Lec2: Introduction of threats and attacks

Threat

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.

Attack

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 Aspects

It is helpful to have a model that can be used as a foundation or a baseline. This gives a consistent set of terminology and concepts for defining the security requirements and characterizing the approaches to satisfying those requirements. The security aspects focus on security attacks, mechanisms, and services. These can be defined briefly as follows:

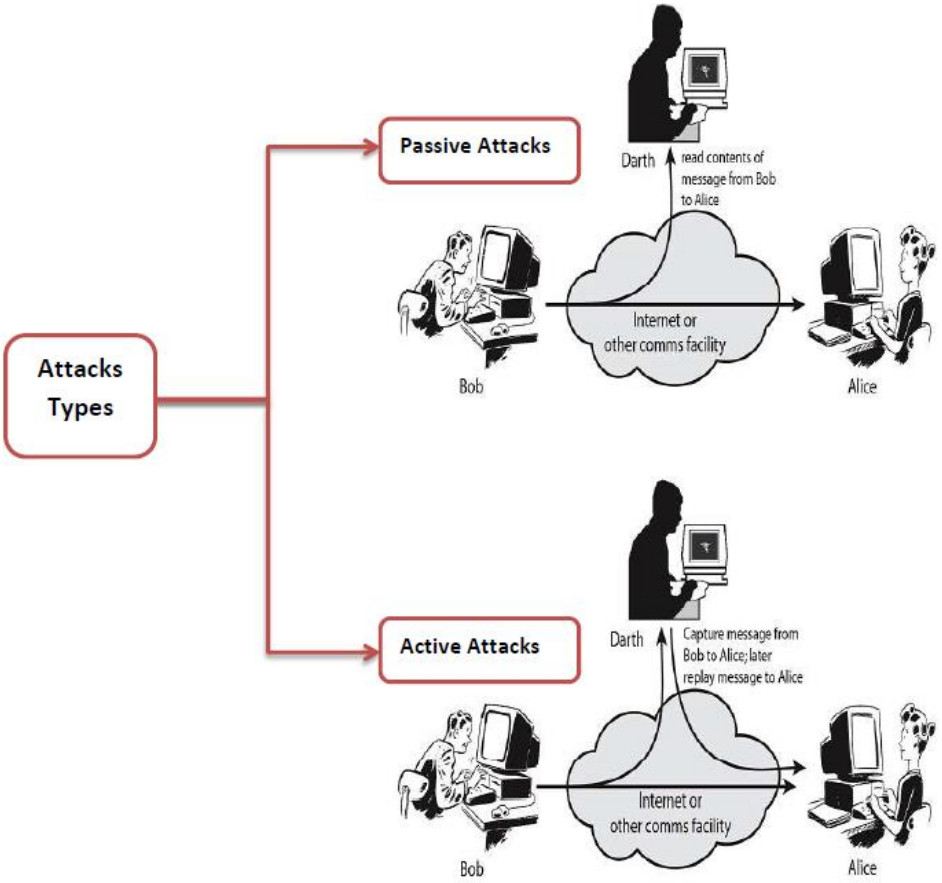
• Security attacks: Any action that compromises the security of information owned by an organization.

• Security mechanism: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

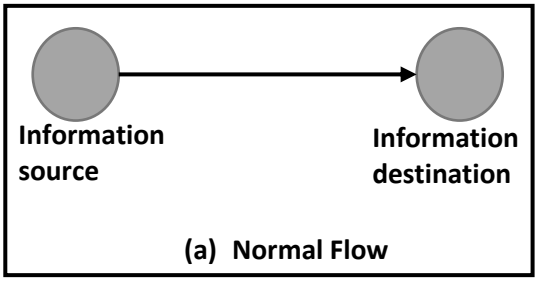
• Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Security Attacks

The security attacks can be classified in to **passive attacks** and **active attacks** as shown in the Figure below. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.



Security is essential when the function of the computer system is to provide information. The normal flow of information from source to destination is shown in figure.



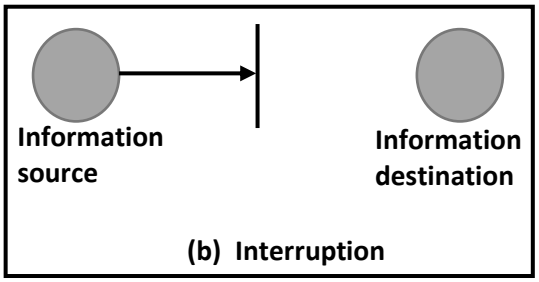
There are four general categories of attack.

- Interruption
- Interception
- Modification

- Fabrication

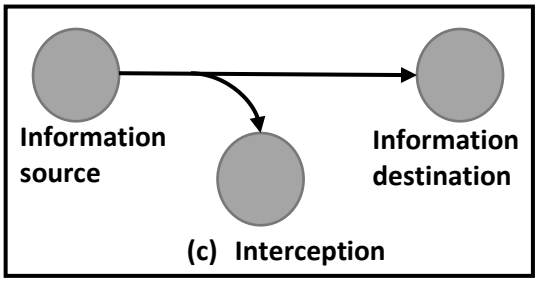
Interruption

An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability. Examples include destruction of a piece of hardware, such as a hard disk, the cutting of a communication line, or the disabling of the file management system.



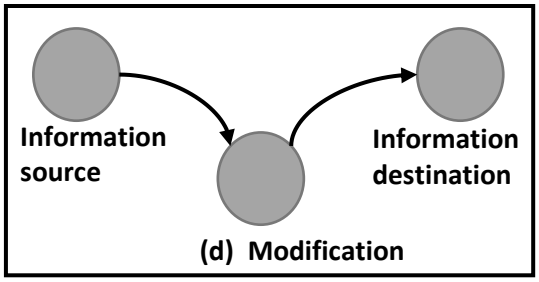
Interception

An unauthorized party gains access to an asset. This is an attack on confidentiality. The unauthorized party could be a person, a program, or a computer. Examples include wiretapping to capture data in a network, and the unauthorized copying of files or programs.



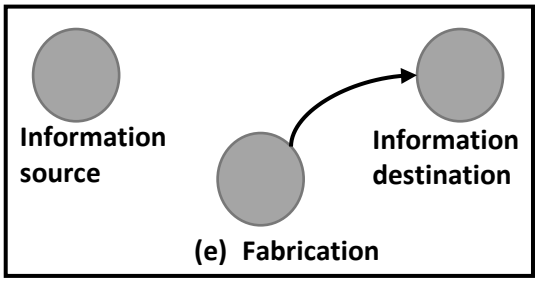
Modification

An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. Examples include changing values in a data file, altering a program so that it performs differently, and modifying the content of messages being transmitted in a network.



Fabrication

An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. Examples include the insertion of spurious messages in a network or the addition of records to a file.



From above we can understand the Attack in Active attacks and Passive attacks with subdivided categories in clear concepts as the following:

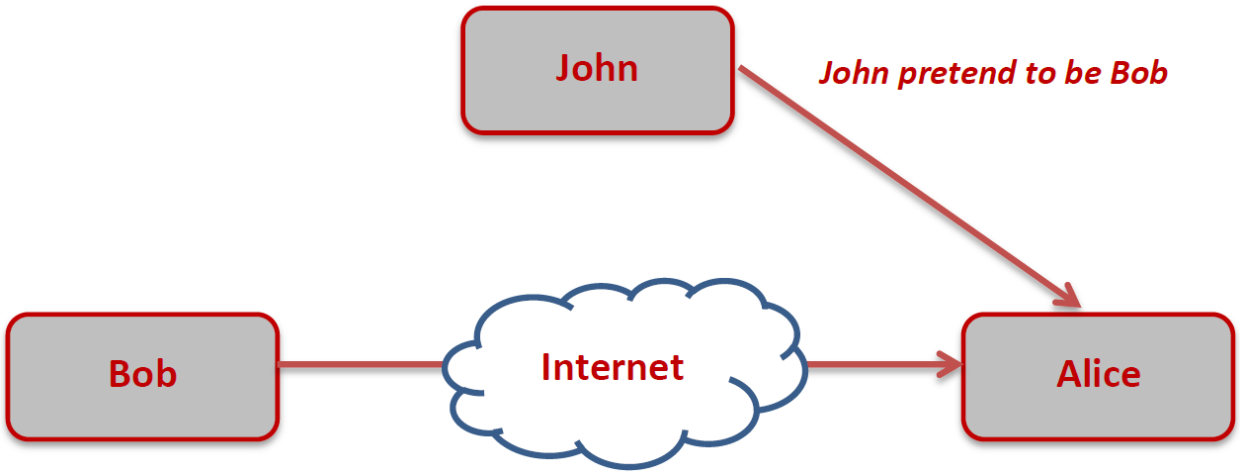
Active attacks

These attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories

- Masquerade
- Replay
- Modification of message contents
- Denial of service

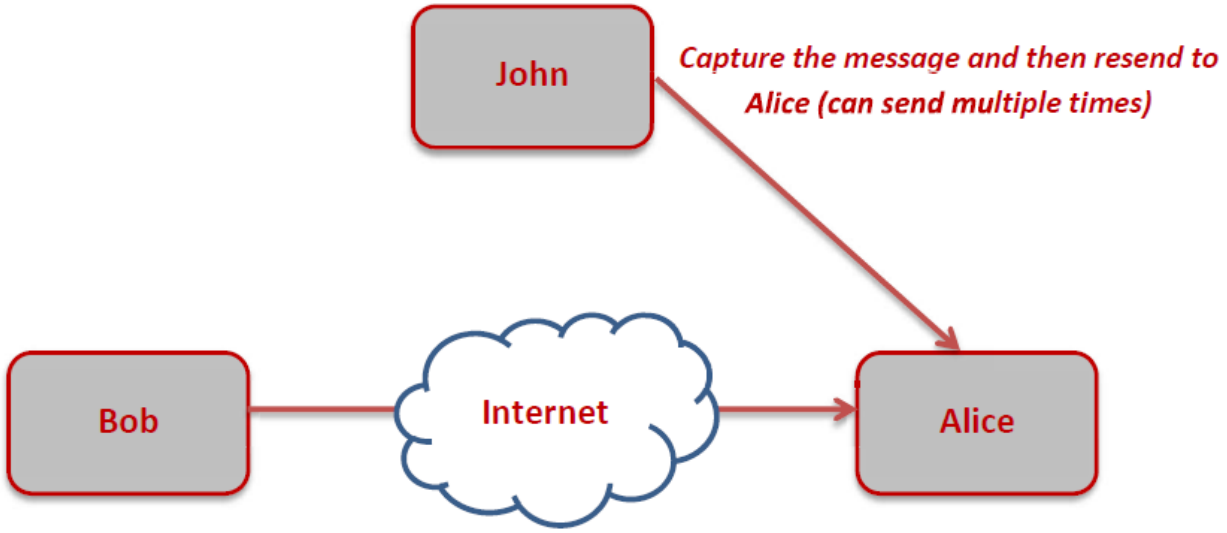
Masquerade

A masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.



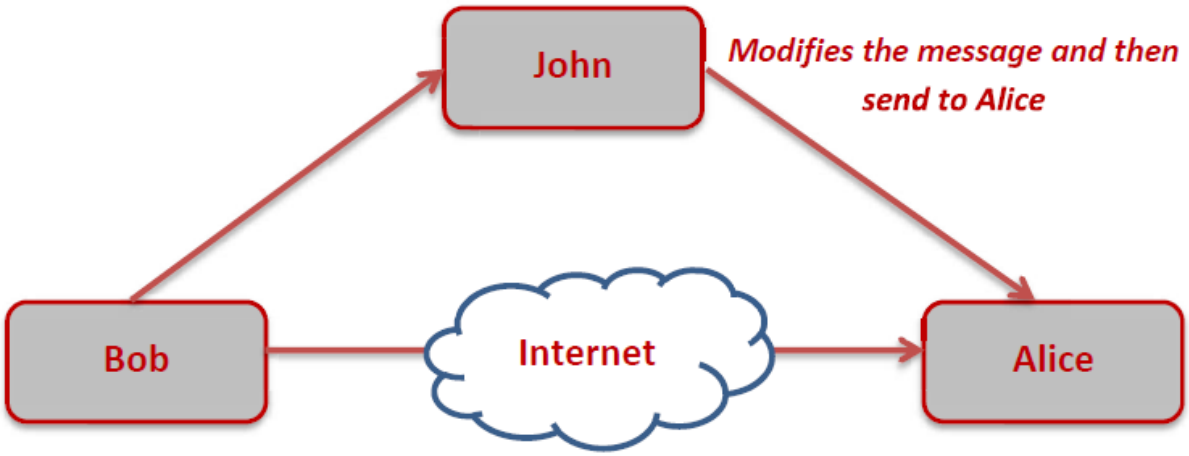
Replay

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.



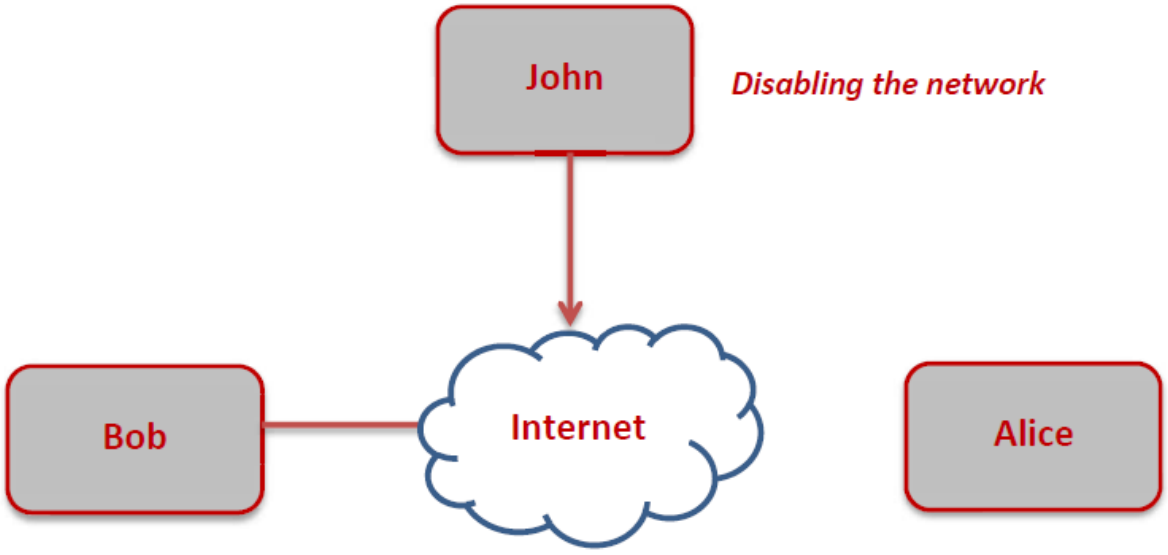
Modification of message contents

It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. For example, a message meaning "Allow Alice to read confidential file X" is modified as "Allow John to read confidential file X".



Denial of service

The denial of service prevents or inhibits the normal use or management of communication facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.



Note: Active attacks present the opposite characteristics of passive attacks. It is quite difficult to prevent active attacks absolutely because of the wide variety of physical, software, and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any delays caused by them. If the detection has a deterrent effect, it may also contribute to prevention.

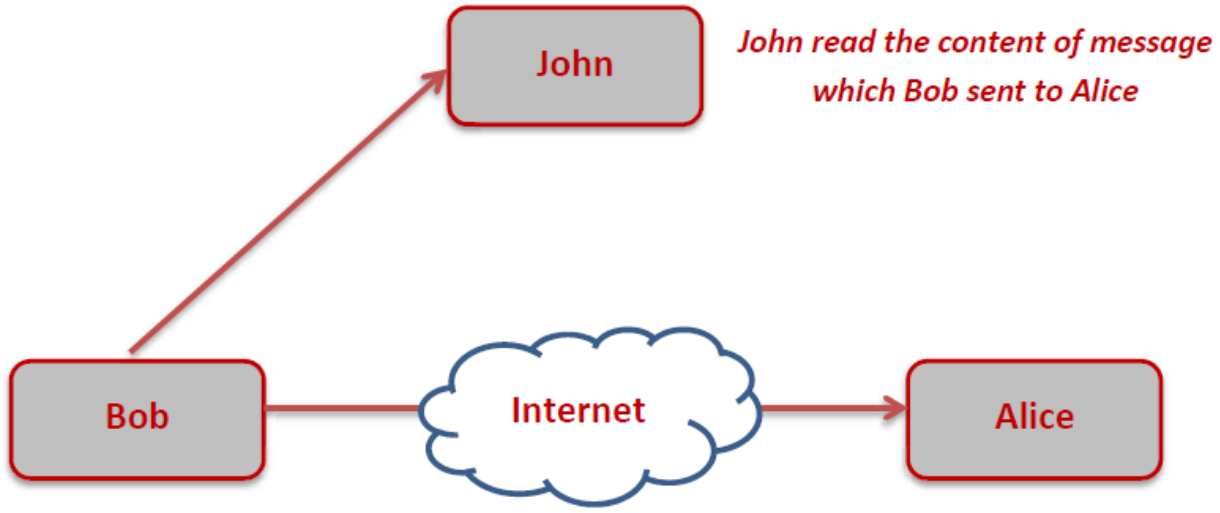
Passive Attacks

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. Two types of passive attacks are

- Release of message contents
- Traffic analysis.

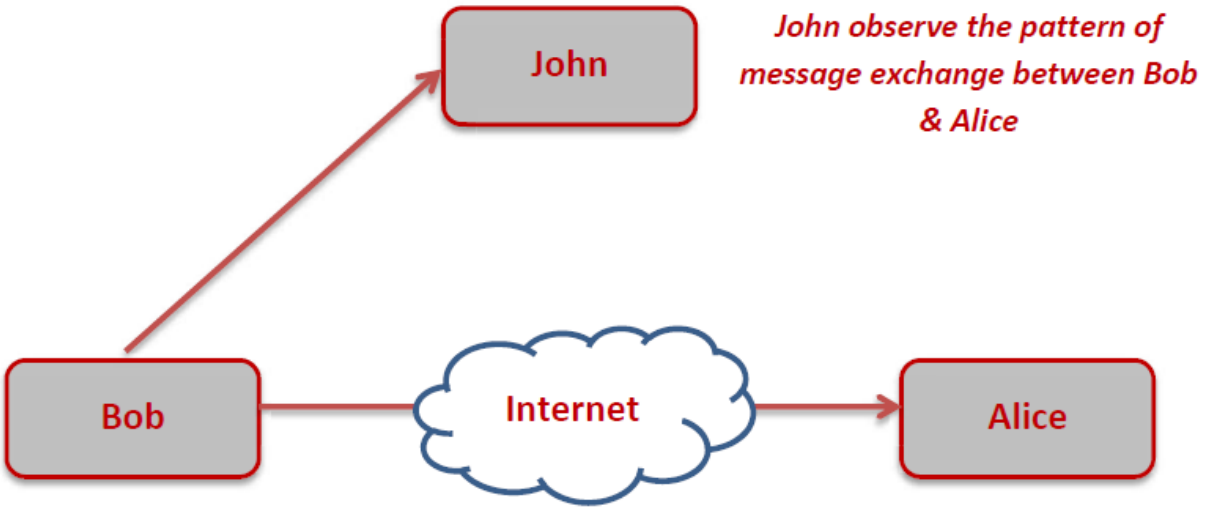
Release of message contents

A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions



Traffic analysis

Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.



Note: passive attacks are **very difficult to detect**, because they do not involve any alteration of the data and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the passive attacks are **prevented rather than detected**.

Threats and Vulnerabilities

Vulnerability is a weakness in the security system, for example, in procedures, design, or implementation that might be exploited to **cause loss or harm**.

A threat to a computing system is a set of circumstances that has the potential to **cause loss or harm**.

To see the difference between a threat and vulnerability consider the illustration in Figure below. Here, a wall is holding water back. The water to the left of the wall is a threat to the man on the right of the wall: The water could rise, overflowing onto the man, or it could stay under the height of the wall. So, **the threat** of harm is the potential for the man to get wet or get hurt. However, the small crack in the wall is a **vulnerability** that threatens the man's security. If the water rises to the level of the crack, it will exploit the vulnerability and harm the man.