Software and Computer Security

SOFE4840U

Lecture 01

Introduction

Dr. Khalid A. Hafeez

Winter, 24

Outline

- Computer Security
- Computer Asset
- Vulnerabilities
- Security Attacks
- Security Objectives (CIA triad)
- OSI Security Architecture [X.800]
- Model for Network Security
- Standards

Introduction

- What is computer security

- The protection (measures and actions) of the assets of a computer or an information system.
  - What assets do we need to protect?
  - How are those assets threatened?
  - What can we do to counter those threats?

What is Asset?

- Data & information
- Network and Infrastructure that support information
- People who use it

- Data & information
  - Printed or written on paper
  - Stored electronically or hard copy archived
  - Transmitted by using electronic means or by post
  - Oral, over the phone or in public

- How is been threatened?

Vulnerabilities

- Weakness in the security of the computer system or networks that can allow harm to occur
  - Policy flaws
  - Weak authentication
  - Protocol weaknesses
  - Lack of access control
  - Errors in programs
  - Misconfiguration
  - Inadequate physical protection

- The entity that takes advantage of the vulnerability is known as the *malicious actor*

Types of Security Attacks

- **Reconnaissance attacks**
  - Discovery process used to find information about the network, users, and victims.
  - Scan for IP addresses and port
  - Passive or active
  - Attacker can use tools such as Shodan, Maltego, Recon-ng, TheHarvester, Spiderfoot
  - Active reconnaissance is carried out by tools called *scanners*
- **Social engineering**
  - Done through email or misdirection of web pages
  - Phishing
  - Pharming
- **Privilege escalation attack**
  - Taking some level of access and achieving an even greater level of access

Types of Security Attacks

- **Backdoors**
  - Threat actors gain access to a system, they usually want future access as well
  - Install a backdoor application by users clicking something without realizing that the link they clicked is a threat
- **Buffer overflows and Code Execution**
  - stack-smashing protection, ASCII armoring
- **Man-in-the-middle attack**
  - can happen at Layer 2 or Layer 3
  - ARP poisoning ← dynamic Address Resolution Protocol (ARP) inspection (DAI)
  - Rogue router
- **Distributed Denial-of-service (DDoS)**
- **Route manipulation attacks**
- **Password attacks**

Why Need Security ?

Protecting Business

Regulatory Compliance

Providing Secure environment to work

Value to the Organization

NIST defines Computer Security as:

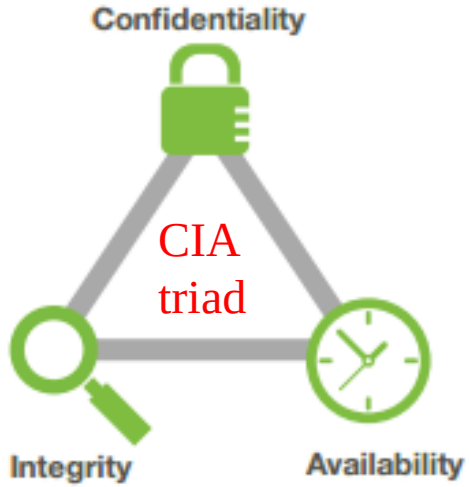
- Computer Security: Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.

- **Assets of a Computer System:**
  - Hardware: Including computer systems and other data processing, data storage, and data communications devices
  - Software: Including the operating system, system utilities, and applications.
  - Data: Including files and databases, as well as security-related data, such as password files.
  - Communication facilities and networks: Local and wide area network communication links, bridges, routers, and so on.

What are the key Security Objectives?

Confidentiality:

- Preserving authorized restrictions on information access and disclosure
- Protecting personal privacy and proprietary information.
- A loss of confidentiality is the unauthorized disclosure of information.
  - Data Confidentiality
  - Privacy



Integrity:

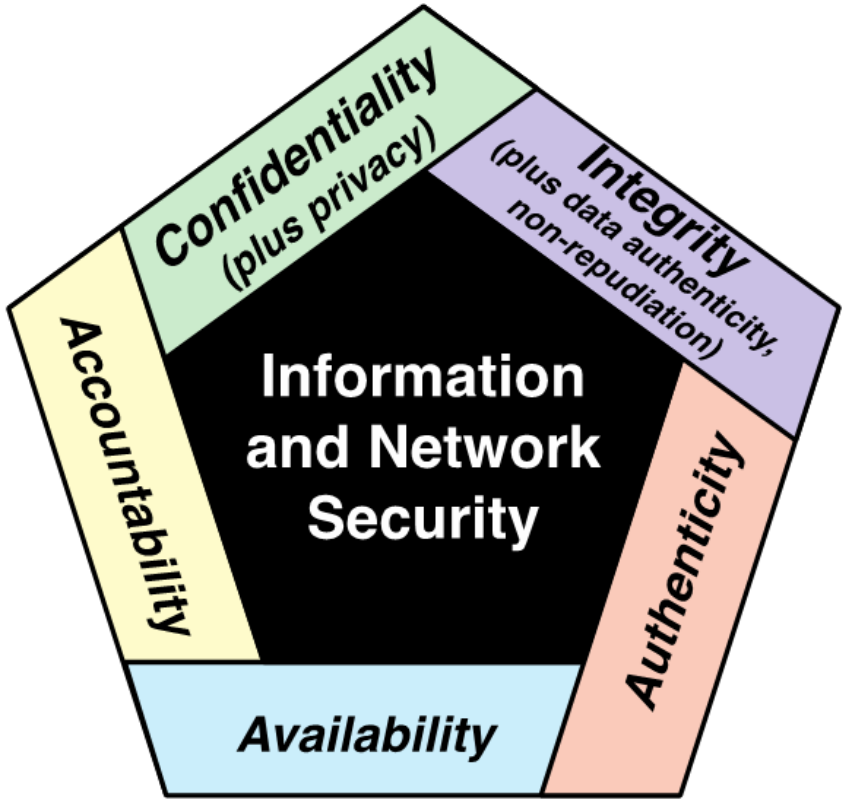
- Guarding against improper modification or destruction.
- Ensuring information nonrepudiation and authenticity.
- A loss of integrity is the unauthorized modification or destruction of information.
  - Data integrity
  - System integrity

Availability:

- Assures that systems work promptly and service is not denied to authorized users.
- A loss of availability is the disruption of access to or use of information or an information system.

CIA Triad

- **We can add two properties to the CIA triad:**
  - **Authenticity**
    - 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



Levels of Impact on Organization and Individuals

Low

The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals

Moderate

The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals

High

The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

Examples of Security Requirements

Confidentiality

Student grade information is an asset whose confidentiality is considered to be highly important by students and parents

Student enrollment information may have a moderate confidentiality rating

Integrity

Patient information stored in a database – inaccurate information could result in serious harm or death to a patient and expose the hospital to massive liability

A Web site that offers a forum to registered users to discuss some specific topic would be assigned a moderate level of integrity

An example of a low-integrity requirement is an anonymous online poll

Availability

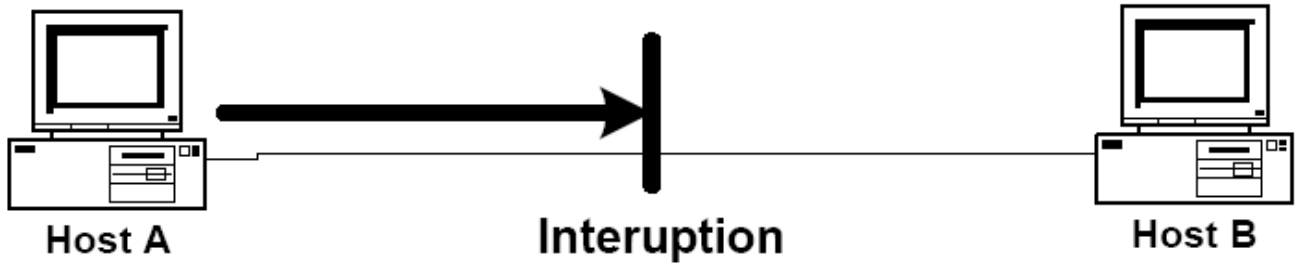
The more critical a component or service, the higher the level of availability required

A moderate availability requirement is a public Web site for a university

An online telephone directory lookup application would be classified as a low-availability requirement

Interruption

An asset of the system is destroyed or becomes unavailable or unusable.



An attack on –

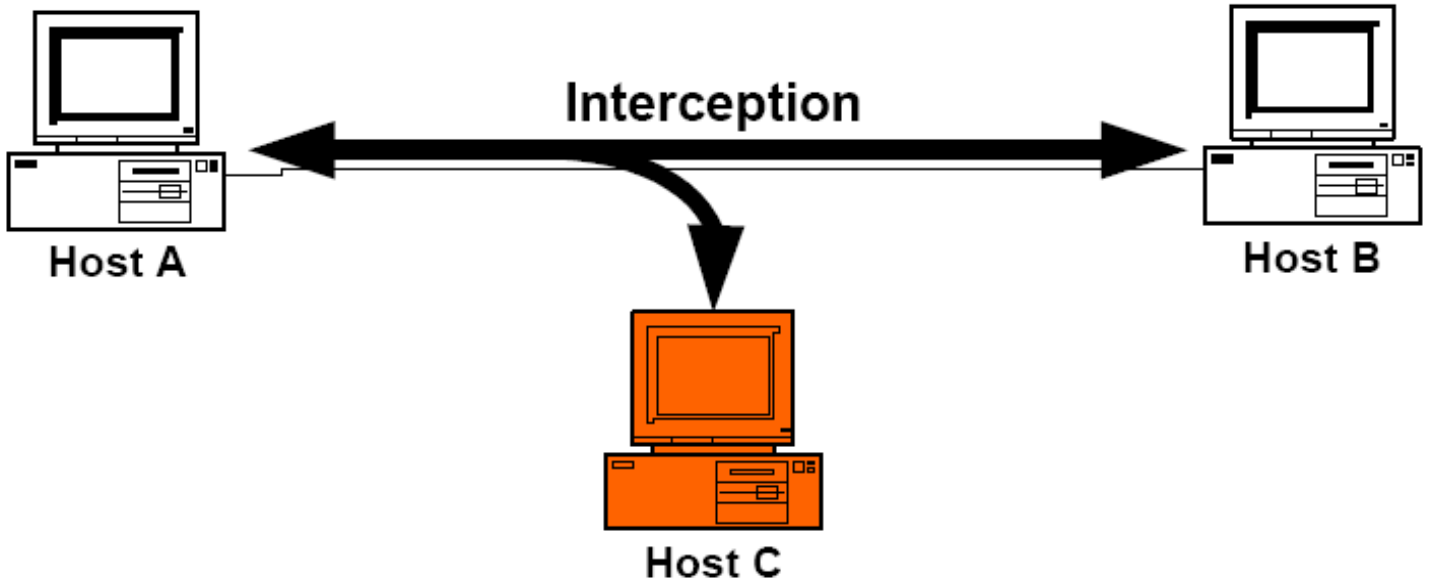
the ***availability***.

Examples:

- Cutting of a communication link.
- Systems services (web, ftp) unavailable

Interception

An unauthorized party gains access to an asset.



An attack on –

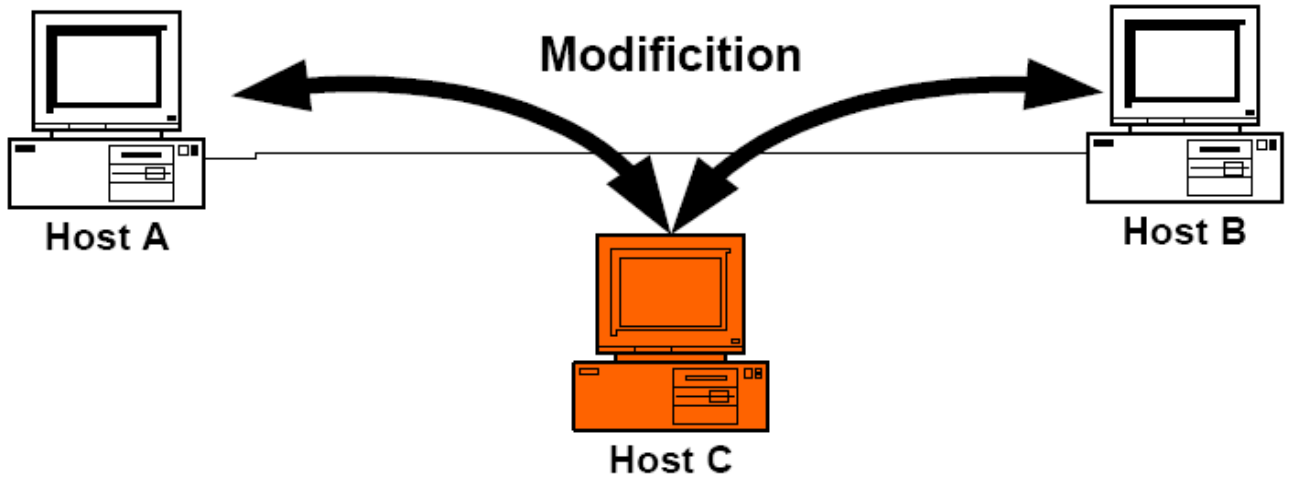
confidentiality.

Examples:

- wiretapping to capture data in a network.
- the illicit copying of files or programs.

Modification

An unauthorized party not only gains access to but tampers with an asset.



This is an attack on --

Integrity.

Examples:

- changing values in a data file
- altering a program so that it performs differently,
- modifying the content of a message being transmitted in a network.

Security Measures Should Ensure

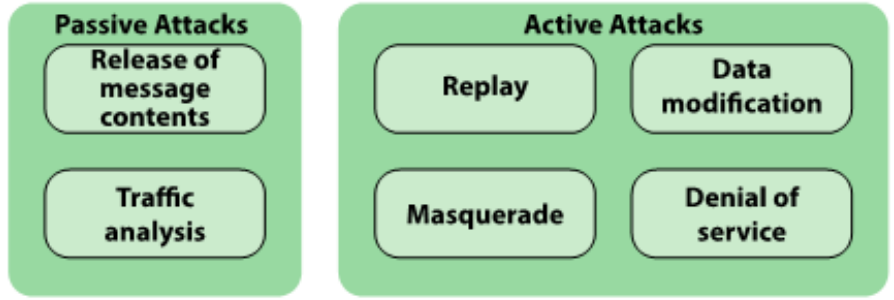
- Users can perform only authorized tasks.
- Users can obtain only authorized information.
- Users cannot cause damage to the data, applications, or operating environment of a system.
- The system can track user actions and the network resources those actions access.

Computer Security Challenges:

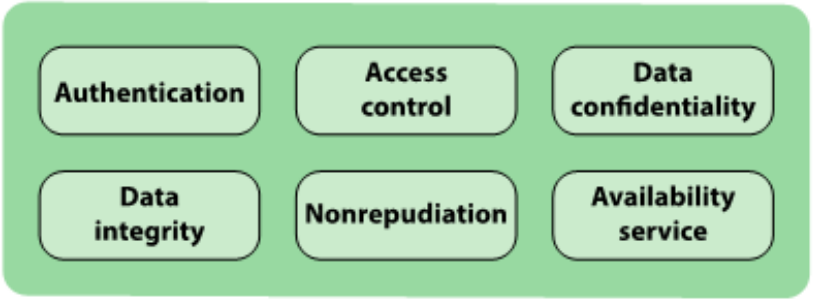
1. Computer security is not as simple as it might first appear to the novice
2. Potential attacks on the security features must be considered
3. Procedures used to provide particular services are often counterintuitive
4. Physical and logical placement needs to be determined
5. Additional algorithms or protocols may be involved
6. Attackers only need to find a single weakness, the developer needs to find and eliminate all weaknesses
7. Users and system managers tend to not see the benefits of security until a failure occurs
8. Security requires regular and constant monitoring
9. Is often an afterthought to be incorporated into a system after the design is complete
10. Thought of as an impediment to efficient and user-friendly operation

OSI Security Architecture [X.800]

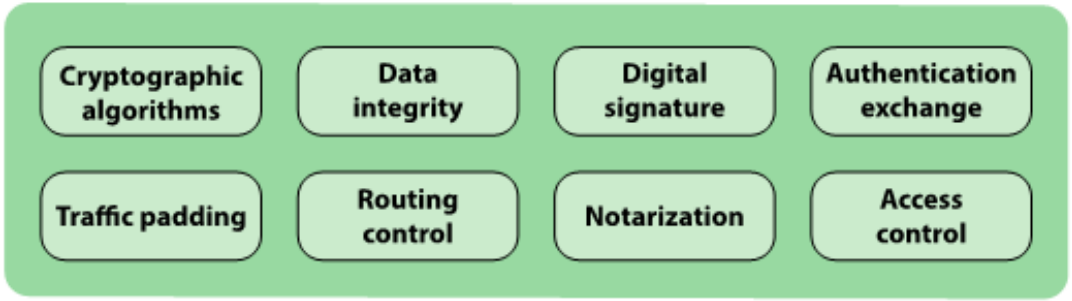
- **Security attack**
  - Any action that compromises the security of information owned by an organization
- Security mechanism
  - A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack
- Security service
  - A processing or communication 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



(a) Attacks



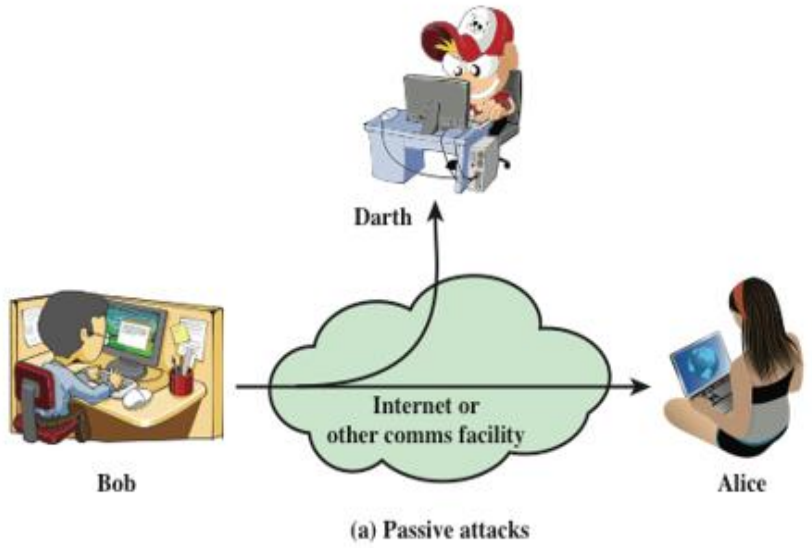
(b) Services



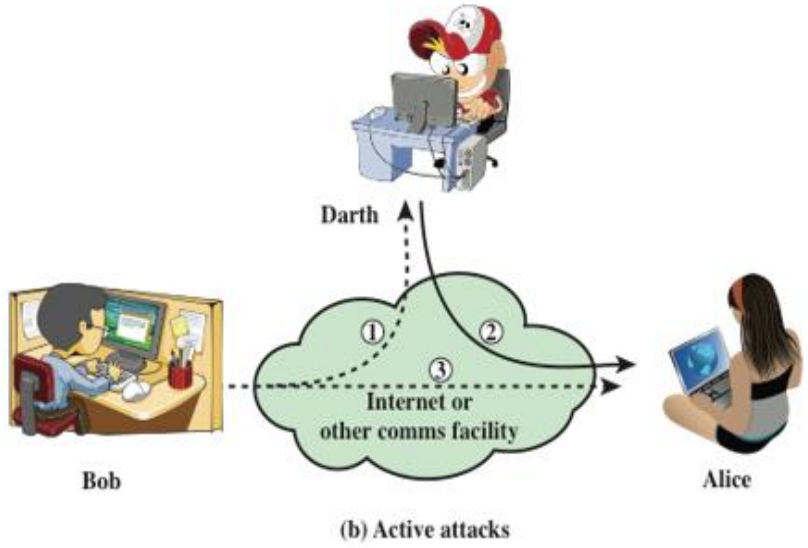
(c) Mechanisms

SECURITY ATTACKS

- **Passive attacks**: attempts to learn or make use of information from the system but does not affect system resources.
  - Eavesdropping or monitoring
  - Goal of the opponent is to obtain information that is being transmitted
  - Two types of passive attacks are:
    - The release of message contents
    - Traffic analysis
- **Active attacks**: attempts to alter system resources or affect their operation
  - Goal is to detect attacks and to recover from any disruption or delays caused by them
  - Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
  - Types of active attacks are:
    - masquerade
    - replay
    - modification of messages
    - denial of service



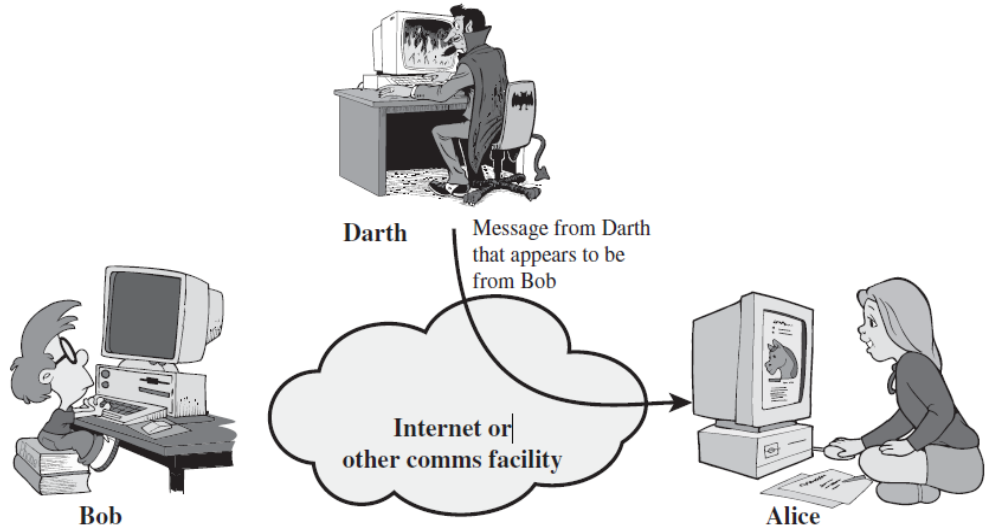
(a) Passive attacks



(b) Active attacks

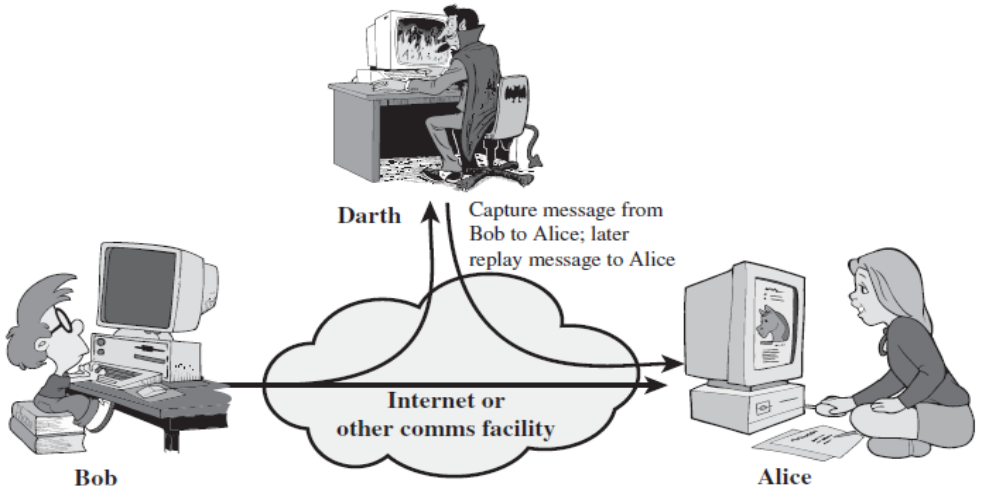
Types of Active Attacks

- Masquerade:
  - Takes place when one entity pretends to be a different entity
  - Usually includes one of the other forms of active attack



Masquerade

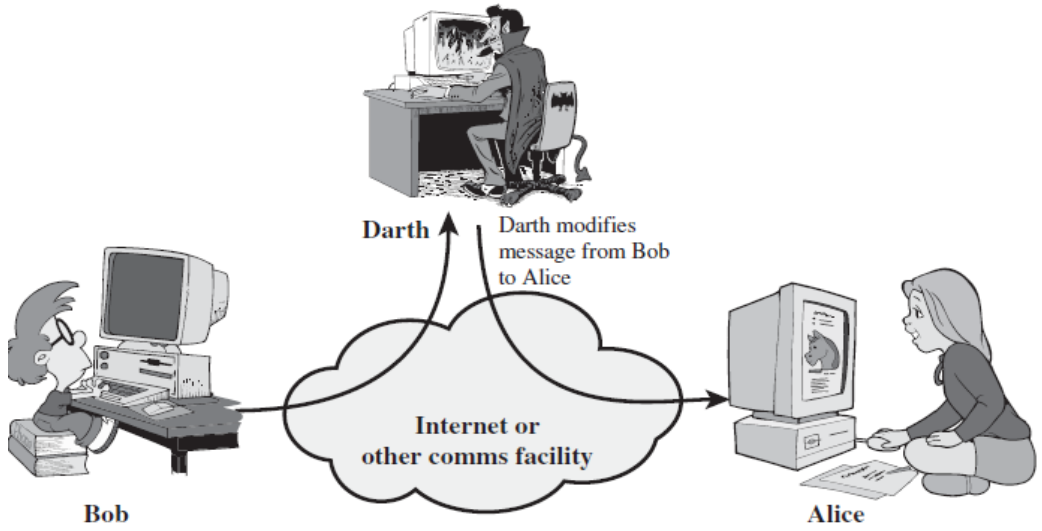
- Replay:
  - Involves the passive capture of a data unit and its subsequent retransmission
  - Produce an unauthorized effect (delay or repeat)



Replay

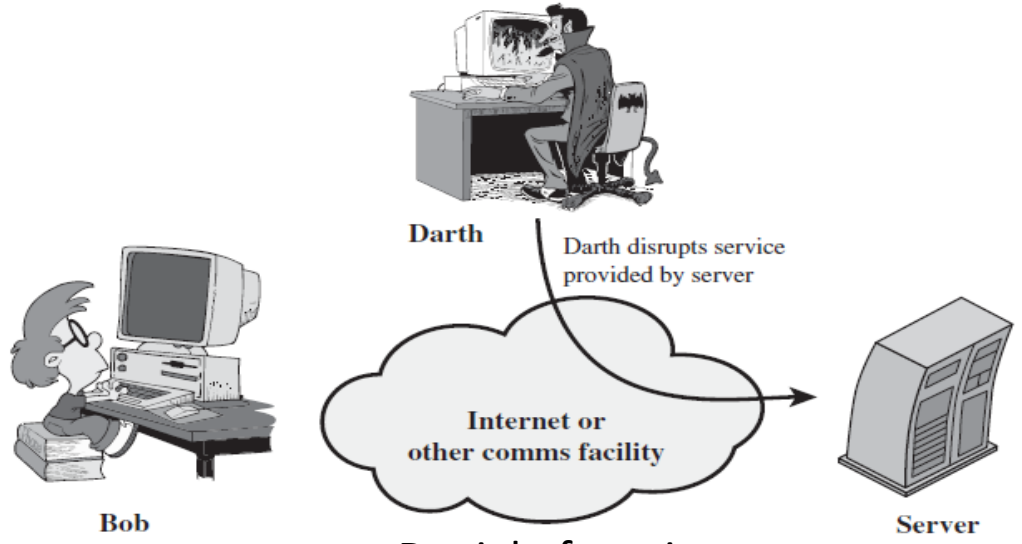
Types of Active Attacks

- Modification of messages:
  - Some portion of a legitimate message is altered
  - Reordered to produce an unauthorized effect



Modification of messages

- Denial of service:
  - Prevents or inhibits the normal use or management of communications facilities



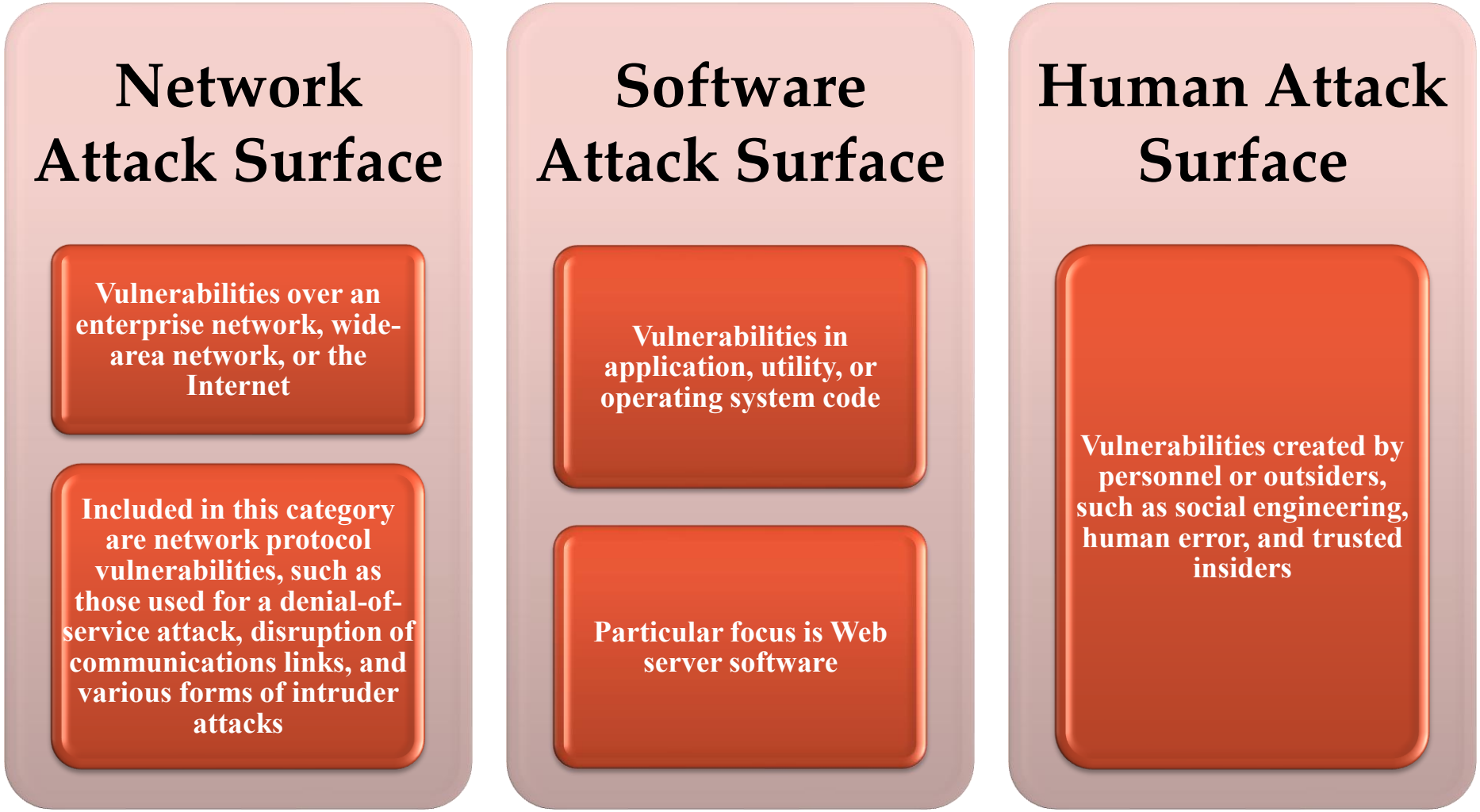
Denial of service

Attackers

- **Who are attackers?**
  - Computer criminals: Convicted or Not convicted
    - Individuals
    - Organized, Worldwide Groups
    - Organized Crime
    - Terrorists
- **What does a cyber criminal look like?**
  - Villains
  - Mentally derange
  - Tempted by personal profit, revenge,…
- **Donn Parker…**
  - "Hackers are characterized by an **immature, excessively idealistic attitude** … They delight in presenting themselves to the media as idealistic do-gooders, champions of the underdog."
- **The author of Tribal Flood Network (TFN)…**
  - It seems that the attackers are pretty **clueless people** who misuse powerful resources and tools for generally **harmful and senseless** activities just "**because they can**."

Attack Surfaces

- **Attack surfaces can be categorized in the following way:**



Attack Surfaces

- The use of layering, or defense in depth, and attack surface reduction complement each other in mitigating security risk.

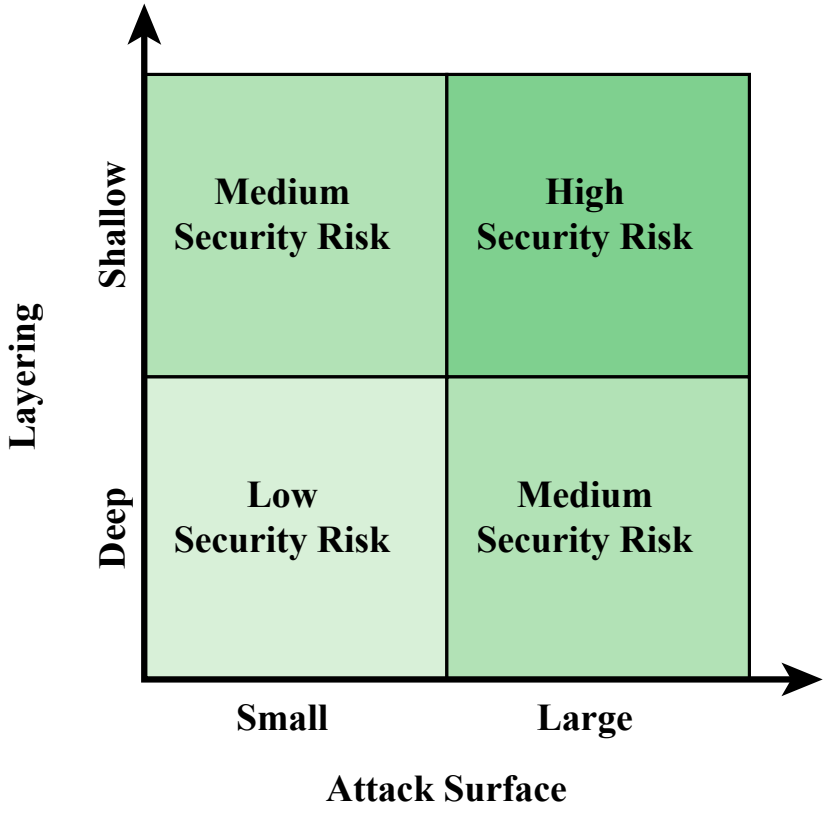


Figure 1.3 Defense in Depth and Attack Surface

Security Services

- A processing or communication service provided by a system to give a specific kind of protection to system resources (RFC 4949)
- X.800 Service Categories:
  - Authentication
  - Access control
  - Data confidentiality
  - Data integrity
  - Nonrepudiation
  - Availability

Security Services (X.800)

- **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.
      - Two entities are considered peers if they implement the same protocol in different systems
    - **Data-Origin Authentication**
      - In a connectionless transfer (such as email), 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 condition access can occur, and what those accessing the resource are allowed to do).
  - The ability to limit and control the access to host systems and applications via communications links

Security Services (X.800)

- **Data Confidentiality**
  - The protection of transmitted data from passive attacks
    - Broadest service protects all user data transmitted between two users over a period of time
    - Narrower forms of service includes the protection of a single message or even specific fields within a message
  - The protection of traffic flow from analysis
    - This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility

Security Services (X.800)

- **Data Integrity**
  - The assurance that data received as exactly as sent by an authorized entity (i.e., contains 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.
  - **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 the user data of a data block; takes the form of determination of whether the selected fields have been modified.

Security Services (X.800)

- **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.
- **Availability**
  - Protects a system to ensure its availability
  - Depends on proper management and control of system resources

Security Mechanisms - X.800

- **Specific security mechanisms**
  - Incorporated into the appropriate protocol layer in order to provide some of the OSI security services.
- **Pervasive security mechanisms**
  - Mechanisms that are not specific to any particular OSI security service or protocol layer.

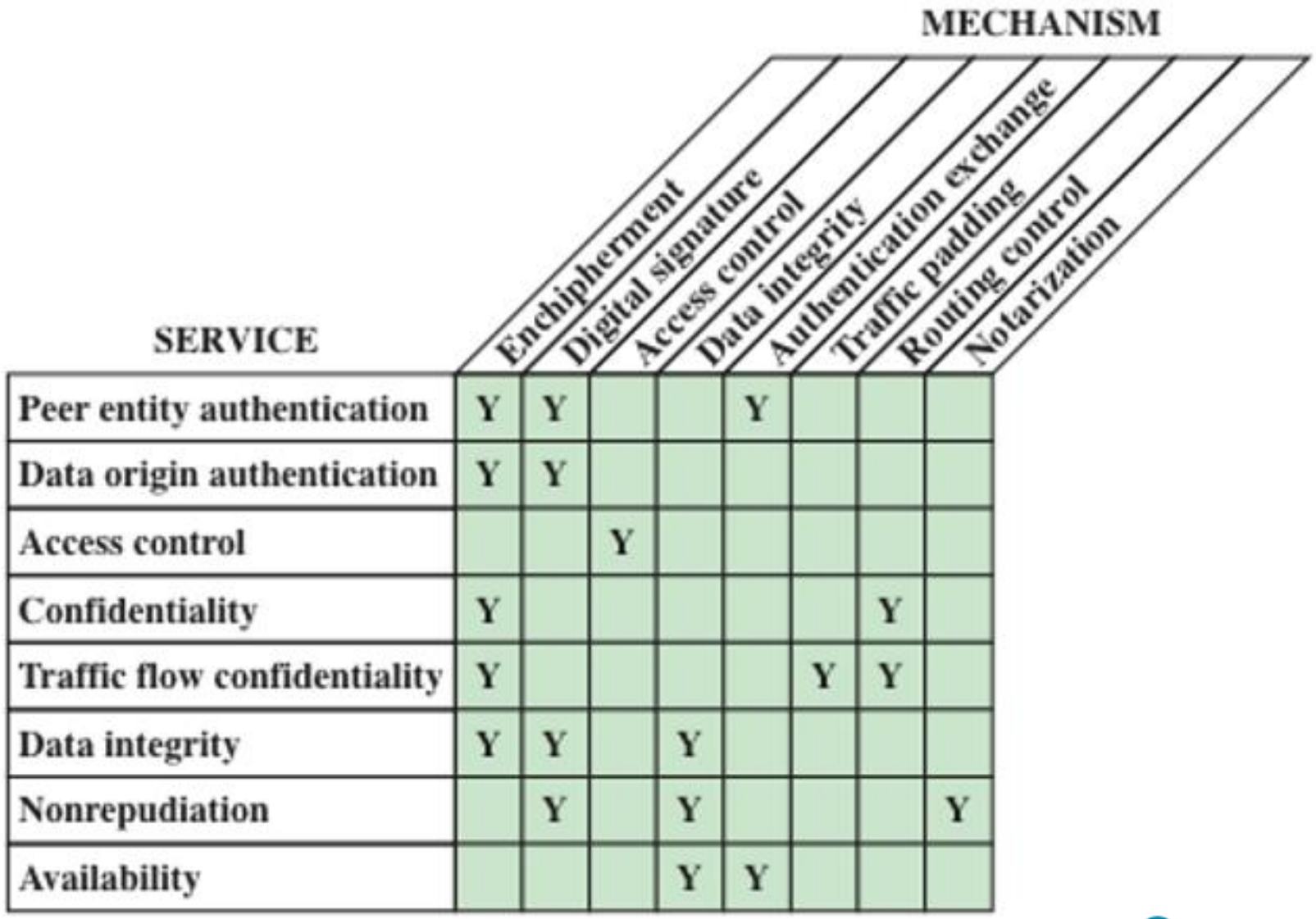
Security Mechanisms - X.800

- **Encipherment/Cryptographic algorithms**
  - *Reversible cryptographic mechanisms*
    - Encryption algorithm that allows data to be encrypted and subsequently decrypted
  - *Irreversible cryptographic mechanisms.*
    - Hash algorithms
    - Message authentication codes
- **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.
- **Data integrity**
  - This category covers a variety of mechanisms used to assure the integrity of a data unit or stream of data units.
- **Access Control**
  - A variety of mechanisms that enforce access rights to resources.

Security Mechanisms - X.800

- **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

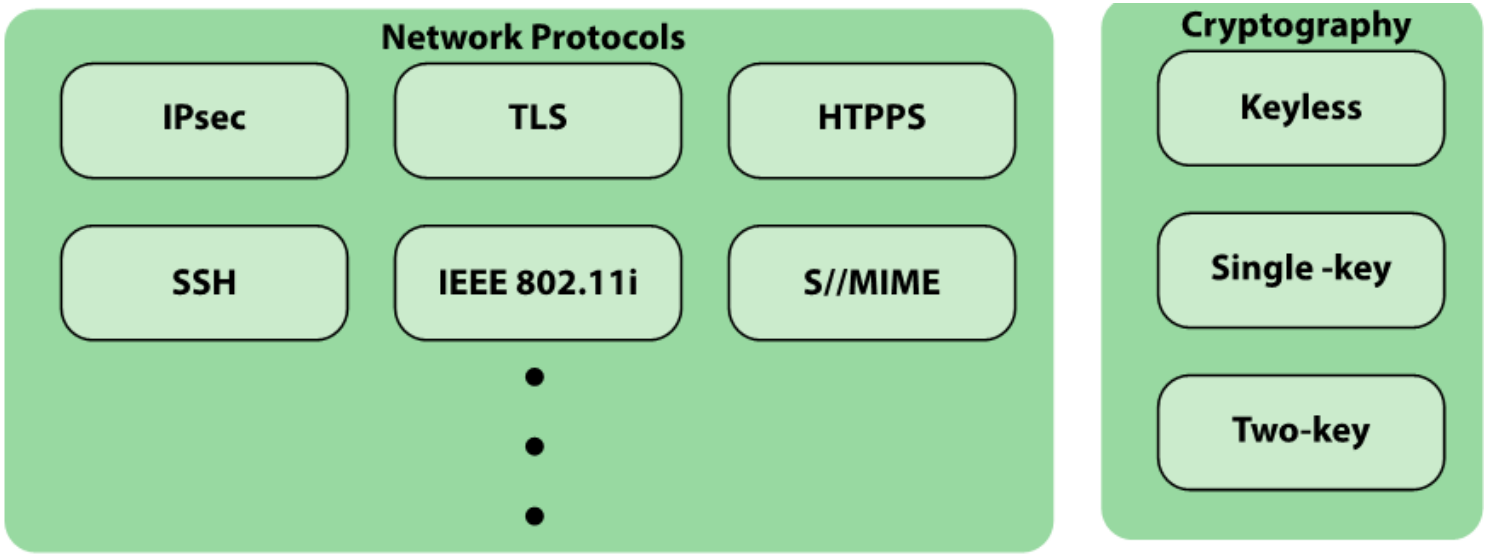
Relationship Between Security Services and Mechanisms



SERVICE \ MECHANISM	Enchipherment	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			

Network Security

- Communications Security
  - Deals with the protection of communications through the network, including measures to protect against both passive and active attacks
  - Communications security is primarily implemented using network protocols
  - With respect to network security, a security protocol may be an enhancement that is part of an existing protocol or a standalone protocol



(a) Communications Security

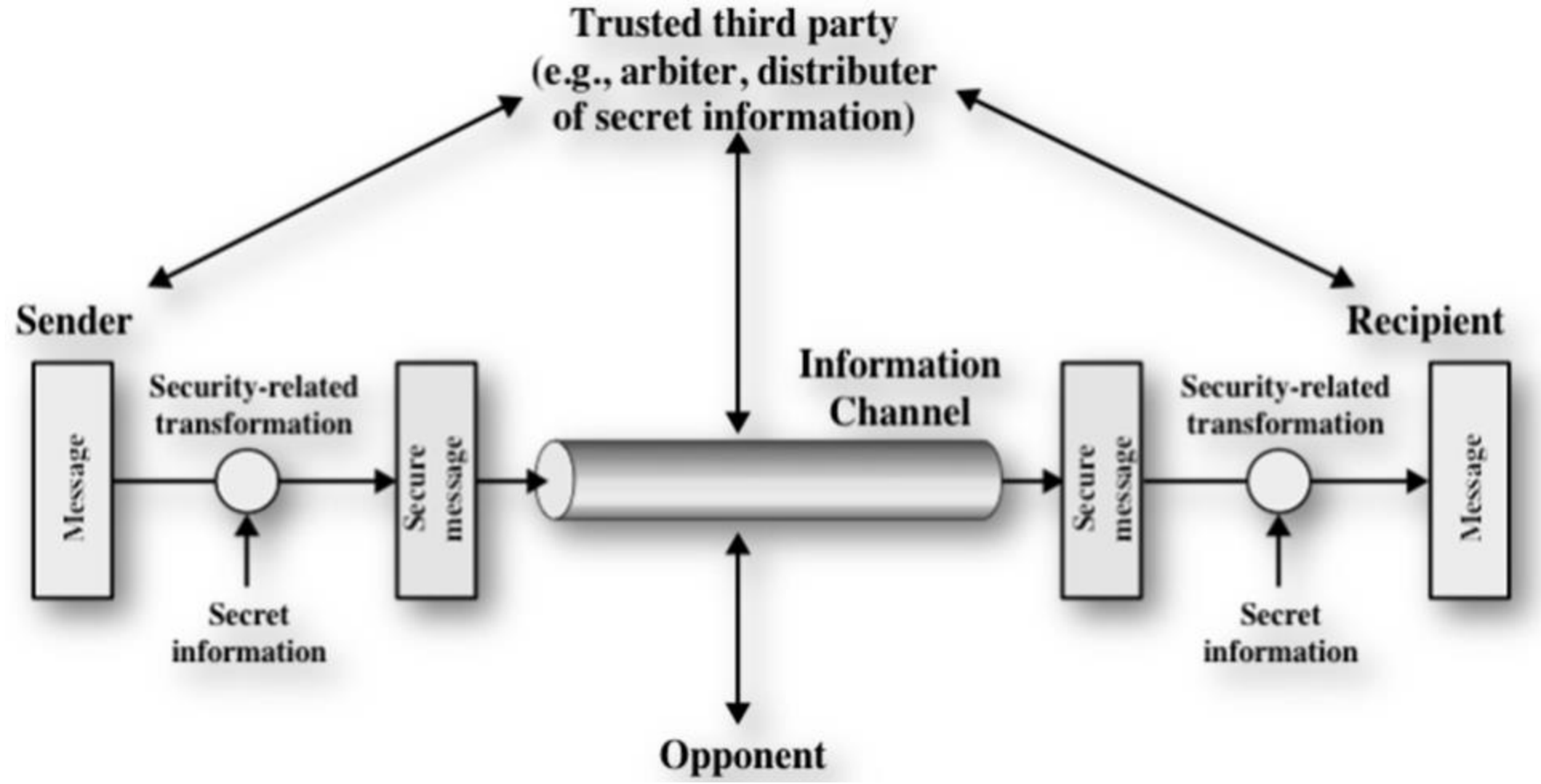
Network Security

Device Security

- Protection of network devices and end systems.
- The primary security concerns are intruders that gain access to the system to perform unauthorized actions, insert malicious software, or overwhelm system resources to diminish availability
- **Three types of device security are:**

1. **Firewall**
   - A hardware and/or software capability that limits access between a network and device attached to the network, in accordance with a specific security policy.
2. **Intrusion detection**
   - Hardware or software products that finds attempts to access system resources in an unauthorized manner
   - Provide real-time or near-real-time warning
3. **Intrusion prevention**
   - Hardware or software products designed to detect intrusive activity and attempt to stop the activity.

Model for Network Security



Cybersecurity

- A process of protecting information by preventing, detecting, and responding to attacks.
- Build on traditional information security programs but also include the following:
  - Cyber risk management and oversight
  - Threat intelligence and information sharing
  - Threat hunting (proactively looking for potential compromises and threats in your organization that have not been detected by your security products or technologies)
  - Third-party organization, software, and hardware dependency management
  - Incident response and resiliency

Security Wheel for Enterprise

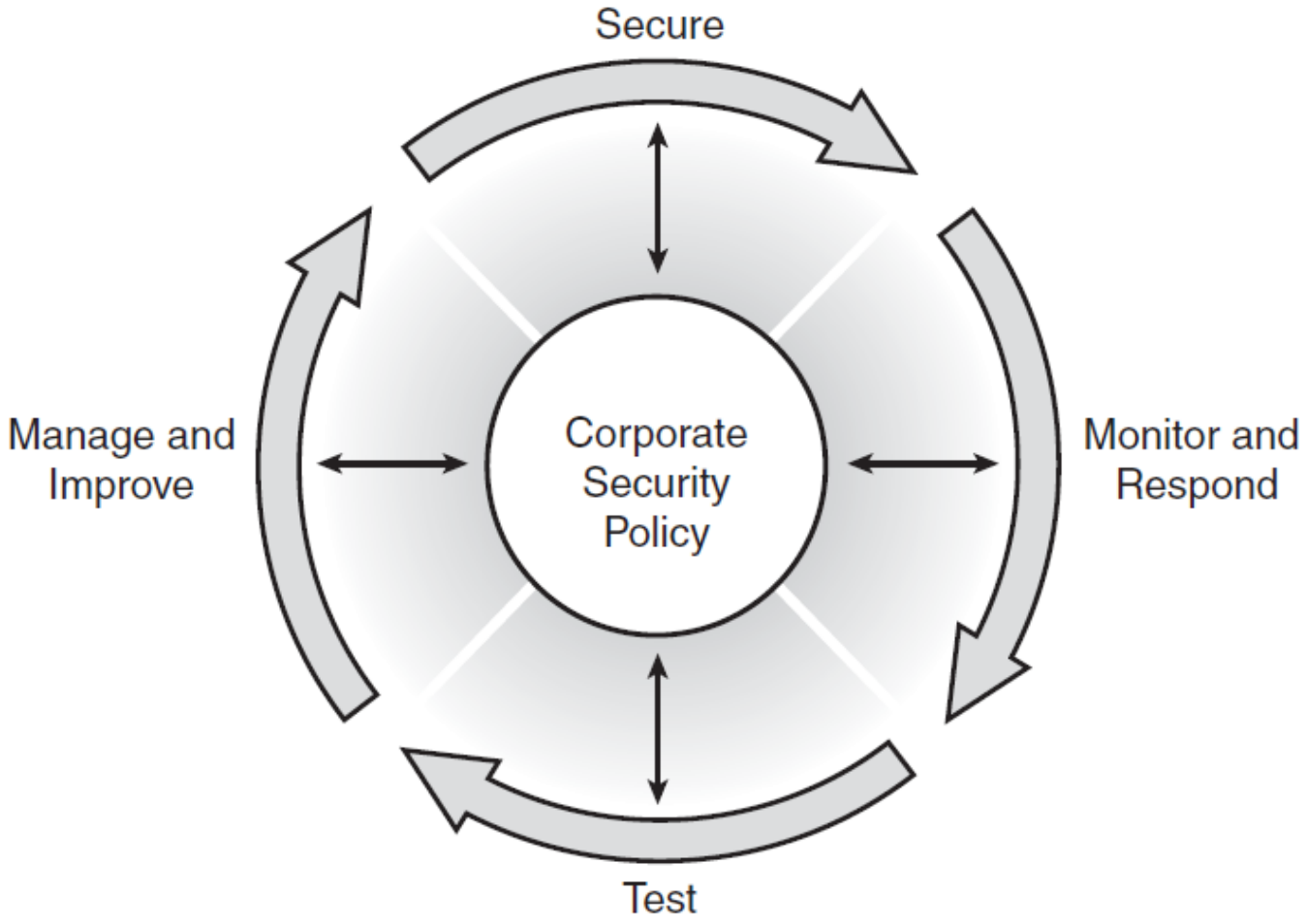
Step 1 Develop a security policy

Step 2 Make the network secure

Step 3 Monitor and respond.

Step 4 Test.

Step 5 Manage and improve.



Security policy

- Is a formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources

- In developing a security policy, a security manager needs to consider the following factors:
  - The value of the assets being protected
  - The vulnerabilities of the system
  - Potential threats and the likelihood of attacks

- The security manger should take the following trade-offs:
  - Ease of use versus security
  - Cost of security versus cost of failure and recovery

Standards

National Institute of Standards and Technology:

- NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private-sector innovation. Despite its national scope, NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact

Internet Society:

- ISOC is a professional membership society with worldwide organizational and individual membership. It provides leadership in addressing issues that confront the future of the Internet and is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). These organizations develop Internet standards and related specifications, all of which are published as Requests for Comments (RFCs).

ITU-T:

- The International Telecommunication Union (ITU) is an international organization within the United Nations System in which governments and the private sector coordinate global telecom networks and services. The ITU Telecommunication Standardization Sector (ITU-T) is one of the three sectors of the ITU. ITU-T's mission is the development of technical standards covering all fields of telecommunications. ITU-T standards are referred to as Recommendations

ISO:

- The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies from more than 140 countries, one from each country. ISO is a nongovernmental organization that promotes the development of standardization and related activities with a view to facilitating the international exchange of goods and services and to developing cooperation in the spheres of intellectual, scientific, technological, and economic activity. ISO's work results in international agreements that are published as International Standards