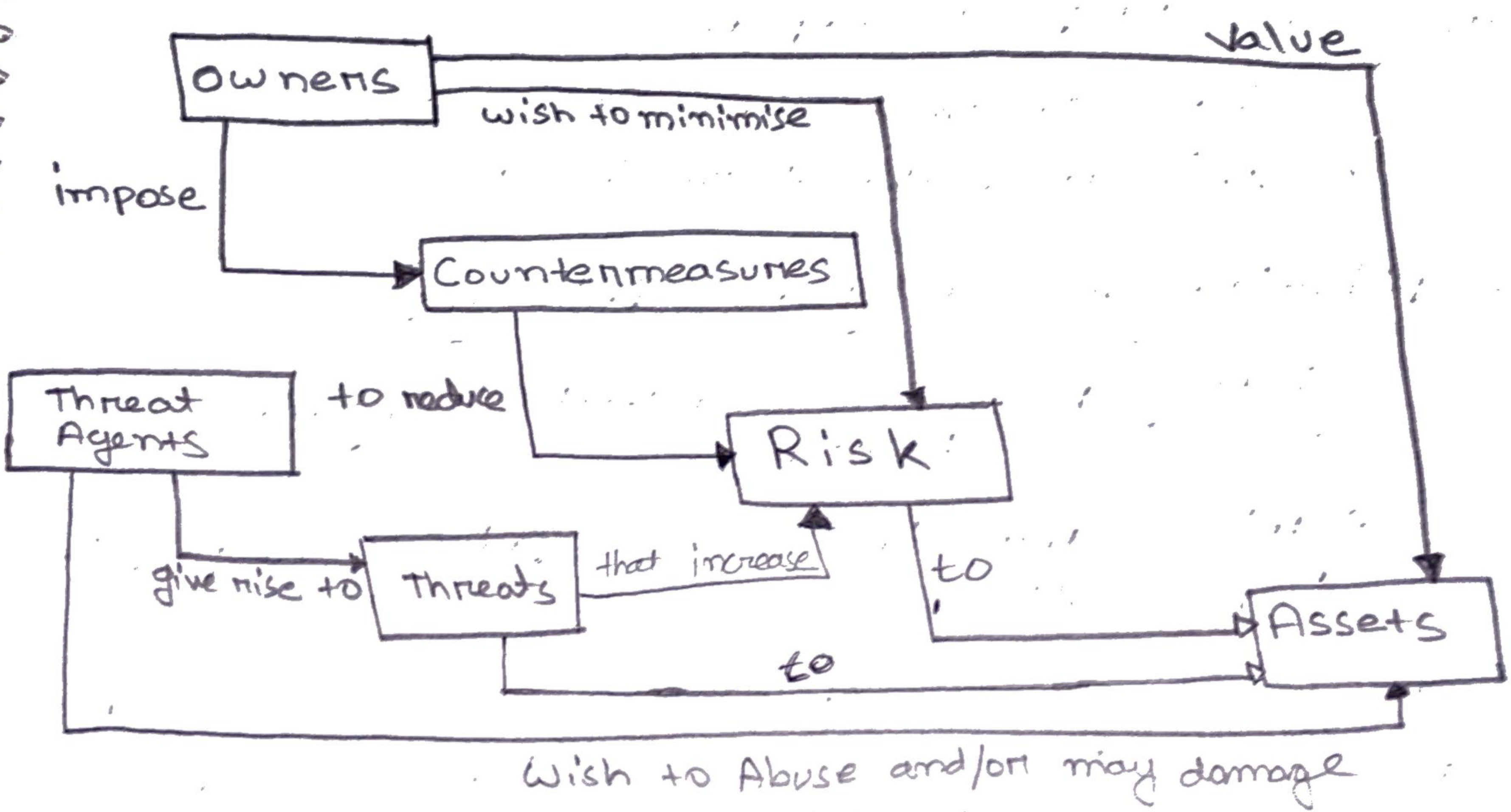
Common Criteria Terminologies



Defining Security,

The Security of a system, application, or protocol is always relative to

- A set of desired properties
- An adversary (attacker) with specific capabilities

Academic study of security (mostly) not about

- Breaking into a system
- How to launch a system

Our focus will be to explore

- why a system is insecure
- How to make them Secure.

Confidentiality: Secrecy and Privacy,

- (Secrecy) Protecting unauthorised information access and disclosure,
- (Privacy) Protecting Personal privacy and proprietary information,

Secrecy assures that ~~privacy~~ Private or confidential information is not made available or disclosed to unauthorised individuals,

Privacy assures that individuals control or influence what information related to them may be collected and stored and by/to whom that may be disclosed,

The need of confidentiality predates computer systems.

- Anonymity: The property that certain records or transactions not to be attributable to any individual.

Tools,

Mixing: The intertwining of transactions, information or communications in a way that cannot be traced to any individual.

Proxies: Trusted agents that are willing to engage in actions for an individual in a way that cannot be traced back to that person.

Pseudonyms: fictional identities that can fill in for real identities in communications and transaction, but are otherwise known only to a trusted entity.

Security attacks,

Two types,

1. Passive
2. Active

Passive attacks,

- eavesdropping on, or monitoring of transmissions. eavesdropping means secretly listening to or monitoring someone else's conversations or communication without their knowledge or permission.

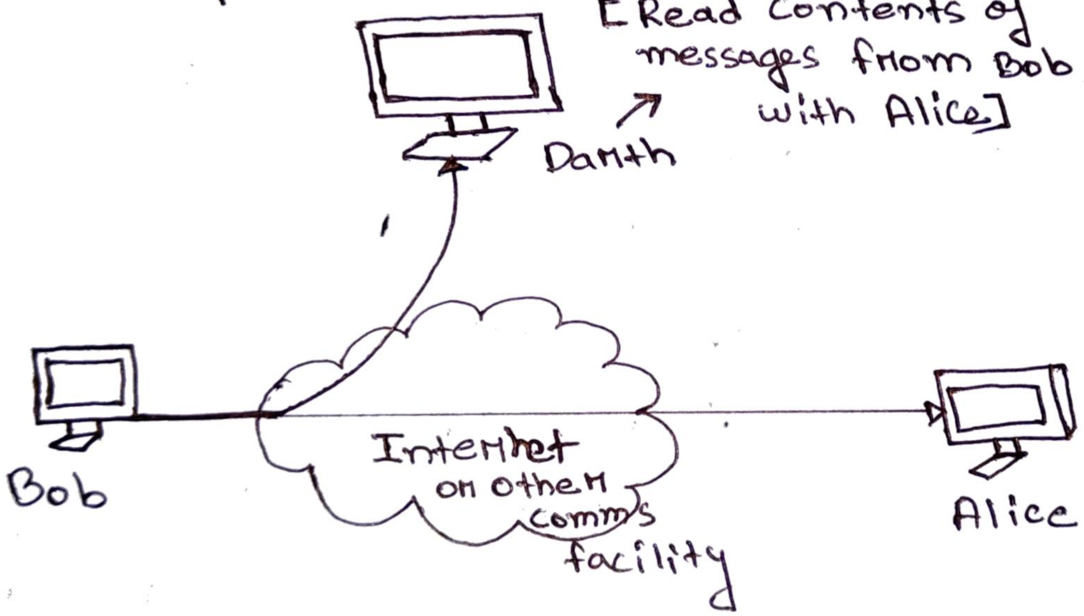
- The goal is to obtain and analyse transmitted information.

Active attacks,

- Involving some modification of the data stream or the creation of a false stream. Modification of the data stream means altering the message being sent, such as changing a message's content. Creation of a false stream means ~~sending~~ generating and sending fake data to mislead or deceive the receiver.

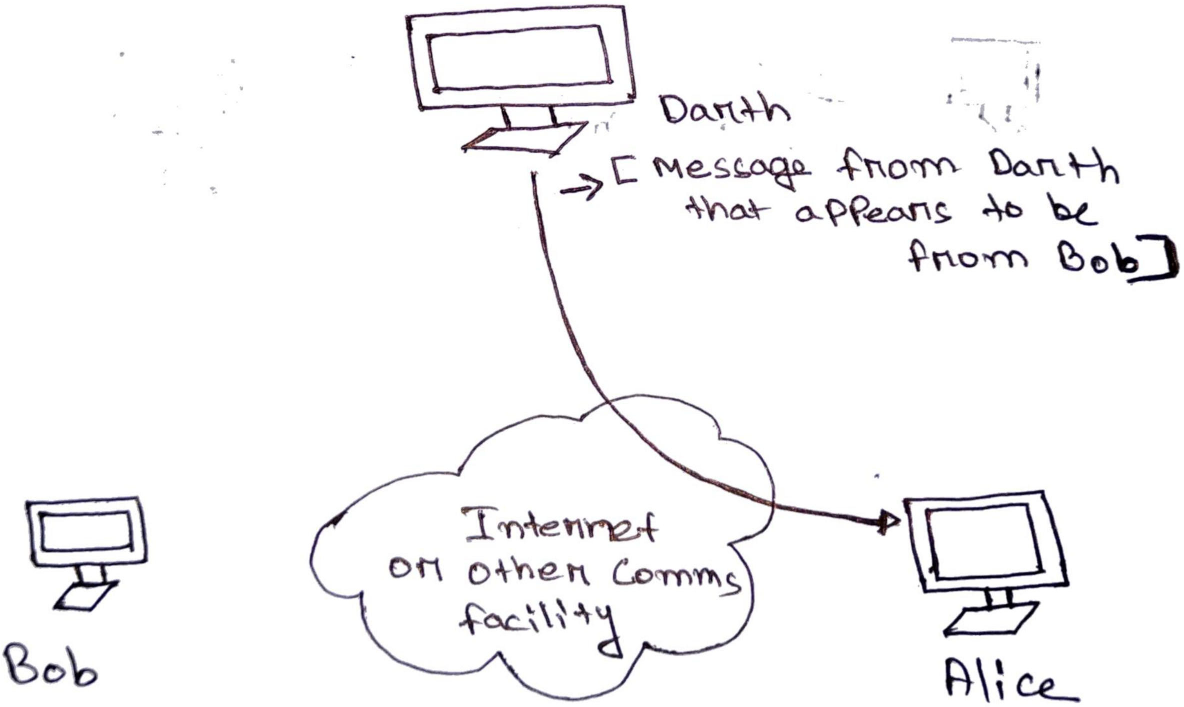
Passive attacks,

- **Eavesdropping:** ~~Eo~~ the interception of information intended for someone else during its transmission over a communication channel. In easy words, eavesdropping means capturing information/ messages before it reaches the person it was meant for.


[Read contents of messages from Bob with Alice]

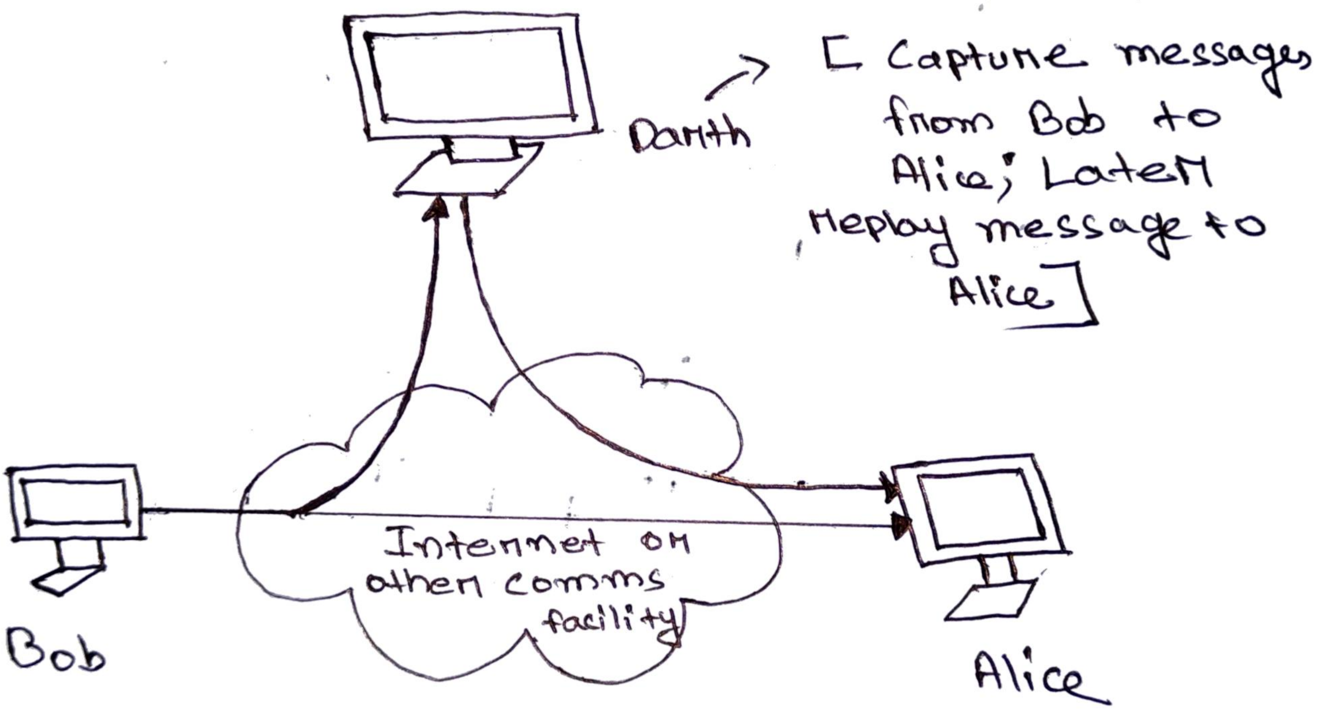
Active attacks,

- Masquerading : the fabrication of information that is purported to be from someone who is not actually the author/ source. In easy words, masquerading is the Creation of false information that Pretends to come from someone who is not actually the author or source. This means making it look like a message is from a trusted or known entity when it really isn't.


Darth
[Message from Darth that appears to be from Bob]
Internet or other Comms facility
Bob
Alice

Active attacks,

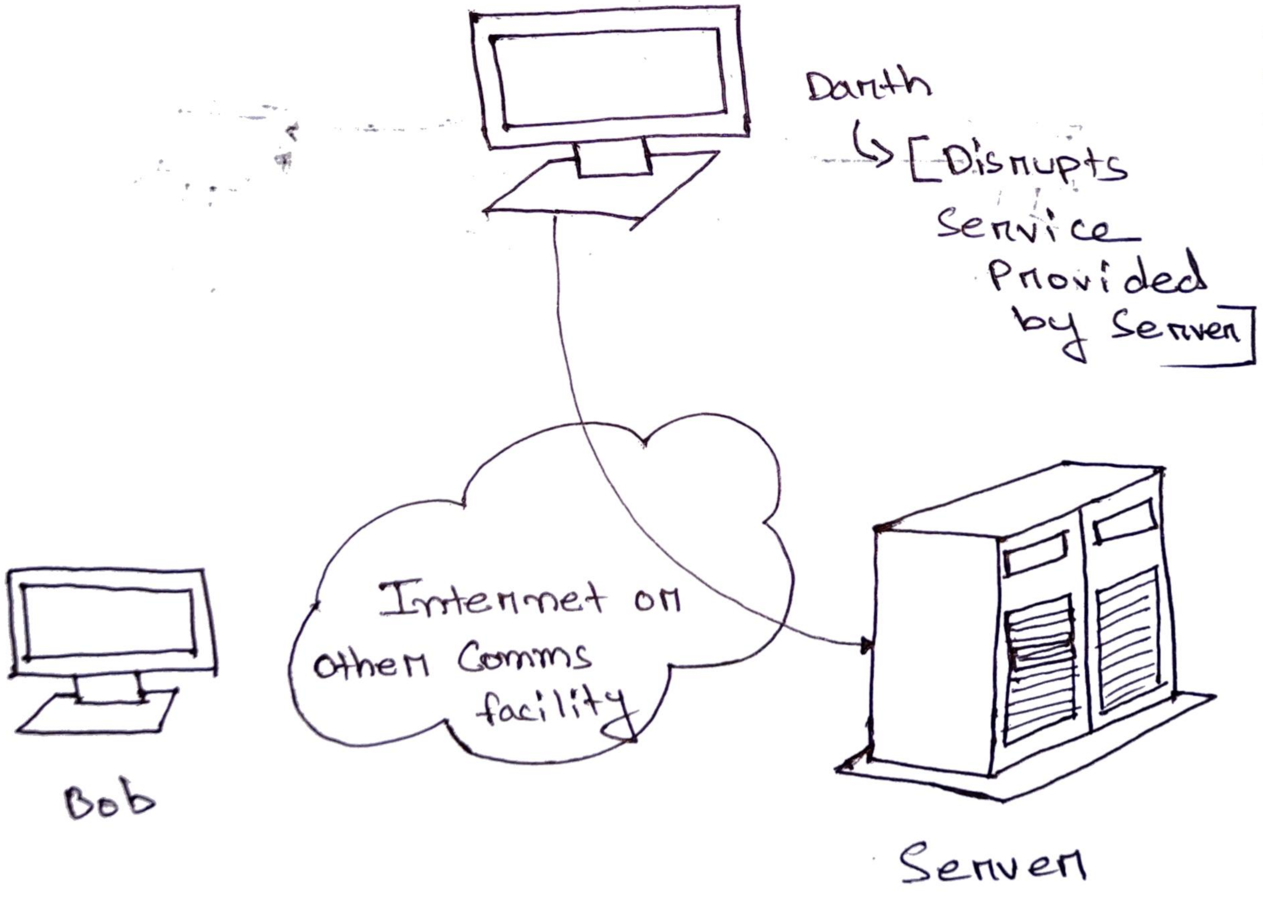
- Replay attack.
  - Modify and then replay, thus forming an active attack.


Darth
[Capture messages from Bob to Alice; Later replay message to Alice]
Internet or other comms facility
Bob
Alice

Active attacks,

○ Denial-of-Service (DOS): the interruption or degradation of a data service or information access.

Example: email spam, to the degree that it is meant to simply fill up a mail queue and slow down an email server.


Darth
[Disrupts service provided by Server]
Internet or other Comms facility
Bob
Server