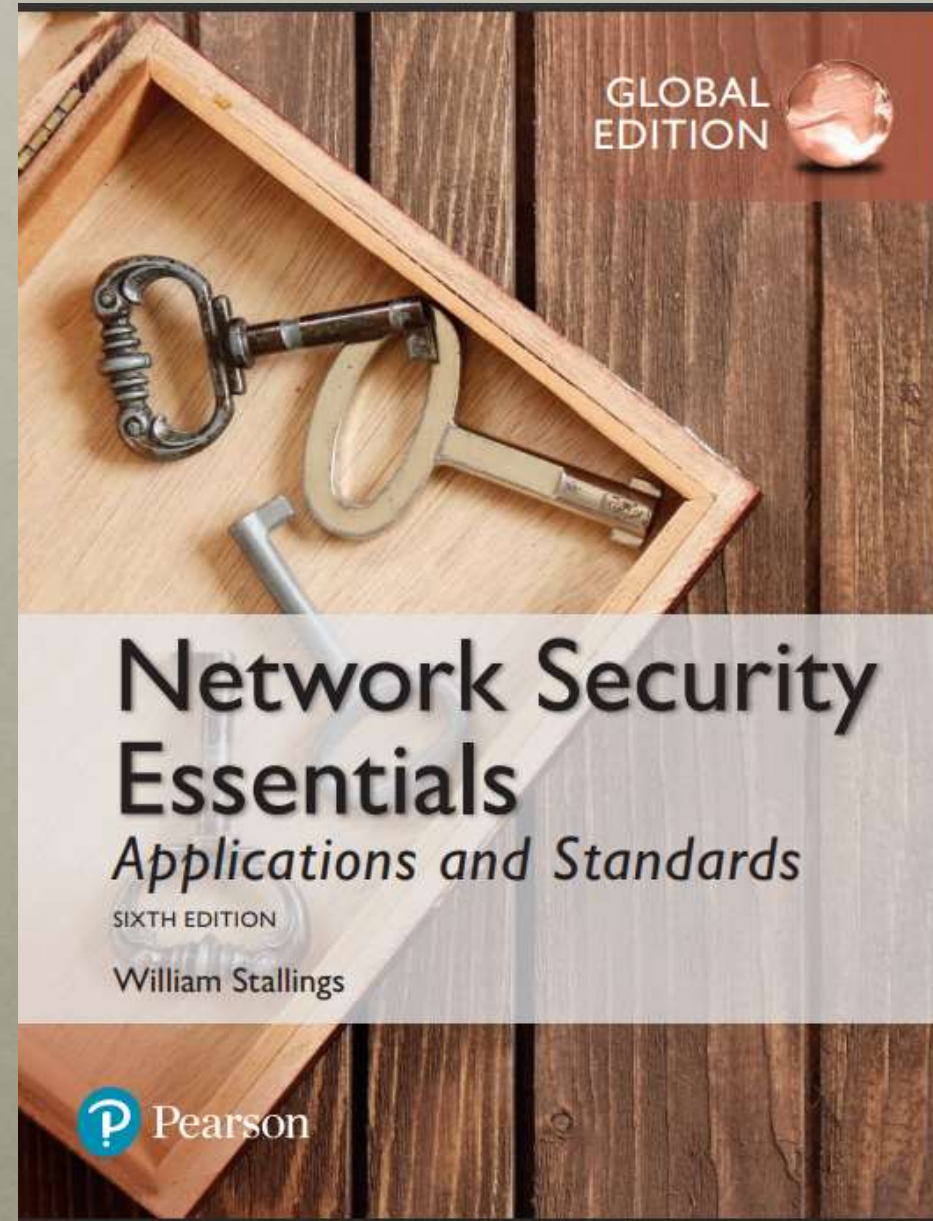


INFORMATION SECURITY

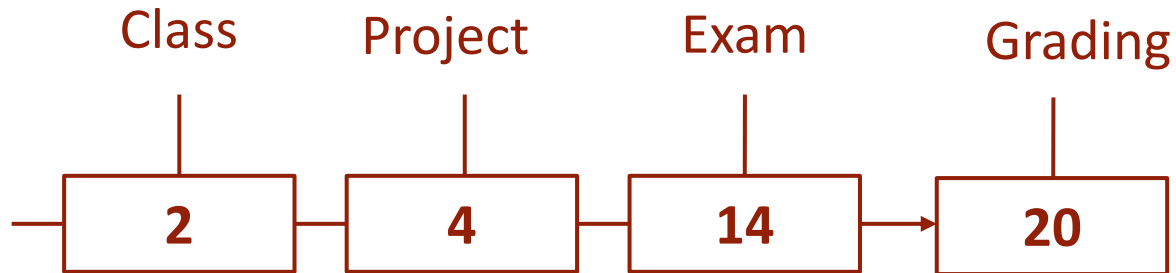
By Dr. Taghinezhad

Mail: a0taghinezhad@gmail.com

Website: ataghinezhad.github.io



ABOUT THIS COURSE



REFERENCES

Download PDFS

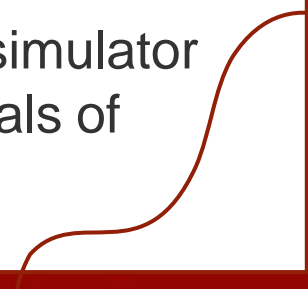
1) اصول امنيت شبکه

2) Network Security Essentials Applications

<https://ataghinezhad.github.io/networkSecurity.html>



PROJECT ASSIGNMENTS THAT COVERS A BROAD RANGE OF TOPICS FROM THE TEXT

- ■ **Hacking** project: This exercise is designed to illuminate the key issues in intrusion detection and prevention.
 - ■ **Research** projects: A series of research assignments that instruct the student to research a particular topic on the Internet and write a report.
 - ■ **Programming** projects: A series of programming projects that cover a broad range of topics and that can be implemented in any suitable language on any platform.
 - ■ **Practical security** assessments: A set of exercises to examine current infrastructure and practices of an existing organization.
 - ■ **Firewall projects**: A portable network firewall visualization simulator is provided, together with exercises for teaching the fundamentals of firewalls.
- 

CHAPTER 1

Introduction

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**
 - 1) rugged filing **cabinets** with a **combination lock** for storing sensitive documents.
 - 2) personnel screening procedures used during the hiring process. (گزینش)
- 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 CONCEPTS

- 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

WHAT ARE AREAS COVERED IN THIS BOOK

Consider the following **examples** of **security violations**:

- 1. **User A transmits** a file to user **B**. The file contains **sensitive information** (e.g., **payroll records**) that is to be protected from disclosure. **User C**, who is **not authorized** to read the file, is able to **monitor** the **transmission** and capture a **copy** of the **file during** its **transmission**.
- 2. A **network manager, D**, **transmits** a message to a computer, **E**, under its management. The message instructs computer **E** to **update** an **authorization** file to **include** the **identities** of a number of **new users** who are to be given access to that computer. **User F intercepts** the **message**, **alters** its **contents** to add or delete entries, and then **forwards** the message to **E**, which accepts the message as coming from manager **D** and updates its authorization file accordingly.
- 3. Rather than intercept a message, user **F constructs its own message** with the desired entries and transmits that message to **E as if it had come from manager D**. Computer **E** accepts the message as coming from manager **D** and updates its authorization file accordingly.

WHAT ARE AREAS COVERED IN THIS BOOK

Consider the following examples of security violations:

- 4. An **employee** is **fired without warning**. The **personnel** manager sends a message to a server system to **invalidate** the **employee's account**. When the invalidation is accomplished, the server is to post a notice to the employee's file as confirmation of the action. The **employee** is able to **intercept** the **message** and **delay** it long **enough** to make a final access to the server to retrieve sensitive information. The message is then forwarded, the action taken, and the confirmation posted. **The employee's action may go unnoticed for some considerable time.**
- 5. A **message** is sent from a **customer** to a **stockbroker** with instructions for various **transactions**. Subsequently, the **investments lose value** and the **customer denies sending** the message

COMPUTER SECURITY

- The NIST(National Institute of Standards and Technology in USA) *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**(یکپارچگی), **availability**(دسترس پذیری), and **confidentiality**(محرمانگی) of information system **resources** (includes hardware, software, firmware, information/data, and telecommunications)”

COMPUTER SECURITY OBJECTIVES

Confidentiality

- Data confidentiality(محرمانگی داده)
 - Assures that private or **confidential information** is **not** made **available** or disclosed to unauthorized individuals
- Privacy(حریم خصوصی)
 - 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

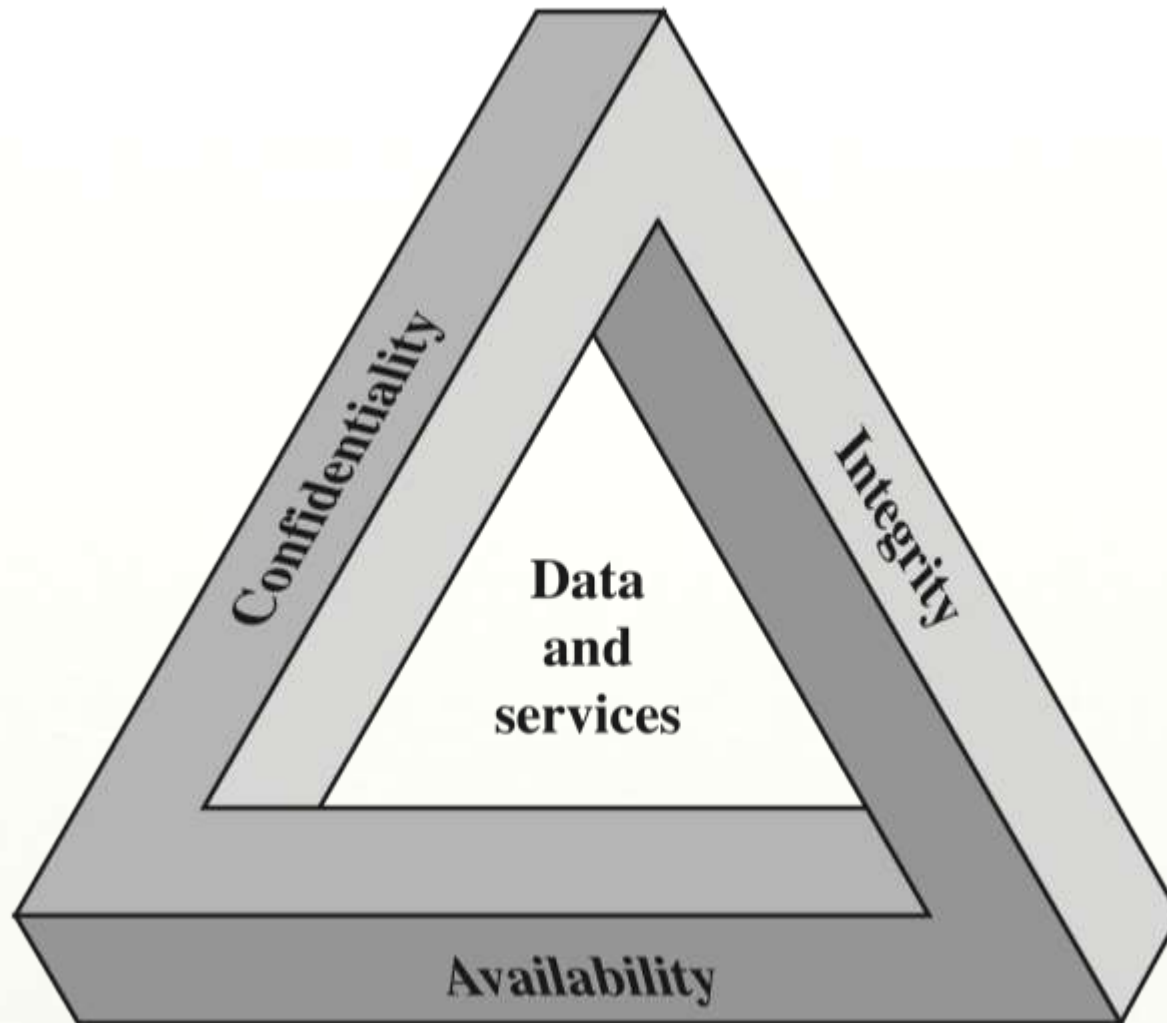
Integrity

- 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



ESSENTIAL NETWORK AND COMPUTER SECURITY REQUIREMENTS

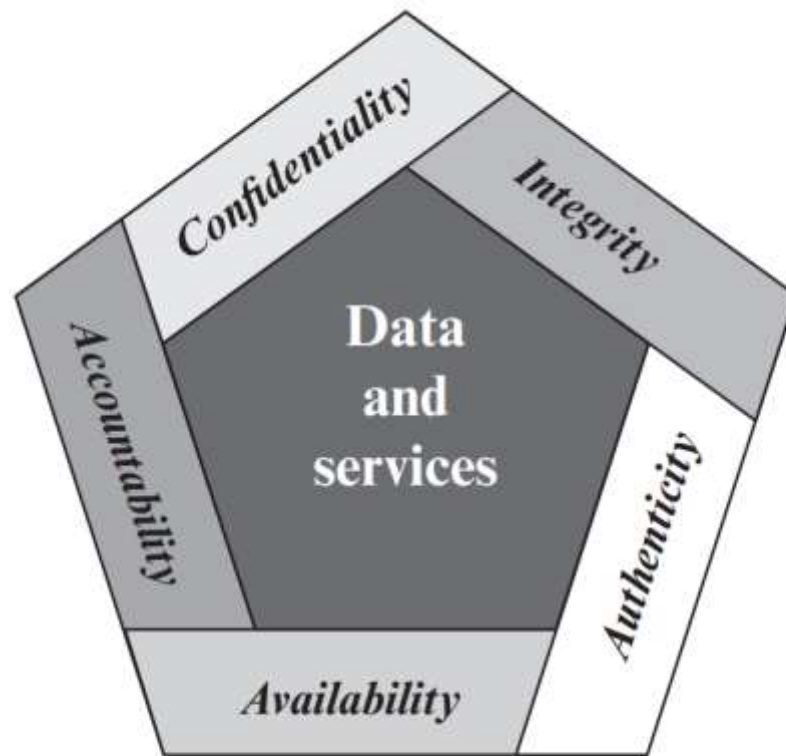


Figure 1.1 Essential Network and Computer Security Requirements

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

High

- The loss could be expected to have a severe or catastrophic 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

Low

- 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

1-Security is not simple

-Potential attacks on the security features need to be considered

3-Procedures used to provide particular services are often counter-intuitive (We can't now what mechanism are need based on a specific requirement)

4-It is necessary to decide where to use the various security mechanisms

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

6-Security is essentially a battle of wits(reasoning power) between a perpetrator and the designer

7-Little benefit from security investment is perceived until a security failure occurs

8-Requires constant monitoring

9-Is too often an afterthought

10-Strong security is often viewed as an impediment(obstruction) 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 (Standard) and RFC 4949(informational document), 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

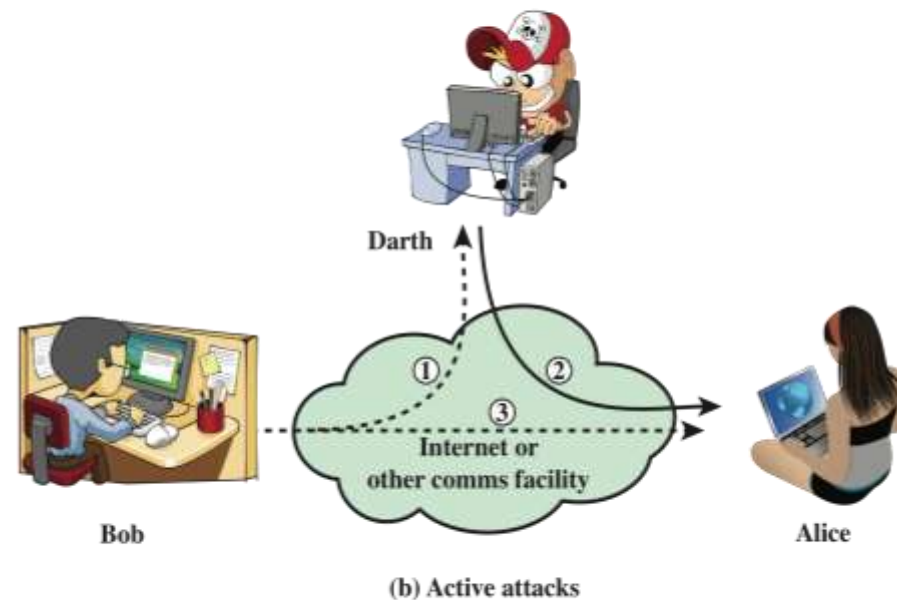
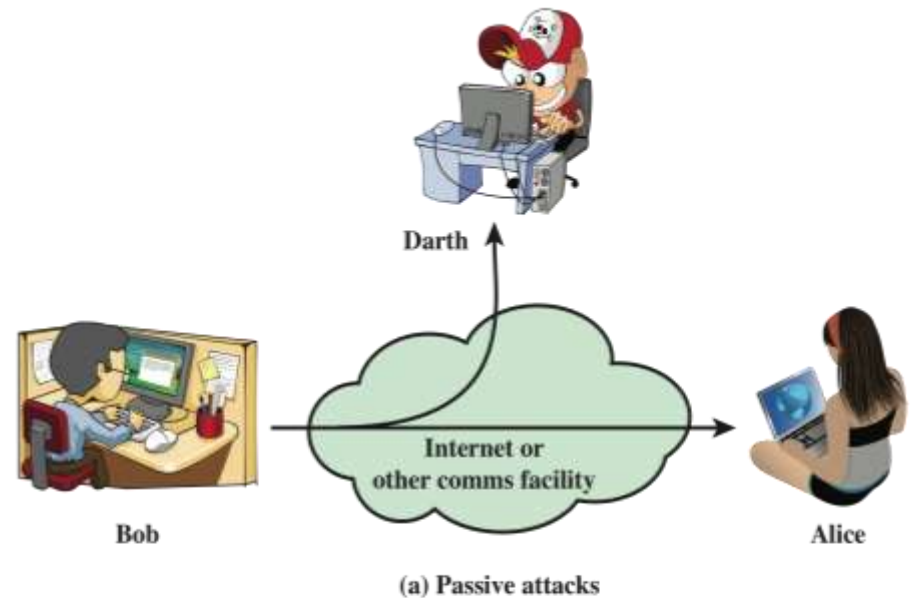


Figure 1.1 Security Attacks

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

21



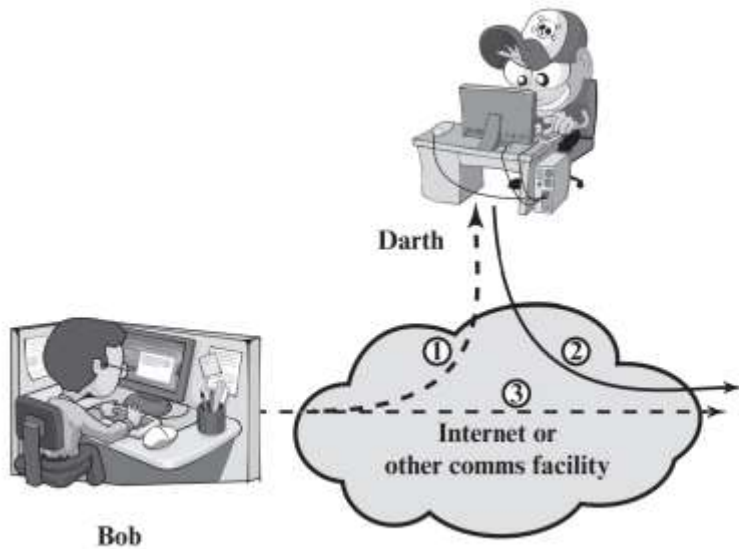
- Two types of passive attacks are:
 - The **release** of **message contents**
 - **Traffic analysis**
- Hard to detect.
- We usually try to **prevent** rather than **detection**

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



ACTIVE ATTACKS



(b) Active attacks

Masquerade

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack (path 2 active)

Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (paths 1,2,3 active)

Modification of messages

- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect (path 1 and 2 active)

Denial of service

- Prevents or inhibits the normal use or management of communications facilities (path 3 active)

ACTIVE ATTACKS EXAMPLES

Masquerade

- authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges. E.x, **Macro virus attack, Stolen or compromised logins, IP address spoofing**

Replay

- For example, consider a scenario where a user logs into their bank account by providing their username and password. The attacker intercepts this communication and records the user's credentials. Later, the attacker replays the same communication to the bank's server, pretending to be the user, and gains access to the user's account without their knowledge
- **Authorizing bank transfers, Compromising SSL sessions**

Modification of messages

- For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."

Denial of service

- an entity may suppress all messages directed to a particular destination
- (e.g., the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

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

- X.800 divides these services into five 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 12 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 (اعتبار سنجي واحد نظير): 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 to same protocol in different systems; for example two TCP modules)
 - Data-Origin Authentication (اعتبار سنجي منبع ديتا): In a connectionless transfer, provides assurance that the source of received data is as claimed. (e.g., Email)

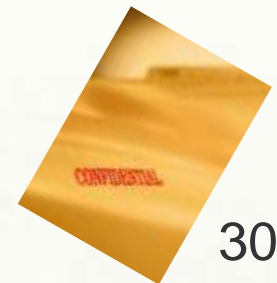
ACCESS CONTROL

- 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 CONFIDENTIALITY

- **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. **only certain parts of the data are kept confidential**, while others may be visible
 - **Traffic-Flow Confidentiality:** The protection of the information that might be derived from observation of traffic flows

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**

DATA INTEGRITY

Data Integrity: The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

1. **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.
2. **Connection Integrity without Recovery:** As above, but provides **only detection** without recovery.
3. **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.
4. **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**.
5. **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

- Prevents either sender or receiver from denying a transmitted message
- Digital signatures can be used to validate the authenticity of a message while tying it to a specific user or organization. They can also provide timestamps to authenticate the message further.
- e.x., when you send an email using PGP (Pretty Good Privacy), you can digitally sign your email message using your private key. The recipient can then verify your digital signature using your public key.



NONREPUDIATION

- 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 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 15 in the textbook)

SPECIFIC SECURITY MECHANISMS

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

- **Encipherment** رمزنگاری: 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** امضا دیجیتال: 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). Creates a virtual fingerprint that is unique to the person or entity.
 - Apply a hash function to a msg using user private key with fix length- hash cannot be reversed.
- **Access Control:** کنترل دستیابی: A variety of mechanisms that enforce access rights to resources.
- **Data Integrity:** صحت داده: A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

SPECIFIC SECURITY MECHANISMS

Specific Security Mechanisms (Continue):

- **Authentication Exchange** مبادلہ اعتبارسنجی : A mechanism intended to ensure the identity of an entity by means of information exchange. . This is achieved at the TCP/IP layer where two-way handshaking mechanism is used to ensure data is sent or not
- **Traffic Padding** لابلا کردن ترافیک : The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
- **Routing Control** کنترل مسیریابی Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.
- **Notarization** ثبت سند The use of a trusted third party to assure certain properties of a data exchange.

PERVASIVE 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. i.e., **data follows security rules** (e.g., as established by a security policy).
 - Trusted functionality is a security mechanism that ensures that the processes or devices that provide or access security services are reliable and trustworthy. It means that they follow some criteria, such as a security policy, and that they are not compromised or corrupted by malicious actors. Trusted functionality can be used to either extend the scope or to establish the effectiveness of other security mechanisms, such as encryption, authentication, access control, etc.
 - **For example, a trusted functionality can verify the integrity of a cryptographic key** before using it for encryption or decryption.
 - **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.

PERVASIVE SECURITY MECHANISMS

- **Pervasive Security Mechanisms 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.
 - **Internal security audit:** This is a security audit that is performed by the organization's own staff or a third-party contractor hired by the organization. The main goal of an internal security audit is to **verify** that the organization's **security policies, procedures, and controls are effective and aligned with the organization's objectives and standards.**
 - **External security audit:** This is a security audit that is **performed by an independent auditor or a regulatory agency.** The main goal of an external security audit is to **validate that the organization's security practices comply with the relevant laws, regulations,** or industry standards. For example, an external security audit may be required for organizations that handle sensitive data, such as health care or financial information.
 - **Penetration test:** This is a type of security audit that simulates a real-world attack on the organization's systems or networks.

PERVASIVE SECURITY MECHANISMS

- **Security Recovery** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.
 - Security recovery is a process of restoring the security of an organization's information systems and data after a cyberattack or a data breach.
 - Security recovery aims to protect the data assets from further damage, loss, or exposure, and to resume normal business operations as soon as possible. Security recovery can involve various activities

مکانیسم								سرویس
ثبت سند	کنترل مسیر یابی	لا به لائی ترافیک	مبادله اعتبارسنجی	صحت داده‌ها	کنترل دست یابی	امضاء دیجیتال	رمزنگاری	
			بلی			بلی	بلی	اعتبارسنجی واحد نظیر
						بلی	بلی	اعتبارسنجی منبع دیتا
					بلی			کنترل دست یابی
	بلی						بلی	محرمانگی
	بلی	بلی					بلی	محرمانگی جریان ترافیک
				بلی		بلی	بلی	صحت داده‌ها
بلی				بلی		بلی		عدم انکار
			بلی	بلی				قابلیت دسترسی

Service	Mechanism							
	Encipherment	Digital signature	Access control	Data integrity	Authentication	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			

SECURITY DESIGN PRINCIPLES

• The National Centers of Academic Excellence in Information Assurance/Cyber Defense, which is jointly sponsored by the U.S. National Security Agency and the U.S. Department of Homeland Security, list the following as fundamental security design principles [NCAE13]:

- ■ Economy of mechanism
- ■ Fail-safe defaults
- ■ Complete mediation Open design
- ■ Separation of privilege
- ■ Least privilege
- ■ Least common mechanism
- ■ Psychological acceptability
- ■ Isolation
- ■ Encapsulation
- ■ Modularity
- ■ Layering
- ■ Least astonishment

- سازکار اقتصادی
- پیش فرض های بی خطر
- میانجی کامل طراحی باز
- تفکیک امتیاز
- کمترین امتیاز
- کمترین مکانیسم رایج
- مقبولیت روانی
- انزوا
- کپسوله سازی
- مدولار بودن
- لایه بندی
- کمترین حیرت

SECURITY DESIGN PRINCIPLES

- **Economy of mechanism** means that the **design** of security measures embodied in both hardware and software **should be as simple and small as possible**. The more complex the mechanism, the more likely it is to possess exploitable flaws. **Simple mechanisms tend to have fewer exploitable flaws and require less maintenance**
- **Fail-safe default** means that **access decisions should be based on permission rather than exclusion**. That is, the default situation is lack of access, and the protection scheme identifies conditions under which access is permitted. This approach exhibits a better failure mode than the alternative approach, where the default is to permit access
- **Complete mediation** means that **every access must be checked against the access control mechanism**. Systems **should not rely** on access decisions retrieved from a cache.
- **Open design** means that the **design of a security mechanism should be open rather than secret**. For example, **although encryption keys must be secret**, encryption algorithms should be open to public scrutiny. **The algorithms can then be reviewed by many experts**
- **Separation of privilege** is defined as a practice in **which multiple privilege attributes** are required to achieve access to a restricted resource. A good example of this is multifactor user authentication, which **requires the use of multiple techniques, such as a password and a smart card, to authorize a user**.

SECURITY DESIGN PRINCIPLES

- **Least privilege** means that every process and every user of the system should operate using the least set of privileges necessary to perform the task. Each role is assigned only those permissions needed to perform its functions.
- **Least common mechanism** means that the design should minimize the functions shared by different users, providing mutual security.
 - This principle helps reduce the number of unintended communication paths and reduces the amount of hardware and software on which all users depend.
- **Layering** refers to the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems. By using multiple, overlapping protection approaches, the failure or circumvention of any individual protection approach will not leave the system unprotected

SECURITY DESIGN PRINCIPLES

- **Isolation** is a principle that applies in three contexts.
 - **1. Public access systems should be isolated from critical resources** (data, processes, etc.)
 - **Physical isolation** may include ensuring that **no physical connection exists between an organization's public access information resources and an organization's critical information.**
 - **logical isolation** 1) **layers of security services and mechanisms should be established between public systems and secure systems responsible for protecting critical resources**
 - **2. Processes and files of individual users should be isolated from one another except where it is explicitly desired.**
 - Like all modern operating systems provide facilities for such isolation,
 - **3. Security mechanisms should be isolated in the sense of preventing access to those mechanisms.**
 - For example, logical access control may provide a means of isolating cryptographic software from other parts of the host system, and for protecting cryptographic software from tampering and the keys from replacement or disclosure

SECURITY DESIGN PRINCIPLES

- **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.
- **Encapsulation** can be viewed as a specific form of isolation based **on object oriented functionality**. Protection is provided by **encapsulating a collection of procedures and data objects in a domain of its own so that the internal structure of a data object is accessible only to the procedures of the protected subsystem**, and the procedures may be called only at designated domain entry points.

SECURITY DESIGN PRINCIPLES

- **Modularity** in the context of security 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.
 - For example, numerous protocols and applications make use of cryptographic functions. Rather than implementing such functions in each protocol or application, a more secure design is provided by developing a common cryptographic module that can be invoked by numerous protocols and applications.
- **Least astonishment** means that a program or user interface should always respond in the way that is least likely to astonish the user. i.e., a user interface should behave in a way that is consistent and predictable
 - For example, the mechanism for authorization should be transparent enough to a user that the user has a good intuitive understanding of how the security goals map to the provided security mechanism

ATTACK SURFACES

Nature of attacks and the types of adversaries that present security threats

ATTACK SURFACES

سطوح حملہ

- **An attack surface consists of the reachable and exploitable vulnerabilities in a system [MANA11, HOWA03].**

Examples of attack surfaces are the following:

- **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, XML, office documents, and industry-specific custom data exchange formats
- **Interfaces: SQL, and Web forms: injection attacks, cross-site scripting, local file inclusion**
- **An employee with access to sensitive information** vulnerable to a social engineering attack

ATTACK SURFACES

سطوح حملہ

Attack surfaces can be categorized in the following way:

- **Network attack surface:** This category refers to vulnerabilities over an enterprise network, wide-area network, or the Internet. Included in this category are network protocol vulnerabilities, such as those used for a **denial-of-service attack, disruption of communications links, and various forms of intruder attacks.**
- **Software attack surface:** This refers to vulnerabilities in application, utility, or operating system code. A particular focus in this category is **Web server software.**
- **Human attack surface:** This category refers to vulnerabilities created by personnel or outsiders, such as **social engineering, human error, and trusted insiders**

ATTACK SURFACES AND ATTACK TREES

- **Attack Trees:** An attack tree is a **branching, hierarchical data structure** that represents a **set of potential techniques for exploiting security vulnerabilities**.
 - The **security incident:** is the goal of the attack is represented as the **root node of the tree**, and the **ways that an attacker** could reach that goal are iteratively and incrementally **represented as branches** and sub nodes of the tree.
 - Each **subnode defines a subgoal**, and each subgoal may have its own set of further subgoals, etc.
 - **The final nodes** on the paths outward from the root, that is, the leaf nodes, **represent different ways to initiate an attack**.
 - **Each node other than a leaf is either an AND-node or an OR-node.** To achieve the goal represented by an AND-node, the subgoals represented by all of that node's subnodes must be achieved;

ATTACK SURFACES AND ATTACK TREES

Layering: This is a network security approach that uses multiple security controls to protect different entryways and aspects of the technology environment from cyberattacks.

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

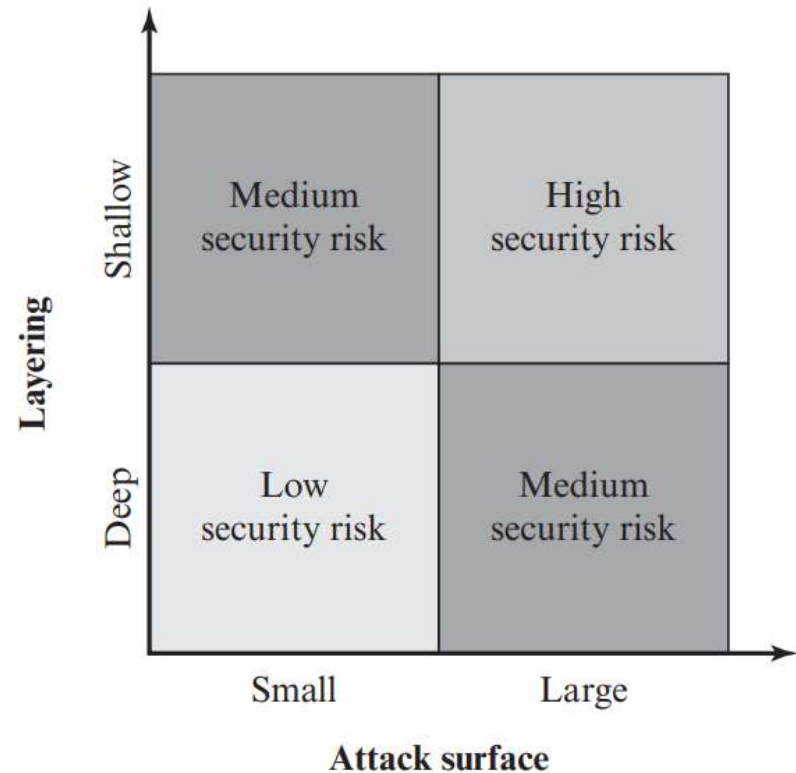
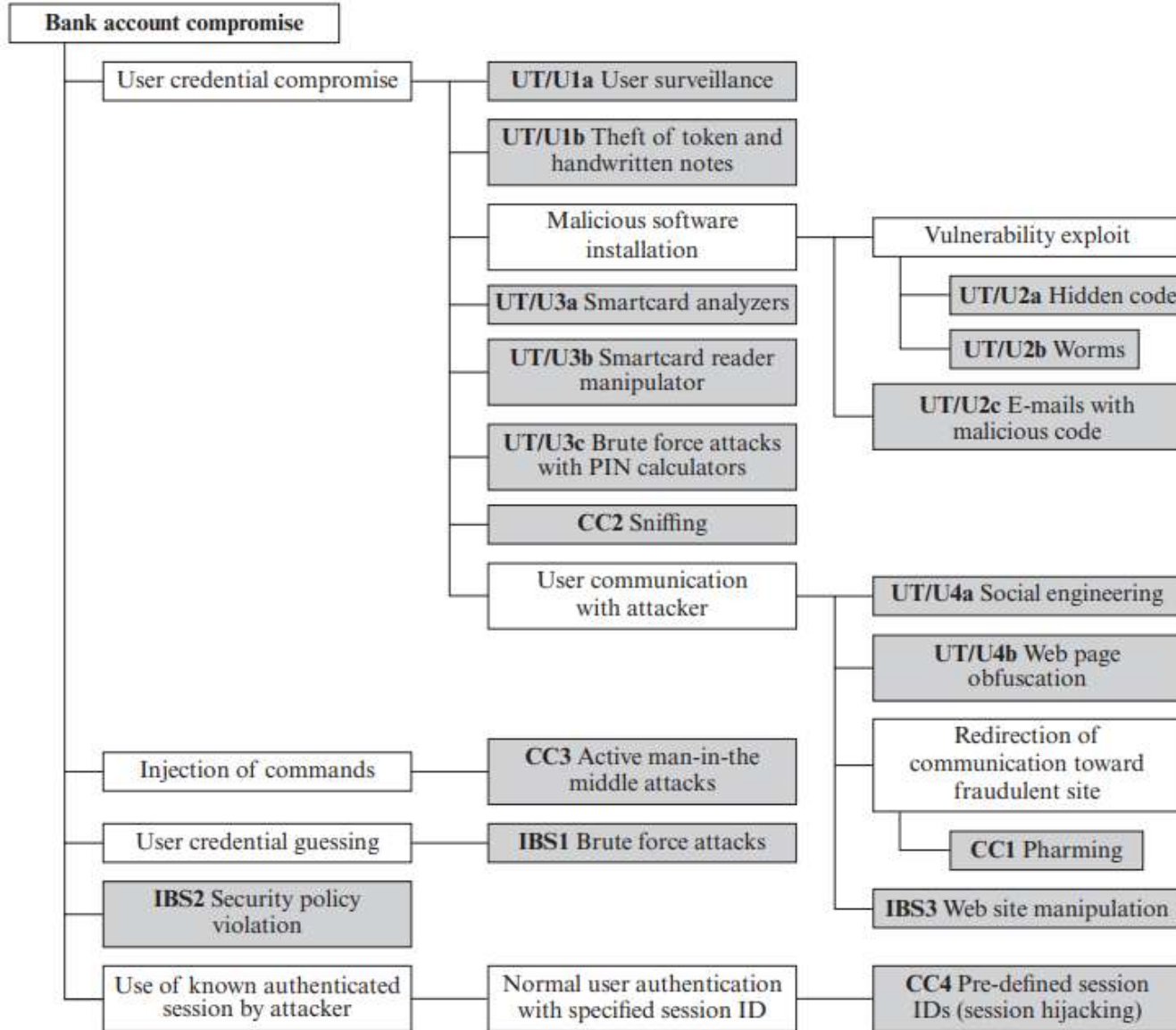


Figure 1.3 Defense in Depth and Attack Surface

ATTACK TREES



- Gray is leaf node, events that comprise the attacks
- Leaf nodes are OR-nodes here.

Figure 1.4 An Attack Tree for Internet Banking Authentication

The analysis to generate this tree considered the three components involved in authentication:

- **Five overall attack strategies can be identified**, each of which exploits one or more of the three components.
- **1-User credential compromise:** There are procedural attacks, such as monitoring a user's action to observe a PIN or other credential, or theft of the user's token or handwritten notes. An adversary may also compromise token information using a variety of token attack tools, such as hacking the smartcard or using a brute force approach to guess the PIN
- **2-Injection of commands:** In this type of attack, the attacker is able to intercept communication between the UT and the IBS.

The analysis to generate this tree considered the three components involved in authentication:

- **3-User credential guessing:** brute force attacks against some banking authentication schemes are feasible by sending random usernames and passwords. The attack mechanism is based on distributed zombie personal computers, hosting automated programs for username- or password-based calculation.
- **4-Security policy violation:** For example, violating the bank's security policy in combination with weak access control and logging mechanisms, an employee may cause an internal security incident and expose a customer's account.
- **5- Use of known authenticated session :** This type of attack persuades or forces the user to connect to the IBS with a preset session ID. Once the user authenticates to the server, the attacker may utilize the known session ID to send packets to the IBS, spoofing the user's identity.

MODEL FOR NETWORK SECURITY

A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent.

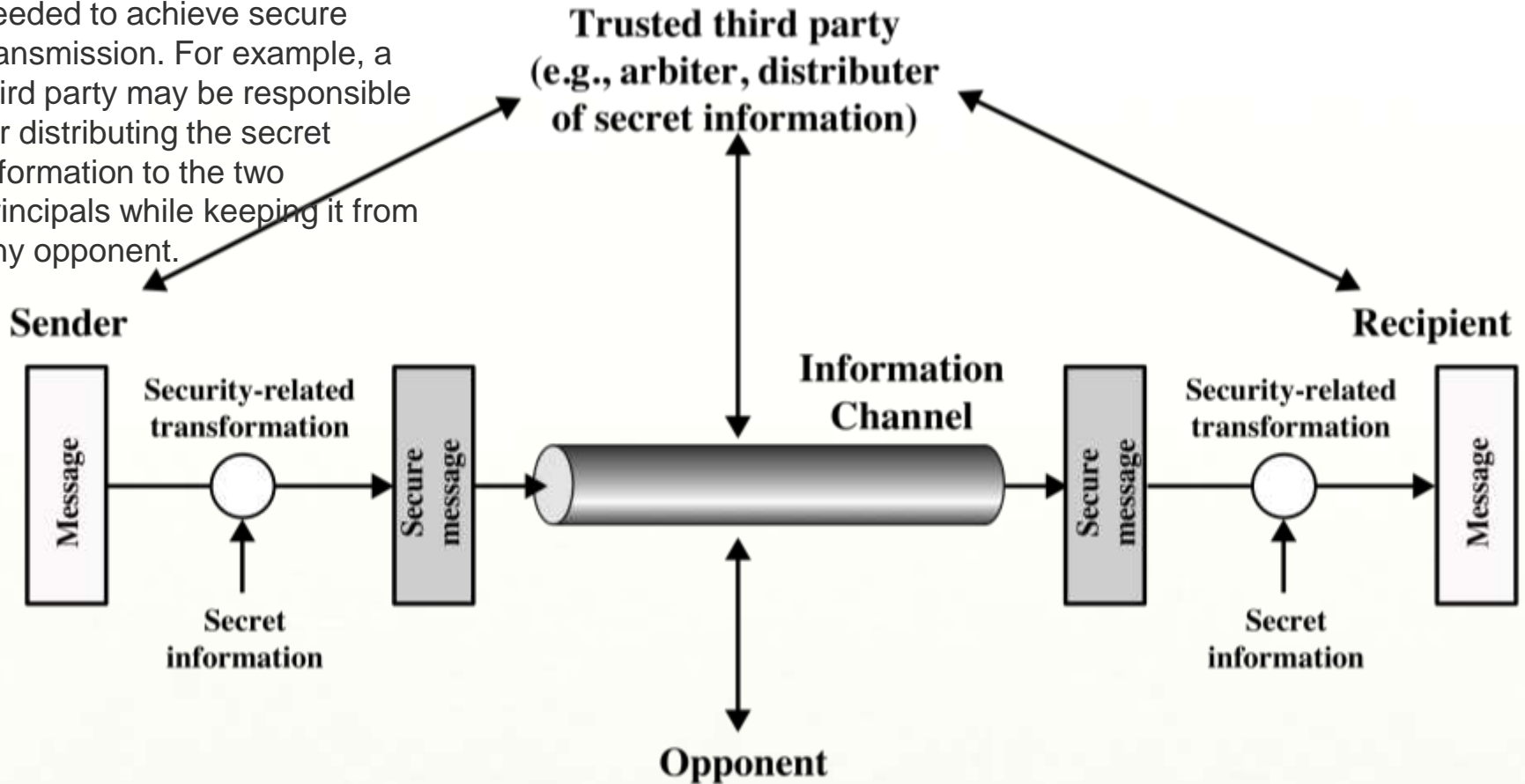


Figure 1.2 Model for Network Security

FOUR BASIC TASKS IN DESIGNING A PARTICULAR SECURITY SERVICE

- This general model shows that there are four basic tasks in designing a particular security service
 - 1. Design an **algorithm** for performing the security-related **transformation**. The algorithm should be such that an opponent cannot defeat its purpose.
 - 2. **Generate** the **secret** information to be used with the algorithm.
 - 3. Develop **methods** for the **distribution** and **sharing** of the **secret information**.
 - 4. Specify a **protocol** to be used by the **two principals** that make use of the security algorithm and the secret information to achieve a particular security service.

HACKER VS INTRUDER

- The **hacker** can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system.
- The **intruder** can be a disgruntled employee who wishes to do damage or a criminal who seeks to exploit computer assets for financial gain

NETWORK ACCESS SECURITY MODEL

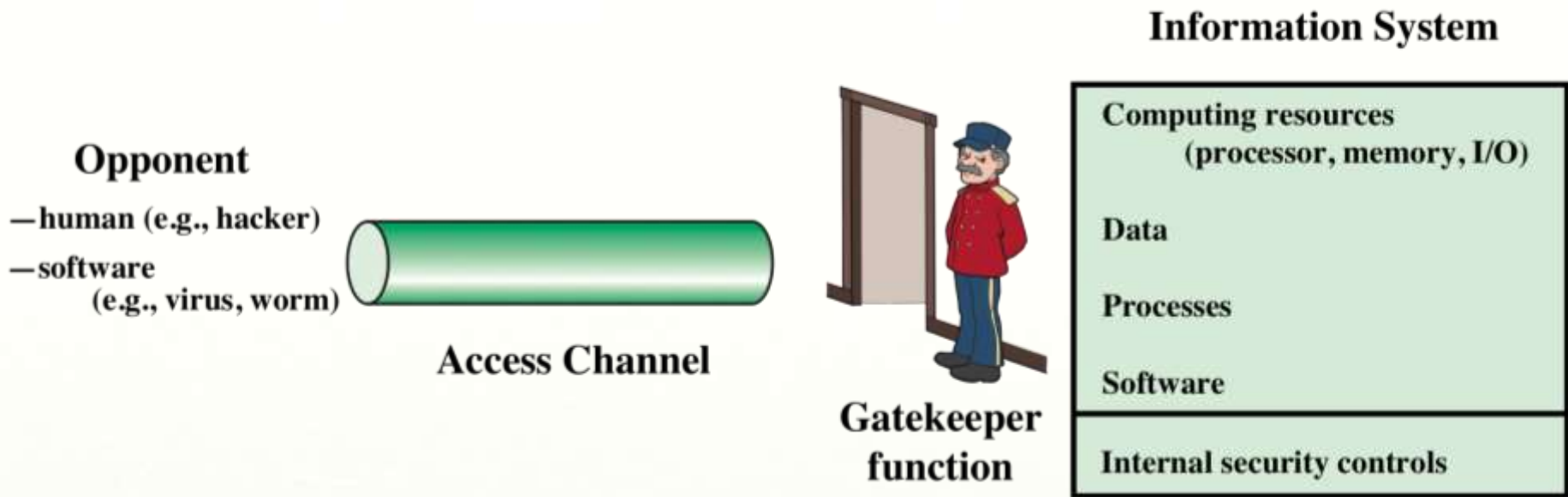
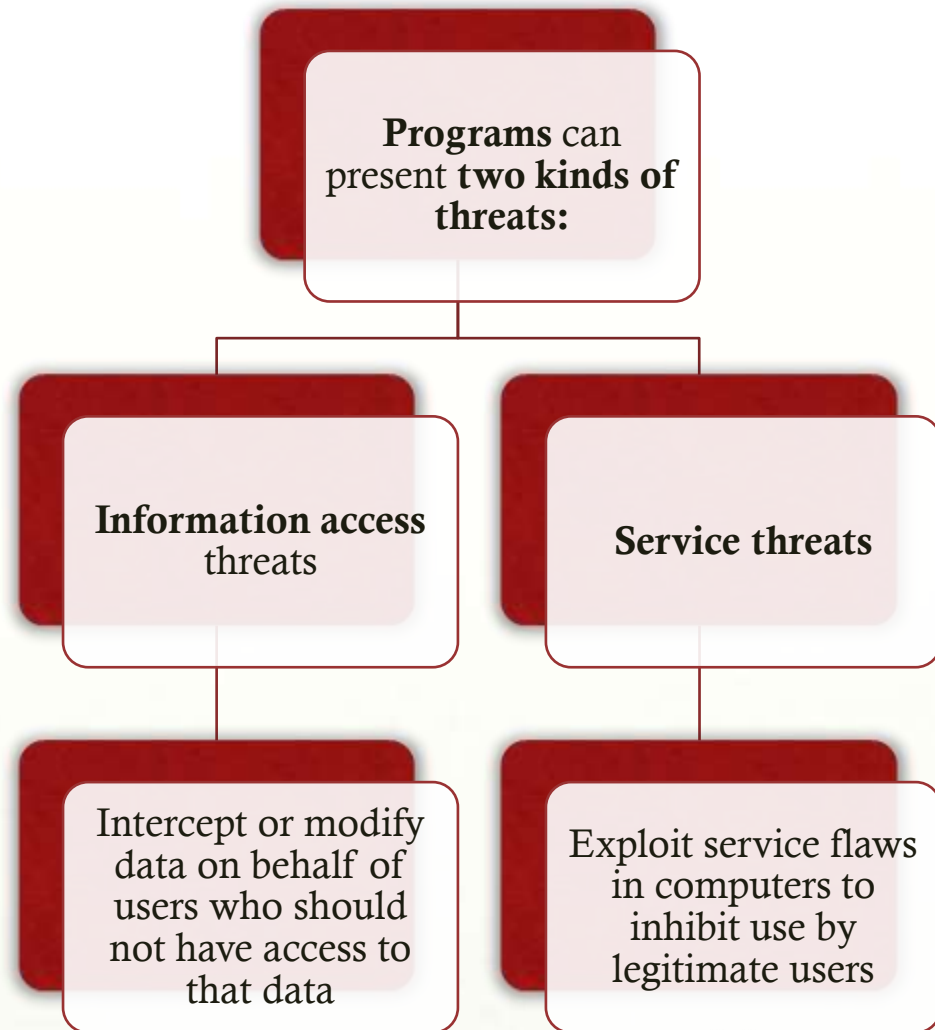


Figure 1.3 Network Access Security Model

UNWANTED ACCESS

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



STANDARDS

Many of the **security techniques** and **applications described** in this book have been specified as standards. Important organizations that involved in development of these standards are as follows.

NIST

- National Institute of Standards and Technology
- It 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
- **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

PROBLEMS A

- 1.1- Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system. In each case, indicate the degree of importance of the requirement.

۱/۱ یک دستگاه باجه خودکار (ATM) را در نظر بگیرید که در آن کاربران یک شماره شناسایی شخصی (PIN) و یک کارت برای دسترسی به حساب ارائه می کنند. مثال هایی از محرمانه بودن، یکپارچگی، و الزامات در دسترس بودن مرتبط با سیستم را ذکر کنید. در هر مورد، درجه اهمیت مورد نیاز را مشخص کنید.

PROBLEMS B

- 1.2- for a telephone switching system that routes calls through a switching network based on the telephone number requested by the caller. Give examples of confidentiality, integrity, and availability requirements associated with the system. In each case, indicate the degree of importance of the requirement.

۱/۲ برای یک سیستم سوئیچینگ تلفن که تماس ها را از طریق یک شبکه سوئیچینگ بر اساس شماره تلفن درخواست شده توسط تماس گیرنده هدایت می کند. مثال هایی از محرمانه بودن، یکپارچگی، و الزامات در دسترس بودن مرتبط با سیستم را ذکر کنید. در هر مورد، درجه اهمیت مورد نیاز را مشخص کنید.

PROBLEM C

- 1.4-For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.
- a. A portal maintained by the Government to provide information regarding its departments and services.
- b. A hospital managing the medical records of its patients.
- c. A financial organization managing routine administrative information (not privacy-related information).
- d. An information system used for large acquisitions in a contracting organization that contains both sensitive, pre-solicitation phase contract information and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.
- e. The Examinations department of a University maintains examination particulars, such as question papers of forthcoming examinations, grades obtained, and examiner details. The University's administrative department maintains the students' attendance particulars and internal assessment results. Assess the impact for the two data sets separately and the information system as a whole

مسئله C

- ۱/۴- برای هر یک از موضوعات زیر، به ترتیب یک سطح تاثیر کم، متوسط یا زیاد برای از دست دادن محرمانگی، دسترسی و یکپارچگی تعیین کنید. پاسخ های خود را توجیه کنید.
- الف- پورتالی که توسط دولت برای نمایش اطلاعات مربوط به بخش ها و خدمات خود نگهداری می شود.
- ب- بیمارستانی که پرونده های پزشکی بیماران خود را مدیریت می کند.
- ج. یک سازمان مالی که اطلاعات اداری معمول را مدیریت می کند (نه اطلاعات مربوط به حریم خصوصی).
- د- یک سیستم اطلاعاتی که برای خریدهای بزرگ در یک سازمان پیمانکاری استفاده می شود که شامل اطلاعات حساس قرارداد مرحله قبل از درخواست و اطلاعات اداری معمول است. تاثیر دو مجموعه داده را به طور جداگانه و سیستم اطلاعاتی را به عنوان یک کل ارزیابی کنید.
- ه. بخش امتحانات یک دانشگاه اطلاعات امتحانی، مانند برگه سوالات امتحانات آینده، نمرات کسب شده و جزئیات امتحان را حفظ می کند. بخش اداری دانشگاه اطلاعات حضور و غیاب دانشجویان و نتایج ارزیابی داخلی را حفظ می کند. تاثیر دو مجموعه داده را به طور جداگانه و سیستم اطلاعاتی را به عنوان یک کل ارزیابی کنید.