COMPUTER AND DATA SECURITY

Basic Concepts

- **Security**-is the state of being free from danger or threat.
- **Computer Security** Refer to the security of computers against intruders (e.g., hackers) and malicious software (e.g., viruses). **NB//** Typically, the computer to be secured is attached to a network and the bulk of the threats arise from the network
- Also includes security applied to computing devices such as **computers** and **smartphones,** as well as **computer networks** such as private and public networks, including the whole Internet.
- It covers all the processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction.
- It is sometimes referred to as "cyber security" or "IT security",

though these terms generally do not refer to physical security (locks and such).

- Before the problem of data security became widely publicized in the media, most people’s idea of computer security focused on the physical machine.

Traditionally, computer facilities have been physically protected for three reasons:

- To prevent theft of or damage to the hardware
- To prevent theft of or damage to the information
- To prevent disruption of service

Terminologies

- **Risk-** A situation involving exposure to danger.
- **A threat-** a specific means by which a risk can be realized by a malicious entity also known as an adversely.
- **A vulnerability** is a weakness which exposes computer systems to attackers. This reduces system's security assurance.

Vulnerability is the intersection of three elements:

1. a system susceptibility or flaw,
2. attacker access to the flaw,
3. attacker capability to exploit the flaw.

What is the source of a vulnerability?

– Bad software (or hardware)

– Bad design or requirements

– Bad policy/configuration

– System Misuse • unintended purpose or environment

- **An attack-** It is an event that occurs when someone attempts to exploit a vulnerability

- **Kinds of attacks**

– Passive (e.g., eavesdropping)

– Active (e.g., password guessing)

– Denial of Service (DOS)

– using many endpoints

A compromise occurs when an attack is successful – Typically associated with taking over/altering resources

- **Tampering** describes an intentional modification of products in a way that would make them harmful to the consumer.
- **Computer crime** refers to any crime that involves a computer and a network.

Principle of security

There are six principles of security.

- However, the first three are the key principles. They are mainly referred to as C.I.A
- They are as follows:

Confidentiality:

The principle of confidentiality specifies that only authorized entities should be able to access secured information. i.e there should be no unauthorized access to information or stored data.

Integrity:

- The main aim is to ensure that data is not corrupted
- With data being the primary information asset, *integrity* provides the assurance that the data is accurate and reliable. Therefore, policies and procedures should support ensuring that data can be trusted.

Availability

- *Availability* is the ability of the users to access an information asset or a computing system whenever they need it. Information is of no use if it cannot be accessed. Systems should have sufficient capacity to satisfy user requests for access, and network architects should consider capacity as part of availability.

Privacy

- *Privacy* relates to all elements of the security. It considers which information can be shared with others (confidentiality), how that information can be accessed safely (integrity), and how it can be accessed (availability).

Identification and Authentication

- Information security is the process of managing the access to resources. To allow a user, a program, or any other entity to gain access to the organization's information resources, you must identify them and verify that the entity is who they claim to be. The most common way to do this is through the process of *identification and authentication*.

Non-repudiation:

- This is where actions can be traced back to the person who did them.
- This means that a person who does something in the computer system cannot deny it later.
- It is mainly done through system logs audit.

Examples of Online Cyber security Threats.

- **Software attacks** means attack by Viruses, Worms, Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behave differently.
- **Malware** is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or a anything that is designed to perform malicious operations on system.
- **Eavesdropping** is the act of secretly listening to a private conversation, typically

between hosts on a network.

- **Theft of intellectual property** means violation of intellectual property rights like copyrights, patents etc.
- **Masquerading/Identity theft/spoofing** means to act as if you are someone else to obtain person's personal information or to access vital information they have. Example accessing the computer or social media account of a person by login into the account by using their login credentials.
- **Denial of service attack:** This refers to overwhelming a computer network with unwarranted traffic with the soul aim of rendering it unavailable to its users.
- **Distributed denial of service attack:** It is a denial of service attack that is being done by more than one attacker/source. i.e multiple sources or attackers collaborate to bring down a computer network.

- **Theft of equipment and information** is increasing these days due to the mobile nature of devices and increasing information capacity.
- **Sabotage** means destroying company's website to cause loss of confidence on part of its customer.
- **Information extortion** means theft of company's property or information to receive payment in exchange.
  For example, ransomware may lock victims file making them inaccessible thus forcing victim to make payment in exchange. Only after

  payment when the victim's files will be unlocked.

New Generation Threats.

- **Social Engineering –** is the art of manipulating people so that they give up their confidential information like bank account details, password etc. These criminals can trick you into giving your private and confidential information or they will gain your trust to get access to your computer to install a malicious software- that will give them control of your computer.
- For example, email or message from your friend, that was probably not sent by your friend. Criminal can access your friend's device and then by accessing the contact list he can send infected email and message to all contacts.
- Since the message/ email is from a known person recipient will definitely check the link or attachment in the message, thus unintentionally infecting the computer.
- **Social media attacks –** In this cybercriminal identify and infect a cluster of websites that persons of a particular

organization visit, to steal information.

- **Mobile Malware –**There is a saying when there is a connectivity to Internet there will be danger to Security.
- Same goes to Mobile phones where gaming applications are designed to lure customer to download the game and unintentionally they will install malware or virus in the device.
- **Outdated Security Software –** With new threats emerging every day, updating security software is a pre-requisite to have a fully secured environment, otherwise one will be exposed to very many security threats.
- **Corporate data on personal devices –** These days every organization follows a rule BYOD. BYOD means Bring your own device like Laptops, Tablets to the workplace.
- Clearly BYOD pose a serious threat to security of data but due to productivity issues organizations are arguing to adopt this.

Hackers and Predators

- Hackers and predators are programmers who victimize others for their own gain by breaking into computer systems to steal, change, or destroy information as a form of cyber- terrorism.
- These online predators can compromise credit card information, lock you out of your data, and steal your identity.

Computer Crime Prevention/ Security measures

1. **Use Strong Passwords** -Use different user ID / password combinations for different accounts and avoid writing them down.

Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.

2. Secure your computer with activate firewall -Firewalls are the first line of cyber defense; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.

3. Use anti-virus/malware software -Prevent viruses from infecting your computer by scanning the files being downloaded or being shared via peripherals such as flash drives. Always ensure that you regularlyupdate your anti-virus software.

4. Be Social-Media Savvy -Make sure your social networking profiles (e.g. Facebook, Twitter, Youtube, etc.) are set to private. Check your security settings.

Be careful what information you post online. Once it is on the Internet, it is there forever!

5. **Secure your Mobile Devices-** Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.

6. **Install the latest operating system updates Keep your applications and operating system** (e.g. Windows, Mac, Linux) current with the latest system updates.

Turn on automatic updates to prevent potential attacks on older software.

7. Protect your Data -Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location. Majority of cloud storage solutions provide encryption of stored data.

8. Secure your wireless network- Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured.

- Review and modify default settings. Public Wi-Fi, “Hot Spots”, are also vulnerable.
- Avoid conducting financial or corporate transactions on public wifi networks.

9. Protect your e-identity Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet.

Make sure that websites are secure (e.g. when making online purchases) or that you’ve enabled privacy settings (e.g. when accessing/using social networking sites).

10. Avoid being scammed -Always think before you click on a link or file of unknown origin.

Don’t feel pressured by any emails.

Check the source of the message. When in doubt, verify the source.

Never reply to emails that ask you to verify your information or confirm your user ID or password.

11. **Install Intrusion detection systems:** They are software that have the capability of scanning data packets and identify malicious packets such as ones generated by attackers. This can help in protecting against hackers

12. **Use of gateways-** they filter network traffic therefore preventing unwanted traffic from getting into the network. Protects against DOS and DDOS

13. Call the right person for help - Don’t panic! If you are a victim, if you encounter illegal Internet content (e.g. child exploitation) or if you suspect a computer crime, identity theft or a commercial scam, report this

Controlling Computer Systems Security (organizational Level)

- There are numerous threats to computer Systems
  - Hardware failures
  - Software failures
  - Upgrade issues
  - Disasters
  - Malicious intent
- To minimize likelihood of threats, there is need to control the environment in which Information Systems are developed and deployed

- Controls are put in place to:
  - Manually control environment of computer Systems
  - Automatically add controls to computer Systems

CONTROLS

Controls are parameters implemented to protect various forms of data and infrastructure important in an organization

They include the following:

- **Software controls**
  - Provide only Authorized access to systems
  - E.g through login (i.e only people with the required

username and password can login)

- **Hardware controls**
  - Physically secure hardware
  - Monitor for and fix malfunction
  - Backup of disk-based data
  - Monitor hardware usage
- **Computer operations controls**
  - Day-to-day operations of computer Systems are regulated
  - Usage procedures are established
  - Backup and recovery procedures are established and enforced

- **Data security controls**
  - Prevent unauthorized access, change or destruction of data
  - Encrypt data while in transit and while in storage
  - Physical access to terminals/ restrictions (e.g locking the server in a secure room)
  - Password protection
  - Data level access controls i.e determining who will access which data
- **Administrative controls**
  - Ensure organizational policies, procedures and standards and enforced
  - Regularly revising procedures to ensure relevance

  - Segregation of functions to reduce errors and fraud
  - Supervision of personnel to ensure policies and procedures are being adhered to.
  - Enforcing disciplinary actions against policy violators

- **Input controls** (protects against GIGO)
  - Data is accurate and consistent on entry
  - Direct keying of data, double entry or automated input
  - Data conversion, editing and error handling
  - Field validation on entry
  - Input authorization and auditing
  - Checks on totals to catch error.

Laws Governing Protection of ICT

Local

- ICT authority standards
- Computer misuse and cybercrime act of 2018

International

- IEE professional code of conduct
- ACM professional code of conduct