Computer Security and Safety, Ethics, and Privacy

Computer Security Risks

- A **computer security risk** is any event or action that could cause a loss of or damage to computer hardware, software, data, information, or processing capability.
- Security risks include;
  - Hardware damage
  - Software corruption/malfunction
  - Data/Information theft/deletion
  - Unauthorized system access/use
  - Processor capabilities reduction

Terms associated with Security Risks

- **computer crime:** Any illegal act involving a computer.
- **Cybercrime** refers to online or Internet-based illegal acts.
- **Crimeware:** Software used by cybercriminals.

Basic categories of cybercrime perpetrators

1. **Hacker (white hat hacker)**, refers to someone who accesses a computer or network illegally.
2. A **cracker (black hat hacker)** is someone who breaks into systems illegality for personal gain, vandalism, or bragging rights..
3. A **script kiddie (skiddie)** is an unskilled individual who uses programs developed by others to attack computer systems and networks and deface websites.

4. **corporate spies** have excellent computer and networking skills and are hired to break into a specific computer or identify risks in their own organization.
5. A **cyber extortionist** is someone who uses e-mail as a vehicle for extortion, threatening others for personal gain.
6. A **cyber terrorist** is someone who uses the Internet or network to destroy or damage computers for personal reasons.
7. **Cyber warfare** describes an attack whose goal ranges from disabling a government's computer network to crippling a country.

Computer Malware

- A **malware** is malicious software designed to act without a user's knowledge and deliberately alter the computer's operations.
- **How malware is spread**
  - Opening an infected file
  - Running an infected program
  - Booting the computer with infected removable media inserted
  - visiting an infected website
  - downloading infected software

Examples of common malwares

- Viruses
- Worms
- Trojan horses
- Ransomware
- Spyware
- Adware
- Scareware
- Rootkit and other malicious programs

Computer Virus

- A **computer virus** is a computer program capable of copying itself and typically has a damaging effect, such as corrupting the system or destroying data without the user's knowledge.

Types of viruses

i. **Resident viruses**: These are permanent viruses lodging in RAM.
ii. **Overwrite viruses:** These viruses delete information that is in the infected files.
iii. **File infectors:** This virus infects executable files or programs.
iv. **Boot viruses:** This virus infects the hard disk's boot sector and makes the computer unable to boot.
v. **Direct action viruses:** This virus replicates itself, then acts when executed and infects files located in the folders or computer directory.

vi. **Directory viruses:** This virus alters the paths indicating a file's location.

vii. **Macro virus:** This virus affects files created using particular programs or applications containing macros.

viii. **FAT Viruses:** These viruses attack the file allocation table (FAT) which is the disc part used to store every information about the available space, location of files, unusable space etc. e.g. the link virus

ix. **Polymorphic Virus:** They encode or encrypt themselves in a different way every time they infect your computer. They use different encryption and algorithms.

x. **Email Virus:** This is a virus spread via an email. Such a virus will hide in an email and when the recipient opens the mail.

xi. **Browser Hijacker:** This virus can spread in many different ways including a voluntary download. If infects certain browser functions especially in form of re-directing the user automatically to certain sites. A good example is the *cool web search*

Computer Worm

- A computer worm is a program that copies itself repeatedly, in memory or on a network, using up resources and shutting down the computer or network. Unlike a computer virus, it does not need to attach itself to an existing program.
- **Worm Viruses Include:** lovgate.F, sobig.D, trile. C, PSWBugbear.B, Mapson

Trojan Horse

- **Trojan horse** is any malicious computer program which misrepresents itself to appear useful, routine, or interesting in order to persuade a victim to install it.
- Trojans can illegally trace important login details of users online. For example E-Banking

Computer Rootkits

- A **rootkit** is a program that hides in a computer and allows someone from a remote location to take full control of the computer. E.g. Execute programs, change settings, etc.

Signs and symptoms that tell computer might be infected by a malware

- OS running slower
- Less available memory
- Corrupted files
- Unusual messages or images
- Unusual sounds playing
- Existing programs and files disappear
- Programs or files not working properly
- Unusual programs or files appear
- OS does not start up or unexpectedly shuts down

How to Safeguards against Computer Viruses and Other Malware

i. Do not start a computer with removable media inserted in the drives. If you must, it must be from a **trusted source**, which is an organization or person you believe will not send a virus.

ii. Never open an e-mail attachment unless you are expecting the attachment and it is from a trusted source.

iii. In extreme cases, you may need to reformat the hard disk to remove malware from an infected computer.

iv. Install an antivirus program and update it frequently.

An **antivirus program** protects a computer against viruses by identifying and removing any computer virus found in memory and files.

A **quarantine** is a separate area of a hard disk that holds infected files until the infection can be removed, ensuring other files will not become infected.

Computer security terminologies

a. A **botnet** is a group of compromised computers connected to a network that are used as part of a network to attacks other networks.
b. **A zombie** is a compromised computer whose owner is unaware the computer is being controlled remotely by an outsider.
c. A **bot** is a program that performs a repetitive task on a network.

d. A **denial of service (DoS) attack**, is an assault whose purpose is to disrupt computer access to an Internet service such as the Web or e-mail.

e. A **back door** is a program that allow users to bypass security controls when accessing a program, computer, or network.

f. **Spoofing** is a technique intruders use to make their network or Internet transmission appear legitimate to a victim computer or network.

g. **E-mail spoofing** occurs when the sender's address or other components of the e-mail header are altered so that it appears the e-mail originated from a different sender.

Safeguards against Botnets, DoS Attacks, Back Doors and Spoofing

- Use of the latest updated antivirus programs.
- Users can also implement firewall solutions.
- install intrusion detection software
- set up honeypots.

Firewalls

- A **firewall** is a hardware and/or software that protects a network's resources from intrusion by users on another network such as the Internet.
- A **proxy server** is a server outside the organization's network that controls which communications pass into the organization's network.
- A **personal firewall** is a utility program that detects and protects a personal computer and its data from unauthorized intrusions.

Intrusion Detection Software

- **Intrusion detection software** automatically analyzes all network traffic, assesses system vulnerabilities, identifies any unauthorized intrusions, and notifies network admins.

Honeypots

- A **honeypot** is a vulnerable computer that is set up to entice an intruder to break into it.
- They appear real to the intruder but are separated from the organization's network.
- They are used to learn how intruders are exploiting organization's network.

Unauthorized Access and Use

- **Unauthorized access** is the use of a computer or network without permission.
- **Unauthorized use/Tampering** is the use of a computer or its data for unapproved or possibly illegal activities.

How to protect system against unauthorized access and use

- **Authorization** is the permission to access a computer or a network and its resources
- **User Identification** verifies that an individual is a valid user.
- **Authentication** verifies that the individual identity is the person he or she claims to be.

- **Password policies:** Defines the criteria that a password must satisfy to be considered valid, for example, age, length, and syntax.
- **Encryption:** When data is encrypted, it is scrambled in a way that only the recipient can understand after data decryption.
- **Access control** is the selective restriction of access to a place or other computer resources. E.g. use of Locks and login credentials.
- **Account inactivation**

Disables a user account or group of accounts so that all authentication attempts are automatically rejected.

- **Secure Sockets Layer (SSL)**

Maintains the integrity of information. If encryption and message digests are applied to the information being sent, the recipient can determine that it was not tampered with during transit.

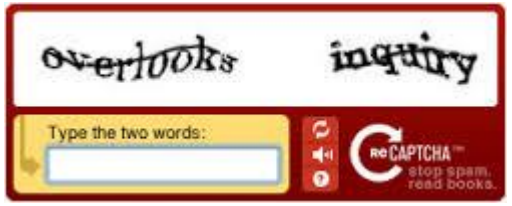
- **Auditing**

Allows you to determine if the security of your directory has been compromised. For example, you can audit the log files maintained by your directory.

Authorization Controls include;

- A **user name**, or *user ID*, is a unique combination of characters (letters, numbers) that identifies a specific user.
- A **password** is a private combination of characters associated with the user name that allows access to certain computer resources.
- **PIN (personal identification number)** is a numeric password, either assigned by a company or selected by a user.
- A **passphrase** is a private combination of words, often containing mixed capitalization and punctuation, associated with a user name, to be used in place of a password.

- A **QR Code** (Quick Response) is a mobile phone readable bar code that can store website URL's, plain text, phone numbers, email addresses and pretty much any other alphanumeric data.
- **CAPTCHA** (Completely Automated Public Turing test to tell Computers and Humans Apart) is a program developed to verify that user input is not computer generated.



Identification controls include;

- A **possessed object** is any item that you must carry to gain access to a computer or computer facility. These include;
  - Access badges
  - identification cards (ID cards)
  - Access key cards

Authentication controls include;

- **Biometric** verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits.
- A **biometric device** authenticates a person's identity by translating a personal characteristic, such as a fingerprint, into digital code that is compared with a digital code stored in the computer verifying a physical or behavioral characteristic.
  - E.g. ***Biometric payment*** is used, where a customer's fingerprint is read and their account is charged.
- Biometric devices have disadvantages.
  - E.g. Cut finger for fingerprint readers.

Biometric Unique identifiers include….

- Face recognition.
- Fingerprint identification. ...
- Hand geometry biometrics. ...
- Retina scan. ...
- Iris scan. ...
- Signature. ...
- Voice waves analysis
- Earlobe
- DNA

Digital Forensics

- **Digital forensics**, also called *computer forensics*, *network forensics*, or *cyberforensics*, is the discovery, collection, and analysis of evidence found on computers and networks.
- **Computer forensics** uses evidence found in computers and digital storage media.
- **Network forensics** is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents.
- **Cyber forensics** is the process of extracting information and data from computers to serve as digital evidence in a cyber crime

Hardware Theft and Vandalism

- **Hardware theft** is the act of stealing computer equipment.
- **Hardware vandalism** is the act of defacing or destroying computer equipment.

Safeguards against Hardware Theft and Vandalism

- Use cables to lock the equipment to a desk.
- Use *real time location system (RTLS)* to track and identify the location of high-risk or high-value items.
- Use extra security on mobile devices, such as logon passwords, encrypted data, and even software to photograph the thief.

Software Theft and Piracy

- **Software theft** is unauthorised duplication and/or use of computer software. This usually means unauthorised copying, either by individuals for use by themselves or their friends or by companies who then sell the illegal copies to users.
- **Software piracy** is the illegal copying, distribution, or use of a copyrighted software

Safeguards against Software Theft and piracy

- All owned software media should be stored securely.
- Purchase a software **license agreement** which is the right to use the software
- Use a **product activation code**, which is conducted either online or by telephone, users provide the software product's identification number to receive an installation identification number unique to the computer on which the software is installed.

Information Theft

- **Information theft** occurs when someone steals personal or confidential information.

Safeguards against Information Theft

- Implement the user identification and authentication controls discussed earlier.

Encryption

- **Encryption** is a process of converting readable data into unreadable characters to prevent unauthorized access.
- To read the data, the recipient must **decrypt**, or decipher, it into a readable form.

Encryption algorithm

- **Plaintext** is the unencrypted, readable data.
- **Ciphertext** is the encrypted (scrambled) data.
- **An encryption algorithm (cypher)** is a set of steps that can convert readable plaintext into unreadable ciphertext.

Simple Encryption Algorithms

Name	Algorithm	Plaintext	Ciphertext	Explanation
Transposition	Switch the order of characters	SOFTWARE	OSTFAWER	Adjacent characters swapped
Substitution	Replace characters with other characters	INFORMATION	WLDIMXQUWIL	Each letter replaced with another
Expansion	Insert characters between existing characters	USER	UYSYEYRY	Letter Y inserted after each character
Compaction	Remove characters and store elsewhere	ACTIVATION	ACIVTIN	Every third letter removed (T, A, O)

Encryption keys

- **An encryption key** is a set of characters that the originator of the data uses to encrypt the plaintext and the recipient of the data uses to decrypt the ciphertext.
- **private key encryption (symmetric key encryption),** both the originator and the recipient use the same secret key to encrypt and decrypt the data.
- **Public key encryption (asymmetric key encryption),** uses two encryption keys, a public and a private.
  - A message generated with a public key can be decrypted only with the private key.

Encryption terms

a. A **digital signature** is an encrypted code that a person, Web site, or organization attaches to an electronic message to verify the identity of the message sender.
b. A **secure site** is a website that uses encryption techniques.
c. A **digital certificate** is a notice that guarantees a user or a website is legitimate.

d. **Transport Layer Security (TLS)** provides encryption of all data that passes between a client and an Internet server. TLS protected websites typically begin with https, instead of http.

e. **Secure HTTP (S-HTTP)** allows users to choose an encryption scheme for data that passes between a client and server.

f. **A Virtual Private Network (VPN)** extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network

Transport Layer Security