Aspects of Security

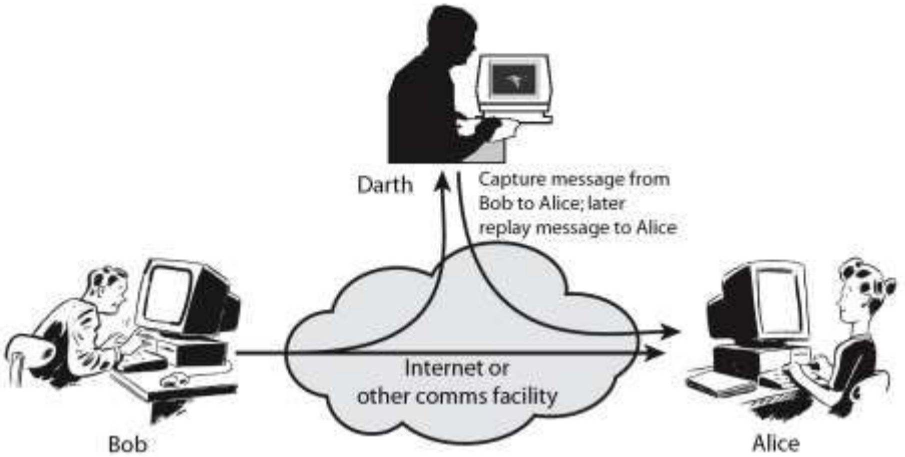
Three aspects of Information Security can be considered. They are

- **Security attack**: Any action that compromises the security of information owned by an organization.
- **Security mechanism**: A process or a device incorporating such a process that is designed to detect, prevent, or recover from a security attack.
- **Security service**: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

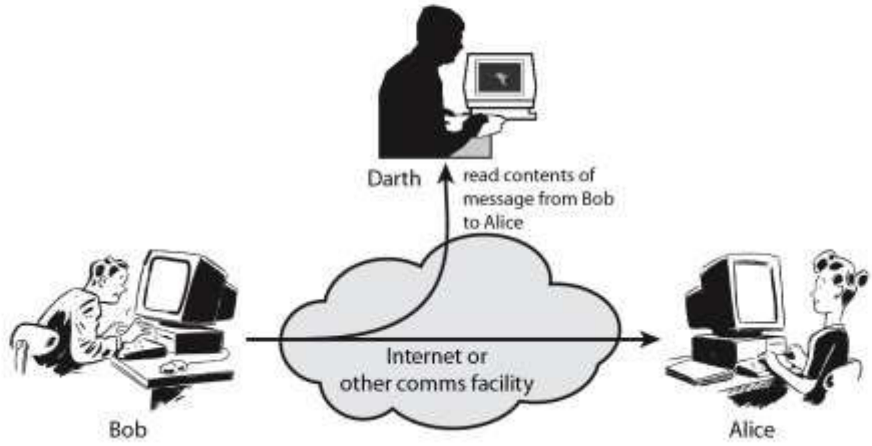
Threat is a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability. **Vulnerability** is a weakness that may be exploited in an asset or collection of assets. **Attack** is an assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Security Attacks

- Active Attack: Active attacks involve some modification of the data stream or the creation of a false stream. Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely, because of the wide variety of potential physical, software, and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them.


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

- Passive Attack: A passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. These attacks are difficult to detect because they do not involve any alteration of the data.


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Security Services

A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. These services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

- **Authentication** is concerned with assuring that a communication is authentic. Two specific authentication services are defined.
    - **Peer entity authentication** provides corroboration of the identity of a peer entity in an association
    - **Data origin authentication** provides corroboration of the source of a data unit.
- **Access control** is the ability to limit and control the access to host systems and applications via communications links.
- **Confidentiality** is the protection of transmitted data from passive attacks, and the protection of traffic flow from analysis.
- **Integrity** assures that messages are received as sent, with no duplication, insertion, modification, reordering, replay, or loss.
- **Non-repudiation** is protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.
    - **Proof of Origin**: Proof that the message was sent by the specified party.
    - **Proof of Delivery**: Proof that the message was received by the specified party.
- **Availability** is the property of a system / resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.

Security Mechanism

Security mechanism is a feature designed to detect, prevent, or recover from a security attack. There is no single mechanism that will support all services required.

The mechanisms are divided into those that are implemented in a specific protocol layer, such as TCP or an application-layer protocol, and those that are not specific to any particular protocol layer or security service. These mechanisms are called "specific security mechanisms" and "pervasive security mechanism".

- **Specific Security Mechanisms**
    - Encipherment: This is the process of using mathematical algorithms to transform data into a form that is not readily intelligible.
    - Digital Signature: Data or cryptographic transformation of a data unit is appended to the data, so that the recipient of the data unit is convinced of the source and integrity of the data unit and this can also serve to protect the data against forgery (e.g., by the recipient).
    - Access Control: A variety of mechanisms are available that enforce access rights to resources.
    - Data Integrity: A variety of mechanisms may be used to assure the integrity of a data unit or stream of data units.
    - Authentication Exchange: This is a mechanism intended to ensure the identity of an entity by means of information exchange.
    - Traffic Padding: The insertion of bits into gaps in a data stream is called traffic padding. This helps to thwart traffic analysis attempts.
    - Routing Control: enables selection of particular physically secure routes for certain data transmission and allows routing changes, especially when a breach of security is suspected.
    - Notarization: This is the use of a trusted third party to assure certain properties of a data exchange
- **Pervasive Security Mechanisms**
    - Trusted Functionality: The process that which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
    - Security Label: This is the technique of marking of a bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
    - Event Detection: Detection of security-relevant events such as forgery, denial of sending or receiving of data, alteration of data etc. is another important essential mechanism.
    - Security Audit Trail: Data can be collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
    - Security Recovery: This deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.