Cryptography

Cryptography

- An original message is known as the **plaintext**, while the coded message is called the **ciphertext**.
- The process of converting from plaintext to ciphertext is known as **enciphering** or **encryption**; restoring the plaintext from the ciphertext is **deciphering** or **decryption**.
- The many schemes used for encryption constitute the area of study known as **cryptography**. Such a scheme is known as a **cryptographic system** or a **cipher**.
- Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of **cryptanalysis**.
- Cryptanalysis is what the layperson calls “breaking the code.” The areas of cryptography and cryptanalysis together are called **cryptology**

Cryptography

- **Cryptography**, a word with Greek origins, means “secret writing.”
- We use the term to refer to the science and art of transforming messages to make them secure and immune to attacks.
- Although in the past cryptography referred only to the encryption and decryption of messages using secret keys
- Now, it is defined as involving three distinct mechanisms: symmetric-key encipherment, asymmetric-key encipherment, and hashing.

Symmetric key encipherment

- Also called secret-key encipherment or secret key cryptography
- Symmetric-key encipherment uses a single secret key for both encryption and decryption.
- Encryption/decryption can be thought of as electronic locking.
- In symmetric key enciphering, Alice puts the message in a box and locks the box using the shared secret key; Bob unlocks the box with the same key and takes out the message.

Asymmetric key encipherment

- Also called public-key encipherment or public-key cryptography
- First, 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.
- The digest is normally much smaller than the message.
- To be useful, both the message and the digest must be sent to Bob.
- Hashing is used to provide checkvalues, to verify the data integrity.

Steganography

- The word steganography, with origin in Greek, means “covered writing,” in contrast with 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.

Steganography

- Historical use
  - Invisible inks (such as onion juice or ammonia salts) were also used to write a secret message between the lines of the covering message or on the back of the paper; the secret message was exposed when the paper was heated or treated with another substance.
  - Some letters in an innocuous message might be overwritten in a pencil lead that is visible only when exposed to light at an angle.
  - the first or second letter of each word in the covering message might compose a secret message. Microdots were also used for this purpose.

Security Goals

- CIA Triad

Figure 1.1 *Taxonomy of security goals*

Confidentiality

- Confidentiality not only applies to the storage of the information, it also applies to the transmission of information.
- When we send a piece of information to be stored in a remote computer or when we retrieve a piece of information from a remote computer, we need to conceal it during transmission.
- e.g In banking, customers' accounts need to be kept secret.

Integrity

- 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 activity.
- An interruption in the system, such as a power surge, may also create unwanted changes in some information.
- e.g 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.

Availability

- The third component of information security is availability.
- The information created and stored by an organization needs to be available to authorized entities.
- Information is useless if it is not available.
- The unavailability of information is just as harmful for an organization as the lack of confidentiality or integrity.
- E.g what would happen to a bank if the customers could not access their accounts for transactions?

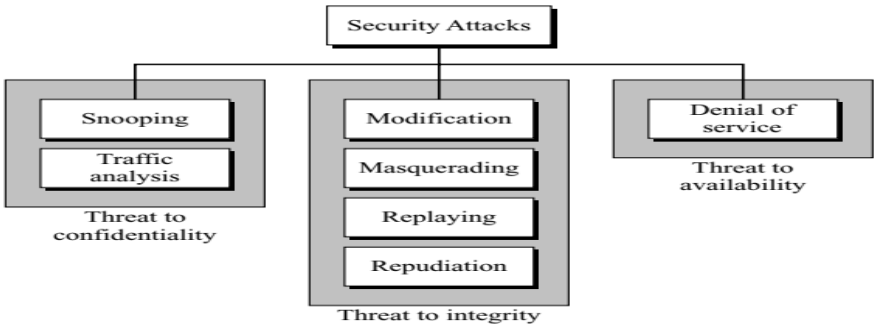
Security goals Cont..

- Although the CIA triad define security objectives, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are as follows:
- **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means 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.
- This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after action recovery and legal action. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

Attacks

- Goals of security can be threatened by security attacks.

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



Attacks Threatening Confidentiality

- Snooping
  - Snooping refers to unauthorized access to or interception of data.
  - 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.
  - 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, she can obtain some other type information by monitoring online traffic.
  - For example, she can *find the e-mail address of the sender or the receiver.*
  - *She can collect pairs* of requests and responses to help her guess the nature of transaction.

Attacks Threatening Integrity

- The integrity of data can be threatened by several kinds of attacks:
- Modification
  - After intercepting or accessing information, the attacker modifies the information to make it beneficial to herself.
  - For 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.
  - Sometimes the attacker simply deletes or delays the message to harm the system or to benefit from it.

Attacks Threatening Integrity Cont..

- Masquerading
  - Masquerading, or spoofing, happens when the attacker impersonates somebody else.
  - For example, an attacker might steal the bank card and PIN of a bank customer and pretend that she is that customer.
  - Sometimes the attacker pretends instead to be the receiver entity.
  - For example, a user tries to contact a bank, but another site pretends that it is the bank and obtains some information from the user.

Attacks Threatening Integrity Cont..

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

Attacks Threatening Integrity Cont..

- Repudiation
  - This type of attack is different from others because it is performed by one of the two parties in the communication: the sender or the receiver.
  - The 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.
  - An example of denial by the sender would be a bank customer asking her bank to send some money to a third party but later denying that she has made such a request.
  - An example of denial by the receiver could occur when a 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.

Attacks Threatening Availability

- Denial of Service
  - Denial of service (DoS) is a very common attack.
  - It may slow down or totally interrupt the service of a system.
  - The attacker can use several strategies to achieve this.
  - She might send so many bogus requests to a server that the server crashes because of the heavy load.
  - The attacker might intercept and delete a server's response to a client, making the client to believe that the server is not responding.
  - The attacker may also intercept requests from the clients, causing the clients to send requests many times and overload the system.

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

Passive Attacks

- Attacker's goal is just to obtain information. i.e the attack does not modify data or harm the system.
- The system continues with its normal operation. However, the attack may harm the sender or the receiver of the message.
- Attacks that threaten confidentiality, snooping and traffic analysis are passive attacks.
- The revealing of the information may harm the sender or receiver of the message, but the system is not affected. For this reason, 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.