BIM

Semester: I

FOUNDATION OF INFORMATION TECHNOLOGY

Computer Security and Privacy

REFERENCE NOTE

Unit-9: Computer Security and Privacy

Computer security

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.

There are various types of computer security which is widely used to protect the valuable information of an organization.

What is Computer Security and its types?

One way to ascertain the similarities and differences among Computer Security is by asking what is being secured. For example,

- **Information security** is securing information from unauthorized access, modification & deletion
- **Application Security** is securing an application by building security features to prevent from Cyber Threats such as SQL injection, DoS attacks, data breaches and etc.
- **Computer Security** means securing a standalone machine by keeping it updated and patched
- **Network Security** is by securing both the software and hardware technologies

- **Cybersecurity** is defined as protecting computer systems, which communicate over the computer networks

The CIA Triad

Computer security is mainly concerned with three main areas:

- *Confidentiality is* ensuring that information is available only to the intended audience
- *Integrity is* protecting information from being modified by unauthorized parties
- *Availability is* protecting information from being modified by unauthorized parties.

Computer security Terminologies

1. Adversary
2. Attack
3. Countermeasure
4. Risk
5. Security policy
6. System resource
7. Vulnerability
8. Threat

1. Adversary (threat agent): Individual, group, organization, or government that conducts or has the intent to conduct detrimental (harmful) activities.

2. Attack: Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

3. Countermeasure: A device or techniques that has as its objective of prevention of spying, disruption, theft, or unauthorized access to or use of sensitive information or information systems.

4. Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.

5. Security policy: A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.

6. System resource (assets): A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

7. Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

8. Threat: A threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation). Organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Unauthorized Access and Unauthorized

Unauthorized access refers to the situation when a person gains entry to a computer network, system, application software, data, or other resources without permission. It is an access to an information system or network that violates the owner or operator's stated security policy. Unauthorized access is also when legitimate users access a resource that they do not have permission to use.

Unauthorized access occurs whenever an individual gains access to a computer, mobile device, network, files or other resources without permission.

The most common reasons for unauthorized access are:

- Steal sensitive data
- Cause damage
- Hold data hostage as part of a ransomware attack

Some common unauthorized access tactics are:

- Guessing passwords
- Exploiting software vulnerabilities
- Social engineering - falsely convincing people

Unauthorized Use

Unauthorized Use means any use, reproduction, distribution, transfer, disposition, disclosure, possession, memory input, alteration, erasure, damage or other activity by the unauthorized user or the system. It involves using a computer resources for unauthorized activities.

- The following examples must be considered unauthorized use by most organizations:
- Downloading, storing or distributing pornography on government-owned ICT facilities and devices.
- Taking inappropriate or pornographic pictures with mobile phone cameras. Forwarding inappropriate jokes and graphics, particularly any material of sexually explicit, racist, defamatory or offensive behavior.
- Using ICT facilities and devices to conduct personal business for personal gain or profit.
- Unauthorized downloading or storage of files and records, such as audio and video files.

Cyber Security

Cyber Security is the technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity. We can divide cybersecurity into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information. In some cases, it is also called **electronic information security** or **information technology security**.

Types of Cyber Security

Every organization's assets are the combinations of a variety of different systems. These systems have a strong cybersecurity posture that requires coordinated efforts across all of its systems. Therefore, we can categorize cybersecurity in the following sub-domains:

- **Network Security:** It involves implementing the hardware and software to secure a computer network from unauthorized access, intruders, attacks, disruption, and misuse. This security helps an organization to protect its assets against external and internal threats.
- **Application Security:** It involves protecting the software and devices from unwanted threats. This protection can be done by constantly updating the apps to ensure they are secure from attacks. Successful security begins in the design stage, writing source code, validation, threat modeling, etc., before a program or device is deployed.
- **Information or Data Security:** It involves implementing a strong data storage mechanism to maintain the integrity and privacy of data, both in storage and in transit.
- **Identity management:** It deals with the procedure for determining the level of access that each individual has within an organization.
- **Operational Security:** It involves processing and making decisions on handling and securing data assets.
- **Mobile Security:** It involves securing the organizational and personal data stored on mobile devices such as cell phones, computers, tablets, and other similar devices against various malicious threats. These threats are unauthorized access, device loss or theft, malware, etc.
- **Cloud Security:** It involves in protecting the information stored in the digital environment or cloud architectures for the organization. It uses various cloud service providers such as AWS, Azure, Google, etc., to ensure security against multiple threats.
- **Disaster Recovery and Business Continuity Planning:** It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost

operations after any disaster happens to the same operating capacity as before the event.

- **User Education:** It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.

Protecting against unauthorized Access and Unauthorized Use / Safety Tips

Let us see how to protect ourselves when any cyberattacks happen. The following are the popular cyber safety tips:

Conduct cybersecurity training and awareness: Every organization must train their staffs on cybersecurity, company policies, and incident reporting for a strong cybersecurity policy to be successful. If the staff does unintentional or intentional malicious activities, it may fail the best technical safeguards that result in an expensive security breach. Therefore, it is useful to conduct security training and awareness for staff through seminars, classes, and online courses that reduce security violations.

Update software and operating system: The most popular safety measure is to update the software and O.S. to get the benefit of the latest security patches.

Use anti-virus software: It is also useful to use the anti-virus software that will detect and removes unwanted threats from your device. This software is always updated to get the best level of protection.

Perform periodic security reviews: Every organization ensures periodic security inspections of all software and networks to identify security risks early in a secure environment. Some popular examples of security reviews are application and network penetration testing, source code reviews, architecture design reviews, and red team assessments. In addition, organizations should prioritize and mitigate security vulnerabilities as quickly as possible after they are discovered.

Use strong passwords: It is recommended to always use long and various combinations of characters and symbols in the password. It makes the passwords are not easily guessable.

Do not open email attachments from unknown senders: The cyber expert always advises not to open or click the email attachment getting from unverified senders or unfamiliar websites because it could be infected with malware.

Avoid using unsecured Wi-Fi networks in public places: It should also be advised not to use insecure networks because they can leave you vulnerable to man-in-the-middle attacks.

Backup data: Every organization must periodically take backup of their data to ensure all sensitive data is not lost or recovered after a security breach. In addition, backups can help maintain data integrity in cyber-attack such as SQL injections, phishing, and ransomware.

Introduction to ICT:

Information System is, which is used to communicate through any medium or by using technology, is called information communication technology. Information Communication Technology (ICT) literally used to clarify its meaning, which refers to the merging of telephone networks with computer networks. Information Technology (IT) is the study, design, development, implementation, support or management of information systems.

Social Impact of the ICT

POSITIVE Impact of ICT:

- Create opportunity for technical employment:
- E-Commerce
- Fast and Cheap Communication
- Education
- Health Care
- Multimedia Presentation

NEGATIVE Impact of ICT:

- Number of Employment Opportunity will Reduced
- Health Problem
- Money Theft
- Digital Divide
- Possibility of Leakage, hacked and Disclosure of Personal Information
- Pornography

Digital Divide:

Digital Divide refers to the gap between individuals, households, business and geographic areas at different socio- economic levels with regard with the opportunity to access Information and Communication Technology (ICT) in the Internet using computers and many other mobile computing devices such as tablet PC, PDA, mobile etc.

Computer Ethics:

The word 'ethics' means 'moral' beliefs and rules about right and wrong. Thus, computer ethics also refers to the responsible use of computers and computer networks. It is a branch of practical. Ethics deals with placing a value on acts according to whether they are good or bad.

Commandments:

1. Do not use a computer to harm other people
2. Do not interfere with other people's computer work
3. Do not snoop or view around in other people's files
4. Do not use a computer to steal
5. Do not use or copy software for which you have not paid
6. Do not use other people's computer resources without authorization

7. Think about the social consequences of the program you write Use a computer in ways that show consideration and respect

Intellectual Properties Right

The term intellectual property refers broadly to a distinct types of the creations of the human mind such as musical, literary, photographic and artistic works; discovers and inventions; and words, phrases , symbols and designs etc. Intellectual property rights protect the interests of creators by giving them property rights over their creations. Common types of intellectual property rights include

- Copyrights
- Trademarks
- Patents
- Industrial Design Rights etc.

Privacy and Anonymity

Privacy: Privacy is the concept for the protection of user's data which is not be examined or viewed by anyone else without his/her permissions. Privacy is the ability to control particular information. Many people use the term to mean universal internet privacy.
Various types of personal information often come under privacy concerns. Some of them are as follows.

i) Financial privacy
ii) Internet Privacy
iii) Medical Privacy
iv) Political privacy

Computer Crime:

Computer crime is the illegal use of a computer by an unauthorized individual, either for pleasure such as by a computer hacker or for profit as by a thief. Thus, it refers to any crime such as tampering, physical danger and unwanted disclosure of data that involves a computer and a computer network.

Technical solutions

If correctly installed, the following can help to block attacks:

- Firewalls:
- Software Solution:
- Authentication
- Hardware Cryptography
- Patches

Cyber law:

Cyber law is commonly known as the law of the internet. It governs the legal issues of cyberspace. The term that cyberspace is not only restricted to the internet. It is a very wide term that includes:

- Computer
- Computers networks
- The internet
- Data
- Software etc.

What Cyber law deals with? Or Area of Cyber Law

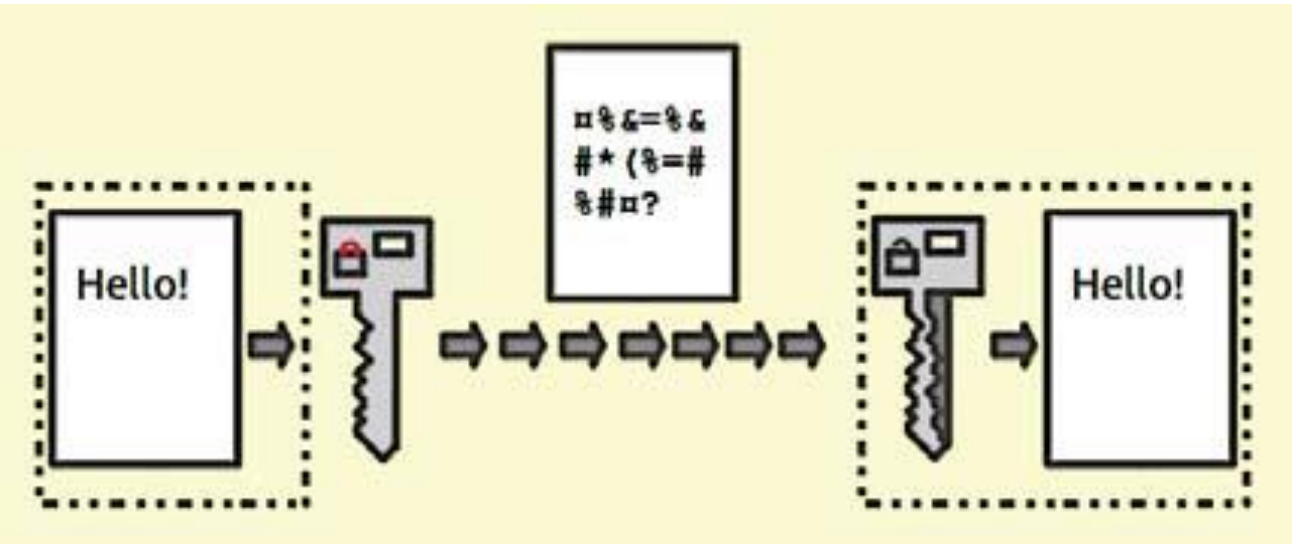
- Electronic and Digital Signatures
- Computer Crime
- Intellectual Property
- Data Protection and Privacy
- Tale-communication laws.

Cryptography

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the Greek word " kryptos", which means hidden. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages. Cryptography includes ensuring that data/ message cannot be understood by an unauthorized user. There are different types of cryptography technology used.

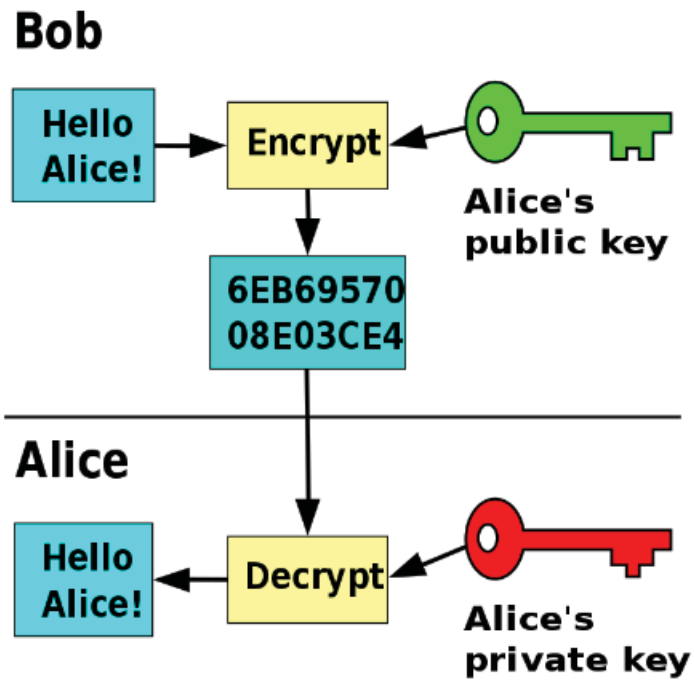
i. Encryption

Encryption is the technology to encode file or message that is being stored or transferred online in intelligible content which cannot be used by an unauthorized person. The encryption is not meant to prevent interception but it makes the file or message unusable to the hacker. Authorized user can read or use the file or message after decrypting it. Generally, encryption is done with the help of key and the key is made available to the authorized user by another medium.



ii. Decryption

The conversion of encrypted data into its original form is decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.



Computer Virus

Computer viruses are the programs or malware which are loaded onto your computer by 'mean' people, without your knowledge. These viruses replicate relentlessly and infect computer programs. They might even delete or corrupt your computer data or erase your hard disk too. These virus programs are placed into commonly used programs. So, when those programs are run, the attached virus infects the executable program or file.

Symptoms of Virus:

- Slowing down of the speed of the computer.
- Change in files' extension.
- A long time in the loading of a program.
- Showing of unusual error message on the screen.
- System data corruption.
- Memory space reduction in a computer.
- Inaccessibility to the location of files.

Causes / Motivations for creating computer viruses

1. Making money:
2. Stealing account information
3. Causing problem and troubles: Malware like virus are also developed for fun and creating problems to others.

4. Proving a point: Sometime, a computer expert creates a virus to prove that certain process works or that a certain network can be penetrated or that certain antivirus software are effective.
5. Fame: Some people create virus to be known for being the person who damaged thousands of computers.
6. Revenge: Virus are also created for revenge of some action. The creator can use virus to crack others computer, steal information, crash the network for revenge.
7. Stealth

Source of Computer Virus

- E-mail attachments
- Internet
- Intranet
- Pirated and cracked software and games
- Virus infected portable devices like pen- drive, memory card, and hard drive.
- Downloading virus infected programs
- Unpatched / un- updated software

Prevention of Virus:

- Password protection should be employed.
- Execute familiar programs only as to their origin. Programs sent by e-mail should always be suspicious.
- Load software only from original CDs or disks instead of pirated or copied ones.
- Check all shareware and free programs downloaded from online services with a virus checking program.
- Computer uploads and "system configuration" changes should be always performed by the computer owner.
- Purchase or download an anti-virus program that runs as you boot or work on your computer. Also, update it frequently.

Types of Viruses

1. **Trojan Horse:** Appearing as a useful and desired function, a Trojan Horse program neither replicates nor copies itself, but causes damages and compromises the security of a computer. This virus program may arrive in the form of software of some sort or a joke program that must send by someone or carried by another program.
2. **Worm:** It is a program that copies and facilitates self-distribution from one disk drive to another or by copying itself using e-mail or any other transport mechanism.

3. **Macro Virus:** These viruses infect documents such as MS Excel or MS Word and other similar documents. These viruses use another application's macro programming language to distribute themselves.
4. **Boot sector Virus:** Normally, spread by floppy disks, this virus attaches itself to the 1st part of the hard disk which is read by the computer upon boot up.
5. **Polymorphic Virus:** A Polymorphic Virus is a very sophisticated virus program as it not only replicates itself by creating multiple files itself but also changes its digital signature each time it replicates.
6. **Memory Resident Virus:** This virus is initiated from a virus within the computer and they stay in a computer's volatile memory (RAM) after its initiating program closes.

Computer Antivirus

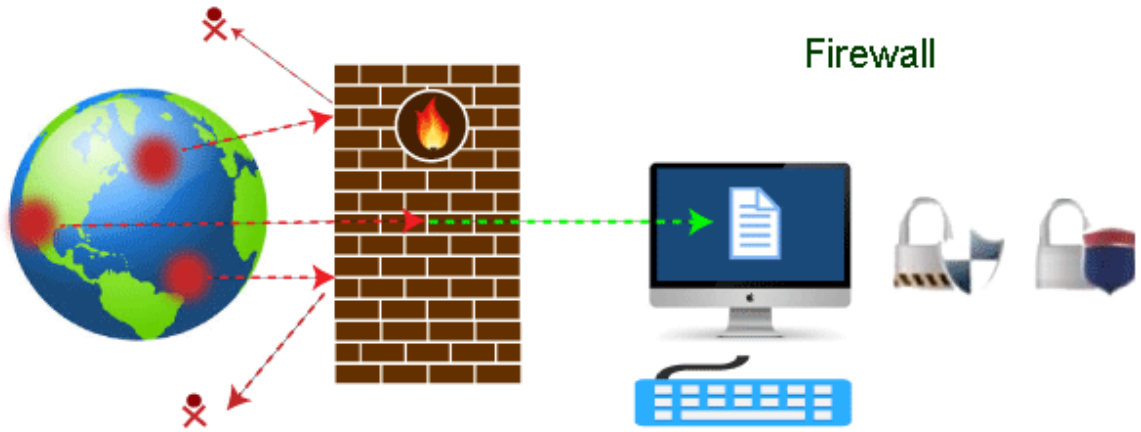
An antivirus is a computer software designed to scan, detect and remove viruses and malicious software from computers. This software defends your computer against computer viruses that threaten to infect your computer files and systems. In order to be an effective defense virus, an antivirus needs to run all the times in the background and should be kept updated frequently.

Originally developed for the detection and removal of computer viruses, with the emerge of several kinds of viruses, antivirus software programs started to protect from other computer threats. Antivirus scans the files and folders and alerts the user if viruses are found. Some known and popular antivirus software are Kasper-sky, Avira, Norton, Avast, AVG, etc.

Firewall

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.



Firewall: Hardware or Software

This is one of the most problematic questions whether a firewall is a hardware or software. As stated above, a firewall can be a network security device or a software program on a computer. This means that the firewall comes at both levels, i.e., hardware and software, though it's best to have both.

Each format (a firewall implemented as hardware or software) has different functionality but the same purpose. A hardware firewall is a physical device that attaches between a computer network and a gateway. For example, a broadband router. On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software.

Apart from that, there are cloud-based firewalls. They are commonly referred to as FaaS (firewall as a service). A primary advantage of using cloud-based firewalls is that they can be managed centrally. Like hardware firewalls, cloud-based firewalls are best known for providing perimeter security.

Privacy	Security
Privacy defines the ability to secure personally identifiable data.	Security define protecting against unauthorized access.
Privacy denotes anyone who feels free from some unwanted attention.	Security is some state of being free through possible threats or private freedom.
Privacy programs concentrate on protection personal information just like passwords, log-in credentials, etc.	The security programs defines the set of regulations and protocols to secure each confidential information resources and assets that an enterprise owns and collects.

Privacy defines protecting sensitive information associated to individuals and organizations.	Security supports protection for some types of data and information such as the ones that are saved electronically.
To a few extent, privacy is implemented with the initiatives of security and security depends on the phpMyAdmin privacy of access and credentials of information.	The three primary security principles are enhancing the accessibility of information and data, maintaining the integrity of data assets, and protecting confidentiality.
Privacy programs concentrate on protection personal information only like passwords, log-in credentials, etc.	The security programs defines the set of regulations and protocols to secure each confidential information resources and assets that an enterprise owns and collects.
Privacy can't be adept without security.	Security can be adept without privacy.