Computer Security is basically the protection of computer systems and information from harm, theft and unauthorized use.

Computer security attempts to ensure the confidentiality, integrity, and availability of computing systems' components.

* Confidentiality ensures that computer-related assets are accessed only by authorized parties. That is, only those who should have access to something will actually get that access. By "access," we mean not only reading but also viewing, printing, or simply knowing that a particular asset exists. Confidentiality is sometimes called secrecy or privacy.
* Integrity means that assets can be modified only by authorized parties or only in authorized ways. In this context, modification includes writing, changing, changing status, deleting, and creating.
* Availability means that assets are accessible to authorized parties at appropriate times. In other words, if some person or system has legitimate access to a particular set of objects, that access should not be prevented. For this reason, availability is sometimes known by its opposite, denial of service.

A vulnerability is a weakness in the security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access.

A threat to a computing system is a set of circumstances that has the potential to cause loss or harm. A human who exploits a vulnerability perpetrates an attack on the system. A threat is blocked by control of a vulnerability.

**Kinds of Threats**

An **interception** means that some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system. Examples of this type of failure are illicit copying of program or data files, or wiretapping to obtain data in a network. Although a loss may be discovered fairly quickly, a silent interceptor may leave no traces by which the interception can be readily detected.

In an **interruption**, an asset of the system becomes lost, unavailable, or unusable. An example is malicious destruction of a hardware device, erasure of a program or data file, or malfunction of an operating system file manager so that it cannot find a particular disk file.

If an unauthorized party not only accesses but tampers with an asset, the threat is a **modification**. For example, someone might change the values in a database, alter a program so that it performs an additional computation, or modify data being transmitted electronically. It is even possible to modify hardware. Some cases of modification can be detected with simple measures, but other, more subtle, changes may be almost impossible to detect.

Finally, an unauthorized party might create a **fabrication** of counterfeit objects on a computing system. The intruder may insert spurious transactions to a network communication system or add records to an existing database. Sometimes these additions can be detected as forgeries, but if skillfully done, they are virtually indistinguishable from the real thing. These four classes of threats interception, interruption, modification, and fabrication describe the kinds of problems we might encounter.

Attacks Threatening Confidentiality

**Snooping**

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

**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 electronic address (such as 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, masquerading, replaying, and repudiation.

**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. Note that sometimes the attacker simply deletes or delays the message to harm the system or to benefit from it.

**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.

**Replaying**

Replaying is another attack. 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.

**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

**TYPES OF ATTACKS**

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. 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, however, 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.

**Methods of Defense**

1. Prevent attack
2. Detect attack: Make attack harder
3. Deflect attack: Make another target more attractive
4. Detect attack
5. Recover from attack

**Security Services**

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

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

1. Data Confidentiality
2. Data Integrity
3. Authentication
4. Non Repudiation
5. Access Control

**Security Mechanisms**

**Encipherment**

Encipherment, hiding or covering data, can provide confidentiality. It can also be used to complement other mechanisms to provide other services. Today two techniques cryptography and steganography-are used for enciphering.

**Data Integrity**

The 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**

A digital signature is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature. The sender uses a process that involves showing that she owns a private key related to the public key that she has announced publicly. The receiver uses the sender’s public key to prove that the message is indeed signed by the sender who claims to have sent the message

**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.

**Notarization**

Notarization means selecting a third trusted party to control the communication between two entities. This can be done, for example, to prevent repudiation. The 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 of proofs are passwords and PINs.

**CRYPTOGRAPHY**

Cryptography involves three distinct mechanisms:

Symmetric key encipherment uses a single Secret Key for both Encryption & Decryption.

Asymmetric key encipherment uses Two Keys, Public Key & Private Key for both Encryption & Decryption.

Fixed length Message Digest is created out of a variable-length message.

Symmetric Key Cryptography:

Also called secret key cryptography. Only 1 key is used for both encryption and decryption.

Execution speed is faster. Less complex and less computational power is required. Used for transfer of bulk data.

Sharing the key between sender and receiver is not safe.

Algo: DES, AES, 2DES, 3DES

Asymmetric Key Cryptography:

2 keys are used (public & private). Public key is used for encryption and private key is used for decryption. They are slower in execution. More complex and more computational power is required.

Algo: RSA, Deffie Hellman, DSA