INFORMATION SECURITY [3 0 0 3]

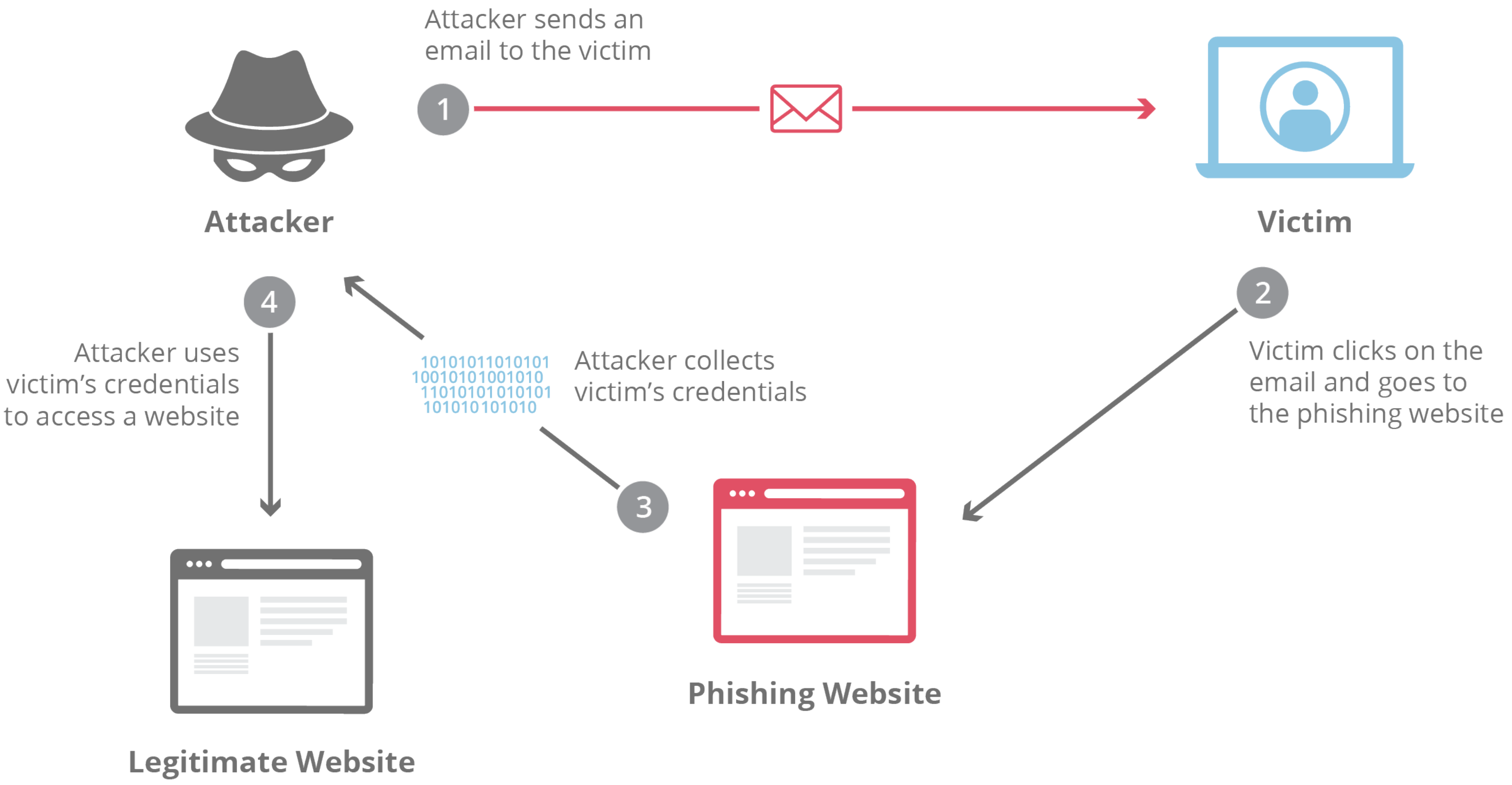
ICT 3172:

References:

1. William Stallings, *Cryptography and Network Security: Principles and Practice (7e),* Pearson Publications, 2016.
2. Charles P. Pfleeger, Shari Lawrence Pfleeger , Jonathan Margulies, *Security in Computing (5e),* Prentice Hall, 2015.
3. Michael E. Whitman and Herbert J. Mattord, *Principles of Information Security (5e),* Cengage Learning, 2015.
4. Mark Stamp, *Information Security: Principles and Practice (2e),* John Wiley & Sons, 2011.
5. Behrouz A. Forouzan, Debdeep Mukhopadhyay, *Cryptography and Network Security (2e), (Revised)*, Tata McGraw-Hill Education India, 2010.

Information is an asset that has a value like any other asset.

As an asset, information needs to be secured from attacks.



1 Attacker sends an email to the victim

2 Victim clicks on the email and goes to the phishing website

3 Attacker collects victim's credentials

4 Attacker uses victim's credentials to access a website

Attacker

Victim

Phishing Website

Legitimate Website

Information needs to be hidden from unauthorized access (confidentiality),

Protected from unauthorized change (integrity)

Available to an authorized entity when it is needed (availability).

Few decades ago,

Information of an organization was stored on physical files.

With the advent of computers, information storage became electronic.

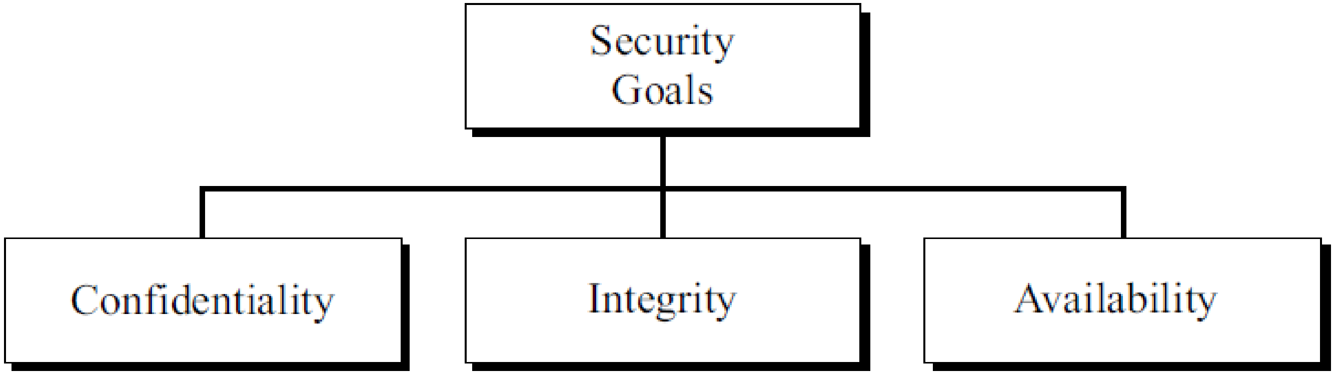
The files stored in computers require confidentiality, integrity, and availability.

Not only should information be confidential when it is stored in a computer; there should also be a way to maintain its confidentiality when it is transmitted from one computer to another.

Discuss

- 3 major goals of information security.
- how attacks can threaten these three goals.
- Security services in relation to these security goals.
- Mechanisms to provide security services and introduce techniques that can be used to implement these mechanisms.

1.1 SECURITY GOALS



Security Goals

Confidentiality

Integrity

Availability

Confidentiality

protect our confidential information.

An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

- Military: concealment of sensitive information.
- Industry, hiding some information from competitors.
- Banking, customers’ accounts need to be kept secret.

Confidentiality not only applies to the storage of the information, it also applies to the transmission of information.

Example: A healthcare provider must ensure that patients' medical records are accessible only to authorized personnel. This prevents unauthorized access to sensitive health information, maintaining patient privacy.

Concealment : act of hiding

Endanger : danger of being harmed

Integrity

Information needs to be changed constantly.

In a bank, when a customer deposits or withdraws money, the balance of her account needs to be changed.

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

Integrity violation is not necessarily the result of a malicious act;

an interruption in the system, such as a power surge, may also create unwanted changes in some information.

Example: In an online banking system, the integrity of transaction records must be maintained so that account balances and transaction histories are accurate and cannot be altered by unauthorized individuals.

Availability

The information created and stored by an organization needs to be available to authorized entities.

Information is useless if it is not available.

What would happen to a bank if the customers could not access their accounts for transactions.

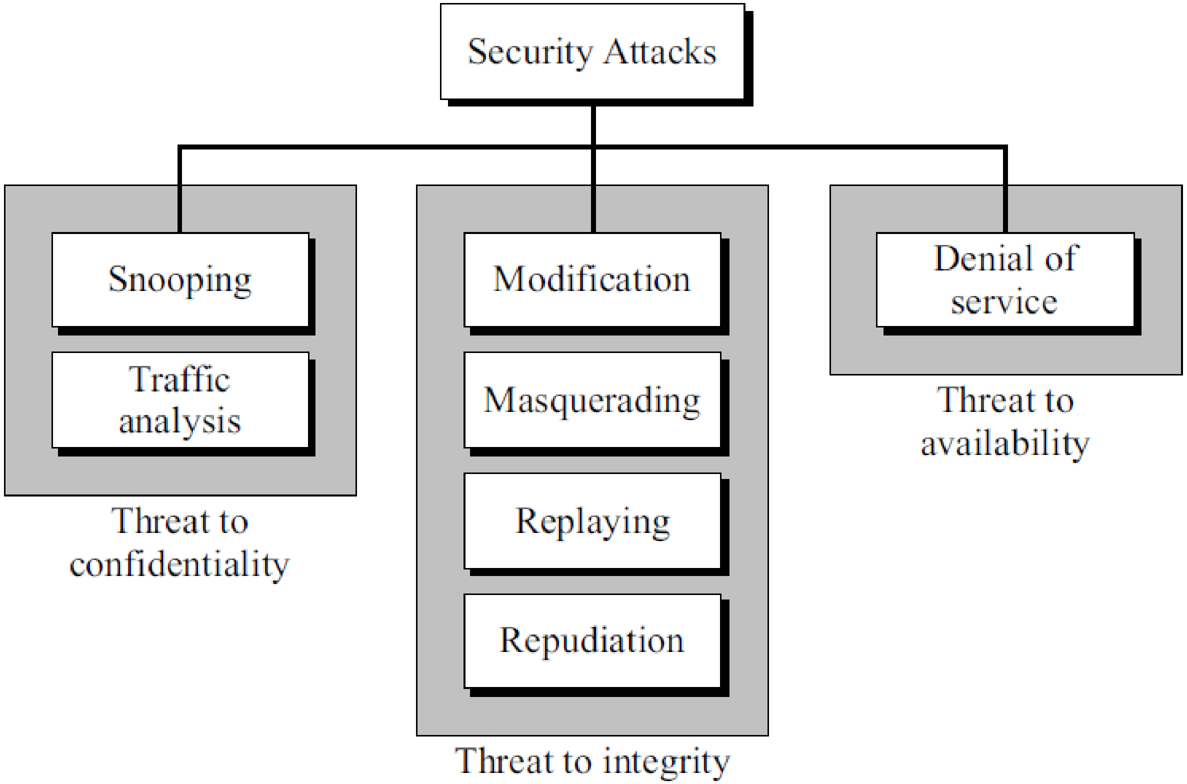
Example: An e-commerce website must be available to customers 24/7 to ensure they can make purchases at any time. Downtime or unavailability can lead to loss of sales and customer trust.

1.2 ATTACKS

3 goals of security can be threatened by security attacks.

- Three groups related to the security goals.
- Two broad categories based on their effects on the system.

1.2 ATTACKS



Security Attacks

Snooping

Traffic analysis

Threat to confidentiality

Modification

Masquerading

Replaying

Repudiation

Threat to integrity

Denial of service

Threat to availability

Snooping

Refers to unauthorized access to or interception of data.

Example:

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

To prevent snooping, the data can be made nonintelligible to the intercepter by using encipherment techniques.

Traffic Analysis

Although encipherment of data may make it nonintelligible for the intercepter, can obtain some other type information by monitoring online traffic.

Example:

- Intruder can find the electronic address of the sender or the receiver.
- Can collect pairs of requests and responses to help him guess the nature of transaction.

Attacks Threatening Integrity

The integrity of data can be threatened by several kinds of attacks:

- modification,
- masquerading,
- replaying, and
- repudiation.

Modification

After intercepting or accessing information, the attacker modifies the information to make it beneficial to herself.

Example,

- ✓ Customer sends a message to a bank to do some transaction.
- ✓ Attacker intercepts the message and changes the type of transaction to benefit herself.

Masquerading

Masquerading, or spoofing, happens when the attacker impersonates somebody else.

Example:

- Attacker might steal the bank card,PIN and pretend that he is that customer.

- Sometimes the attacker pretends instead to be the receiver entity.

- User tries to contact a bank, but another site pretends that it is the bank and obtains information from the user.

- Using John's credentials, the attacker logs into the company's internal network. They now have the same access rights as John, allowing them to access sensitive data, modify records, or disrupt services.

Replaying

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

Example:

- Person sends a request to her bank to ask for payment to the attacker, who has done a job for her.

- Attacker intercepts the message and sends it again to receive another payment from the bank.

Example of a Replay Attack:

Scenario:

- An attacker intercepts a valid login session between a user and a banking website.

Steps of the Attack:

1. **Intercepting the Data:**

   The attacker uses a network sniffing tool to capture data packets as they are transmitted between the user's device and the banking server. This might include capturing the user’s login credentials or session tokens.

2. **Replaying the Data:**

   The attacker then retransmits these captured packets to the banking server. The server, believing these packets to be from the legitimate user, grants access to the attacker.

Repudiation

Performed by one of the two parties in the communication: the sender or the receiver.

Sender of the message deny that she has sent the message;
Receiver of the message deny that he has received the message.

Example:

- Bank customer asking her bank to send some money to a third party but later denying that she has made such a request.
- When a person buys a product from a manufacturer and pays for it, but the manufacturer later denies having received the payment.

Example of a Repudiation Attack

Scenario: An attacker performs a financial transaction and later denies it to avoid responsibility.

Steps of the Attack:

1. **Performing the Transaction:**

   The attacker, Bob, logs into his online banking account and transfers $1,000 to another account.

2. **Denying the Transaction:**

   Bob then contacts the bank's customer service, claiming that he never authorized the $1,000 transfer and that it must have been a mistake or a result of unauthorized access to his account.

Attacks Threatening Availability

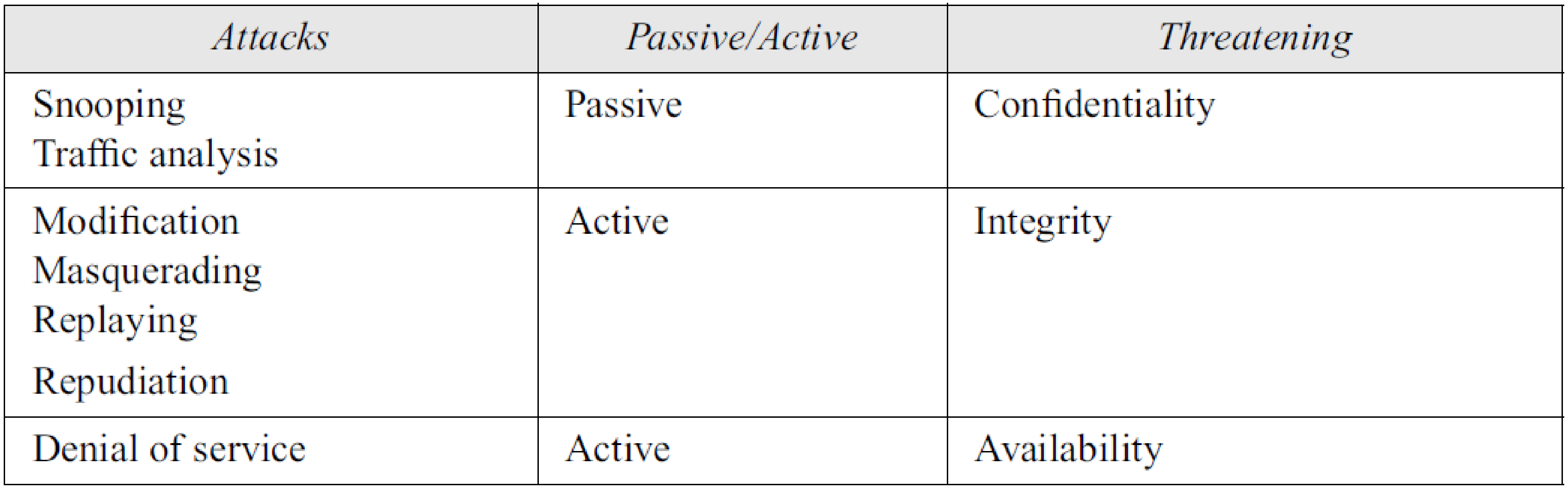
Denial of Service

It may slow down or totally interrupt the service of a system.

The attacker can use several strategies to achieve this.

- Send so many bogus requests to a server that the server crashes because of the heavy load.
- Attacker might intercept and delete a server’s response to a client, making the client to believe that the server is not responding.

Passive Versus Active Attacks



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

Passive Attacks

The attacker’s goal is just to obtain information. The attack does not modify data or harm the system.

The revealing of the information may harm the sender or receiver of the message, but the system is not affected.

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

Passive attacks can be prevented by encipherment of the data.

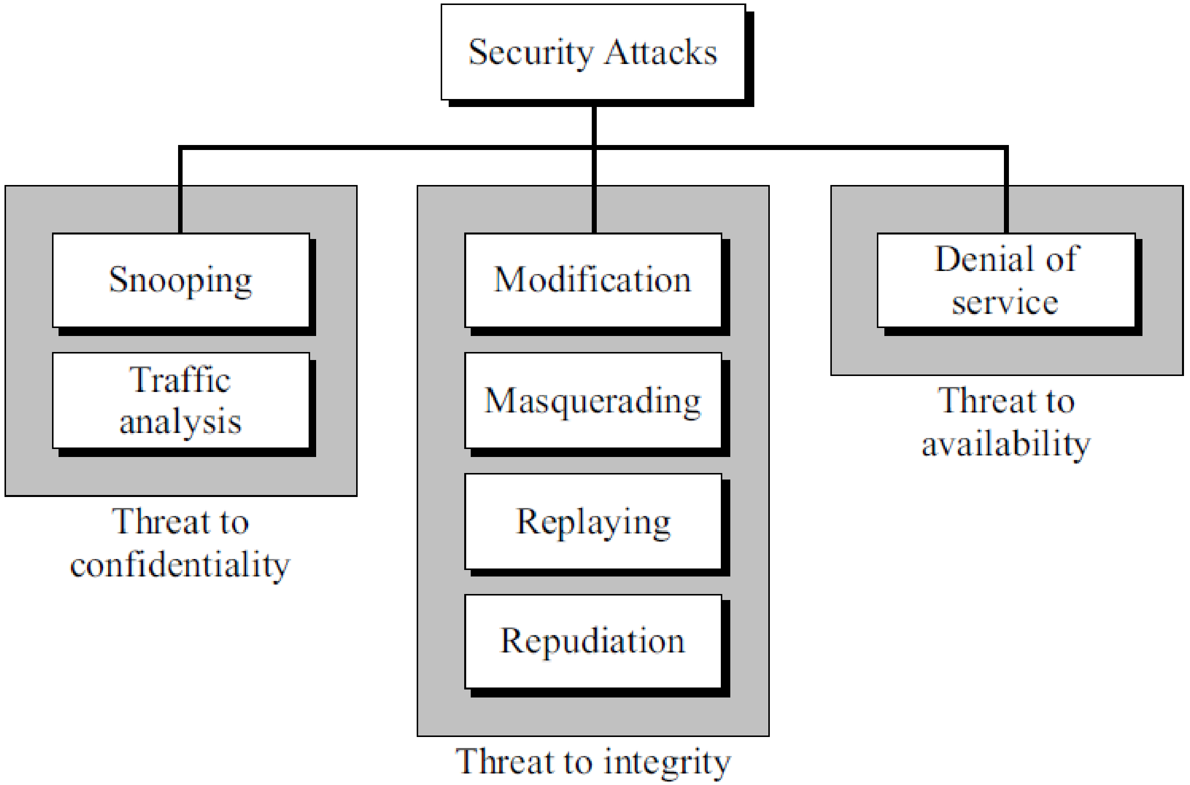
Active Attacks

An active 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.

1.2 ATTACKS



Security Attacks

Snooping

Traffic analysis

Threat to confidentiality

Modification

Masquerading

Replaying

Repudiation

Threat to integrity

Denial of service

Threat to availability

1.3 SERVICES AND MECHANISMS

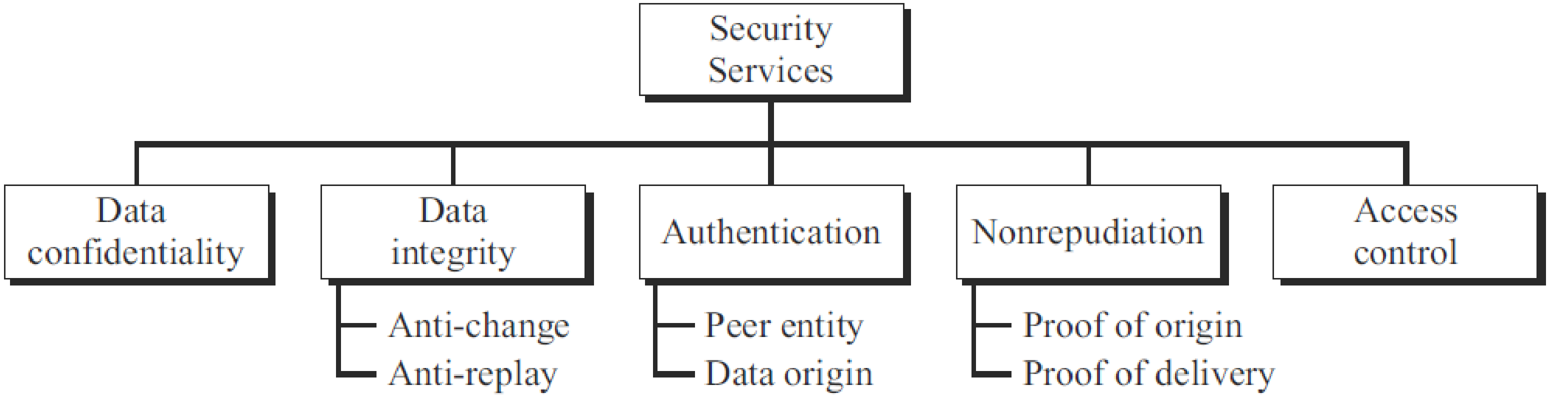
International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) provides some security services and some mechanisms to implement those services.

Mechanism or combination of mechanisms are used to provide a service.

Also, a mechanism can be used in one or more services.

Security Services

5 services related to the security goals and attacks.



It is easy to relate one or more of these services to one or more of the security goals.

Services have been designed to prevent the security attacks.

Data Confidentiality

- Data confidentiality is designed to protect data from disclosure attack.
- Service defined is very broad and encompasses confidentiality of the whole message or part of a message and also protection against traffic analysis.
- It is designed to prevent snooping and traffic analysis attack.

Data Integrity

- Data integrity is designed to protect data from modification, insertion, deletion, and replaying by an adversary.
- It may protect the whole message or part of the message.

Authentication

- Provides the authentication of the party at the other end of the line.
- Provides authentication of the sender or receiver during the connection establishment.

Nonrepudiation

- Protects against repudiation by either the sender or the receiver of the data.
- In nonrepudiation :
  - ✓ with proof of the origin, the receiver of the data can later prove the identity of the sender if denied.
  - ✓ with proof of delivery, the sender of data can later prove that data were delivered to the intended recipient.

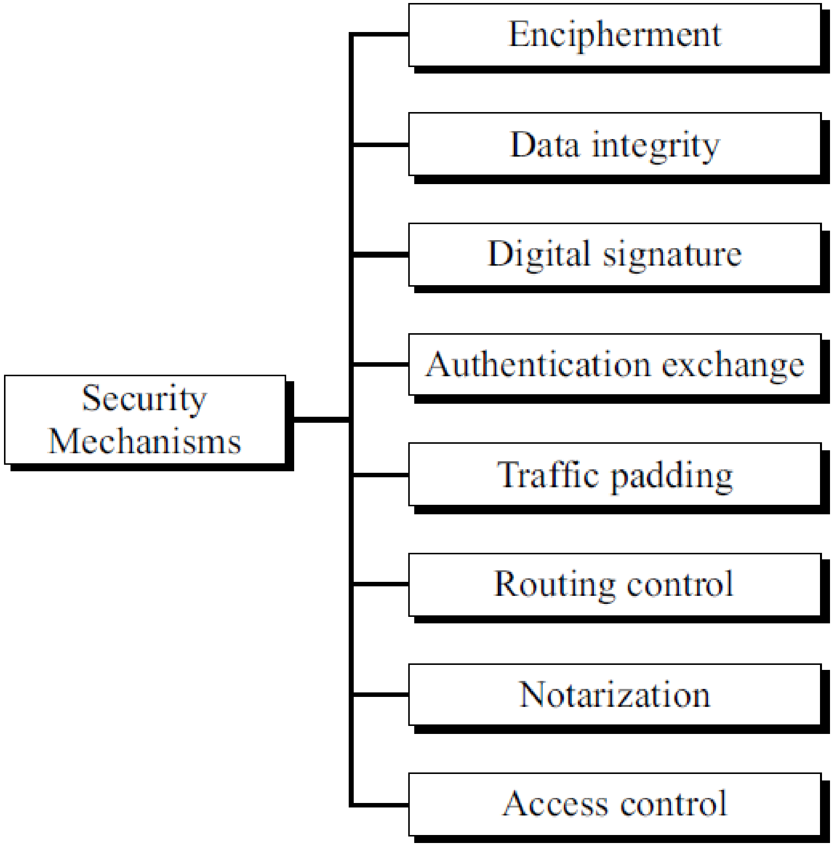
Access Control

Access control provides protection against unauthorized access to data.

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

Security Mechanisms

ITU-T also recommends some security mechanisms to provide the security services.



Encipherment

- Encipherment, hiding or covering data, can provide confidentiality.

- It can also be used to complement other mechanisms to provide other services.

- 2 techniques used for enciphering are -cryptography and steganography.

Data Integrity

- Data integrity mechanism appends to the data a short checkvalue that has been created by a specific process from the data itself.
- The receiver receives the data and the checkvalue.
- He creates a new checkvalue from the received data and compares the newly created checkvalue with the one received.
- If the two checkvalues are the same, the integrity of data has been preserved.

Digital Signature

- Sender can electronically sign the data and the receiver can electronically verify the signature.
- Using public key , private key

Authentication Exchange

- In authentication exchange, two entities exchange some messages to prove their identity to each other.
- For example, one entity can prove that she knows a secret that only she is supposed to know.

Traffic Padding

Traffic padding means inserting some bogus data into the data traffic to thwart the adversary’s attempt to use the traffic analysis.

Routing Control

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.

Thwart: To stop someone from doing something

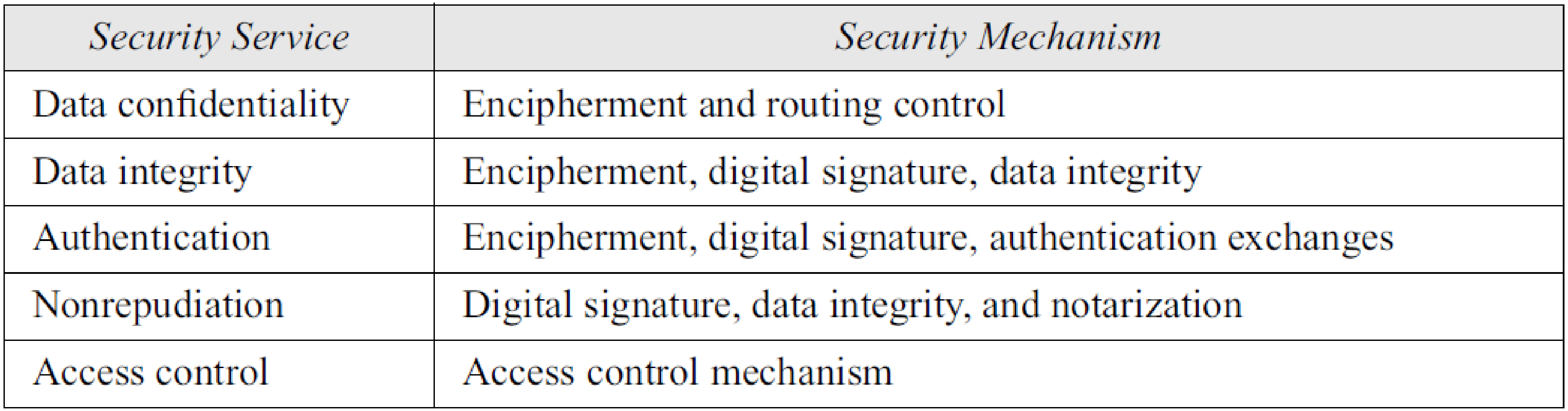
Notarization

- Selecting a third trusted party to control the communication between two entities.
- To prevent repudiation.
- Receiver can involve a trusted party to store the sender request in order to prevent the sender from later denying that she has made such a request.

Access Control

- Access control uses methods to prove that a user has access right to the data or resources owned by a system.
- Examples: passwords and PINs.

Relation between 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

- Table shows that 3 mechanisms (encipherment, digital signature, and authentication exchange) can be used to provide authentication.
- Table also shows that encipherment mechanism may be involved in 3 services (data confidentiality, data integrity, and authentication)

1.4 TECHNIQUES

- Mechanisms are only theoretical recipes to implement security.

- Actual implementation of security goals needs some techniques.

- Two techniques are : one is very general (cryptography) and one is specific (steganography).

Cryptography

- Some security mechanisms can be implemented using cryptography.

- Cryptography, a word with Greek origins, means “secret writing.”

- Refer to the science and art of transforming messages to make them secure and immune to attacks.

  - ✓ symmetric-key encipherment,
  - ✓ asymmetric-key encipherment,
  - ✓ hashing.

Symmetric-Key Encipherment

- In symmetric-key encipherment (secret-key encipherment or secretkey cryptography), an entity, say Alice, can send a message to another entity, say Bob, over an insecure channel with the assumption that an adversary, say Eve, cannot understand the contents of the message by simply eavesdropping over the channel.

- Alice encrypts the message using an encryption algorithm; Bob decrypts the message using a decryption algorithm.

- Uses a single secret key for both encryption and decryption.

Asymmetric-Key Encipherment

In asymmetric-key encipherment (public-key encipherment or public-key cryptography), There are two keys instead of one: one public key and one private key.

To send a secured message to Bob, Alice first encrypts the message using Bob's public key.

To decrypt the message, Bob uses his own private key.

Hashing

- In hashing, a fixed-length message digest is created out of a variable-length message.
- Both the message and the digest must be sent to Bob.
- Hashing is used to provide checkvalues, in relation to providing data integrity.

Steganography

Steganography, with origin in Greek, means “covered writing”

cryptography, which means “secret writing.”

Cryptography means concealing the contents of a message by enciphering.

Steganography means concealing the message itself by covering it with something else.

Example of Steganography

Steganography is the practice of hiding a secret message within another medium, such as an image, video, or audio file, in such a way that the presence of the message is concealed.

Image Steganography:

1. **Original Image**:
2. **Secret Message**: "Hello, Steganography!"
3. **Stego Image**:

Process:

4. **Convert the secret message** into binary format.
5. **Embed the binary message** into the least significant bits (LSBs) of the image's pixel values.
6. **Generate the stego image** which looks almost identical to the original image but contains the hidden message.

Historical Use

- In China : war messages were written on thin pieces of silk and rolled into a small ball and swallowed by the messenger.

- In Rome and Greece : messages were carved on pieces of wood, that were later dipped into wax to cover the writing.

- Invisible inks were also used. The secret message was exposed when the paper was heated.

- Some letters in a message might be overwritten in a pencil lead that is visible only when exposed to light at an angle.

Modern Use

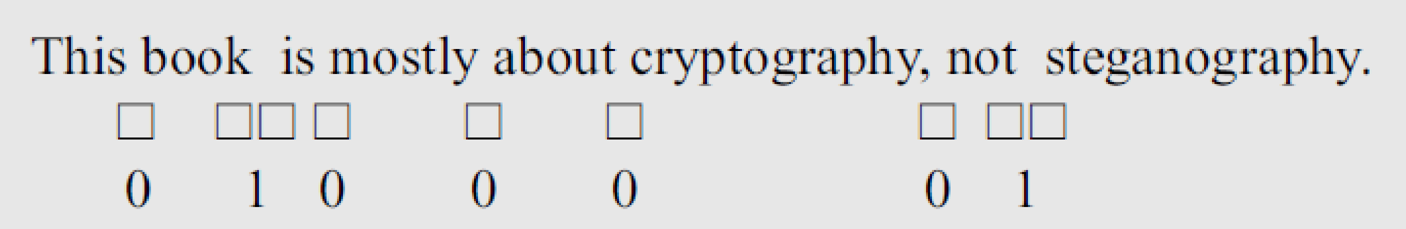
Today, any form of data, such as text, image, audio, or video, can be digitized, and it is possible to insert secret binary information into the data during digitization process.

Can also be used to protect copyright, or add extra information.

Text Cover

- The cover of secret data can be text.
- There are several ways to insert binary data into an innocuous text.

- single space between words to represent the 0 and double space to represent 1.
- Example : hiding the letter A (ASCII code :01000001).



This book is mostly about cryptography, not steganography.

□ □□ □ □ □ □ □□

0 1 0 0 0 0 1

innocuous : harmless

Text Cover

Other method: Use a dictionary of words organized according to their grammatical usages.
Example:

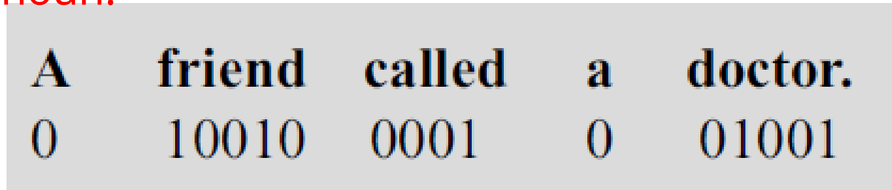
- ✓ We can have a dictionary containing 2 articles, 8 verbs,32 nouns, and 4 prepositions.
- ✓ Then agree to use cover text that always use sentences with the pattern article-noun-verb-article-noun.

- The secret binary data can be divided into 16-bit chunks.
  - ✓ First bit of data can be represented by an article (0 for a and 1 for the).
  - ✓ The next five bits can be represented by a noun (subject of the sentence),
  - ✓ the next four bits can be represented by a verb,
  - ✓ the next bit by the second article, and
  - ✓ the last five bits by another noun (object).

Text Cover

For example, the secret data “Hi”, which is 01001000 01001001 in ASCII, could be a sentence like the following:

article- noun- verb- article- noun.



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

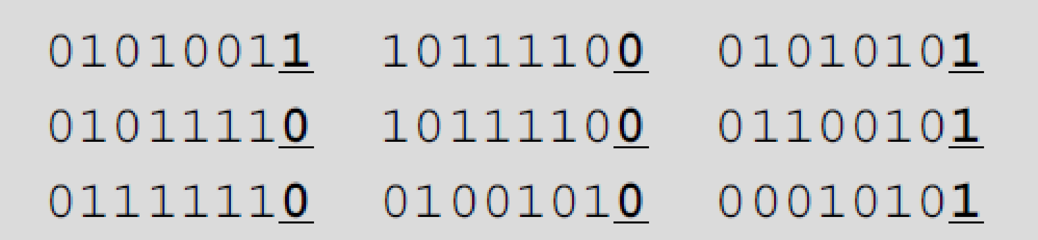
Image Cover

- Secret data can also be covered under a color image.
- Digitized images are made of pixels (picture elements), in which normally each pixel uses 24 bits (three bytes).
- Each byte represents one of the primary colors (red, green, or blue).

- In a method called LSB (least significant bit), the least significant bit of each byte is set to zero. This may make the image a little bit lighter in some areas, but this is not normally noticed.
- Now we can hide a binary data in the image by keeping or changing the least significant bit. If our binary digit is 0, we keep the bit; if it is 1, we change the bit to 1.
- In this way, we can hide a character (eight ASCII bits) in three pixels.

Image Cover

For example, the following three pixels can represent the letter M.



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

Other Covers

Other covers are also possible.
The secret message can be covered under audio and video.

End