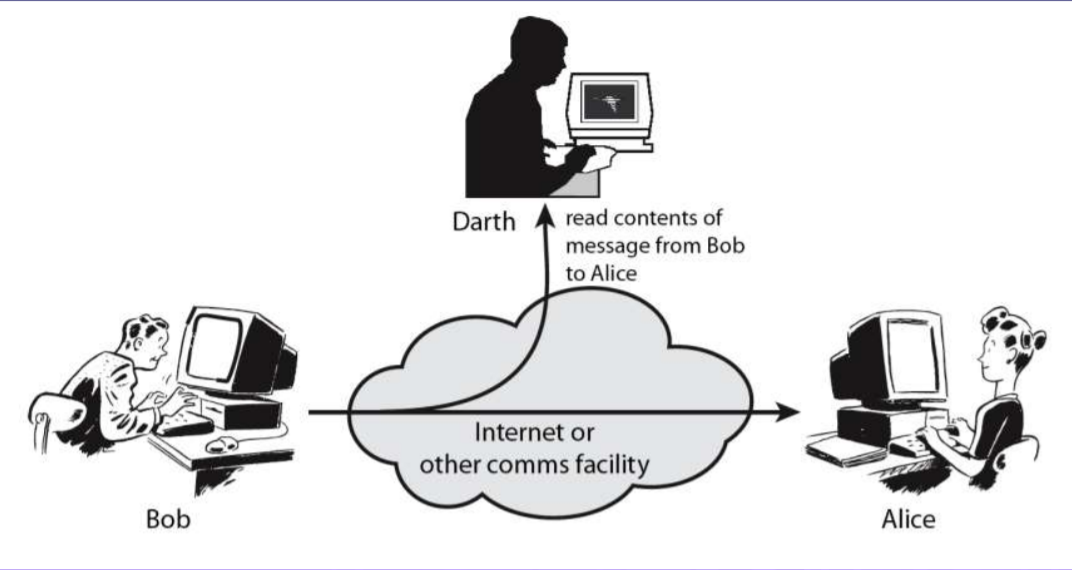
**Security Attacks**

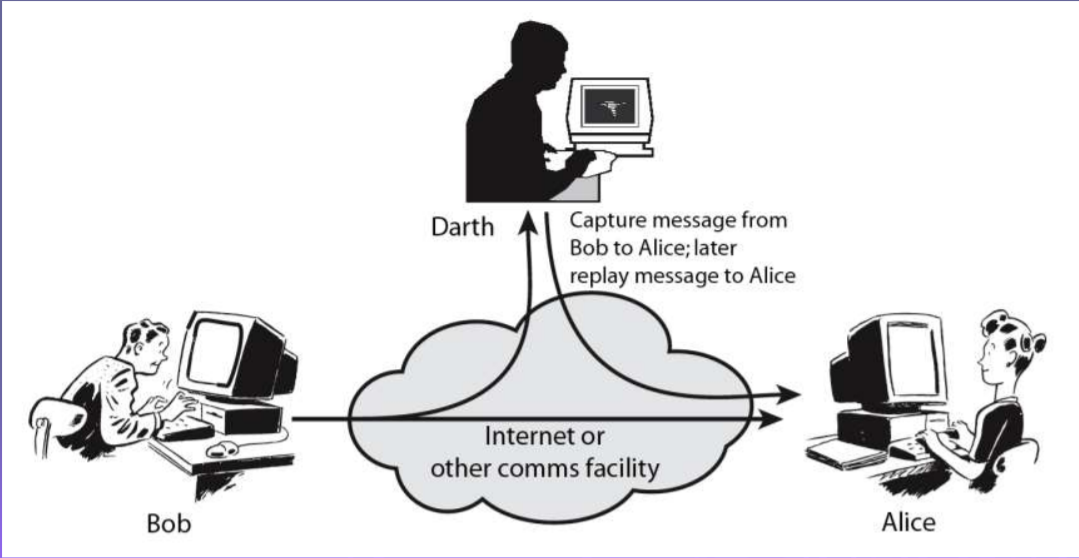
* A security attack is an unauthorized attempt to steal, damage, or expose data from an information system such as your website or data owned by an organization.
* Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems.
* often threat & attack used to mean same thing
* There are 2 types of security attacks:
  + Active
  + Passive

**Passive attacks**

****

* 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 transmission. The goal of the opponent is to obtain information that is being transmitted. Types of Passive attacks are as following:
  + The release of message contents is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.
  + A second type of passive attack, traffic analysis, is subtlers. 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.
* Passive attacks are very difficult to detect, because they do not involve any alteration of the data.

**Active attacks**



* An Active attack attempts to alter system resources or effect their operations. Active attack involve some modification of the data stream or creation of false statement. Types of active attacks are as following:
  + Masquerade:
    - Masquerade attack takes place when one entity pretends to be a different entity. A Masquerade attack involves one of the other forms of active attacks.
  + Modification of messages:
    - 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 JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.
  + Replay:
    - It involves the passive capture of a message and its subsequent transmission to produce an authorized effect.
  + Repudiation:
    - This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has send or receive a message. For example, customer ask his Bank “To transfer an amount to someone” and later on the sender(customer) deny that he had made such a request. This is repudiation.
  + **Denial of Service:**
    - A Denial of Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

**Security Service**

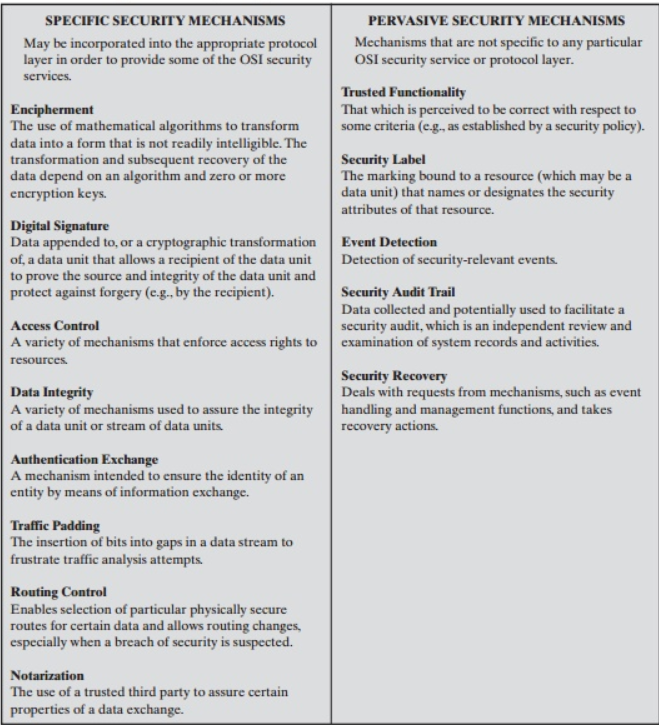
* enhance security of data processing systems and information transfers of an organization
* intended to counter security attacks
* using one or more security mechanisms
* **X.800**
  + “a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers”
* **RFC 2828**
  + “a processing or communication service provided by a system to give a specific kind of protection to system resources”

**Security Services (X.800)**

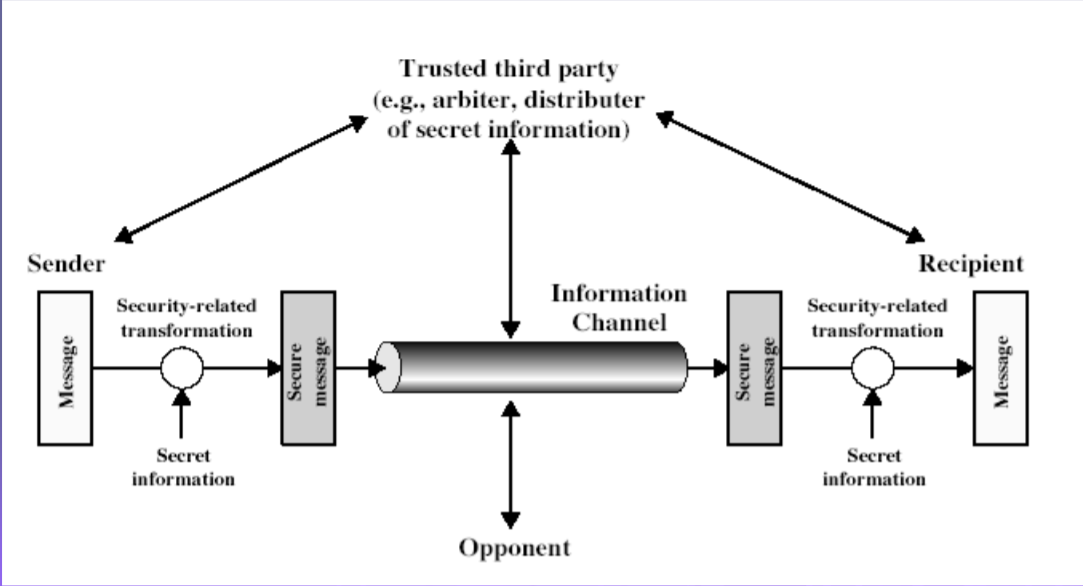
* Authentication
  + assurance that the communicating entity is the one claimed
* Access Control
  + prevention of the unauthorized use of a resource
* Data Confidentiality
  + protection of data from unauthorized disclosure
* Data Integrity
  + assurance that data received is as sent by an authorized entity
* Non-Repudiation
  + protection against denial by one of the parties in a communication

**Security Mechanism**

* feature designed to detect, prevent, or recover from a security attack
* no single mechanism that will support all services required
* however, one particular element underlies many of the security mechanisms in use
  + cryptographic techniques

****

**Model for Network Security**

****

* When we send our data from source side to destination side we have to use some transfer method like the internet or any other communication channel by which we are able to send our message. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. When the transfer of data happened from one source to another source some logical information channel is established between them by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.
* When we use the protocol for this logical information channel the main aspect security has come. who may present a threat to confidentiality, authenticity, and so on.
* A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.
* Using this model requires us to:
  1. Design a suitable algorithm for the security transformation.
  2. Generate the secret information (keys) used by the algorithm.
  3. Develop methods to distribute and share the secret information.
  4. Specify a protocol enabling the principals to use the transformation and secret information for a security service.