Unit 1

# Computer and Network Security

# Introduction to 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.
- Computer Security mainly focuses on three factors:
  I. Security Attacks
  II. Security Services
  III. Security Mechanisms

# Why is Computer Security Important?

- Cyber Crime is on the rise
- Damage is Significant
- Cyber Security builds trust
- Our identities protect our data
- Every organization has vulnerabilities.

# QUICK FACTS

- 95% of Computer Security breaches are due to human error.
- There is a hacker attack every 39 seconds
- Share prices fall 7.27% on average after a breach
- Approximately $6 trillion is expected to be spent globally on cybersecurity by 2021
- Unfilled cybersecurity jobs worldwide is already over 4 million

# Security threat and security attack

- Threat is a possible danger that might exploit vulnerability. The actions that cause it to occur are the security attacks.
- A security attack may be a passive attack or an active attack.
  - The aim of a passive attack is to get information from the system but it does not affect the system resources. Passive attacks are difficult to detect but can be prevented.
  - An active attack tries to alter the system resources or affect its operations. Active attack may modify the data or create a false data. Active attacks are difficult to prevent.

# Security Attacks on Users, Computer hardware and Computer Software

- Attacks on users could be to the identity user and to the privacy of user. Identity attacks result in someone else acting on your behalf by using personal information like password, PIN number in an ATM, credit card number, social security number etc. Attacks on the privacy of user involve tracking of users habits and actions—the website user visits, the buying habit of the user etc. Cookies and spam mails are used for attacking the privacy of users.
- Attacks on computer hardware could be due to a natural calamity like floods or earthquakes; due to power related problems like power fluctuations, etc or by destructive actions of a burglar.
- Software attacks harm the data stored in the computer. Software attacks may be due to malicious software, or, due to hacking. Malicious software or malware is a software code included into the system with a purpose to harm the system. Hacking is intruding into another computer or network to perform an illegal act.

This chapter will discuss the malicious software and hacking in detail.

# Basic Security Terminology

**Hacker Slang-** A *hacker* is an expert on a particular system or systems

1. A *white hat hacker*
2. A *black hat hacker*
3. A *gray hat hacker*

**Script Kiddies-** Someone who calls himself a hacker but lacks the expertise

**Ethical Hacking:** *sneaker/* Penetration Testers

**Phreaking-** One specialty type of hacking involves breaking into telephone systems.

The action of using mischievous and mostly illegal ways in order to not pay for some sort of telecommunications bill, order, transfer, or other service

**Professional Terms-** security professional terminology describes defensive barrier devices, procedures, and policies

**Security Devices-** The most basic security device is the *firewall*

A firewall is a barrier between a network and the outside world
A firewall filters traffic entering and exiting the network.

**Security Activities-**

- *Authentication*
- *Auditing*

# Concepts and Approaches

## Concepts

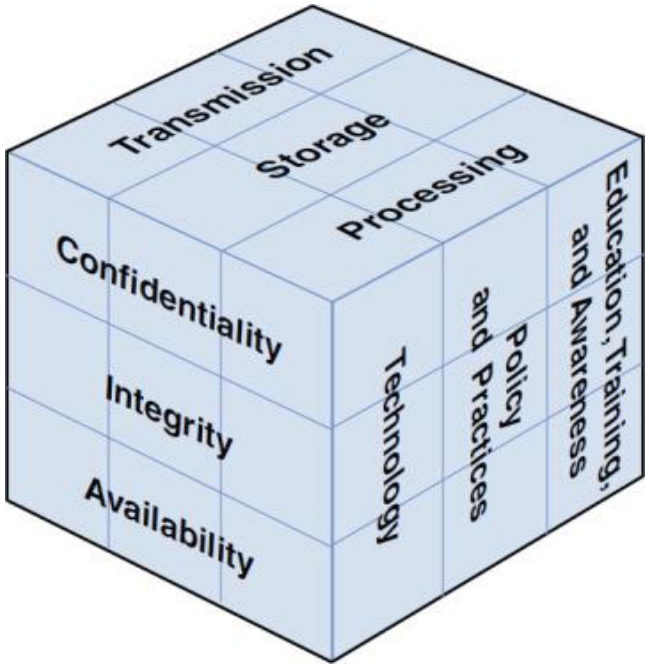
1. **CIA triangle**

   Refer to the three pillars of security: confidentiality, integrity, and availability

   1. Confidentiality : are you keeping the data confidential?
   2. Integrity : Does your approach help guarantee the integrity of data?
   3. Availability does your approach still make the data readily available to authorized users?

**2. McCumber cube:**

- A multi-faceted approach to describing security.
- A way of evaluating security of a network, looking at all aspects.
- It looks at security as a three-dimensional cube-
  1. Goals
  2. Information states
  3. Safeguards




**3. Least privileges**

Each user or service running on your network should have the least number of privileges/access required to do her job

# Approaches

1. Perimeter security approach-
    - The bulk of security efforts are focused on the perimeter of the network.
    - This focus might include firewalls, proxy servers, password policies, or any technology or procedure to make unauthorized access of the network less likely.
    - Little or no effort is put into securing the systems within the network.
    - In this approach, the perimeter is secured, but the various systems within that perimeter are often vulnerable.

2.Layered security approach-
    - Individual systems within the network are also secured.
    - All servers, workstations, routers, and hubs within the network are secure.
    - One way to accomplish this is to divide the network into segments and secure each segment as if it were a separate network.

# Online Security Resources

## CERT

The *Computer Emergency Response Team* (CERT; www.cert.org) is sponsored by Carnegie-Mellon University. CERT was the first computer incident-response team, and it is still one of the most respected in the industry.

## Microsoft Security Advisor

Because so many computers today run Microsoft operating systems, another good resource is the Microsoft Security Advisor website: https://www.microsoft.com/en-us/msrc?rtc=1. This site is a portal to all Microsoft security information, tools, and updates

## F-Secure

The F-Secure corporation maintains a website at www.f-secure.com. This site is, among other things, a repository for detailed information on virus outbreaks. Here you will find not only notifications about a particular virus but detailed information about the virus, such as how the virus spreads, and ways to recognize the virus, and, possibly, specific tools for cleaning an infected system of a particular virus

## SANS Institute

The SANS Institute website (www.sans.org) is a vast repository of security-related documentation. On this site you will find detailed documentation on virtually every aspect of computer security you can imagine.