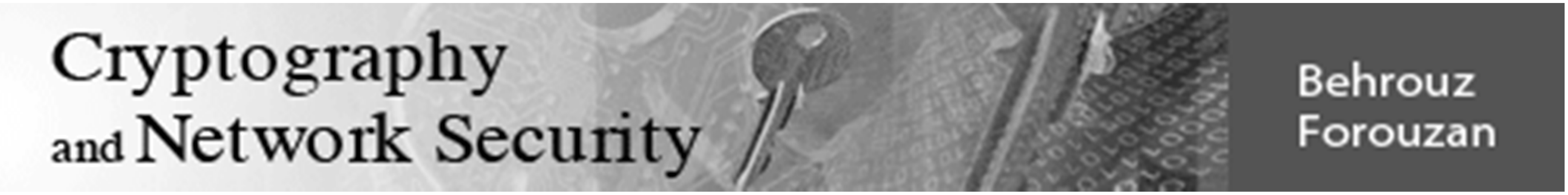


Chapter 1

Introduction

Chapter 1

Objectives

- To define three security goals
- To define security attacks that threaten security goals
- To define security services and how they are related to the three security goals
- To define security mechanisms to provide security services
- To introduce two techniques, cryptography and steganography, to implement security mechanisms.

1-1 SECURITY GOALS

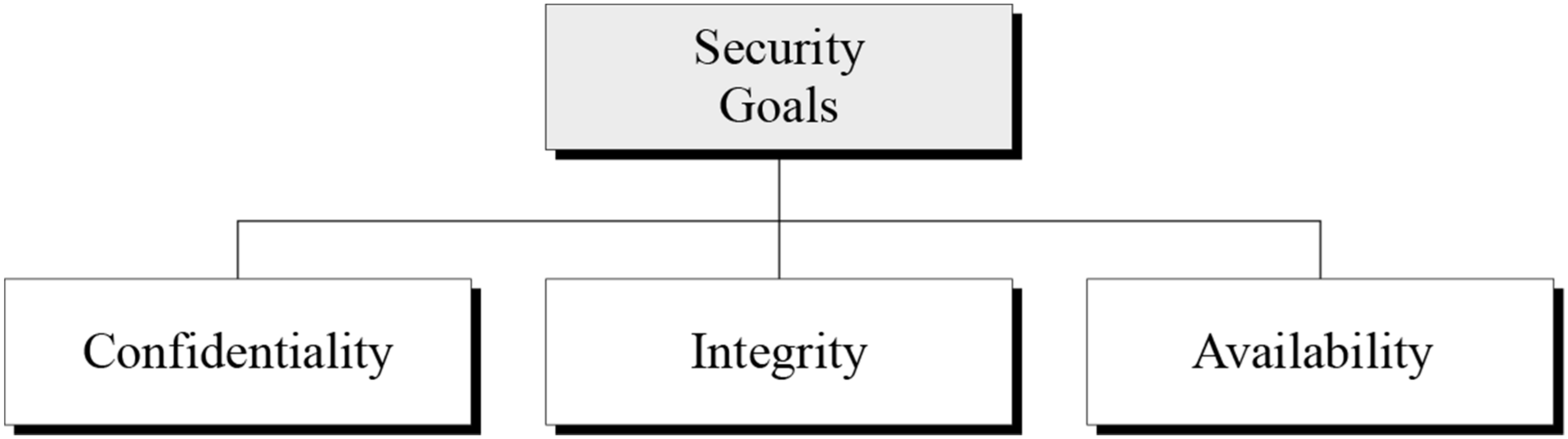
This section defines three security goals.

<u>Topics discussed in this section:</u>

1.1.1 Confidentiality
1.1.2 Integrity
1.1.3 Availability

1.1 Continued

Figure 1.1 ***Taxonomy of security goals***



1.1.1 Confidentiality

Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

Examples:

Military: concealment of sensitive information

Industry: hiding information from competitor

Banking: customer account need to be secret

Confidentiality:

- ✓ ***Storage of information***
- ✓ ***Transmission of information***

1.1.1 Confidentiality

محرمانگی مفهومی است که در دنیای واقعی مرتباً با آن سر و کار داریم. به طور مثال:

- ✓ ما انتظار داریم که پزشک سابقه‌ی درمانی ما را به صورت محرمانه نگهداری کند.
- ✓ دوستانمان رازهای ما را به صورت محرمانه نگهداری کنند.
- ✓ در دنیای تجارت، محرمانگی را به عنوان مشخصه‌ای تعریف می‌کنیم که به ما این اطمینان را می‌دهد که دسترسی به یک منبع فقط به کاربرها، کاربردها یا سیستم‌های کامپیوتری مجاز محدود می‌شود.

امّا تعریف محرمانگی چیست؟

به طور خلاصه، محرمانگی شامل نگهداری اطلاعاتِ شبکه‌ها و سیستم‌ها به صورت امن و به دور از دسترسی غیرمجاز می‌باشد.

1.1.2 Integrity

Information needs to be changed constantly. Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.

جامعیت به این معنی است که تغییرات اعمال شده بر روی اطلاعات بایستی توسط موجودیت‌های مجاز و از طریق مکانیزم‌های مجاز انجام گیرد.

Integrity violation:

- ✓ ***Malicious act***
- ✓ ***System interruption such as power surge***

1.1.3 Availability

a resource being accessible to a user, application, or computer system when required. In other words, availability means that when a user needs to get to information, he or she has the ability to do so.

دسترس پذیری به این معنی است که وقتی‌که کاربر نیاز به دسترسی به اطلاعات داشته باشد، قابلیت دسترسی به اطلاعات را داشته باشد.

The unavailability of information is just as harmful as the lack of confidentiality or integrity.

Example:

Denial Of Service (DOS) attacks or network worms that impact vulnerable systems and their availability.

Defining Threats and Risk Management

Risk management is the process of identifying, assessing, and prioritizing threats and risks.

مدیریت ریسک فرآیند تشخیص، ارزیابی و اولویت‌بندی تهدیدها و ریسک‌ها می‌باشد.

A risk is generally defined as the probability that an event will occur.

احتمال این‌که یک پیشامد یا رویداد اتفاق بیافتد را **ریسک** گویند.

Threat is an action or occurrence that could result in the breach, outage, or corruption of a system by exploiting known or unknown vulnerabilities.

هر عمل یا رخدادی که با بهره‌برداری از آسیب‌پذیری‌های (شناخته شده یا ناشناخته) یک سیستم، باعث نفوذ، قطع یا خرابی آن سیستم گردد را **تهدید** گویند.

Understanding Attack Surface

An attack surface consists of the set of methods and avenues an attacker can use to enter a system and potentially cause damage. The larger the attack surface of a particular environment, the greater the risk of a successful attack.

سطح حمله شامل مجموعه‌ای از روش‌ها و راه‌هایی است که یک حمله‌کننده می‌تواند از آن برای ورود به یک سیستم و آسیب زدن به آن سیستم استفاده کند.

Understanding Social Engineering

Social engineering is a method used to gain access to data, systems, or networks, primarily through misrepresentation.

مهندسی اجتماعی روشی است برای به دست‌آوردن دسترسی به داده‌ها، سیستم‌ها یا شبکه‌ها از طریق جعل یا قلب واقعیت.

This attack can be perpetrated in person, through email, or via phone. Attackers will try techniques ranging from pretending to be a help desk or support department staffer, claiming to be a new employee, or in some cases, even offering credentials that identify them as an employee of the company.

ارتکاب این حمله می‌تواند به صورت شخصی، ازطریق ایمیل یا تلفن باشد. حمله‌کنندگان از تکنیک‌های همچون وانمود کردن کارمند پشتیبانی، ادعای کارمند جدید شرکت یا در بعضی موارد حتی ارائه گواهی که شما آنها را به عنوان کارمند شرکت شناسایی کنید، استفاده می‌کنند.

1-2 ATTACKS

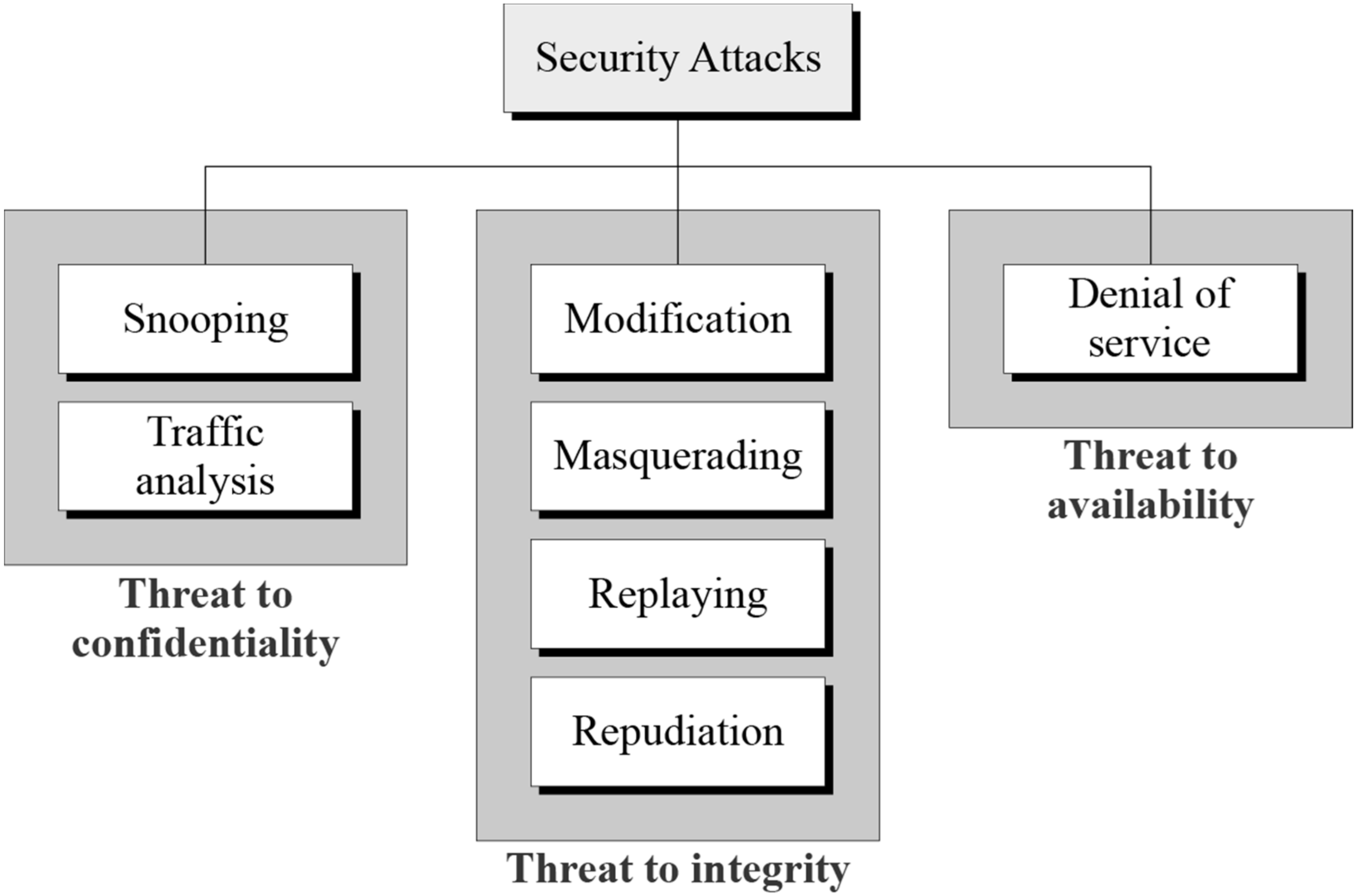
The three goals of security—confidentiality, integrity, and availability—can be threatened by security attacks.

<u>Topics discussed in this section:</u>

1.2.1 Attacks Threatening Confidentiality
1.2.2 Attacks Threatening Integrity
1.2.3 Attacks Threatening Availability
1.2.4 Passive versus Active Attacks

1.2 Continued

Figure 1.2 ***Taxonomy of attacks with relation to security goals***



1.2.1 Attacks Threatening Confidentiality

Snooping refers to unauthorized access to or interception of data.

لغت Snoop به معنی نگاه تجسس‌آمیز کردن یا مخفیانه تحقیق کردن می‌باشد.
Snooping در حقیقت به دسترسی غیرمجاز یا متوقف کردن داده‌ها اشاره می‌کند.

Example:

a file transferred through the Internet may contain confidential information. An unauthorized entity may intercept the transmission and use the contents for her own benefit.

Prevention:

the data can be made non-intelligible to the intercepter by using encipherment techniques.

1.2.1 Attacks Threatening Confidentiality

Traffic analysis refers to obtaining some other type of information by monitoring online traffic.

تحلیل ترافیک به بدست آوردن اطلاعات از طریق مونیتورینگ برخط ترافیک اشاره دارد.

Example:

- ✓ ***Sender and receiver mail address***
- ✓ ***Type of transaction***
- ✓ ***During the Allied invasion of Normandy in World War II, the Germans deduced which vessels were the command ships by observing which ships were sending and receiving the most signals. The content of the Computer Security: Art and Science signals was not relevant; their source and destination were.***

1.2.2 Attacks Threatening Integrity

Modification means that the attacker intercepts the message and changes it.

Modification به این معنی است که حمله‌کننده پیام را متوقف کرده و آن‌را تغییر می‌دهد.

Example:

a customer sends a message to a bank to do some transaction. The attacker intercepts the message and changes the type of transaction to benefit herself.

1.2.2 Attacks Threatening Integrity

Masquerading or spoofing happens when the attacker impersonates somebody else.

لغت Masquerade به معنی تغییرِ قیافه و لغت spoofing به معنی حقه‌بازی، کلاه‌برداری است. این نوع حمله هنگامی اتفاق می‌افتد که حمله‌کننده هویت شخص دیگری را جعل کند.

Examples:

- ✓ ***An attacker might steal the bank card and pretend that she is that customer.***
- ✓ ***A user tries to contact a bank, but another site pretends that it is the bank and obtains some information from the user.***

1.2.2 Attacks Threatening Integrity

Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.

Replaying به این معنی است که حمله کننده یک کپی از پیام فرستاده شده توسط کاربر را به‌دست آورده و بعداً سعی می‌کند که آن پیام را تکرار کند.

Example:

A person sends a request to her bank to ask for payment to the attacker, who has done a job for her. The attacker intercepts the message and sends it again to receive another payment from the bank.

1.2.2 Attacks Threatening Integrity

Repudiation means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

Repudiation در لغت به معنی انکار و رد می‌باشد. در امنیت به این معنی است که فرستنده یاگیرنده‌ی پیام ارسال یا دریافت پیام را انکار کند.

Examples:

✓ ***Denial by Sender:***

bank customer asking her bank to send some money to a third party but later denying that she has made such a request

✓ ***Denial by Receiver:***

person buys a product from a manufacturer and pays for it electronically, but the manufacturer later denies having received the payment and asks to be paid.

1.2.3 Attacks Threatening Availability

Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.

Denial of Service یکی از رایج‌ترین حمله‌ها می‌باشد. این حمله ممکن است
باعث کندی یا سرانجام توقف سرویس یک سیستم گردد.

Examples:

attacker can use several strategies

- ✓ ***send so many bogus requests to a server that the server crashes because of the heavy load***
- ✓ ***intercept and delete a server's response to a client, making the client to believe that the server is not responding***
- ✓ ***intercept requests from the clients, causing the clients to send requests many times and overload the system.***

Passive and Active attacks

Passive attack

The attacker's goal is just to* obtain information. *This means that the attack does not* modify data or harm *the system. The system continues with its normal operation.

The attack may* harm the sender or the receiver of the message. *Attacks that threaten* confidentiality *–snooping and traffic analysis –are passive attacks.

***It is difficult to detect until* the sender or receiver finds out about the leaking of confidential information.**

Prevention:

encipherment of the data

Passive and Active attacks

حمله‌ی غیرفعال (Passive)

هدف حمله‌کننده فقط و فقط به‌دست آوردن اطلاعات است. به این معنی که این حمله هیچ داده‌ای را تغییر نداده یا آسیبی به سیستم وارد نمی‌کند و سیستم به کار عادی خود ادامه می‌دهد. این حمله‌ها که محرمانگی را مورد تهدید قرار می‌دهند را حمله‌های غیرفعال یا passive گویند. مثل snooping و traffic analysis.

تشخیص این نوع حمله تا وقتی‌که فرستنده یا گیرنده‌ی پیام از فاش شدن اطلاعات محرمانه‌ی خود با خبر نشوند، دشوار است.

Passive and Active attacks

Active attack

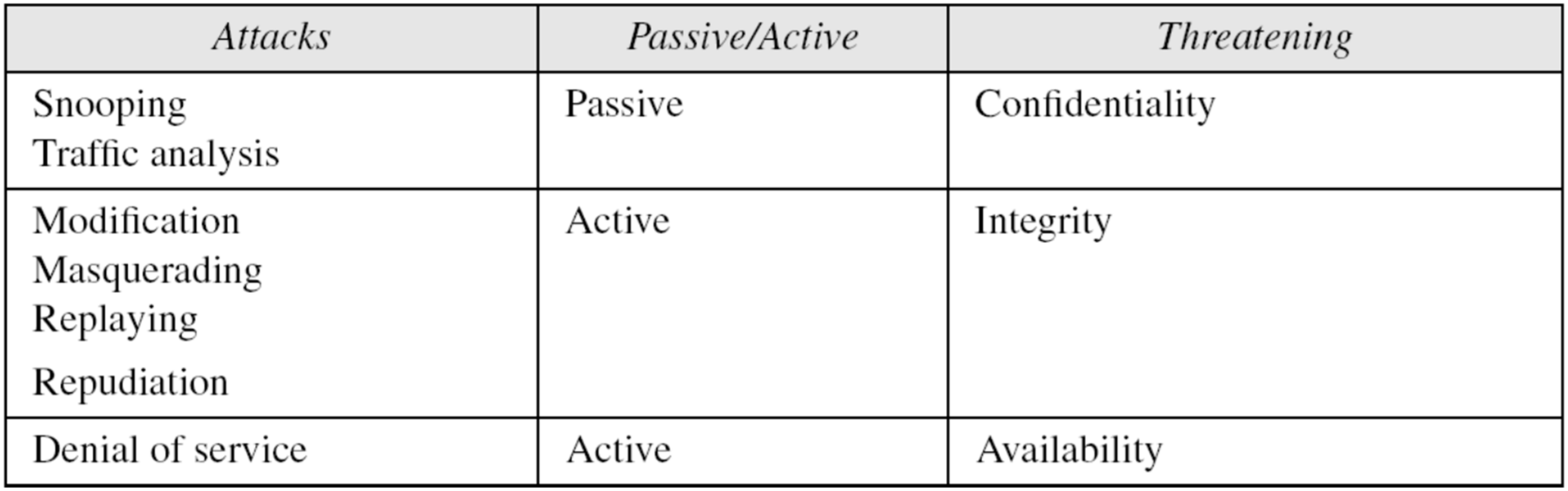
This attack may change the data or harm the system. Attacks that threaten the integrity and availability are active attacks. Active attacks are normally easier to detect than to prevent, because an attacker can launch them in a variety of ways.

این نوع حمله داده‌ها را تغییر داده و به سیستم آسیب می‌رساند. این حمله جامعیت و دسترس‌پذیری را مورد تهدید قرار می‌دهد.

تشخیص این نوع حمله بسیار آسان است امّا پیش‌گیری این حمله بسیار سخت است. به این دلیل پیشگیری این حمله دشوار است که حمله‌کننده‌ها می‌توانند از روش‌های متنوعی برای حمله استفاده کنند.

1.2.4 Passive Versus Active Attacks

Table 1.1 ***Categorization of passive and active attacks***



Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

1-3 SERVICES AND MECHANISMS

ITU-T provides some security services and some mechanisms to implement those services. Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service.

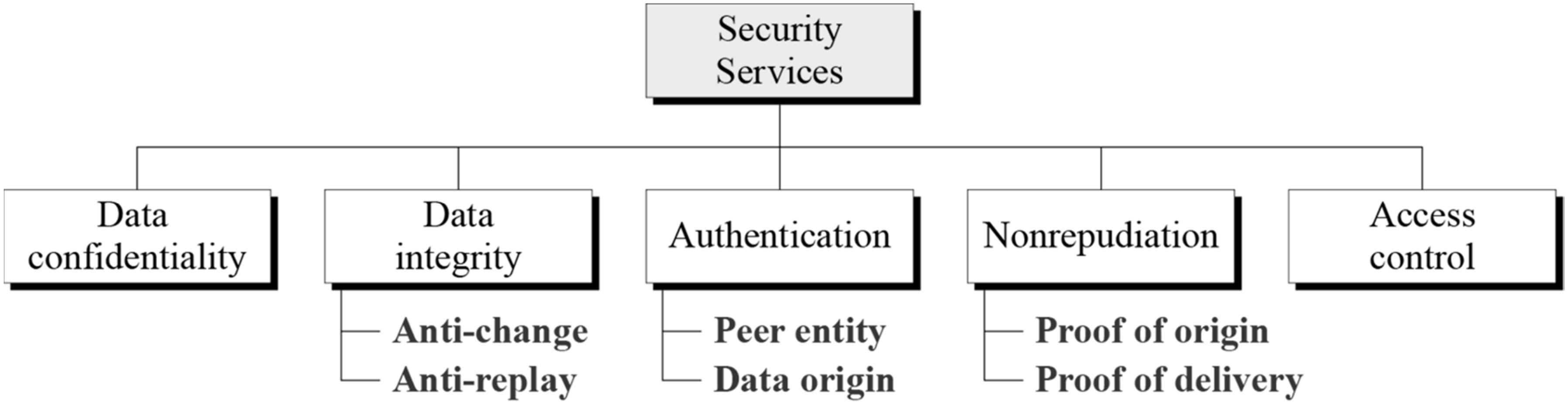
Topics discussed in this section:

1.3.1 Security Services
1.3.2 Security Mechanism
1.3.3 Relation between Services and Mechanisms

1.3.1 Security Services (ITU X.800)

Figure 1.3 ***Security services***

ITU-T (X.800) has defined five services related to the security goals and attacks we defined in the previous sections.



1.3.1 Security Services (ITU X.800)

Data Confidentiality

Designed to protect data from disclosure attack that is, it is designed to prevent snooping and traffic analysis attacks.

Protect whole or part of message.

این سرویس برای حفاظت از داده در برابر حمله افشاء استفاده مـی‌شـود. بـه ایـن معنی که این سرویس برای حفاظت در برابر حملـه‌هـای snooping و traffic analysis طراحی شده است.

Data Integrity

Designed to protect data from modification, insertion, deletion, and replaying by an adversary.

Protect whole or part of message.

این سرویس برای حفاظت از داده در برابر تغییر، درج، حذف و تکرار توسط حمله‌کننده طراحی شده است.

1.3.1 Security Services (ITU X.800)

Authentication (تایید)

Provide authentication of the party at the other end of the line.

- ✓ *Connection-oriented Communication*

  authentication of the sender or receiver during the connection establishment

- ✓ *Connectionless Communication*

  authenticates the source of the data

Nonrepudiation

Service protects against repudiation by either the sender or the receiver of the data.

- ✓ *Nonrepudiation with proof of the origin, the receiver of the data can later prove the identity of the sender if denied.*
- ✓ *Nonrepudiation with proof of delivery, the sender of data can later prove that data were delivered to the intended recipient.*

1.3.1 Security Services (ITU X.800)

Access Control

Provide protection against unauthorized (غيرمجاز) access to data.

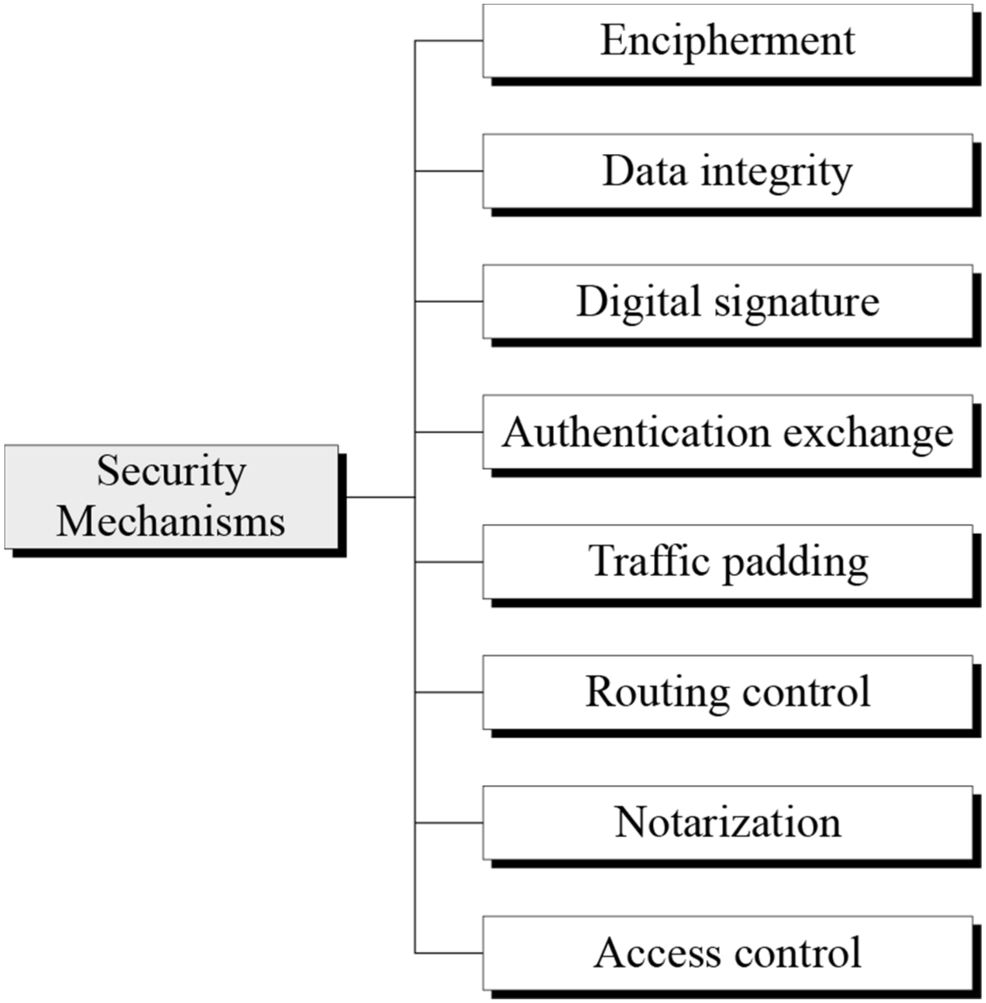
The term access in this definition is very broad and can involve reading, writing, modifying, executing programs, and so on.

1.3.2 Security Mechanism (ITU X.800)

ITU-T (X.800) also recommends some security mechanisms to provide the security services defined in the previous slides.

1.3.2 Security Mechanism (ITU X.800)

Figure 1.4 ***Security mechanisms***



1.3.2 Security Mechanism

Encipherment, hiding or covering data, can provide confidentiality.

Cryptography and Steganography are used for enciphering.

The data integrity mechanism appends to the data a short checkvalue that has been created by a specific process from the data itself.

A digital signature is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature.

1.3.2 Security Mechanism

In authentication exchange, two entities exchange some messages to prove their identity to each other.

Traffic padding means inserting some bogus data into the data traffic to thwart (خنثی کردن) the adversary's attempt to use the traffic analysis.

Routing control means selecting and continuously changing different available routes between the sender and the receiver to prevent the opponent from eavesdropping on a particular route.

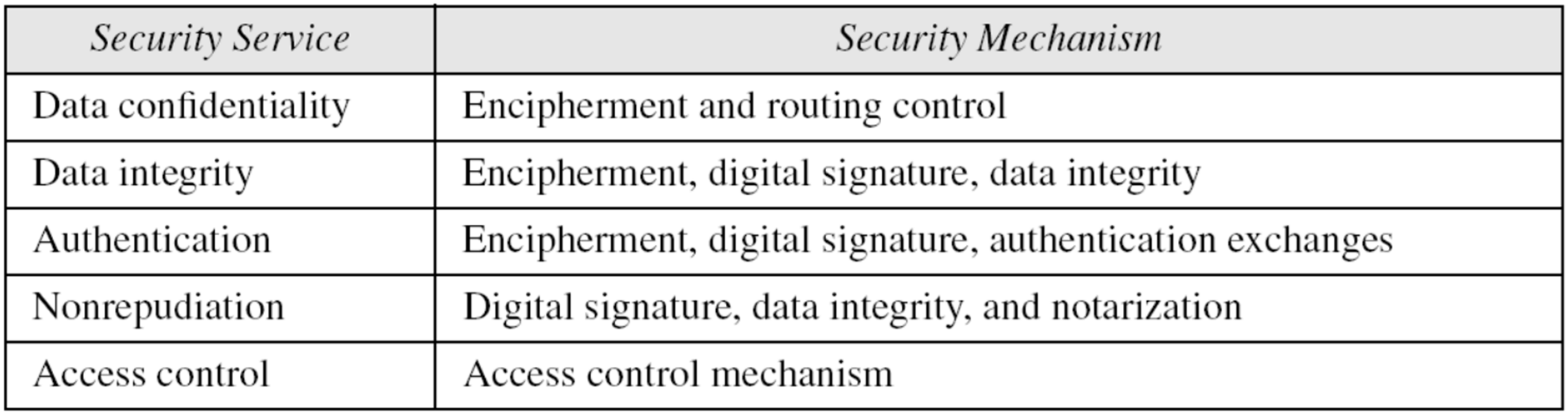
1.3.2 Security Mechanism

***Notarization* means selecting a third trusted party to control the communication between two entities.**

***Access control* uses methods to prove that a user has access right to the data or resources owned by a system.**

1.3.3 Relation between Services and Mechanisms

Table 1.2 ***Relation between security services and mechanisms***



Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

1-4 TECHNIQUES

Mechanisms discussed in the previous sections are only theoretical recipes to implement security. The actual implementation of security goals needs some techniques. Two techniques are prevalent today: cryptography and steganography.

<u>Topics discussed in this section:</u>

1.4.1 Cryptography
1.4.2 Steganography

1.4.1 Cryptography

Cryptography, a word with Greek origins, means “secret writing.” However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks.

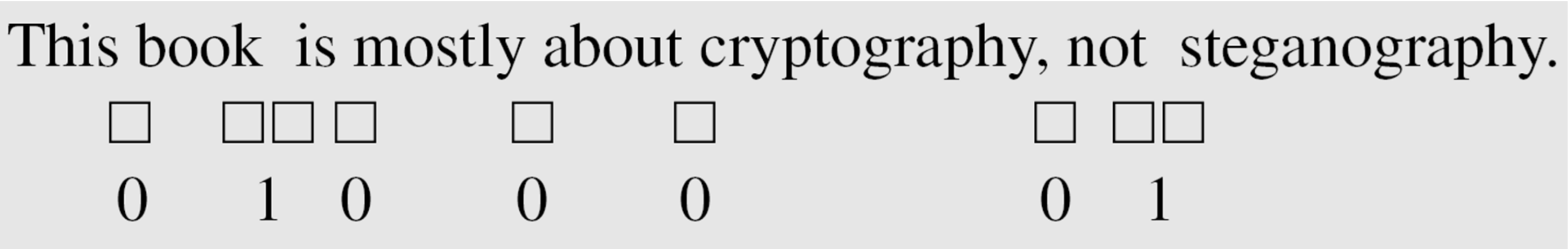
علم و هنر تبدیل پیام‌ها به منظور ایجاد پیام‌هایی که در مقابل حملات ایمن و مصون باشند.

In the ***past*** cryptography referred only to ***the encryption and decryption of messages using secret keys, today*** it is defined as involving three distinct mechanisms: **symmetric-key encipherment, asymmetric-key encipherment**, and ***hashing***.

1.4.2 Steganography

The word steganography, with origin in Greek, means "covered writing," in contrast with cryptography, which means "secret writing."

Example: covering data with text



This book is mostly about cryptography, not steganography.

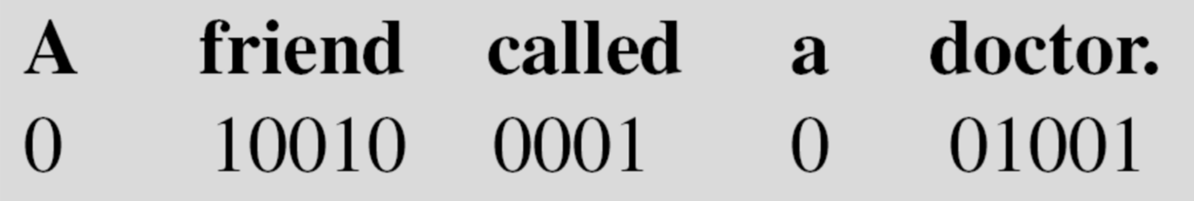
□ □□ □ □ □ □ □□

0 1 0 0 0 0 1

Single space between words = binary digit 0
Double space between words = binary digit 1
0100001

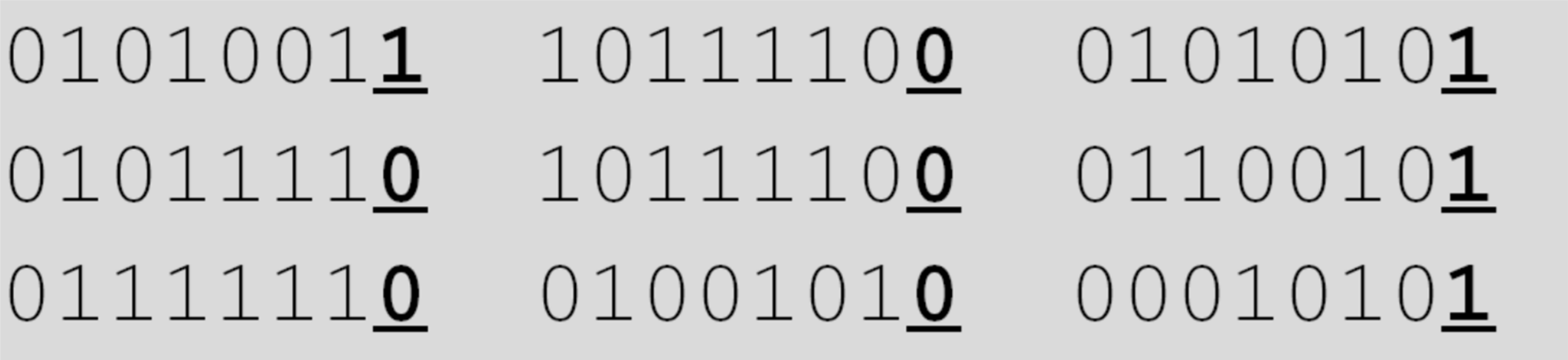
1.4.2 Continued

Example: using dictionary



A	**friend**	**called**	**a**	**doctor.**
0	10010	0001	0	01001

Example: covering data under color image



0101001**1**	1011110**0**	0101010**1**
0101111**0**	1011110**0**	0110010**1**
0111111**0**	0100101**0**	0001010**1**

1-5 THE REST OF THE BOOK

The rest of this book is divided into four parts.

Part One: Symmetric-Key Encipherment

Part Two: Asymmetric-Key Encipherment

Part Three: Integrity, Authentication, and Key Management

Part Four: Network Security