# 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

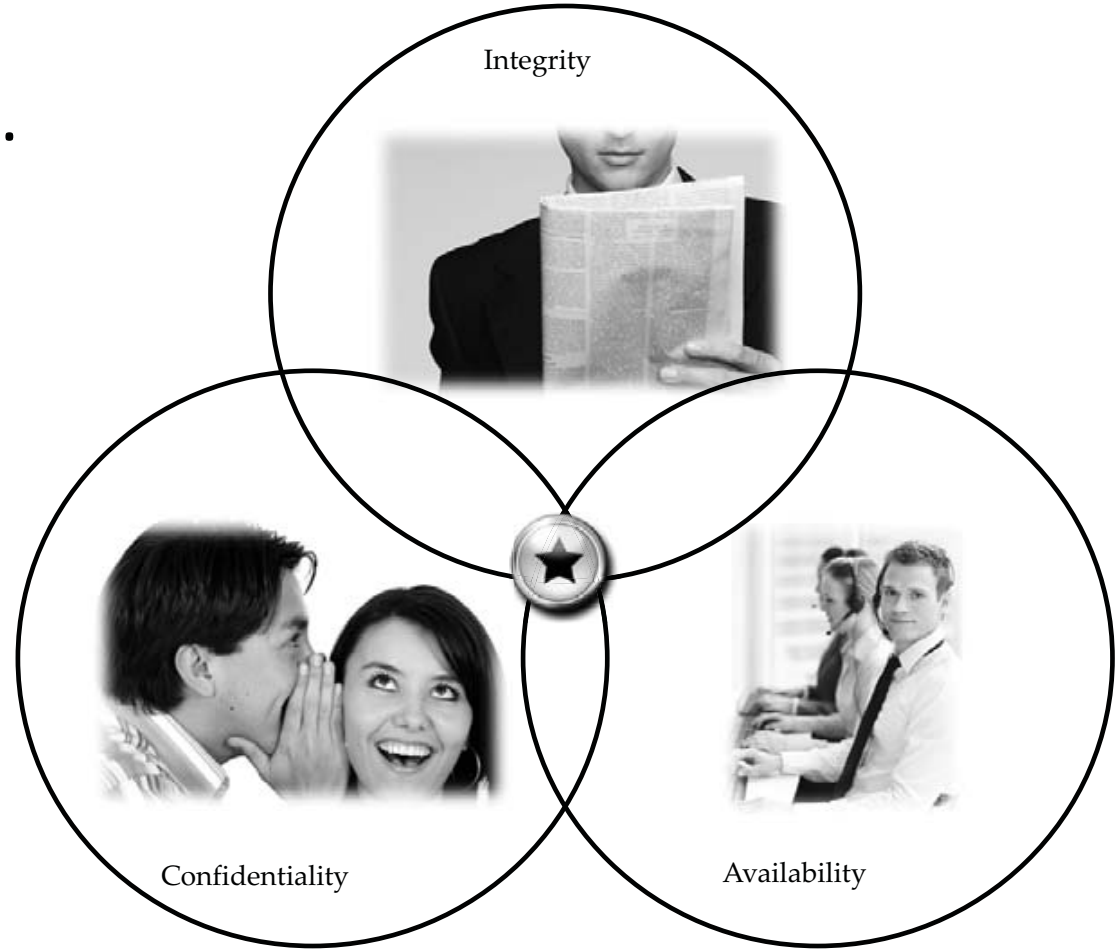
- Security definition
- Security goals
- Security attacks

# 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.

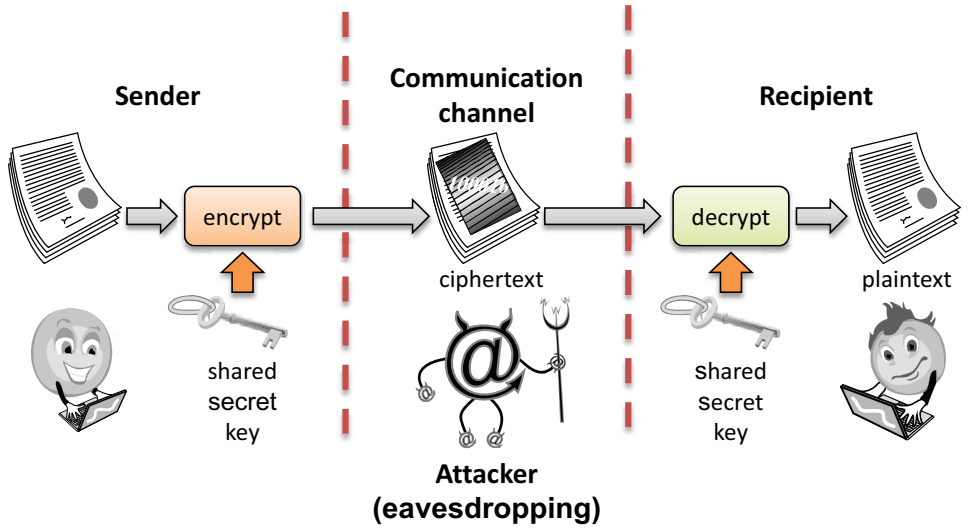


# Confidentiality: Secrecy & Privacy


- Confidentiality:
  - protecting unauthorized information access and disclosure (secrecy)
  - protecting personal privacy and proprietary information (privacy)
- Two dimensions: Secrecy and & 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)

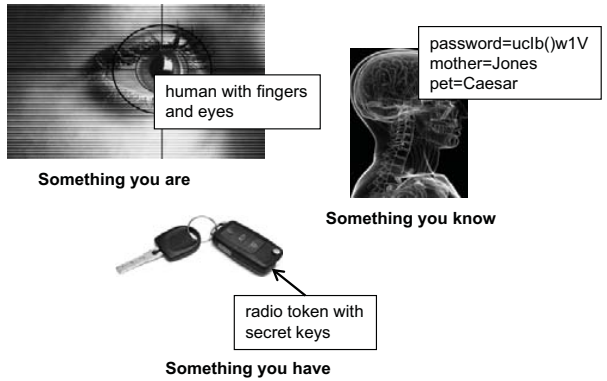


# Tools of Confidentiality

- **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

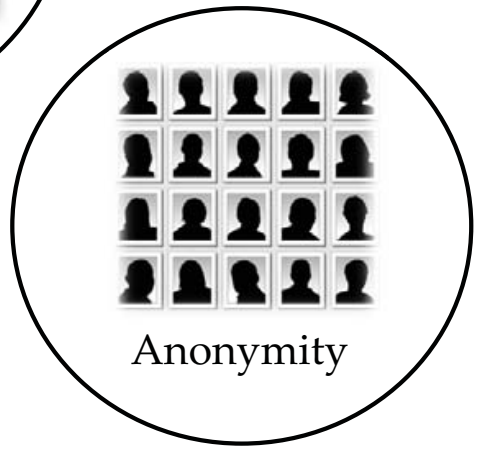
# Availability

- 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 requirements

- A.A.A.





# Assurance

- **Assurance** refers to how trust is provided and managed in computer systems
- **Trust management** depends on:
  - **Policies,** which specify behavioural expectations that people or systems have for themselves and others
    - For example, the designers of an online music system may specify policies that describe how users can access and copy songs
  - **Permissions,** which describe the behaviours that are allowed by the agents that interact with a person or system
    - For instance, an online music store may provide permissions for limited access and copying to people who have purchased certain songs
  - **Protections,** which describe mechanisms put in place to enforce permissions and polices
    - We could imagine that an online music store would build in protections to prevent people from unauthorized access and copying of its songs

# Authenticity

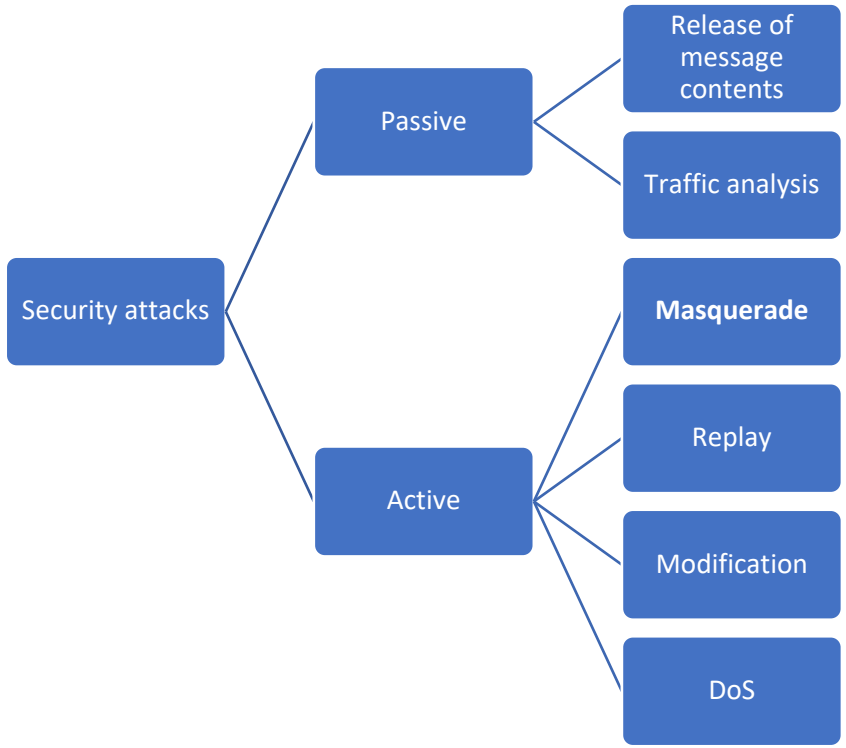
- **Authenticity** is the ability to determine that statements, policies, and permissions issued by persons or systems are genuine and/or have originated from the desired source
- **Primary tool:**
  - **digital signatures -** These are cryptographic computations that allow a person or system to commit to the authenticity of their documents in a unique way that achieves **nonrepudiation**, which is the property that authentic statements issued by some person or system cannot be denied

# Anonymity

- **Anonymity:** the property that certain records or transactions not to be attributable to any individual
- **Tools:**
  - **Aggregation:** the combining of data from many individuals so that disclosed sums or averages cannot be tied to any individual
  - **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

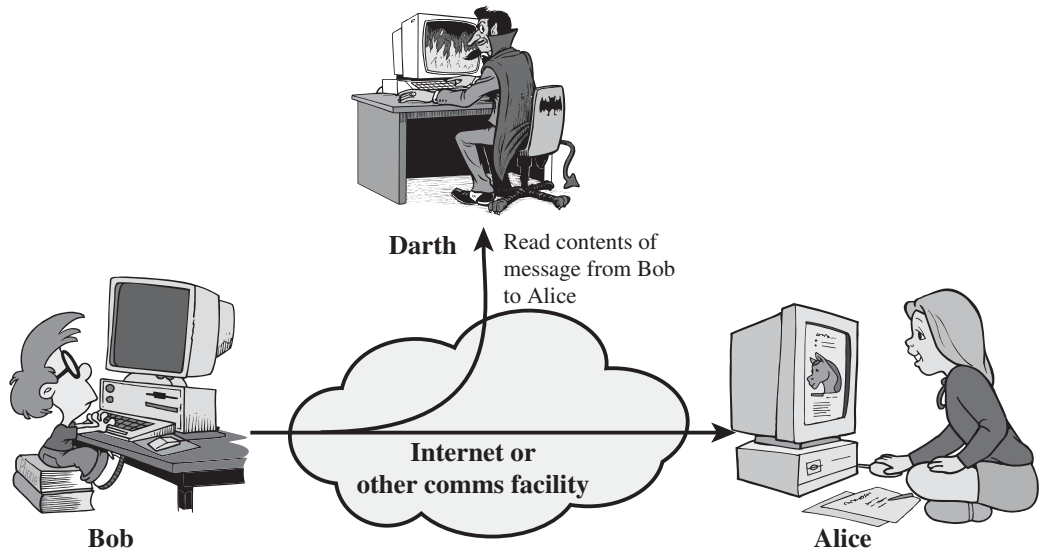
# Security attacks

- 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

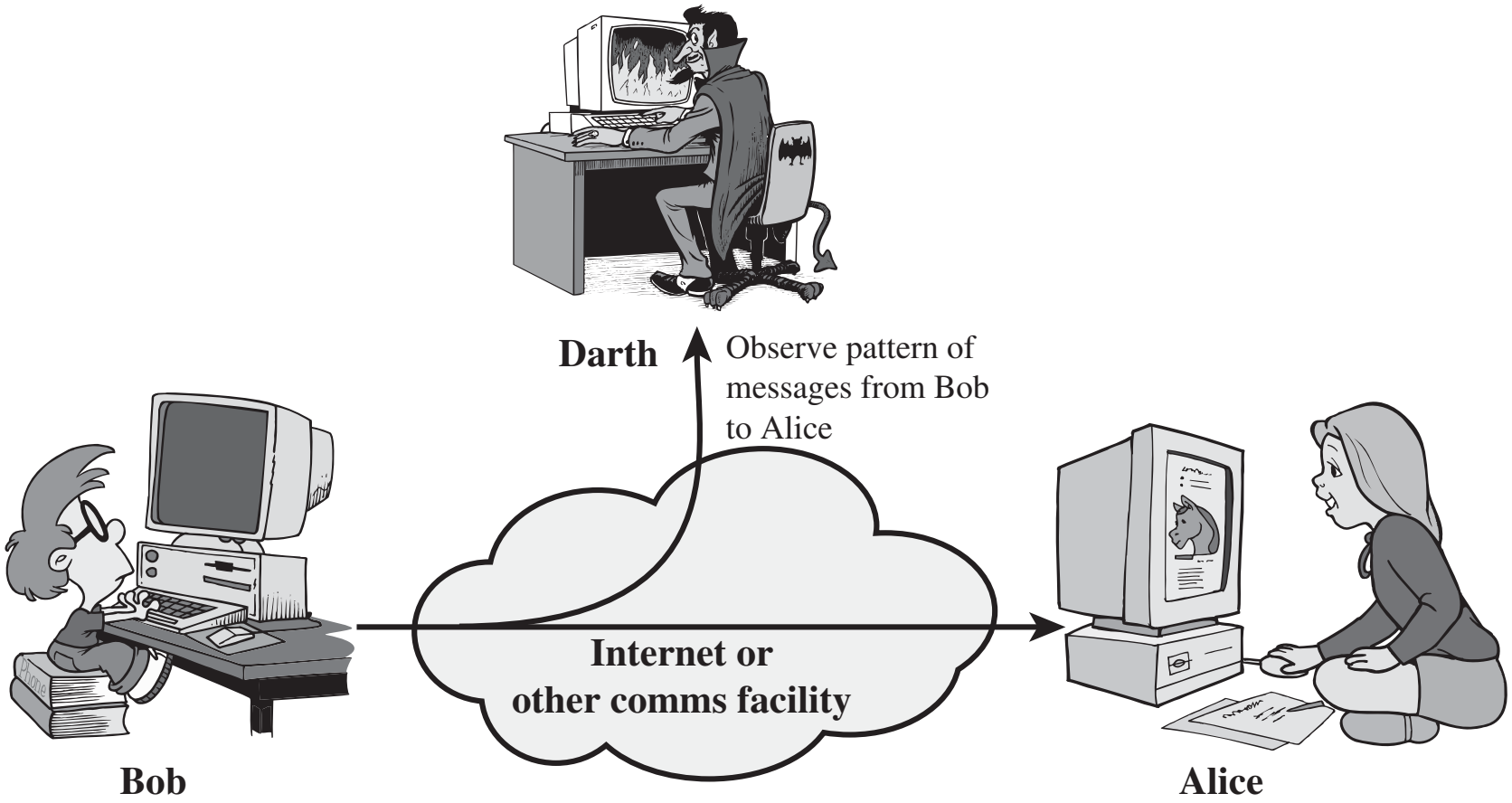


# Security attacks: passive attacks

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



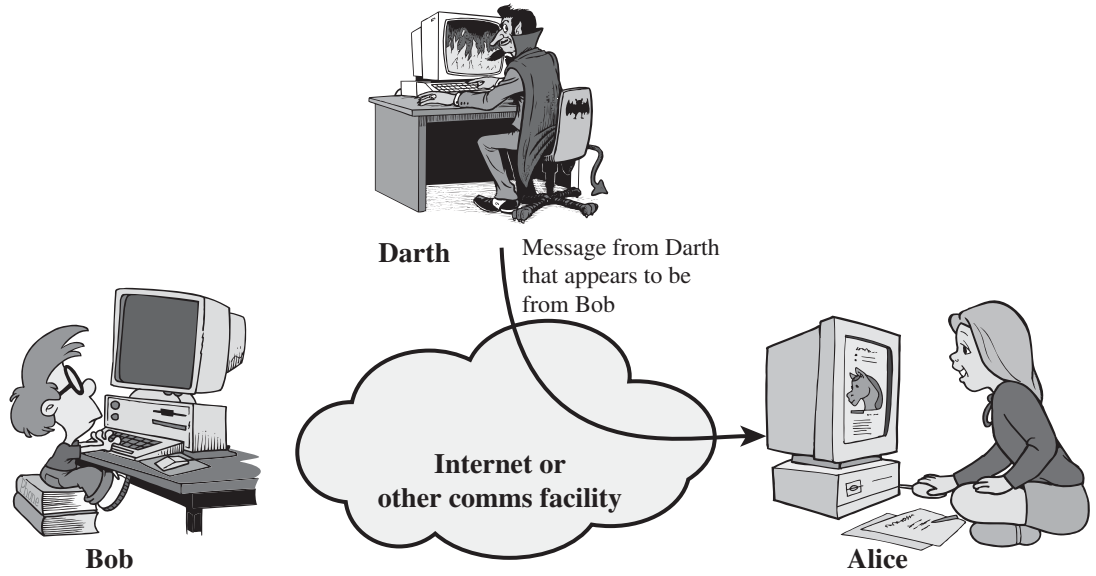
# Security attacks: passive attacks




**(b) Traffic analysis**

# Security attacks: active attacks

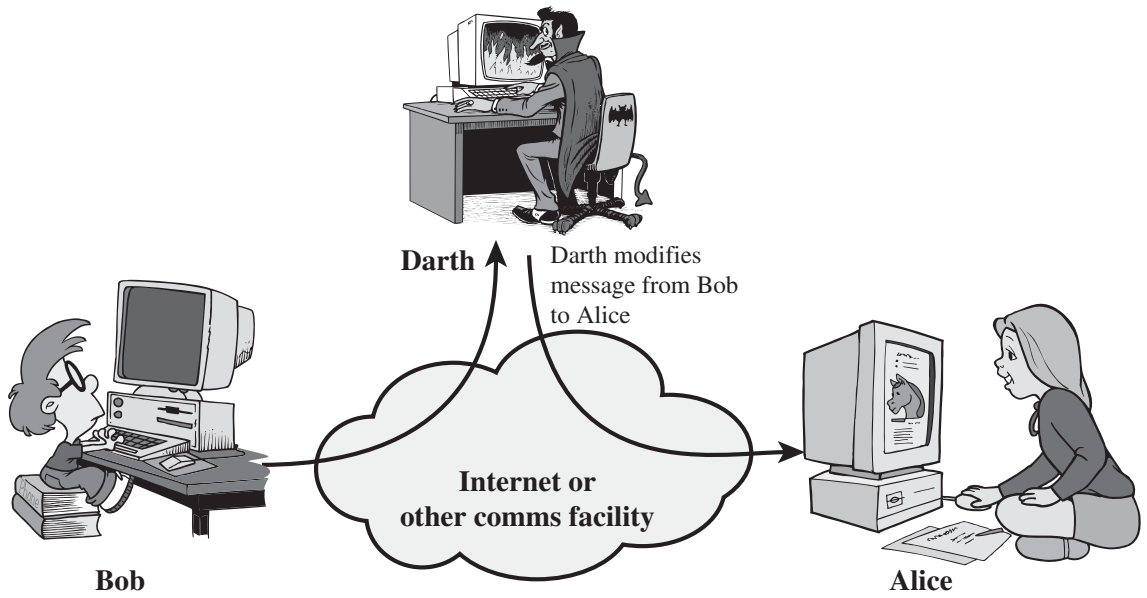
**Masquerading:** the fabrication of information that is purported to be from someone who is not actually the author/source




(a) Masquerade

# Security attacks: active attacks

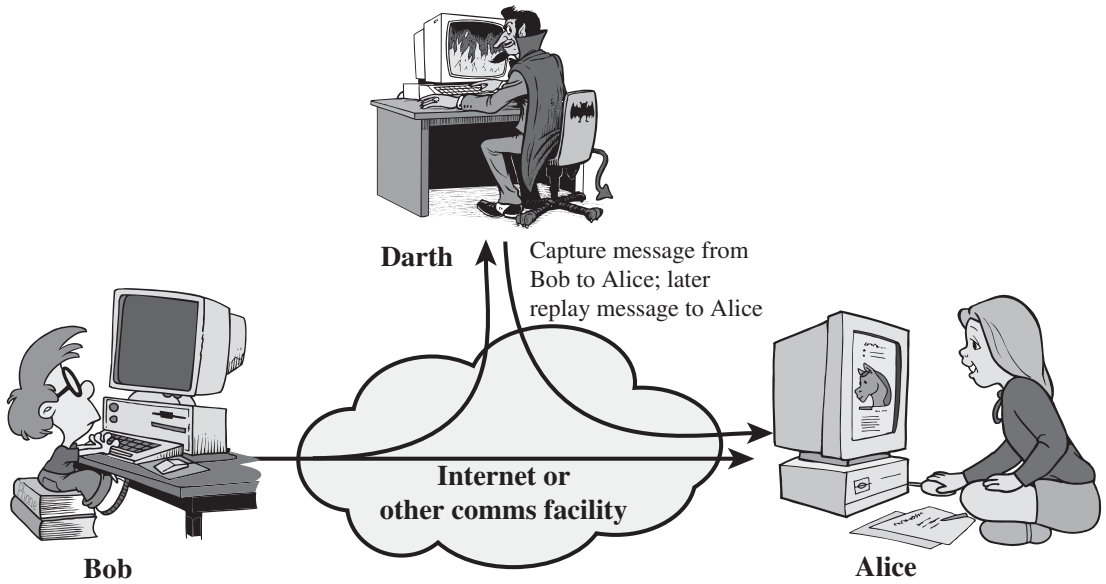
**Alteration:** unauthorised modification of information




(c) Modification of messages

# Security attacks: active attacks

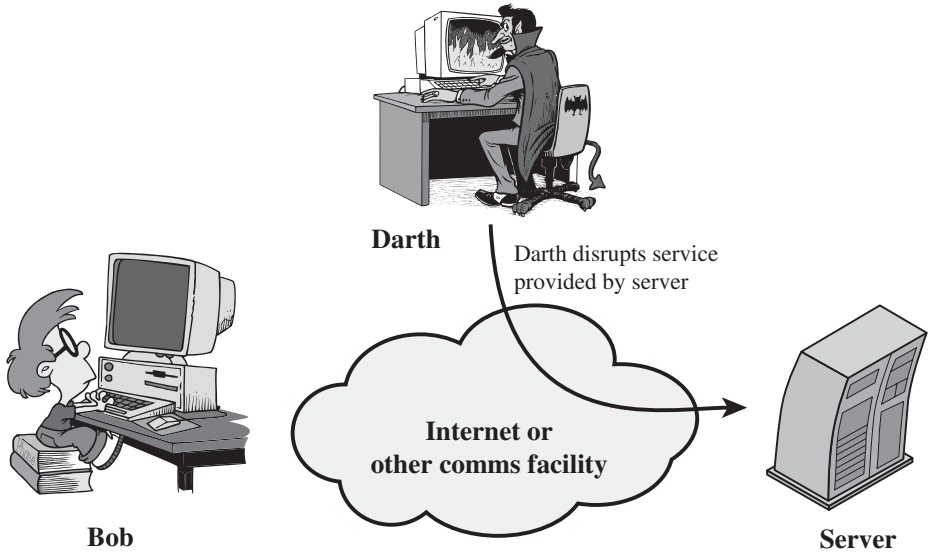
- Two forms
  - Modify and then replay, thus forming an active attack
  - Observe and analyse and then replay, thus forming a passive attack




(b) Replay

# 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




(d) Denial of service

# Other security attacks

- **Repudiation:** the denial of a commitment or data receipt
  - This involves an attempt to back out of a contract or a protocol that requires the different parties to provide receipts acknowledging that data has been received
- **Correlation** and **traceback:**
  - The integration of multiple data sources and information flows to determine the source of a particular data stream or piece of information

The lecture slides can be found in the following location!