# Computer & Network Security Concepts


Dr. Mana Khatua
Assistant Professor
Dept. of CSE, IIT Guwahati
Email: manaskhatua@iitg.ac.in

# Computer and Network Security

Computer and Network Security consists of:

"measures to deter, prevent, detect, and correct security violations that involve the transmission of information"

The NIST *Computer Security Handbook* defines the term *computer security* as:

"the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources"

(resources includes hardware, software, firmware, information/data, and telecommunications)

NIST: National Institute of Standards and Technology

# Fundamental Security Objectives

## Confidentiality

- Data confidentiality
  - ✓ Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
  - ✓ Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

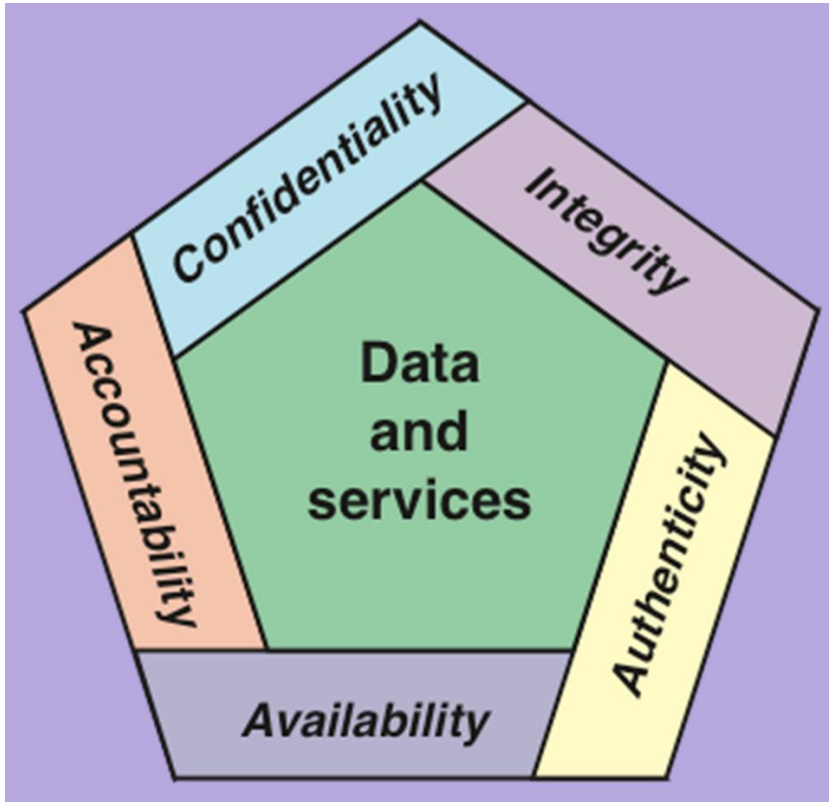
## Integrity

- Data integrity
  - ✓ Assures that information and programs are changed only in a specified and authorized manner
- System integrity
  - ✓ Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

## Availability

- Assures that systems work promptly and service is not denied to authorized users

# Essential Security Requirements




## Authenticity

- The property of being genuine and being able to be verified and trusted.
- This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

## Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
- Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

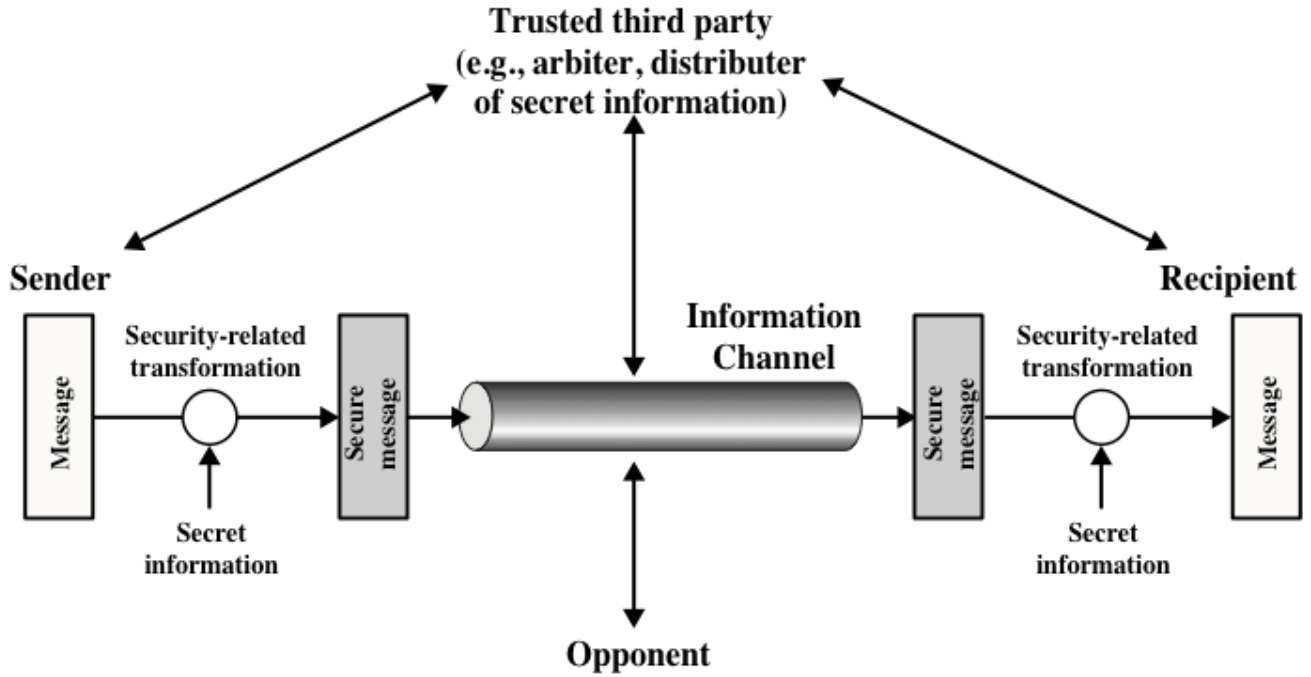
# Computer Security Challenges

- ✓Security is not simple !
- ✓Potential attacks on the security features need to be considered

- ✓Security mechanisms typically involve more than a particular algorithm or protocol

- ✓Security is essentially a battle of wits between a perpetrator and the designer
- ✓It is necessary to decide where to use the various security mechanisms
- ✓Requires constant monitoring
- ✓Strong security is often viewed as an impediment to efficient and user-friendly operation

# Network Security Model

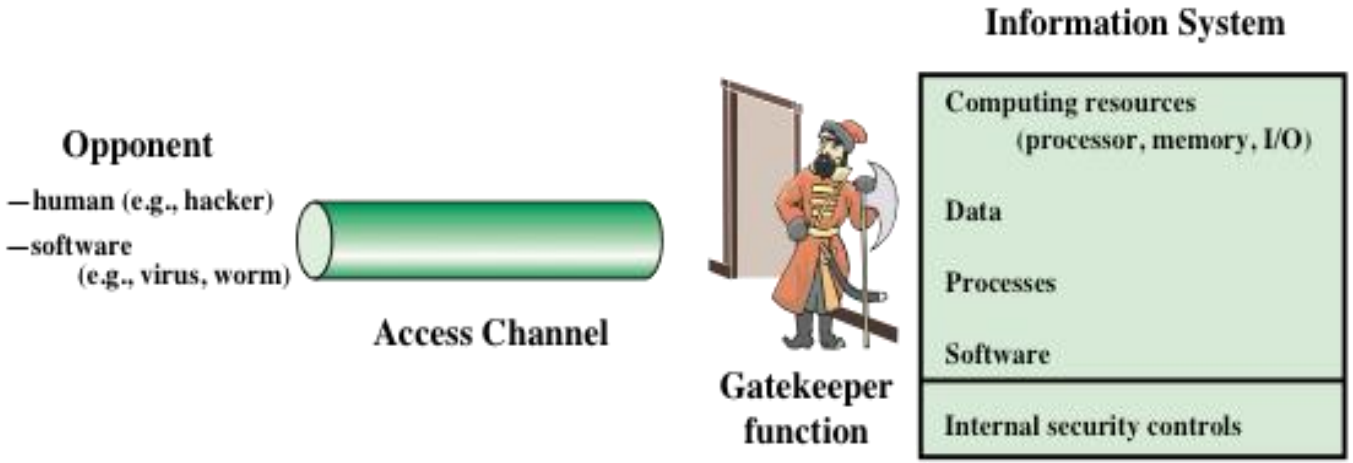



All the techniques for providing security have two components:

- A security-related transformation on the information to be sent
- Some secret information shared by the two principals and, it is hoped, unknown to the opponent.

A message is to be transferred from one party to another across some sort of Internet service.

# Network Access Security Model




The security mechanisms needed to cope with unwanted access fall into two broad categories:

- Like gatekeeper function (e.g. login procedure)
- Variety of internal controls that monitor activity and analyze stored information

A general model which reflects a concern for protecting an information system from unwanted access.

# OSI Security Architecture

- Security attack
  - Any action that compromises the security of information owned by an organization

- Security mechanism
  - A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack

- Security service
  - A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization

  - Intended to counter security attacks, and they make use of one or more security mechanisms to provide the service

# Threats and Attacks

the terms *threat* and *attack* are commonly used to mean more or less the same thing.

**Threat**

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

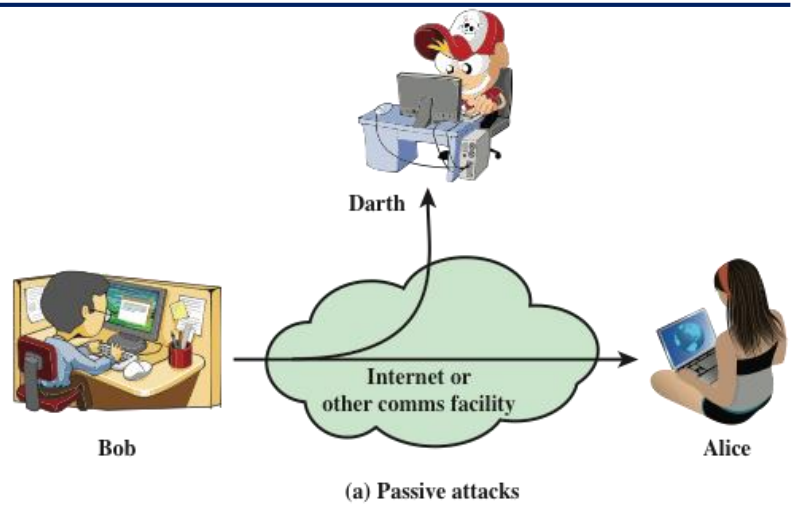
**Attack**

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

-- RFC 4949

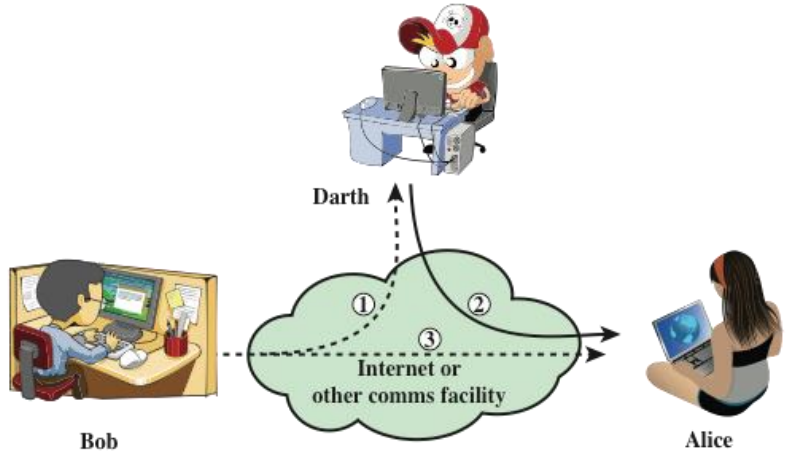
# Security Attacks

- A passive attack attempts to learn or make use of information from the system but does not affect system resources
  - Are in the nature of eavesdropping on, or monitoring of, transmissions
  - Goal is to obtain information that is being transmitted



(a) Passive attacks

- An active attack attempts to alter system resources or affect their operation
  - Goal is to do some modification of the data stream or the creation of a false stream



(b) Active attacks

# Types of Attacks

- Types of passive attacks
  - ✓ The **release of message contents**
    - Release of sensitive or confidential information.
  - ✓ **Traffic analysis**
    - observe the pattern of the messages
    - could observe the frequency and length of messages being exchanged
- Type of active attacks
  - ✓ **Masquerade**
    - Takes place when one entity pretends to be a different entity
  - ✓ **Replay**
    - Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
  - ✓ **Modification** of messages
    - Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect
  - ✓ Denial of Service (**DoS**)
    - Prevents or inhibits the normal use or management of communications facilities

# Security Services

## AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

**Peer Entity Authentication**

Used in association with a logical connection to provide confidence in the identity of the entities connected.

**Data-Origin Authentication**

In a connectionless transfer, provides assurance that the source of received data is as claimed.

## ACCESS CONTROL

The prevention of unauthorized use of a resource

(i.e., this service controls

- who can have access to a resource,
- under what conditions access can occur, and
- what those accessing the resource are allowed to do).

# Security Services

## DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

**Connection Confidentiality**

- The protection of all user data on a connection.

**Connectionless Confidentiality**

- The protection of all user data in a single data block.

**Selective-Field Confidentiality**

- The confidentiality of selected fields within the user data on a connection or in a single data block.

**Traffic-Flow Confidentiality**

- The protection of the information that might be derived from observation of traffic flows.

## NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

**Nonrepudiation, Origin**

✓ Proof that the message was sent by the specified party.

**Nonrepudiation, Destination**

✓ Proof that the message was received by the specified party.

# Security Services

## DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity

(i.e., contain no modification, insertion, deletion, or replay).

### Connection Integrity with Recovery

- Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

### Connection Integrity without Recovery

- As above, but provides only detection without recovery.

### Selective-Field Connection Integrity

- Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

### Connectionless Integrity

- Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

### Selective-Field Connectionless Integrity

- Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

# Security Mechanisms

**SPECIFIC SECURITY MECHANISMS**

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

**Encipherment**

The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

**Digital Signature**

Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

**Access Control**

A variety of mechanisms that enforce access rights to resources.

**Data Integrity**

A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

**Authentication Exchange**

A mechanism intended to ensure the identity of an entity by means of information exchange.

**Traffic Padding**

The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

**Routing Control**

Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

**Notarization**

The use of a trusted third party to assure certain properties of a data exchange.

# Security Mechanisms

## PERVASIVE SECURITY MECHANISMS

Mechanisms that are not specific to any particular OSI security service or protocol layer.

**Trusted Functionality**

That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

**Security Label**

The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

**Event Detection**

Detection of security-relevant events.

**Security Audit Trail**

Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

**Security Recovery**

Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

# Relationship: Security Services and Mechanisms

| SERVICE \ MECHANISM | Encipherment | Digital signature | Access control | Data integrity | Authentication exchange | Traffic padding | Routing control | Notarization |
|---|---|---|---|---|---|---|---|---|
| Peer entity authentication | Y | Y | | | Y | | | |
| Data origin authentication | Y | Y | | | | | | |
| Access control | | | Y | | | | | |
| Confidentiality | Y | | | | | | Y | |
| Traffic flow confidentiality | Y | | | | | Y | Y | |
| Data integrity | Y | Y | | Y | | | | |
| Nonrepudiation | | Y | | Y | | | | Y |
| Availability | | | | Y | Y | | | |

# Few Security related terms

### Malware

Viruses, worms, Trojans, and bots are all part of a class of software called malware or malicious code (malcode).

It is code or software that is specifically designed to damage, disrupt, steal, or in general inflict some other “bad” or illegitimate action on data, hosts, or networks.

### Virus

a type of malware that propagates by inserting a copy of itself into and becoming part of another program. It spreads from one computer to another, leaving infections as it travels.

the virus may exist on a system but will not be active or able to spread until a user or operating system(OS) runs or opens the malicious host file or program.

### Worms

they replicate functional copies of themselves and can cause the damage of the system.

To spread, worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them.

### Social Engineering

"any act that influences a person to take an action that may or may not be in their best interests.“ It is the psychological manipulation of people into performing actions .

e.g. Phishing SMS/Email: “your account is about to be suspended unless a link provided is clicked to update your card/account information”.

# Few Security related terms

### Trojan

It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems.

Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate. It creates back doors to give malicious users access to the system.

### Backdoors

A back door is an undocumented way of accessing a system, bypassing the normal authentication mechanisms.

### Exploit

Exploits are piece of software which are not always malicious in intent — they are sometimes used only as a way of demonstrating that a vulnerability exists.

### Bots

Bots often automate tasks and provide information or services that would otherwise be conducted by a human being.

A malicious bot is self-propagating malware designed to infect a host and connect back to a central server or servers that act as a command and control (C&C) center for an entire network of compromised devices, or "botnet."


Thank
You