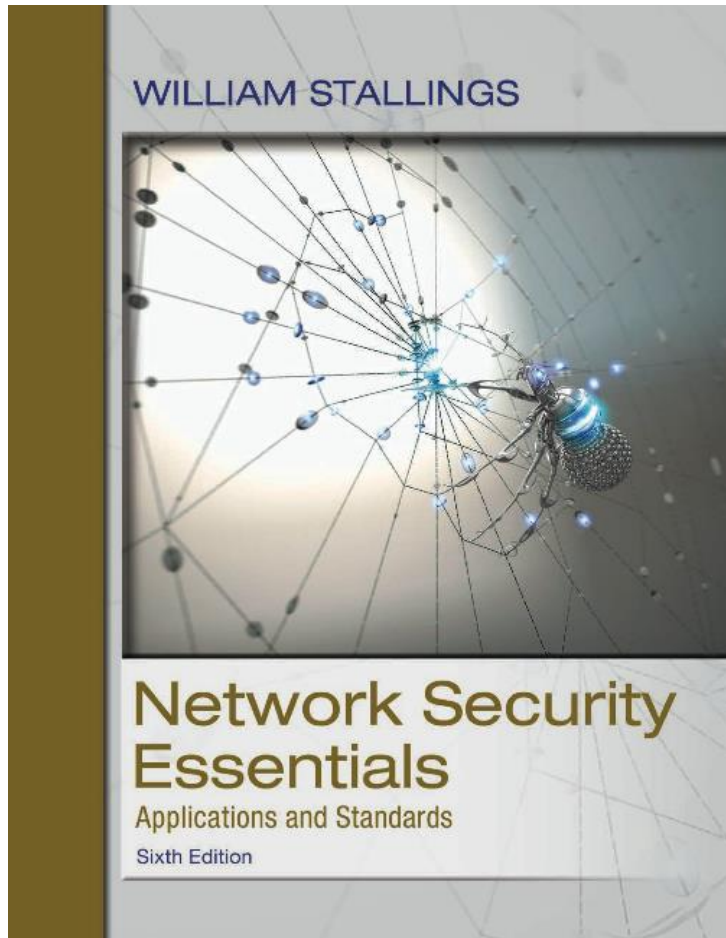


# Network Security Essentials: Applications and Standards

Sixth Edition



## Chapter 1

### Introduction

# Computer Security-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** (includes hardware, software, firmware, information/data, and telecommunications)”

# Computer Security Objectives (1 of 3)

**Confidentiality:** Keeping information **secret and private**, ensuring that only authorized users can access it.

- 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

# Computer Security Objectives (2 of 3)

## 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

# Computer Security Objectives (3 of 3)

## Availability

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

# Possible additional concepts:

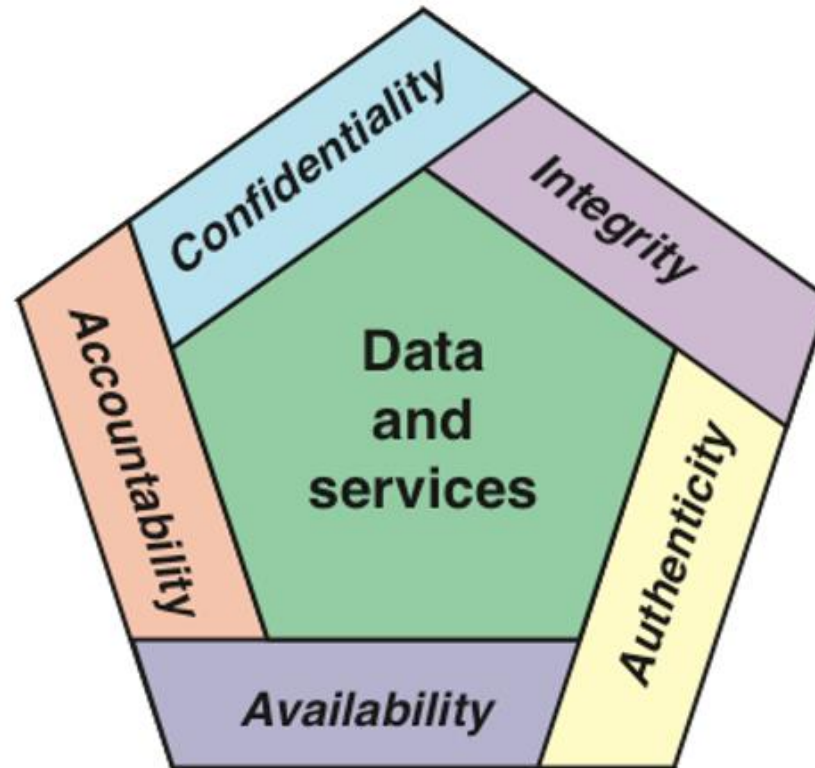
## **Authenticity**

- Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

## **Accountability**

- Actions in a system can be traced back to the responsible entity.

# CIA Triad



**Figure 1-1** Essential Network and Computer Security Requirements

# Examples of Security Requirements (1 of 3)

## Confidentiality

- Student grade information is an asset whose confidentiality is considered to be highly important by students
- Regulated by the Family Educational Rights and Privacy Act (FERPA)

# Examples of Security Requirements (2 of 3)

## 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

# Examples of Security Requirements (3 of 3)

## Availability

- The more critical a component or service, the higher the level of availability required. Some popular websites are examples: [www.amazon.com](http://www.amazon.com), [www.google.com](http://www.google.com).

# OSI Security Architecture (1 of 2)

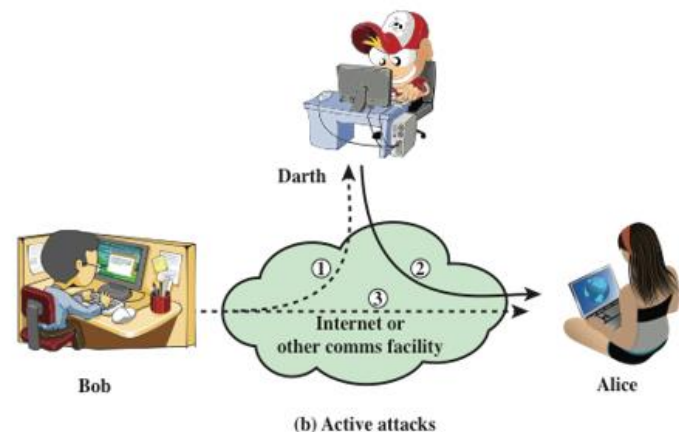
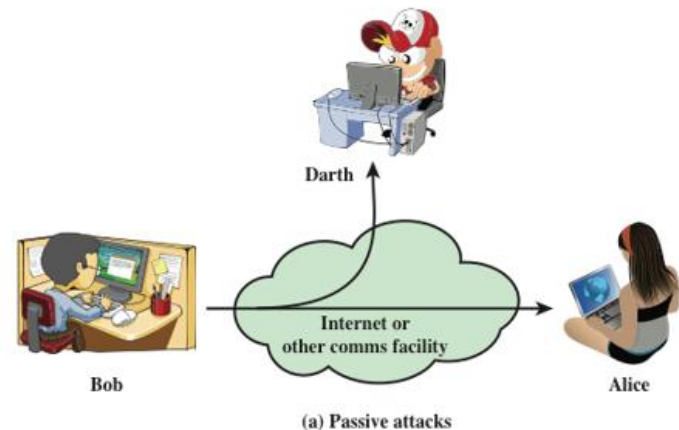
- Developed by the International Telecommunication Union (ITU-T) in Recommendation X.800.
- A systematic framework for understanding and designing network security
- Define **security attacks**, **security mechanisms**, and **security services** and shows how they are related.

# OSI Security Architecture (2 of 2)

- Security attack
  - Any action that compromises the security of information owned by an organization
  - In the literature, the terms security attack and security threat often have a similar meaning.
- 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 by preventing or detecting security attacks.
  - A security service makes use of one or more security mechanisms.

# Security Attacks

- A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of **passive attacks** and **active attacks**
- A **passive attack** attempts to learn or make use of information from the system but does not affect system resources
- An **active attack** attempts to alter system resources or affect their operation



# Passive Attacks

- Are in the nature of eavesdropping on, or monitoring of, transmissions
- 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 (1 of 3)

- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them



# Active Attacks (2 of 3)

## Masquerade

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

## Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect



# Active Attacks (3 of 3)

## 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

- Prevents or inhibits the normal use or management of communications facilities



# Security Services

- Defined by X.800 as:
  - A service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers

# X.800 Service Categories

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Nonrepudiation



# Authentication (1 of 2)

- Ensures that the entity (user or system) is who they claim to be.
  - In the case of a single message, assures the recipient that the message is from the source that it claims to be from
  - In the case of ongoing interaction, assures the two entities are authentic and that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties

# Authentication (2 of 2)

**Two specific authentication services are defined in X.800:**

- **Peer entity authentication**
- **Data origin authentication**

# Access Control

- Prevents unauthorized use of resources
  - The ability to limit and control the access to host systems and applications via communications links
  - To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual



# Data Confidentiality



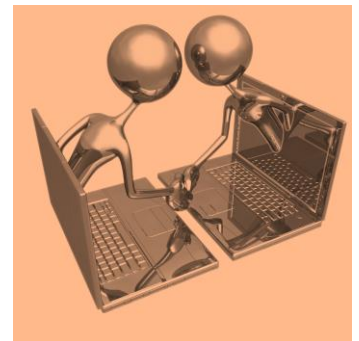
- Protects data from unauthorized disclosure.
  - The protection of transmitted data from passive attacks
  - The protection of traffic flow from analysis
    - This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility

# Data Integrity

- Protects data from unauthorized modification.
  - Can apply to a stream of messages, a single message, or selected fields within a message
  - Connection-oriented integrity service deals with a stream of messages and assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays
  - A connectionless integrity service deals with individual messages without regard to any larger context and generally provides protection against message modification only

# Nonrepudiation

- Prevent entities from denying their action
  - When a message is sent, the receiver can prove that the alleged sender in fact sent the message
  - When a message is received, the sender can prove that the alleged receiver in fact received the message



# Availability

- Ensures that resources are accessible when needed.
  - Addresses the security concerns raised by denial-of-service attacks
  - Depends on proper management and control of system resources

# Specific Security Mechanisms (X.800) (1 of 4)

- Security mechanisms are technical methods and processes to implement security services and counter security attacks. Following are some specific security mechanisms in X.800.

**Encipherment** converts data into unreadable form

- 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.

# Specific Security Mechanisms (X.800) (2 of 4)

**Digital Signature:** provides authentication, integrity and non-repudiation

- 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:** restricts access to resources

- A variety of mechanisms that enforce access rights to resources.

# Specific Security Mechanisms (X.800) (3 of 4)

**Data Integrity:** detect and recover from data modification

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

**Authentication Exchange:** verify identities using credentials

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

**Traffic Padding:** add extra data to conceal message pattern.

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

# Specific Security Mechanisms (X.800) (4 of 4)

**Routing Control:** selects secure network paths

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

**Notarization:** use a trusted third party to confirm data

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

# Table 1-4 Relationship Between 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			

# Pervasive (general) Security Mechanisms (1 of 2)

- Security mechanisms that provide overall support for system-wide security, not specific to any particular OSI security service or protocol layer.

## Trusted Functionality

- Only trustworthy modules are used to maintain system integrity.

# Pervasive (general) Security Mechanisms (1 of 2)

## Event Detection

- Detect abnormal or unauthorized activities in real time.  
Example: IDS

## Security Audit Trail

- Keeps records of security-relevant events for later review. Data collected and potentially used to facilitate a security audit.

## Security Recovery

- Ensures the system can recover after a security breach or failure. Examples: backup, failover system.

# Fundamental Security Design Principles (1 of 8)

- The National Centers of Academic Excellence in Information Assurance/Cyber Defense, which is jointly sponsored by the U.S. Department of Homeland Security, list the following as fundamental security design principles

# Fundamental Security Design Principles (2 of 8)

- Economy of mechanism
  - The design of security measures embodied in both hardware and software should be as simple and small as possible
- Fail-safe default
  - Access decisions should be based on permission rather than exclusion-the default situation is lack of access, and the protection scheme identifies conditions under which access is permitted

# Fundamental Security Design Principles (3 of 8)

- Complete mediation
  - Every access must be checked against the access control mechanism
- Open design
  - The design of a security mechanism should be open rather than secret
- Separation of privilege
  - A practice in which multiple privilege attributes are required to achieve access to a restricted resource

# Fundamental Security Design Principles (4 of 8)

- Least privilege
  - Every process and every user of the system should operate using the least set of privileges necessary to perform the task
- Least common mechanism
  - The design should minimize the functions shared by different users, providing mutual security

# Fundamental Security Design Principles (5 of 8)

- Psychological acceptability
  - Implies that the security mechanisms should not interfere unduly with the work of users, while at the same time meeting the needs of those who authorize access
- Isolation
  - A principle that applies in three contexts: first, public access systems should be isolated from critical resources to prevent disclosure to tampering; second, the processes and files of

# Fundamental Security Design Principles (6 of 8)

- individual users should be isolated from one another except where it is explicitly desired; third, security mechanisms should be isolated from one another.
- Encapsulation
  - Viewed as a specific form of isolation based on object-oriented functionality

# Fundamental Security Design Principles (7 of 8)

- Modularity
  - Refers both to the development of security functions as separate, protected modules and to the use of a modular architecture for mechanism design and implementation
- Layering
  - Refers to the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems

# Fundamental Security Design Principles (8 of 8)

- Least astonishment
  - A program or user interface should always respond in the way that is least likely to astonish the user

# Attack surface (1 of 3)

- Consists of the reachable and exploitable vulnerabilities in a system
  - Examples:
    - Open ports on outward facing Web and other servers, and code listening on those ports
    - Services available on the inside of a firewall
    - Code that processes incoming data, e-mail, XLM, office documents, and industry-specific custom data exchange formats
    - Interfaces, SQL, and Web forms

# Attack surface (2 of 3)

- An employee with access to sensitive information vulnerable to a social engineering attack
- Can be categorized in the following way:
  - Network attack surface
    - This category refers to vulnerabilities over an enterprise network, wide-area network, or Internet
  - Software attack surface
    - Vulnerabilities in application, utility, or operating system code

# Attack surface (3 of 3)

- Human attack surface
  - Refers to vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders
- A common practice is to minimize attack surface (to maximize security).

# Summary (1 of 2)

- Computer security concepts
  - Definition
  - Examples
- The OSI security architecture
- Security attacks
  - Passive attacks
  - Active attacks
- Security mechanisms
  - Encipherment
  - Digital signature
  - Access control
  - Data integrity mechanisms
  - Authentication exchange
  - Traffic padding
  - Routing control
  - Notarization

# Summary (2 of 2)

- Security services
  - Authentication
  - Access control
  - Data confidentiality
  - Data integrity
  - Nonrepudiation
  - Availability service
- Attack surfaces

# Copyright



**This work is protected by United States copyright laws and is provided solely for the use of instructors in teaching their courses and assessing student learning. Dissemination or sale of any part of this work (including on the World Wide Web) will destroy the integrity of the work and is not permitted. The work and materials from it should never be made available to students except by instructors using the accompanying text in their classes. All recipients of this work are expected to abide by these restrictions and to honor the intended pedagogical purposes and the needs of other instructors who rely on these materials.**