is used to secure and protect data during communication.

Features of Cryptography

a) Confidentiality: Information can only be accessed by the person for whom it is intended and no other person except him can access it.

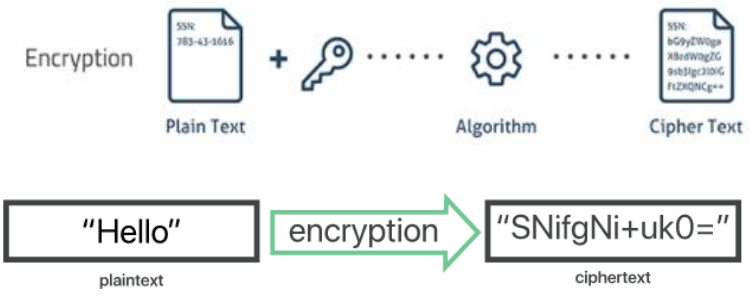
b) Integrity: Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

c) Non-repudiation: The creator/sender of information cannot deny his or her intention to send information at later stage.

d) Authentication: The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Encryption

Encryption is the process of encoding data or information into an unreadable text (Cipher text), especially to prevent unauthorized access. Authorized user can read or use the data or information after decrypting it.



A cryptographic key is a string of characters used within an encryption algorithm for altering data so that it appears random. Like a physical key, it locks (encrypts) data so that only someone with the right key can unlock (decrypt) it.

Decryption

Decryption is the process of decoding encrypted data (cipher text) back to original text. It occurs at the receiver's end. It uses decryption algorithms and a key to transform the cipher text back to original plaintext.

What are the different types of encryption?

The two main kinds of encryption are **symmetric encryption** and **asymmetric encryption**. Asymmetric encryption is also known as public key encryption.

In symmetric encryption, there is only one key, and all communicating parties use the same secret key for both encryption and decryption.

In asymmetric, or public key, encryption, there are two keys: one key is used for encryption, and a different key is used for decryption. The decryption key is kept private (hence the "private key" name), while the encryption key is shared publicly, for anyone to use (hence the "public key" name). Asymmetric encryption is a foundational technology for TLS (often called SSL).

What is an encryption algorithm?

An encryption algorithm is the method used to transform data into cipher text. An algorithm will use the encryption key in order to alter the data in a predictable way, so that even though the encrypted data will appear random, it can be turned back into plaintext by using the decryption key.

What are some common encryption algorithms?

Commonly used symmetric encryption algorithms include: a) AES b) 3-DES 3) SNOW

Commonly used asymmetric encryption algorithms include: a) RSA b) Elliptic curve cryptography

Refer to Home - CryptoTools.net for trying cryptographic key generations.

2.4 Antivirus software

Antivirus software is designed to detect, prevent and remove virus from computer system and ensures virus free environment. Today's antivirus software can protect from browser hijackers, key loggers, rootkits, Trojan horses, worms, adware, spyware, and many more.

E.g. Kaspersky, NAV, MSAV, McAfee, NOD 32, Avast etc.

2.5 Backup system

Backup system is copying data and programs into different storage location or creating a duplicate copy of it in a secured place. Backups can be kept in different storages such as hard disks, compact disc, and external hard drive and on the cloud storage. So, Backups are important methods of data and software security measures against data corruption or loss.

3.0 Hardware Security

Hardware security refers to the protection of computer hardware from intended harm, theft, negligence, unauthorized access or unintended accident/natural disaster etc.

Different hardware security measures are:

a) Regular Maintenance
b) Insurance
c) Dust free environment
d) Protection from Fire

e) Protection from Thief
f) Air condition system
g) Power Protection device (Volt guard, Spike guard, UPS)

3.1 Regular Maintenance
Regular maintenance keeps the computer hardware in good working condition and it also helps to correct the problems before they cause severe damages.
E.g. CPU cooler not working properly and if we don't repair or replace on time then it can damage microprocessor.

3.2 Insurance is a way of protection from financial loss. If a computer is damaged or stolen then we can claim for the insurance amount and get the economic support.

3.3 Dust Free Environment
Dust particles can cause the failure of hardware components. Computer room should be absolutely free from dust and air pollution. It is necessary to regularly vacuum cleaning the room and blurring the hardware.

3.4 Protection from Fire

- Due to faulty wiring, loose connection, smoking in the computer room and overload on power socket can cause fire in a room.

- Using fire alarms, fire doors, fire detectors and fire extinguishers can minimize the damage of hardware components and loss of information from fire.

3.5 Protection from Theft

- Use of Lighting system, Grills on the windows, Safety Lock on the doors, Alarms, CCTV (Closed Circuit Television) helps to protect from thieves.

3.6 Air Condition System maintains the suitable temperature and humidity of the room. Room temperature should be maintained between 21^0C to 24^0C.

3.7 Power Protection Device
An electric device that controls electric voltage and provides enough backup to the computer system when there is power failure. Computer needs working voltages constantly.
Some common power protection devices are:
a) UPS b) Volt Guard c) Spike Guard d) Surge Suppressor

Why Power Protection Device needed? To protect computer system from damage, expensive data loss and unnecessary down time.

Volt Guard A power protection device that provides constant output voltage to the computer system in case of fluctuating voltage coming from the source.

UPS (Uninterruptible Power Supply) is a battery supported power protection device which continuously supply power to the computer system even during main power failures.

Spike Guard is designed to protect electrical devices from immediate voltage spikes.