CSE 477: Introduction to Computer Security

Lecture – 2

Course Teacher: Dr. Md Sadek Ferdous
Assistant Professor, CSE, SUST
E-mail: ripul.bd@gmail.com

Outline

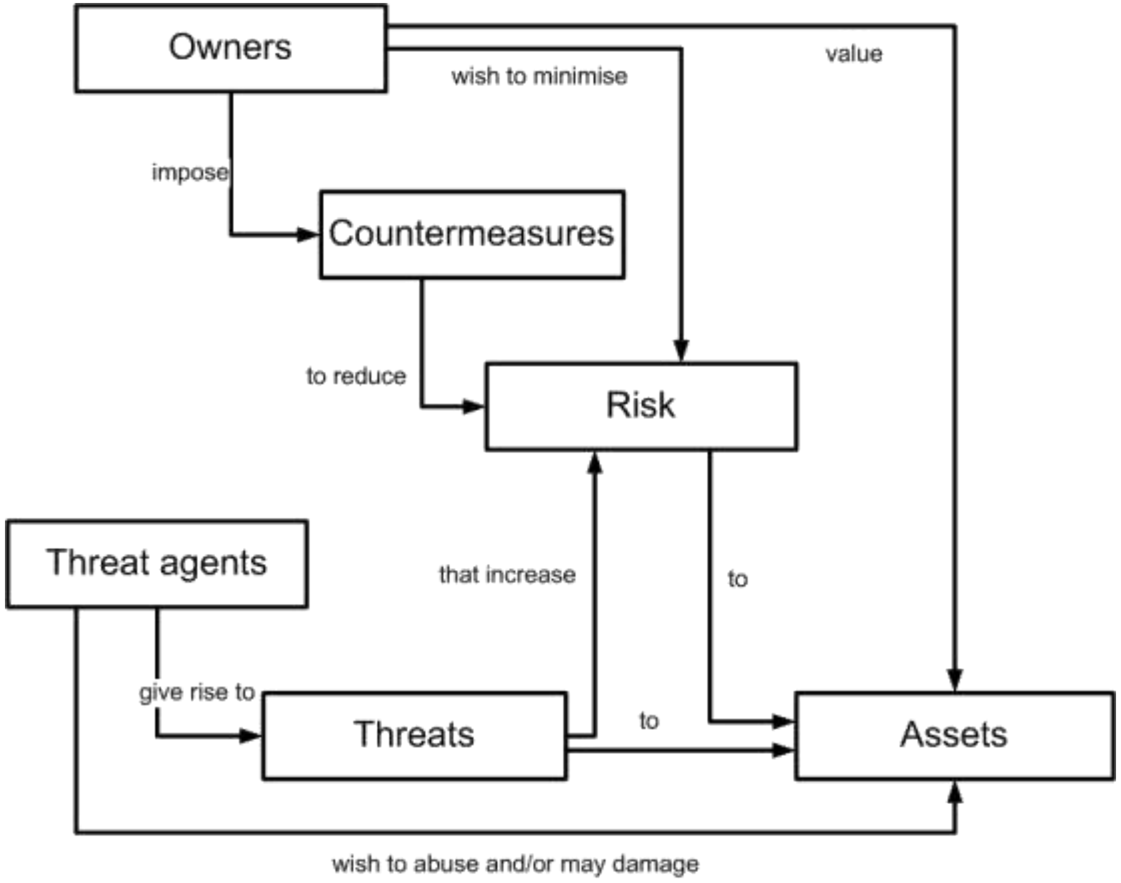
- Security definition
- Security goals
- Security attacks

Terminologies: Common Criteria (CC)

- CC is an international set of guidelines and specifications by ISO
  - for evaluating information security products,
  - specifically to ensure they meet an agreed-upon security standard for government deployments
- Asset is something that is valuable to its owner
- Vulnerabilities are weaknesses in the asset
- Threats exploit vulnerabilities within an asset to violate its security in some environments
- Threats increase the risk of abuse of an asset
- Threat agents (attackers/adversaries) value assets and want to abuse them
- Owners adopt countermeasures to minimise risks

Terminologies: Common Criteria (CC)

- Relationships among the concepts

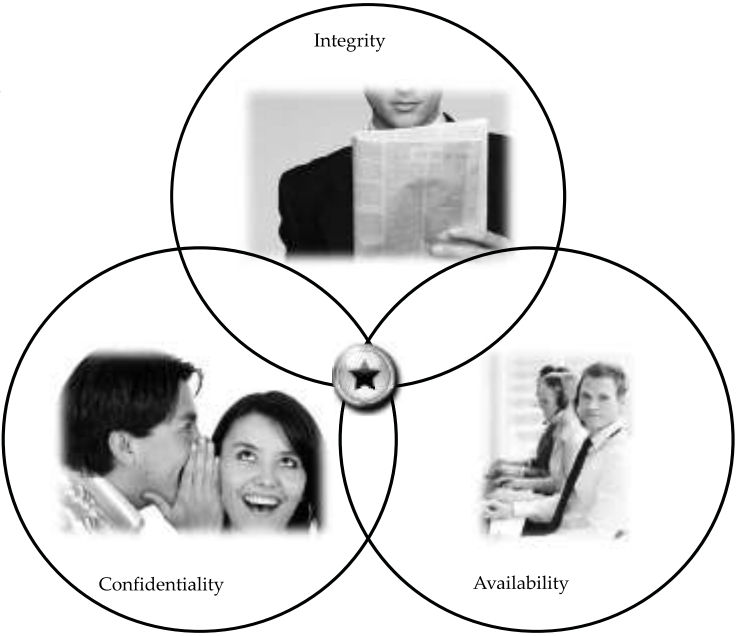


Defining security

- 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 not about
  - Breaking into a system
  - How to launch an attack
- Our focus will be explore
  - Why a system is insecure
  - How to make them secure

Security goals

- C.I.A.



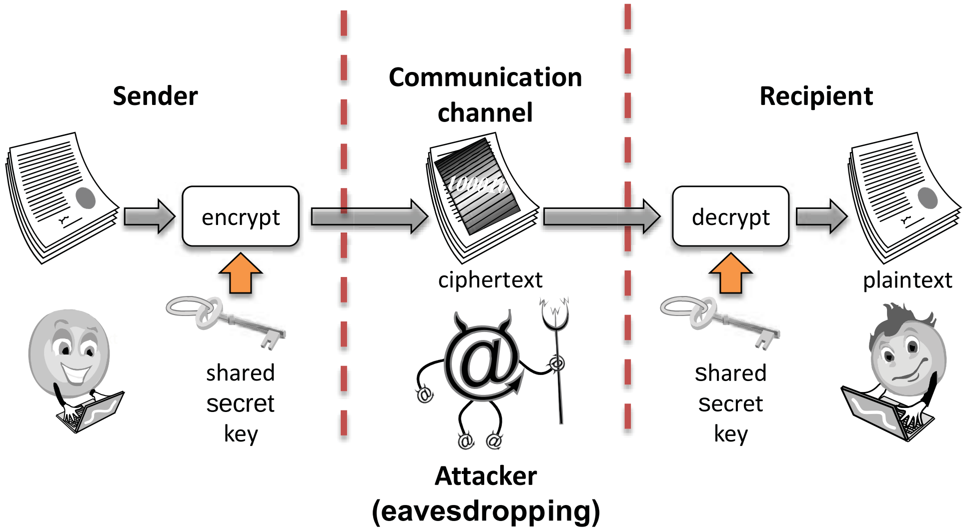
Properties	Brief description
Confidentiality	Keeping information secret from all but those who are authorised to see it
Integrity	Ensuring information has not been altered by unauthorized or unknown means
Availability	Data/information is available when required

Confidentiality: Secrecy & Privacy

- Two dimensions for confidentiality: Secrecy and & Privacy
  - protecting unauthorized information access and disclosure (secrecy)
  - protecting personal privacy and proprietary information (privacy)
- Secrecy assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed
- The need of confidentiality predates computer systems:
  - For example, in the first recorded use of cryptography, Julius Caesar communicated commands to his generals using a simple cipher (will be studied later)

Tools of Confidentiality

- **Encryption:**
  - the transformation of information using a secret, called an encryption key, so that the transformed information can only be read using another secret, called the decryption key (which may, in some cases, be the same as the encryption key)

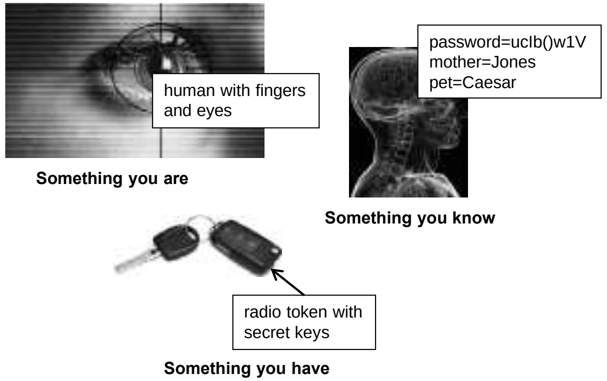


Tools of Confidentiality

- **Access control:**
  - Rules and policies that limit access to confidential information to those people and/or systems with a “need to know”
- This need to know may be determined
  - By identity, such as a person’s name or a computer’s serial number
  - And / Or by a role that a person has, such as being a manager or a computer security specialist

Tools of Confidentiality

- **Authentication:**
    - the determination of the identity or role that someone has
- This determination can be done in a number of different ways, but it is usually based on a combination of
    - Something the person has (like a smart card or a radio key fob storing secret keys)
    - Something the person knows (like a password)
    - Something the person is (like a human with a fingerprint)



Tools of Confidentiality

- **Authorization:**
  - the determination if a person or system is allowed access to resources, based on an access control policy
- Such authorizations should prevent an attacker from tricking the system into letting him have access to protected resources
- **Physical security:**
  - the establishment of physical barriers to limit access to protected computational resources.
- Such barriers include locks on cabinets and doors, the placement of computers in windowless rooms, the use of sound dampening materials, and even the construction of buildings or rooms with walls incorporating copper meshes (called **Faraday cages)** so that electromagnetic signals cannot enter or exit the enclosure

Integrity

- **Integrity:** the property that information/system has not be altered in an unauthorized way
- Two dimensions: data integrity and system integrity
- Data integrity
  - Assures that information and programs are changed only in a specified and authorized manner
- System integrity
  - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Tools of Integrity

- **Backups:** the periodic archiving of data
- **Checksums:** the computation of a function that maps the contents of a file to a numerical value
- A checksum function depends on the entire contents of a file and is designed in a way that even a small change to the input file (such as flipping a single bit) is highly likely to result in a different output value
- **Data correcting codes:** methods for storing data in such a way that small changes can be easily detected and automatically corrected

Availability

- Ensuring timely and reliable access to and use of information or a system
- A loss of availability is the disruption of access to or use of information or an information system
- Information or systems might be unavailable:
    - due to unintentional and accidental events: fire, damage to hard disk/system
    - due to intentional or malicious attacks: Distributed Denial of Service (DDoS)
- **Tools:**
    - **Physical protections:** infrastructure meant to keep information available even in the event of physical challenges
    - **Computational redundancies:** computers and storage devices that serve as fallbacks in the case of failures

Additional security properties

Properties	Brief description
Authenticity	Data/information origin is identifiable accurately (source authenticity); corroboration of the identity of an entity (entity authentication)
Accountability/Non-repudiation	Actions involving data/information is traceable/preventing the denial of previous commitments or actions
Anonymity	Actions or data not relatable to a particular individual

Authenticity

- The property of an entity or the source of data (person/system/org) being genuine and being able to be verified and trusted
  - confidence in the validity of a transmission, a message, or message originator
- This means verifying
  - that users are who they say they are and
  - that each input arriving at the system came from a trusted source.
  - Example: purporting someone else's identity for malicious purposes
- Data authentication deals with source authenticity
  - Mechanism: **Digital signature**
- Entity authentication deals with Identity authenticity. For a person:
  - **something you have** e.g., id cards
  - **something you know** e.g., a password or secret key
  - **something you are** e.g., a biometric (fingerprint, face or iris scanning)

Accountability/non-repudiation

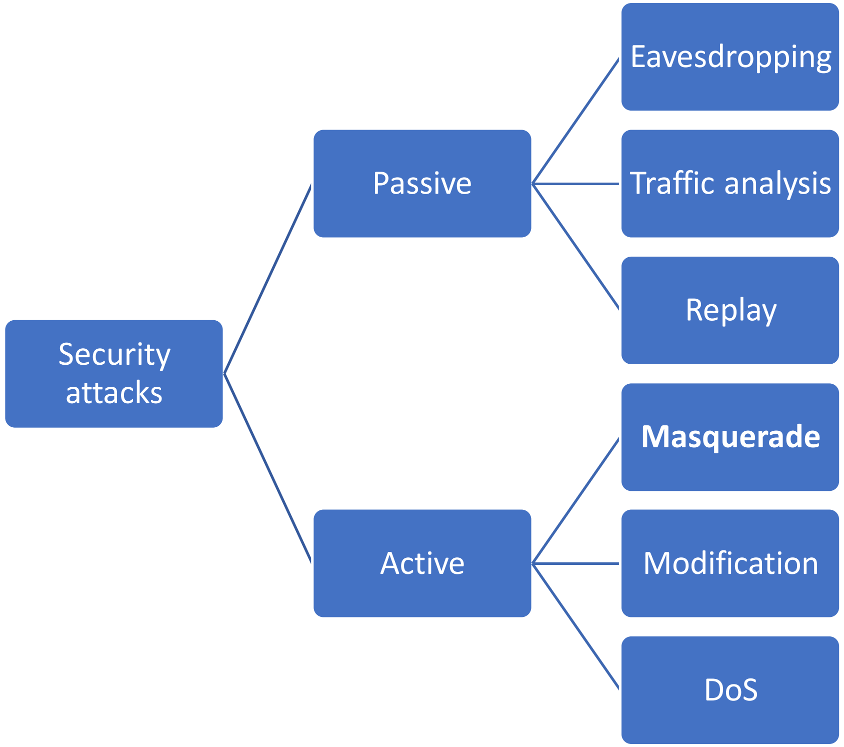
- Ensures the actions of an entity to be traced uniquely to that entity
- True secure systems are not yet an achievable goal ☹
  - we must be able to trace a security breach to a responsible party
- This supports
  - non-repudiation (a party cannot deny a certain action),
  - fault isolation and
  - after-action recovery and legal action
- Mechanism: **via a secure audit trail**
  - creating an audit trail with machine logs is tricky: if a system is compromised, logs may also be tampered with
  - how about: send log messages to an append-only file?

Anonymity

- **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 transactions, but are otherwise known only to a trusted entity

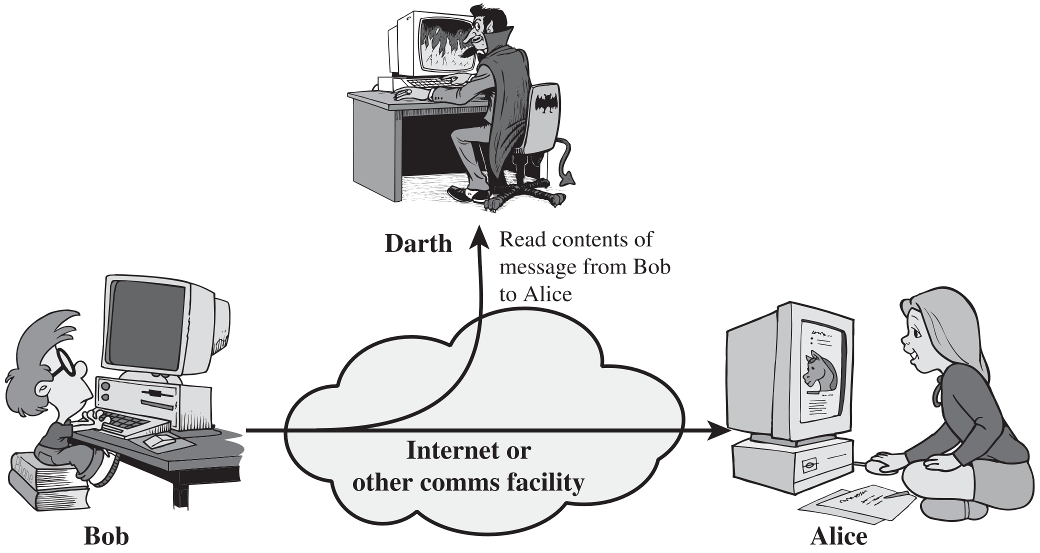
Security attacks

- Largely two types: passive and active
- Passive attacks
  - eavesdropping on, or monitoring of, transmissions.
  - 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

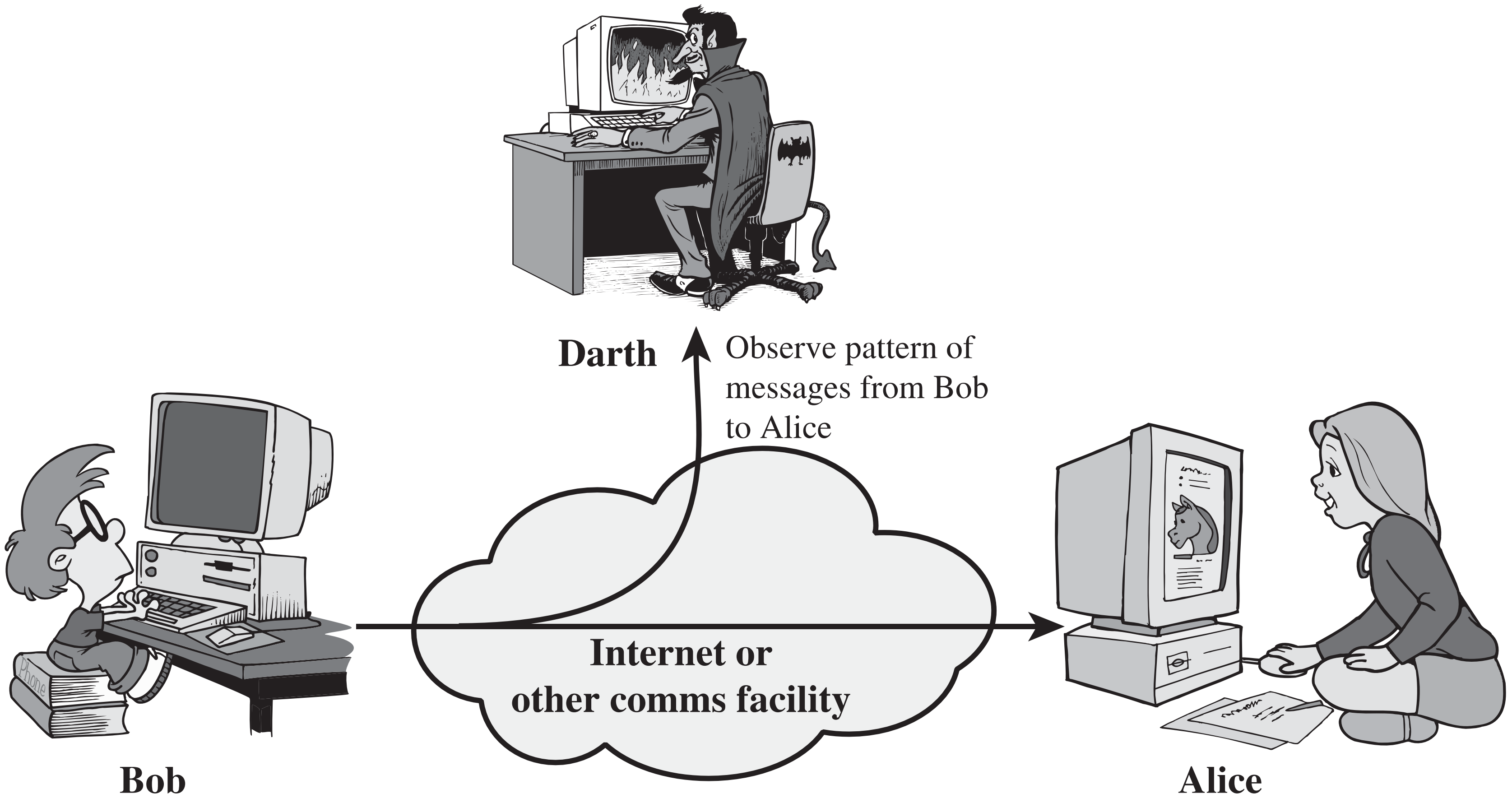

Security attacks
Passive
Active
Eavesdropping
Traffic analysis
Replay
Masquerade
Modification
DoS

Security attacks: passive attacks

Eavesdropping: the interception of information intended for someone else during its transmission over a communication channel


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

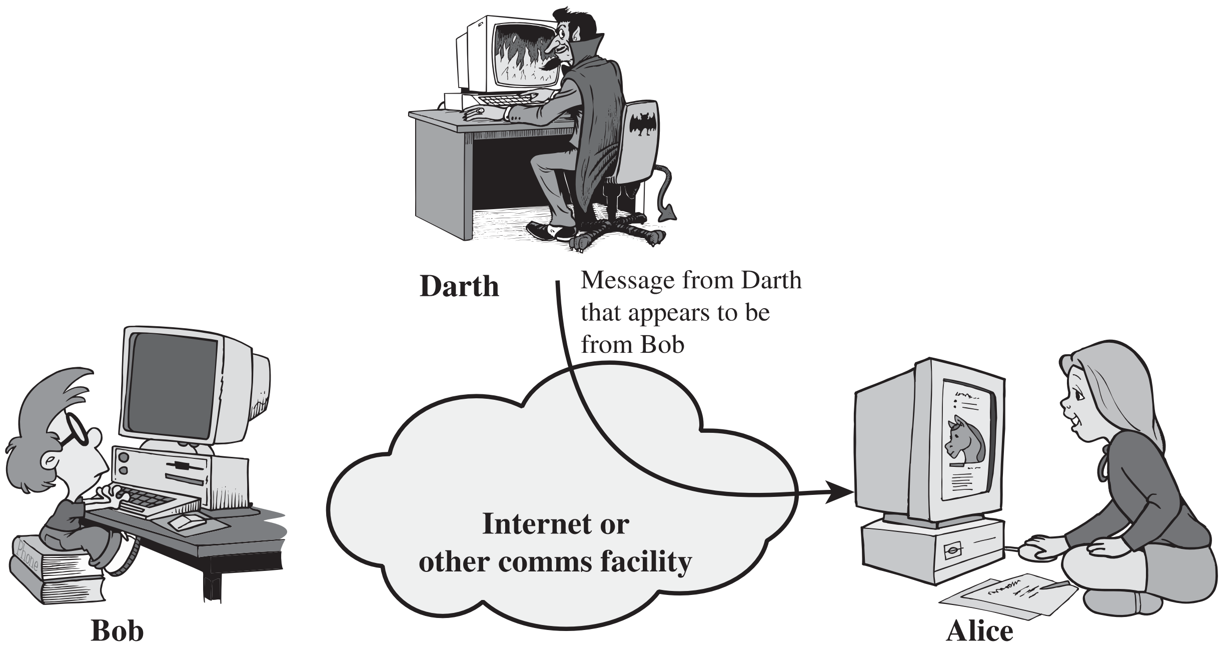
Security attacks: passive attacks


Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

(b) Traffic analysis

Security attacks: active attacks

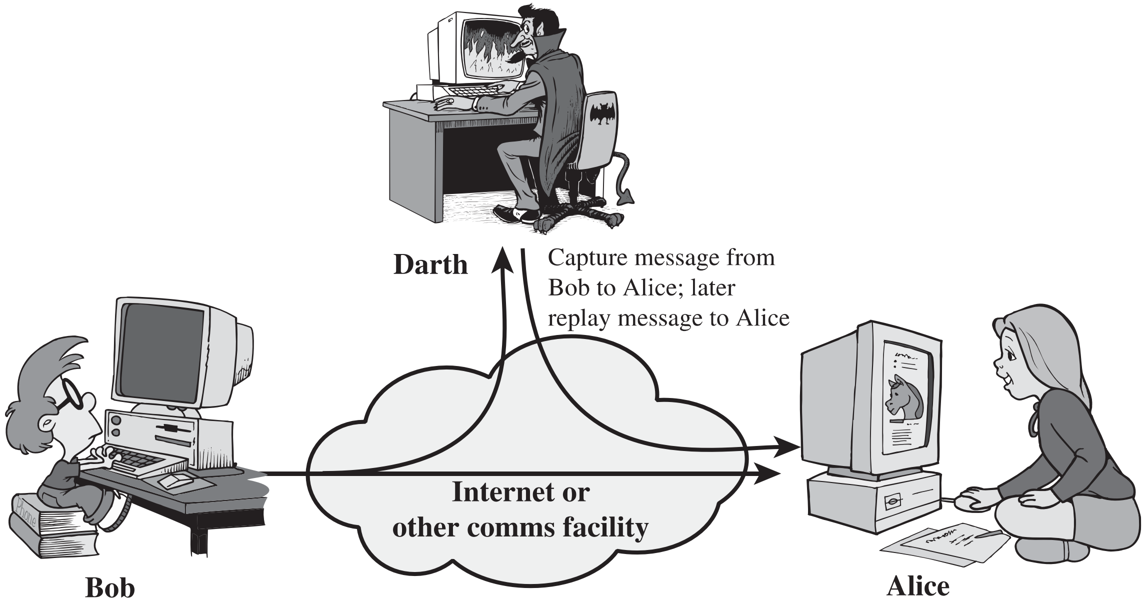
Masquerading: the fabrication of information that seems to be from someone who is not actually the author/source


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

(a) Masquerade

Security attacks: passive attacks

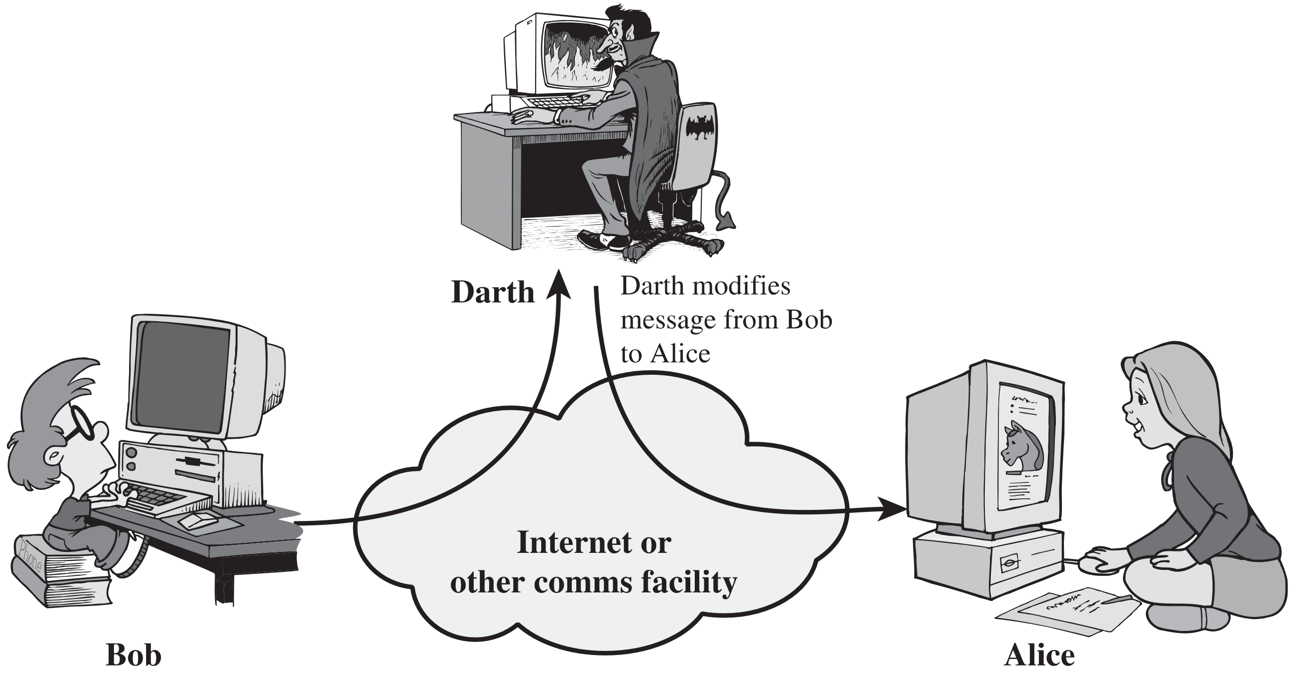
- Observe, analyse and then replay



Capture message from
Bob to Alice; later
replay message to Alice

Security attacks: active attacks

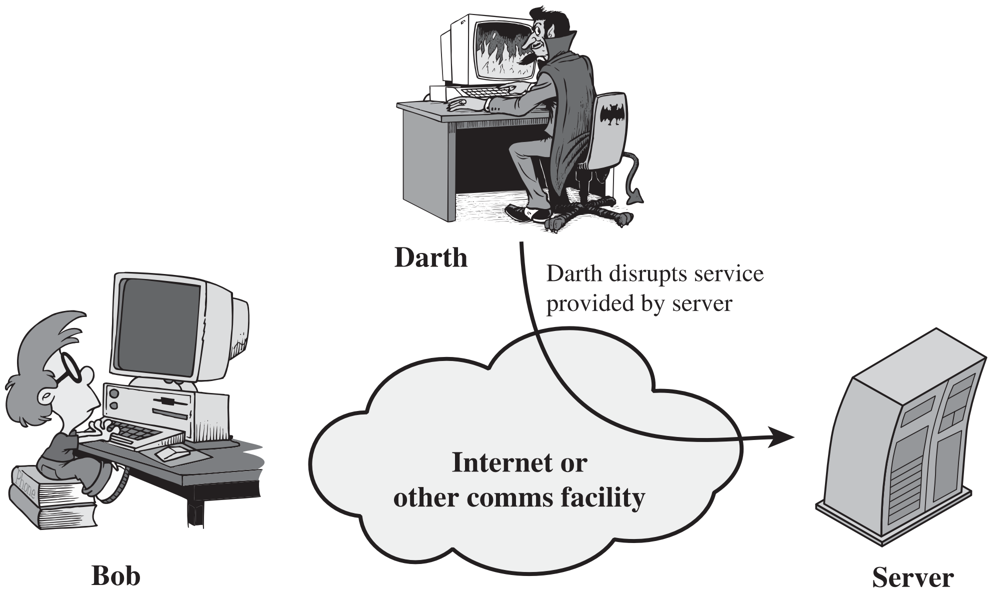
Alteration: unauthorised modification of information


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

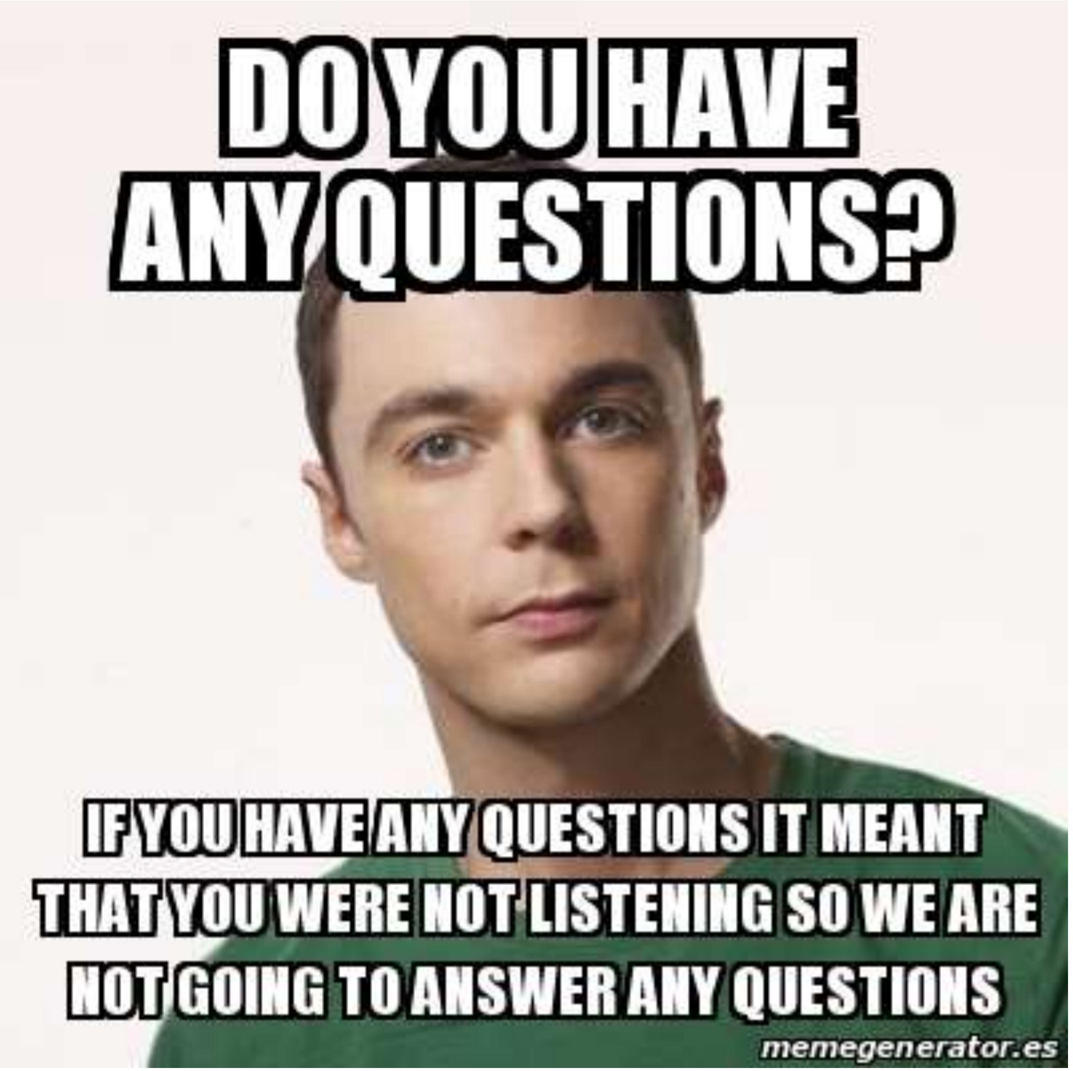
(c) Modification of messages

Security attacks: active attacks

- **Denial-of-service:** 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
Darth disrupts service provided by server
Bob
Internet or other comms facility
Server

(d) Denial of service


DO YOU HAVE ANY QUESTIONS?
IF YOU HAVE ANY QUESTIONS IT MEANT THAT YOU WERE NOT LISTENING SO WE ARE NOT GOING TO ANSWER ANY QUESTIONS
memegenerator.es