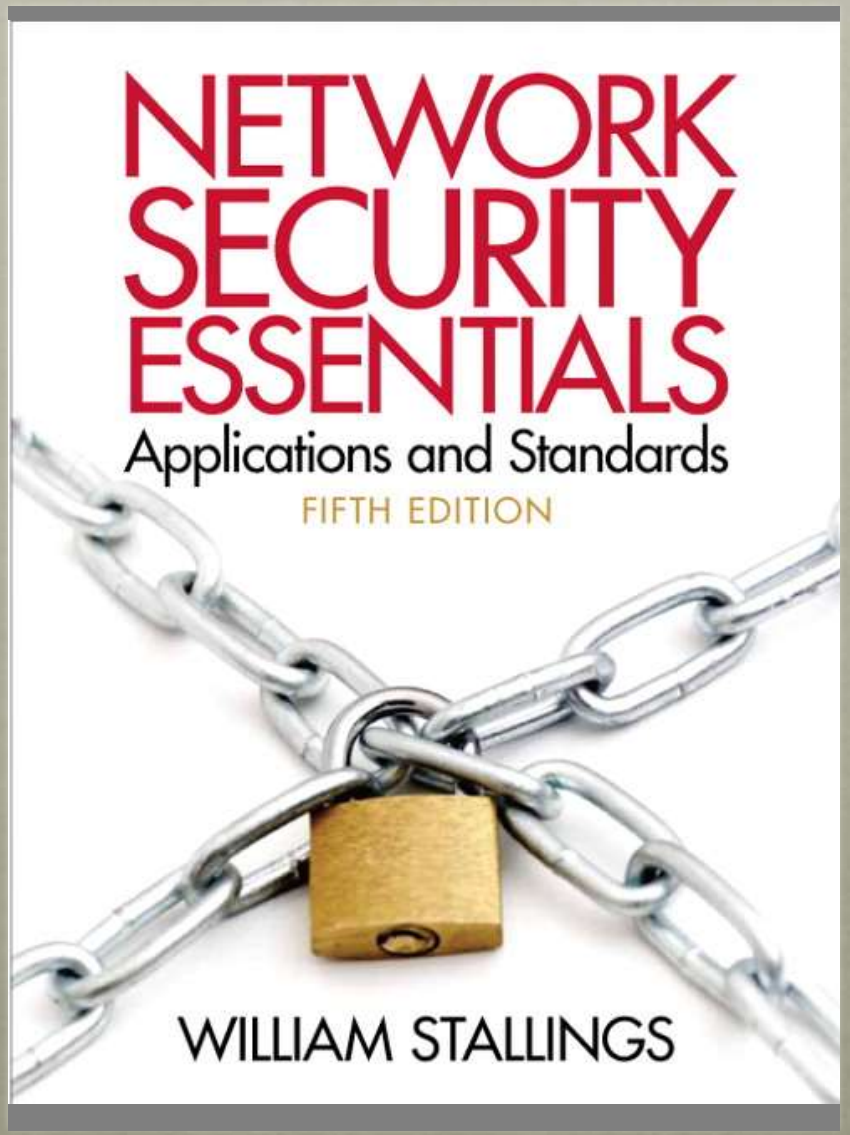
NETWORK SECURITY ESSENTIALS

Fifth Edition

by William Stallings



CHAPTER 1

Introduction

The combination of space, time, and strength that must be considered as the basic elements of this theory of defense makes this a fairly complicated matter. Consequently, it is not easy to find a fixed point of departure.

— *On War,* Carl Von Clausewitz

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

—*The Art of War,* Sun Tzu

COMPUTER SECURITY CONCEPTS

- Before the widespread use of data processing equipment, the security of information valuable to an organization was provided primarily by physical and administrative means
- With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident
- Another major change that affected security is the introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer and between computer and computer
- Computer security
  - The generic name for the collection of tools designed to protect data and to thwart hackers
- internet security (lower case "i" refers to any interconnected collection of network)
  - Consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information

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

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

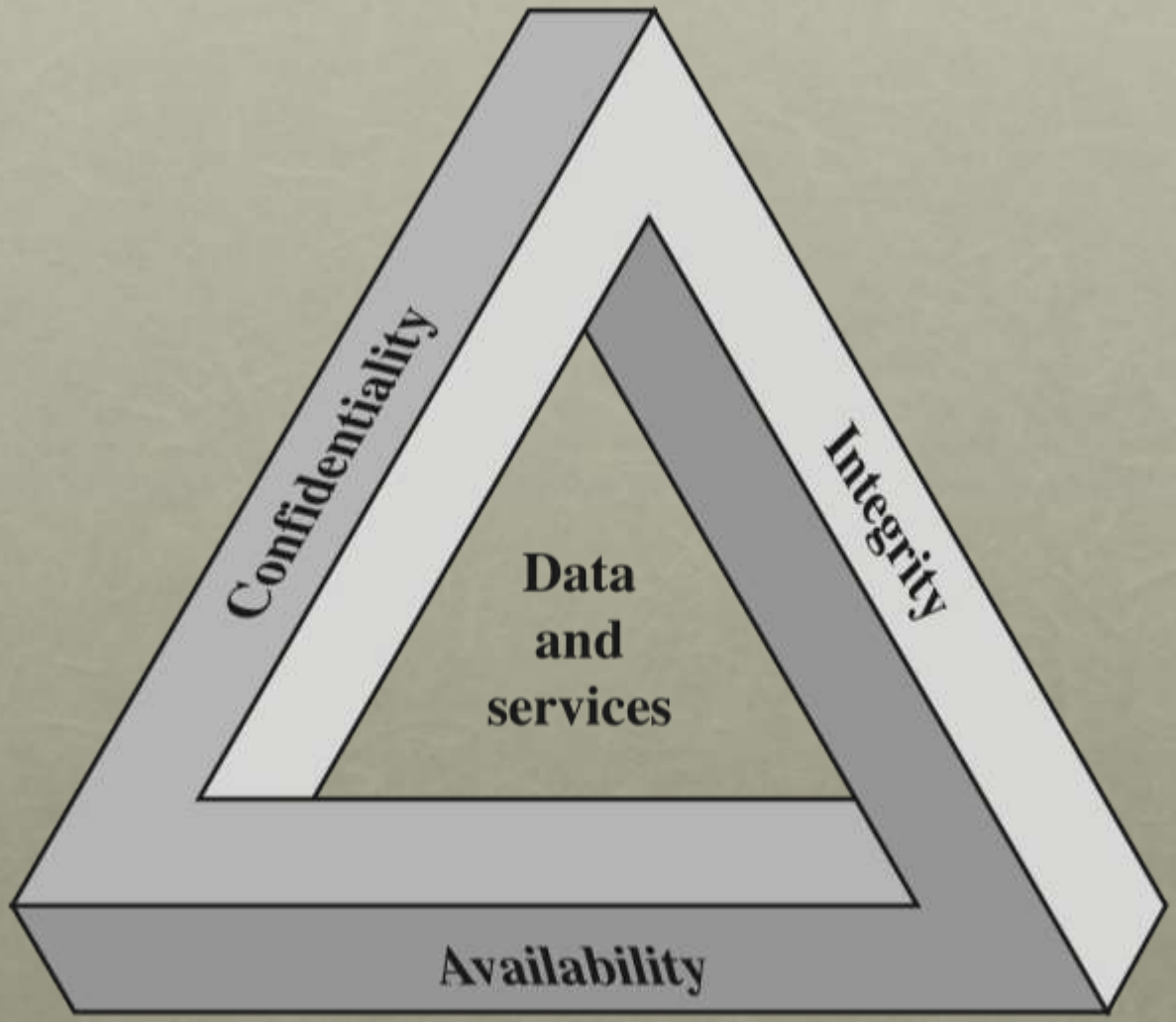
Integrity

- 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

CIA TRIAD


Confidentiality
Integrity
Data
and
services
Availability

Possible Additional Concepts:

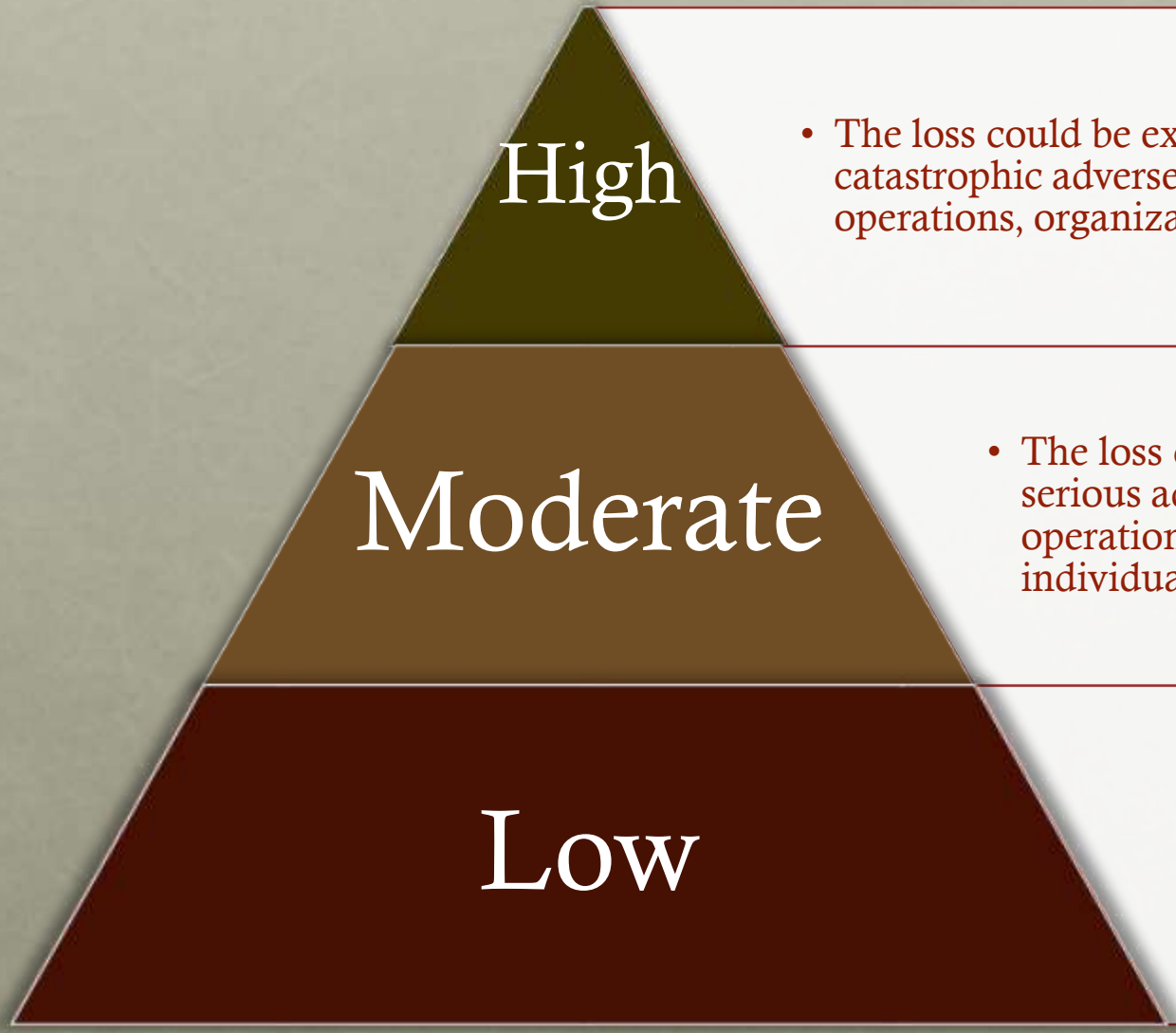
Authenticity

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

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity

BREACH OF SECURITY LEVELS OF IMPACT



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

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

- The loss could be expected to have a limited 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

Regulated by the Family Educational Rights and Privacy Act (FERPA)

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

COMPUTER SECURITY CHALLENGES

- Security is not simple
- Potential attacks on the security features need to be considered
- Procedures used to provide particular services are often counter-intuitive
- It is necessary to decide where to use the various security mechanisms
- Requires constant monitoring
- Is too often an afterthought
- Security mechanisms typically involve more than a particular algorithm or protocol
- Security is essentially a battle of wits between a perpetrator and the designer
- Little benefit from security investment is perceived until a security failure occurs
- Strong security is often viewed as an impediment to efficient and user-friendly operation

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

TABLE 1.1
THREATS AND ATTACKS (RFC 4949)

Threat

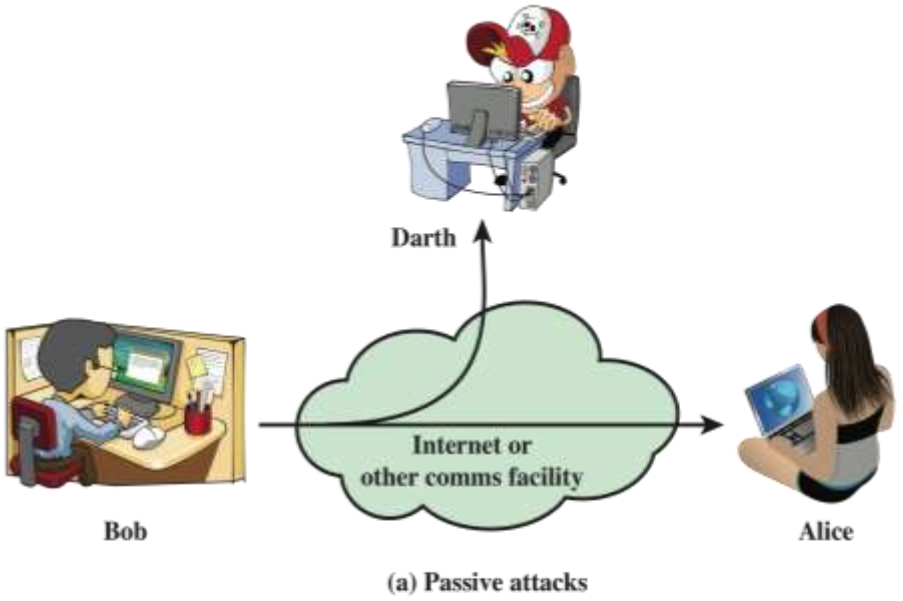
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

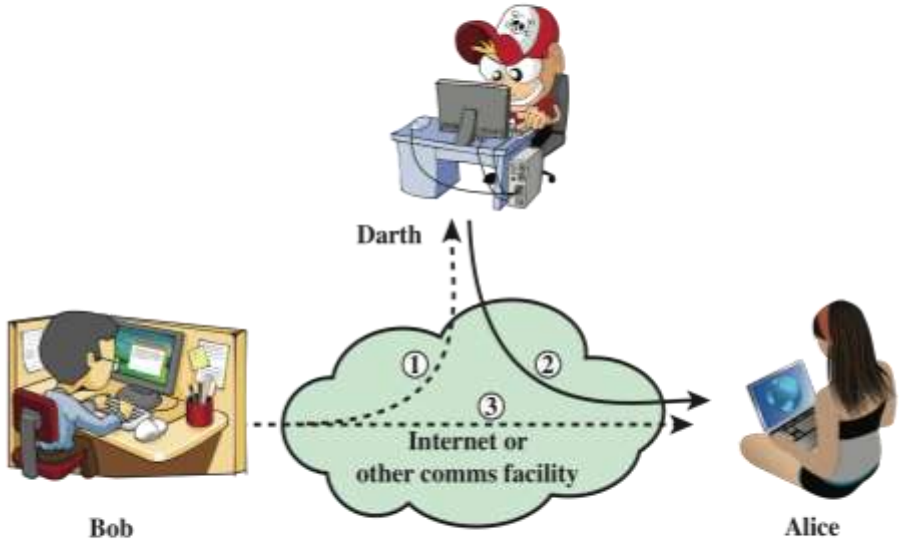
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

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



(a) Passive attacks



(b) Active attacks

Figure 1.1 Security Attacks

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

Packet Sniffing and Spoofing

How Packets are Received

- NIC (Network Interface Card) is a physical or logical link between a machine and a network
- Each NIC has a MAC address
- Every NIC on the network will hear all the frames on the wire
- NIC checks the destination address for every packet, if the address matches the cards MAC address, it is further copied into a buffer in the kernel

PROMISCUOUS MODE

- The frames that are not destined to a given NIC are discarded
- When operating in promiscuous mode, NIC passes every frame received from the network to the kernel
- If a sniffer program is registered with the kernel, it will be able to see all the packets
- In Wi-Fi, it is called Monitor Mode

PACKET SNIFFING

Packet sniffing describes the process of capturing live data as they flow across a network

Let's first see how computers receive packets.

Packet Spoofing: Scapy v.s C

- Python + Scapy
  - Pros: constructing packets is very simple
  - Cons: much slower than C code
- C Program (using raw socket)
  - Pros: much faster
  - Cons: constructing packets is complicated
- Hybrid Approach
  - Using Scapy to construct packets
  - Using C to slightly modify packets and then send packets

SUMMARY

- Packet sniffing
  - Using raw socket
  - Using PCAP APIs
- Packet spoofing using raw socket
- Sniffing and the spoofing
- Endianness

ACTIVE ATTACKS

- 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

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
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
- Defined by RFC 4949 as:
  - A processing or communication service provided by a system to give a specific kind of protection to system resources

X.800 Service Categories

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

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).

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.

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.

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.

Table 1.2

Security Services (X.800)

(This table is found on page 28 in the textbook)

AUTHENTICATION

- Concerned with assuring that a communication is authentic
  - 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

Two specific authentication services are defined in X.800:

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

ACCESS CONTROL

- 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 indentified, or authenticated, so that access rights can be tailored to the individual

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 include 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

DATA INTEGRITY

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

- Prevents either sender or receiver from denying a transmitted message
- 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 SERVICE

- Availability
  - The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system
- Availability service
  - One that protects a system to ensure its availability
  - Addresses the security concerns raised by denial-of-service attacks
  - Depends on proper management and control of system resources

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.

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.

Table 1.3

Security Mechanisms (X.800)

(This table is found on page 30 in the textbook)

MODEL FOR NETWORK SECURITY

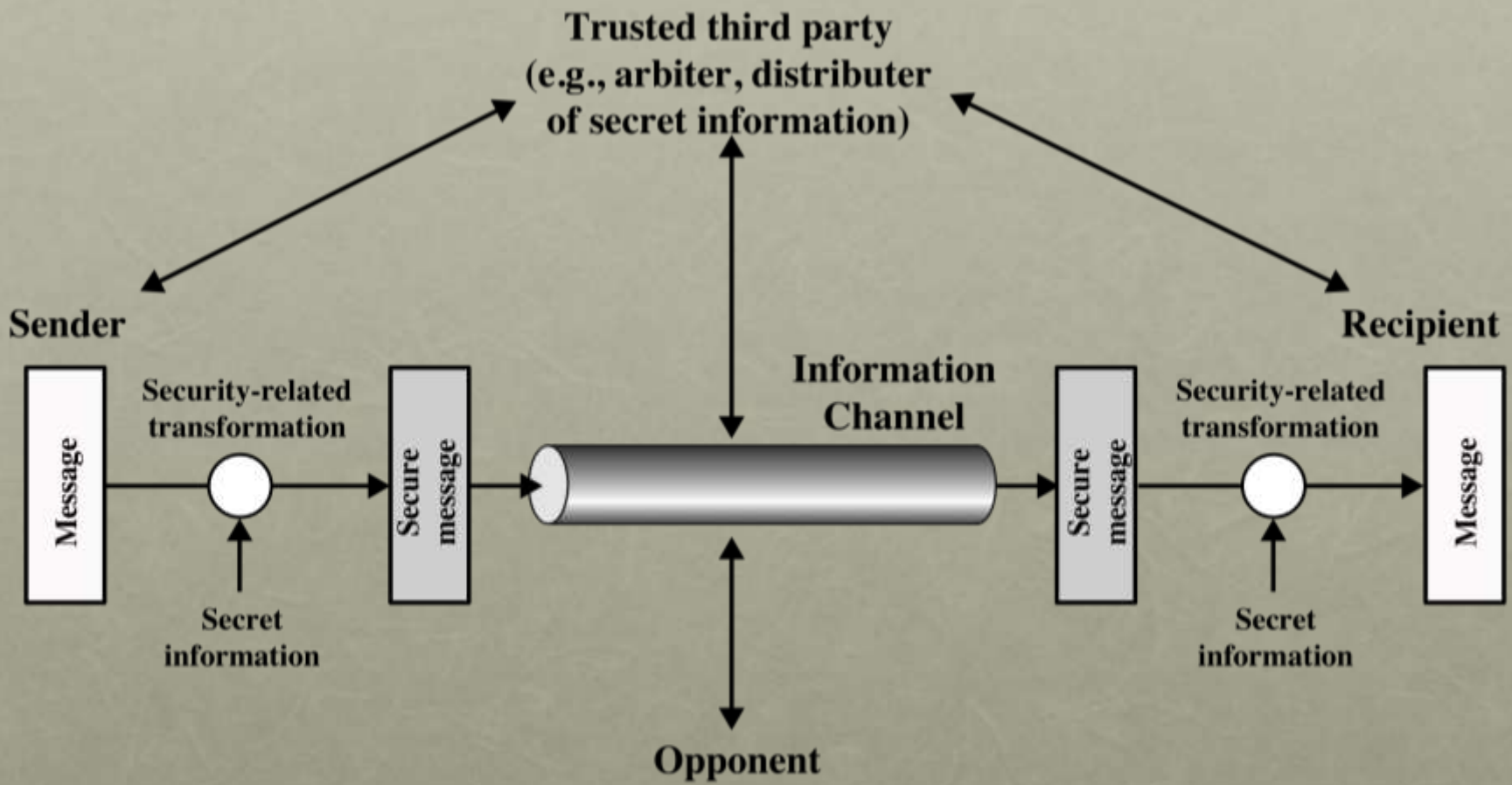


Figure 1.2 Model for Network Security

A MODEL FOR NETWORK SECURITY

- Using this model requires us to:
  1. Design a suitable algorithm for the security transformation
  2. Generate the secret information (keys) used by the algorithm
  3. Develop methods to distribute and share the secret information
  4. Specify a protocol enabling the principals to use the transformation and secret information for a security service
- Parts One and Two (Chap. 2-8)
  [or Chap. 2-9 in 5th ed.]

NETWORK ACCESS SECURITY MODEL

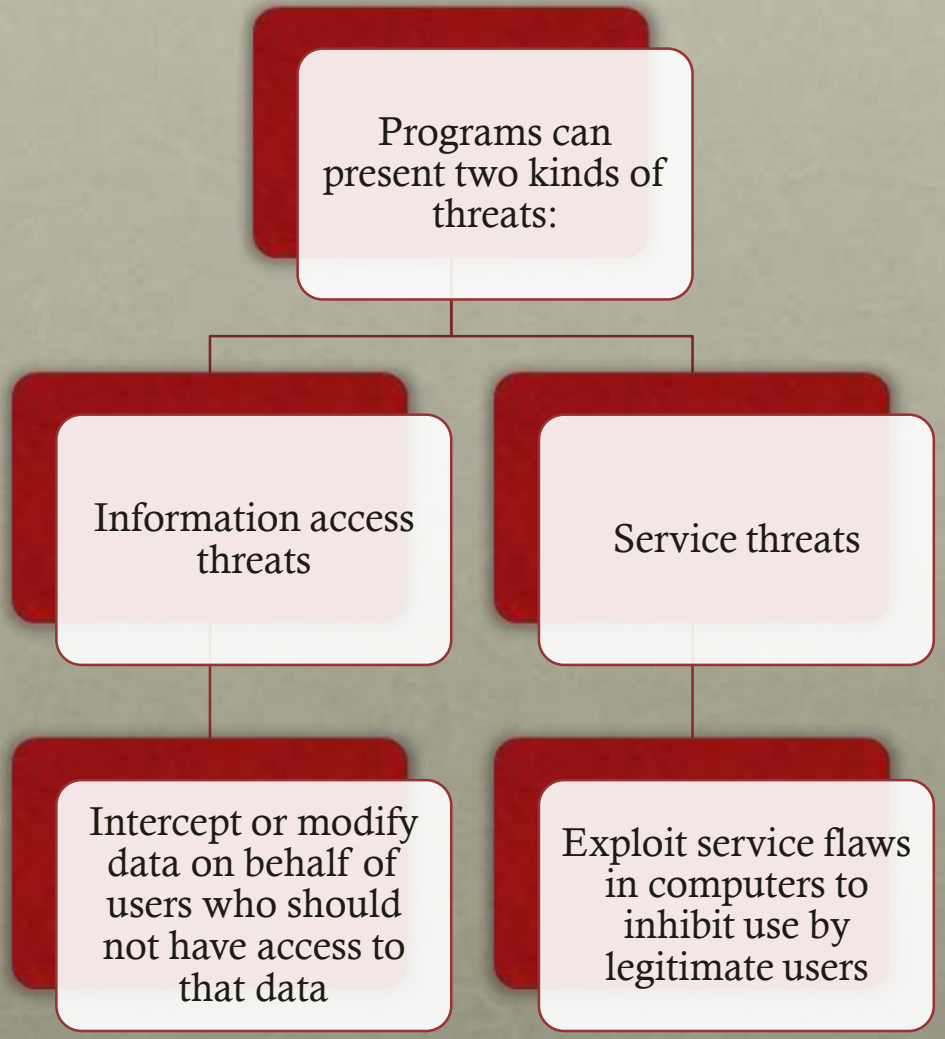
Figure 1.3 Network Access Security Model

A MODEL FOR NETWORK ACCESS SECURITY

- Using this model requires us to:
  1. Select appropriate gatekeeper functions to identify users
  2. Implement security controls to ensure only authorized users access designated information or resources
- Part Three (Chap. 9-11) [Chap. 10-12 in 5th ed.]

UNWANTED ACCESS

- Placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs



STANDARDS

NIST

- National Institute of Standards and Technology
- 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
- NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact

ISOC

- Internet Society
- Professional membership society with worldwide organizational and individual membership
- Provides leadership in addressing issues that confront the future of the Internet
- 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)
- Internet standards and related specifications are published as Requests for Comments (RFCs)

SUMMARY

- Computer security concepts
  - Definition
  - Examples
  - Challenges
- The OSI security architecture
- Security attacks
  - Passive attacks
  - Active attacks
- Security services
  - Authentication
  - Access control
  - Data confidentiality
  - Data integrity
  - Nonrepudiation
  - Availability service
- Security mechanisms
- Model for network security
- Standards

WEB RESOURCES

- Book Web site: http://williamstallings.com/NetworkSecurity
  - Student resources
- Other Web sites:
  - (p.38)