Name : Afsana Akter Mitu
Date : 16-04-2025

Lecture – 2

Cryptography and Cyber Law

Security Goals:

In cryptography, the primary security goals are to ensure confidentiality, integrity and authentication. These goals aim to protect data privacy, verify its authenticity and origin and prevent modification or denial of sender identity.

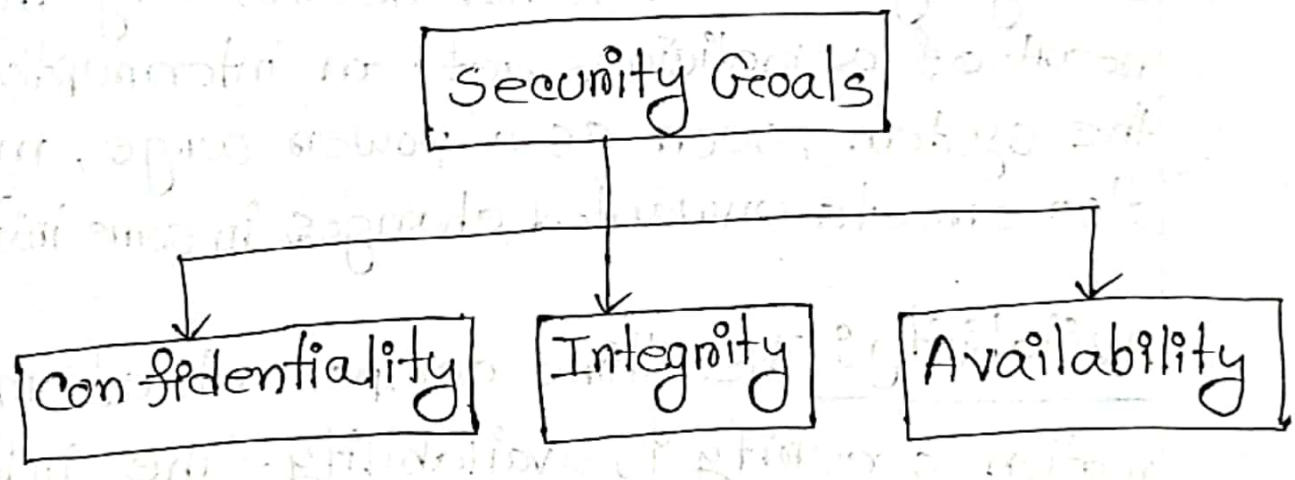


Figure : Taxonomy of security goals

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 action that endangers the confidentiality of its information.

Integrity: Information needs to be changed constantly. Integrity means that changes need to be done by only by authonized entities and through authonized mechanism. 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.

Availability: The thind component of information security is availability. The information created and stored by an organization needs to be available to authonized entities. Information is useless if it is not available..

Cyber Attacks:

Our three goals of security - confidentiality, integrity and availability - can be threatened by security attacks. Although the literature uses different approaches to catagonizing the attacks, we will first divide them into three groups related to the security goals.

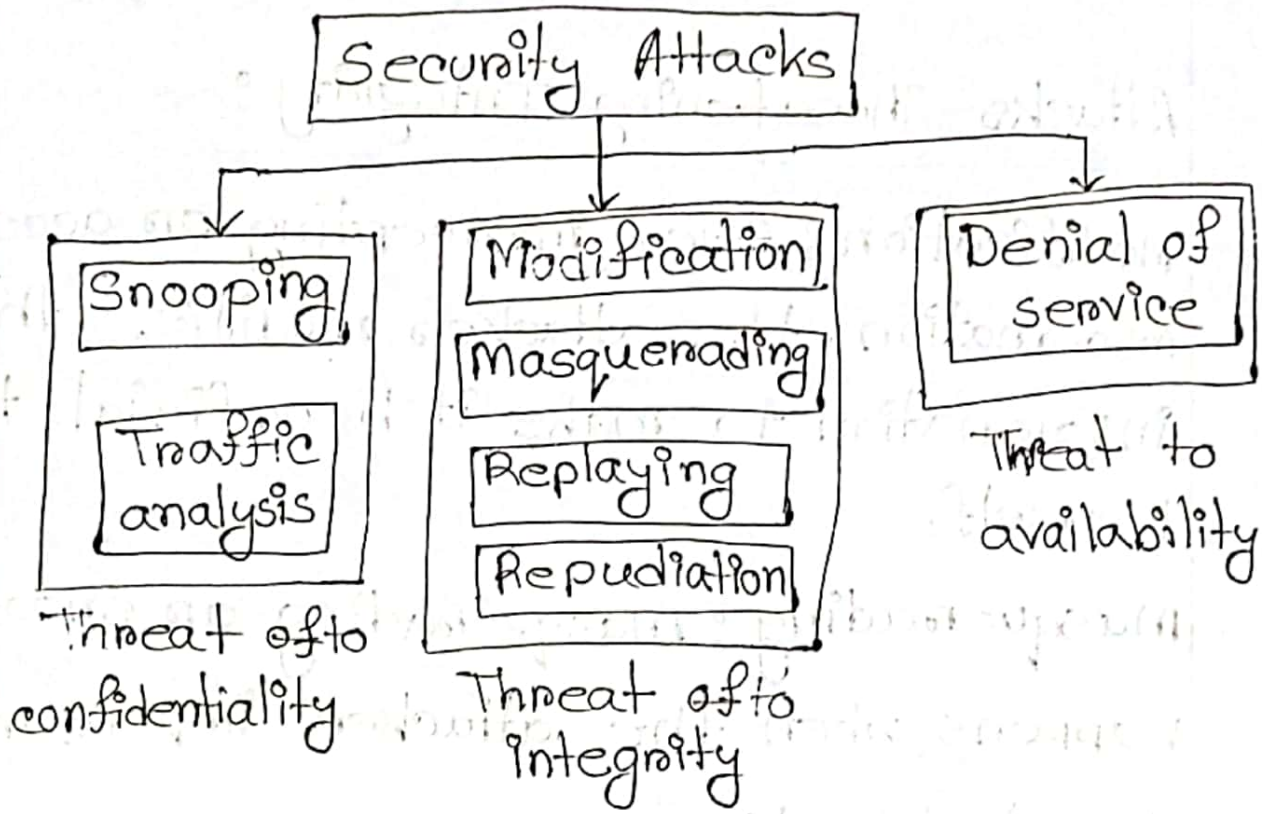


Figure: Taxonomy of attacks with relation to security goals

Attacks Threating Confidentiality:

Snooping: Snooping refers to unauthorized access to or interception of data.

Traffic Analysis: Although encipherment of data may make it nonintelligible for the interceptor, she can obtain some other type information by monitoring online traffic.

Attacks Threatening Integrity:

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

masquerading: Masquerading or snoofing happens when the attacker impersonates somebody else.

Replaying : Replaying is another attack. The attacker obtains a copy of message sent by a user and later tries to reply it.

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.

Attacks Threatening Availability :

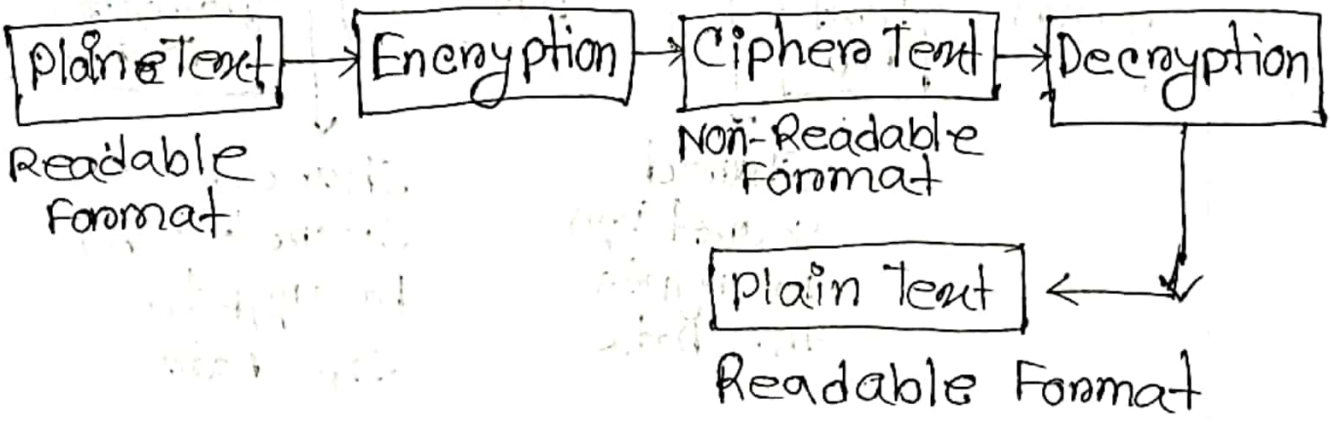
Denial of Service : Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.

Passive Attacks: In a 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. However, the attack may harm the sender or the receiver of the message. Attacks that threaten confidentiality snooping and traffic analysis - are passive attacks.

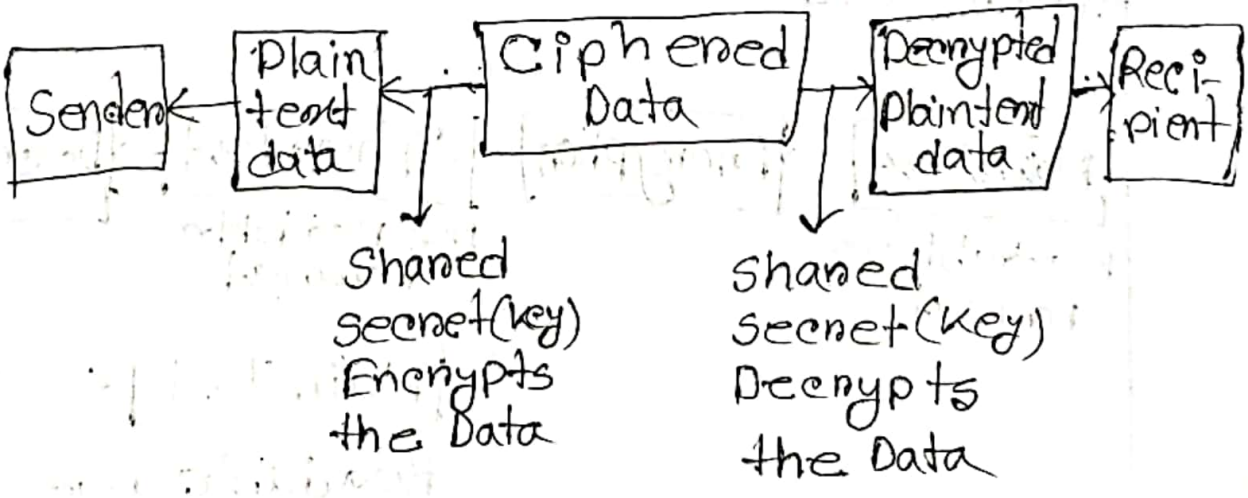
Active Attacks: An active attack may change the data or harm the system. Attacks that threaten the integrity and availability are active attacks. Active attacks are normally easier to detect than to prevent, because an attacker can launch them in a variety of ways.

Cryptography :

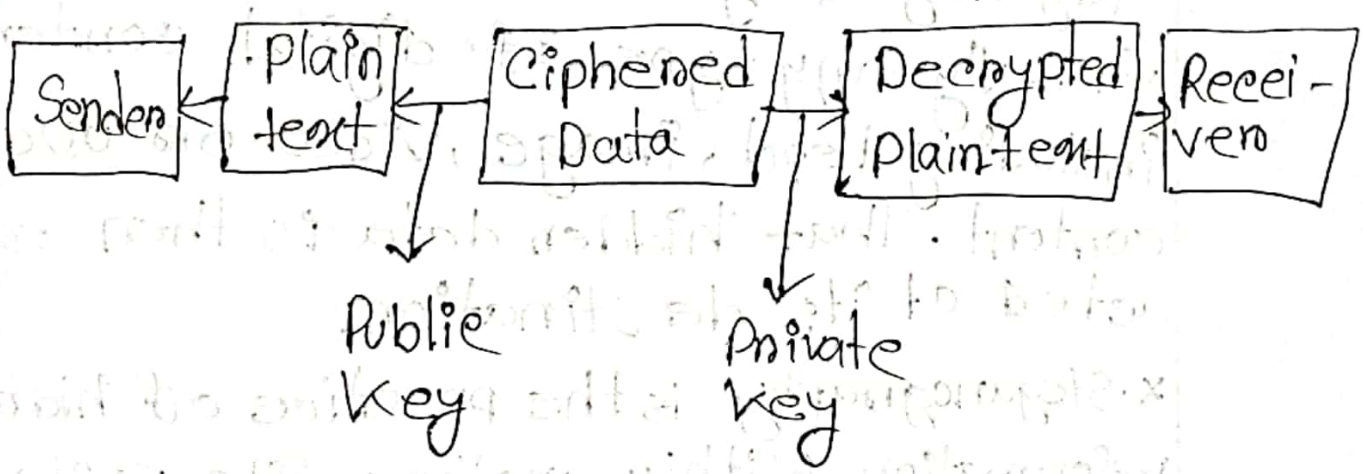
Cryptography is a technique of securing information and communications through the use of codes so that only those person for whom the information is intended can understand and process it. Thus, preventing unauthonized access to information. In cryptography, the techniques that are used to protect information are obtained from mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in ways that make it hard to decode them.



Symmetric key Cryptography: It is an encryption system where the sender and receiver of a message use a single common key to encrypt and decrypt messages. Symmetric key cryptography is faster and simpler but the problem is that the sender and receiver have to somehow exchange keys securely. The most popular symmetric key cryptography system are Data Encryption Systems (DES) and Advanced Encryption systems (AES)



Asymmetric key cryptography: In asymmetric key cryptography, a pair of keys is used to encrypt and decrypt information. A sender's public key is used for encryption and receiver's private key is used ~~to~~ for decryption. Public keys and Private keys are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone known his private key. The most popular asymmetric key cryptography algorithm is the RSA algorithm.



Hashing : In hashing, a fixed-length message digest is created out-of a variable-length message. The digest is normally much smaller then the message. To be useful, both the message and the digest must be sent to Bob. Hashing is used to provide check values, which were discussed earlier in relation to providing data integrity.

Steganography : Steganography is the practice of concealing information within another message or physical object to avoid detection. steganography can be used to hide virtually any type of digital content, including text, image, video or audio content. That hidden data is then extracted at its destination.

* Steganography is the practice of hiding information within another file or object.