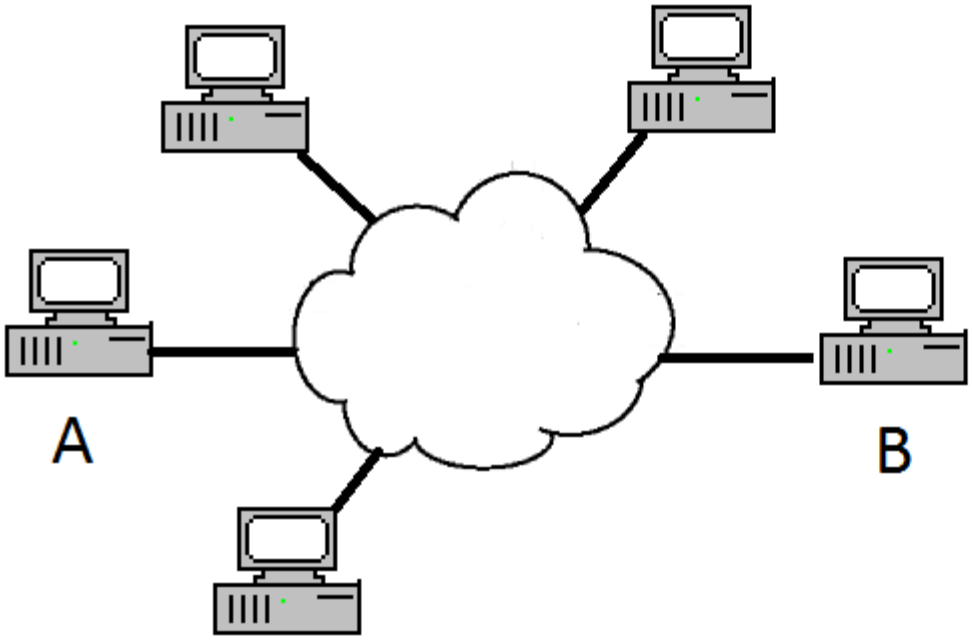
Network Security overview

A Definition

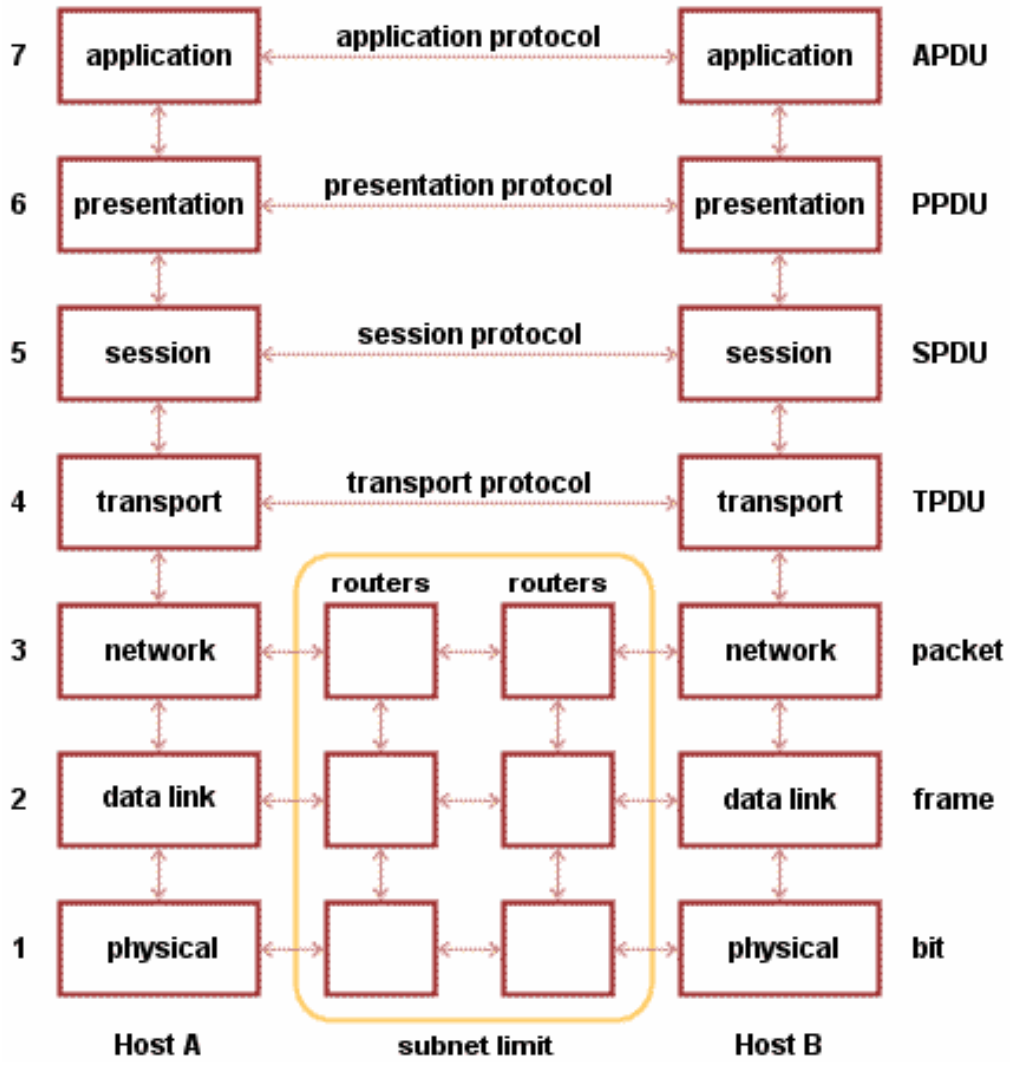
Network Security consists of measures to prevent, detect, and correct security violations that involve the transmission of information.

Pictorial representation

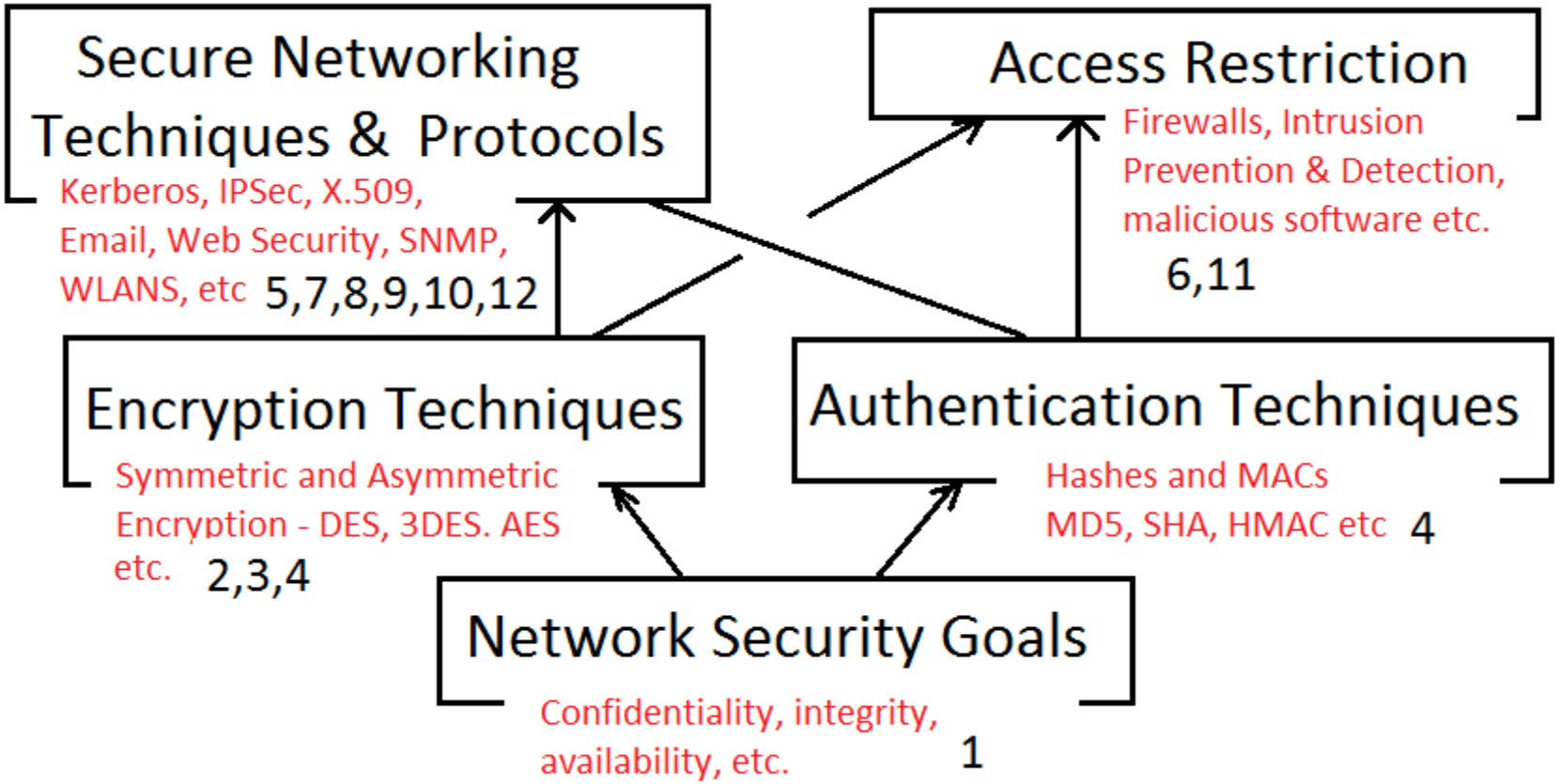


The network context of network security is that 2 devices (A and B) are communicating over a shared medium. Other devices are also using the network.
A and B want certain features to apply to their communications.

Open Systems Interconnection (OSI)



An alternative taxonomy



Today's Lecture –Introduction

- **Security Goals (very important!)**
- Security Policies
- Organizations and individuals involved in Network Security development.
- Attacks, threats, vulnerabilities and weaknesses.

Abstract Goals of Network Security

Major Goals

- Confidentiality
- Integrity
- Availability

Other Goals

- Entity Authentication
- Message Origin Authentication
- Timeliness
- Non-Repudiation
- Authorisation
- Access Control

Goals of Network Security(1) Confidentiality

- A and B do not want their messages read by other people. This is the network security goal of confidentiality.
- The general technique used to ensure confidentiality is encryption of messages.
- An example of a breach of confidentiality :
- Someone reads the plaintext packets being exchanged between A and B by running a program such as Wireshark.
- If the packets are securely encrypted even though they are captured they cannot be read.

Goals of Network Security(2) Integrity

- A and B do not want their messages changed by other people. This is the network security goal of integrity.
- The general techniques used to ensure integrity are hashes and Message Authentication Codes (MAC).
- The term Message Authentication is also used as a synonym for integrity.

Goals of Network Security(3) Availability

- Availability refers to the ability for a service to be available.
- A wants to be able to connect to B (ignoring considerations of entity authentication etc.). A situation where B is deliberately sent a large number of false requests or other unnecessary traffic, making it difficult for a legitimate request for a connection is a Denial of Service (DOS) attack. When a lot computers are involved in sending the unnecessary traffic to B, it is a Distributed Denial of Service (DDOS).

Goals of Network Security(4) Entity Authentication

- A wants to be sure that the entity saying it is B really is B and not an imposter. Similarly, B wants to be sure that the entity that says it's A really is A.
- The general techniques used to ensure entity authentication are passwords, authentication protocols, key exchange protocols and third party certificates.
- Entity Authentication is also relevant in the context of users identifying themselves to use resources on a network or to log on to a particular host. Entity authentication is also called identification.

Goals of Network Security(5) Message Origin Authentication

- A wants to be sure that the messages supposedly coming to it from B, really are coming from B. Similarly B wants to be sure that messages supposedly coming from A really are coming from A. This is Message Origin Authentication. It is sometimes called Data Origin Authentication.
- Techniques used to verify the origin of a message include Message Authentication Codes (MACs), digital signatures and appending an authenticator to a message before encryption.

Goals of Network Security(6) Timeliness

- If A and B conduct a completely secure conversation over a network, it is conceivable that a third party may copy the conversation and use it to masquerade as either A or B in a future conversation. This is known as a replay attack.
- Timeliness means that a secure conversation cannot be used as a basis for a replay attack. Some of the techniques used to prevent a replay attack include timestamps, nonces and random numbers.

Goals of Network Security(7) Non-repudiation (origin) (8) Non-repudiation (destination)

- A may want to be sure that B cannot deny having sent a particular message to A. This feature is Non-repudiation (origin).
- A wants to be sure that B really received a particular message that A sent. This feature is Non-repudiation (destination).

Goals of Network Security(9) Authorisation

- Authorization is official permission to carry out certain actions. For example, a particular computer on a network has resources that are available to a particular set of users. Not all users of the network are authorised users of the particular computer.

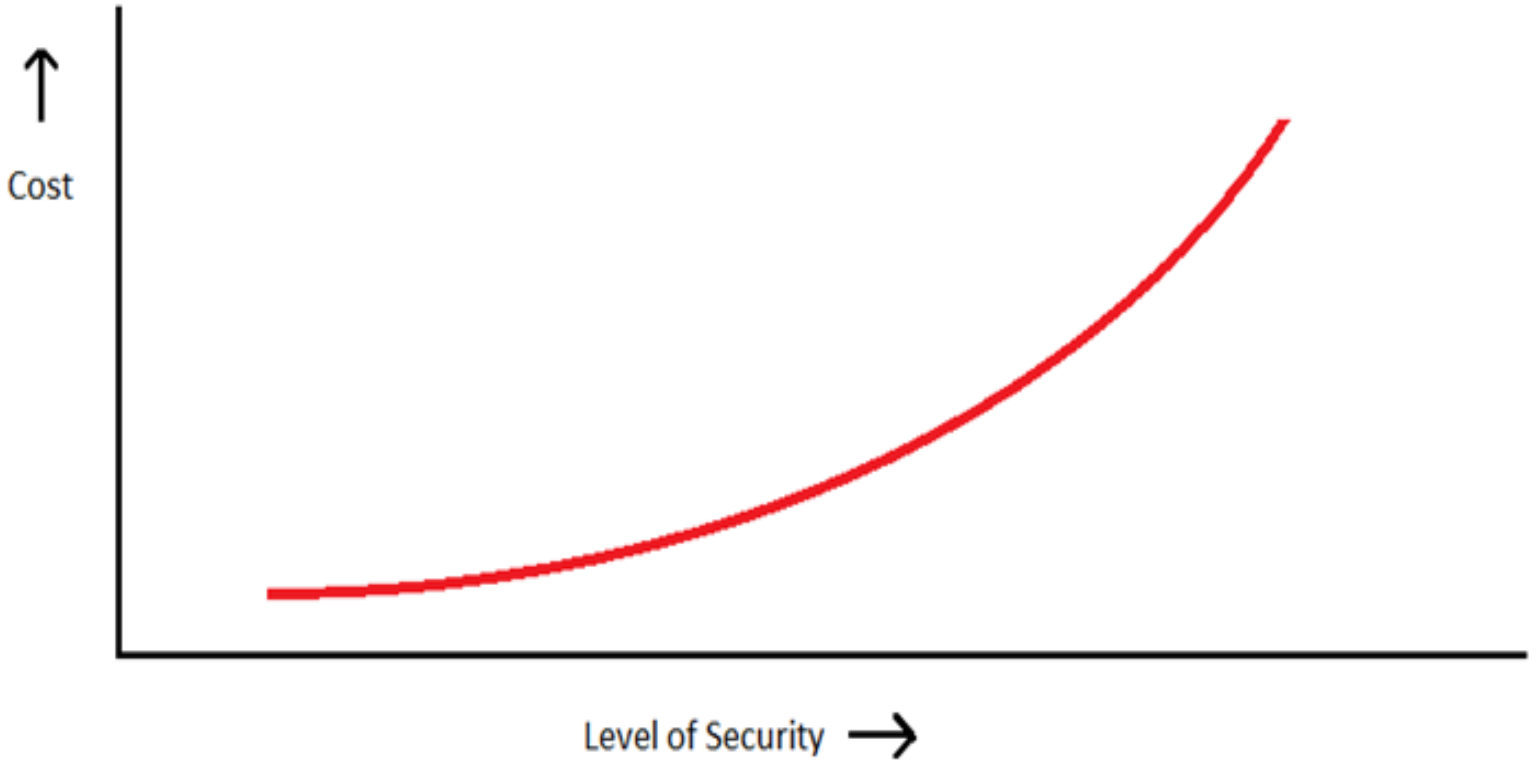
  Authorisation allows users to do certain things.

- Passwords are an authorisation technique. Upon entering their username and password, authorised users are given access to some resources on the computer. The concept is related to but different from access control.

Goals of Network Security(10)
Access Control

- Access control refers to the ability to restrict access to resources to certain users. The concept is closely related to authorization but different. Access control restricts users from doing certain things.
- A good example of access control is the rights granted to users of database systems –different users are restricted in what tables they can read and what tables they can write to. Only the database administrator has full rights over all tables. The restriction of the privileges of normal database users is an example of access control.

The economic realities of Network Security



Security Policy

- In order to maximise the likelihood that security goals will be met, organisations need to have a security policy.
- Security Policy : A set of principles that guides decision making processes and enables leaders in an organisation to distribute authority confidently.
- Extent and detail varies with: business type, its size, number of users, threats to the organization and vulnerabilities.

Security Policy Goals

- Informs users, staff and management of duties and obligations.
- Provides a mechanism for attaining security goals.
- Provides a baseline to audit systems for compliance to the policy.
- My experience

Some of the parties involved in Network Security

- Standards Bodies
  - IETF
  - ITU-T
- Governments and their agencies
  - US government and others
- Academics, Researchers, Civil Libertarians
  - Network researchers, mathematicians, cryptographers, ethical hackers
- Businesses and other organisations
  - Organisations specialising in network security services.
  - Businesses with a significant interest in network security
- Malfeasors
  - Hackers, crackers, script kiddies

Parties involved in Network Security Standards Organisations

- IETF : Internet Engineering Task Force
  - This organisation is responsible for the protocols that run the internet (including those concerned with security) e.g. ssh, IPSec, SSL/TLS and SNMP.
  - http://www.ietf.org
- ITU-T : International Telecommunication Union – Telecommunication Sector
  - A UN specialised agency. Releases some standards relevant to network security. In particular the X.509 PKI (Public Key Infrastructure) standard and the X.800 Security Architecture Standard.

Parties involved in Network Security Governments and their agencies

- Governments have a huge interest in all aspects of network security.
- Protection of their own systems (websites, data, etc.).
- Providing legal framework for enforcement of laws concerned with network security.
- Espionage and cyber-warfare.
- Some governments also provide encryption and hash standards e.g. DES (Data Encryption Standard) and AES (Advanced Encryption Standard).

Parties involved in Network Security Academics, Researchers and Civil Libertarians

- Academics (not just inside universities but in government, business and private organisations)
  - Academics have been active in researching all aspects of network security. In particular, the have done most of the mathematical work involved in the development of cryptographic techniques.
- Researchers and Civil Libertarians
  - Some individual researchers (Bruce Schneier, Phillip Zimmerman) and Organisations (Electronic Frontiers Foundation) have made significant contributions to Network Security.

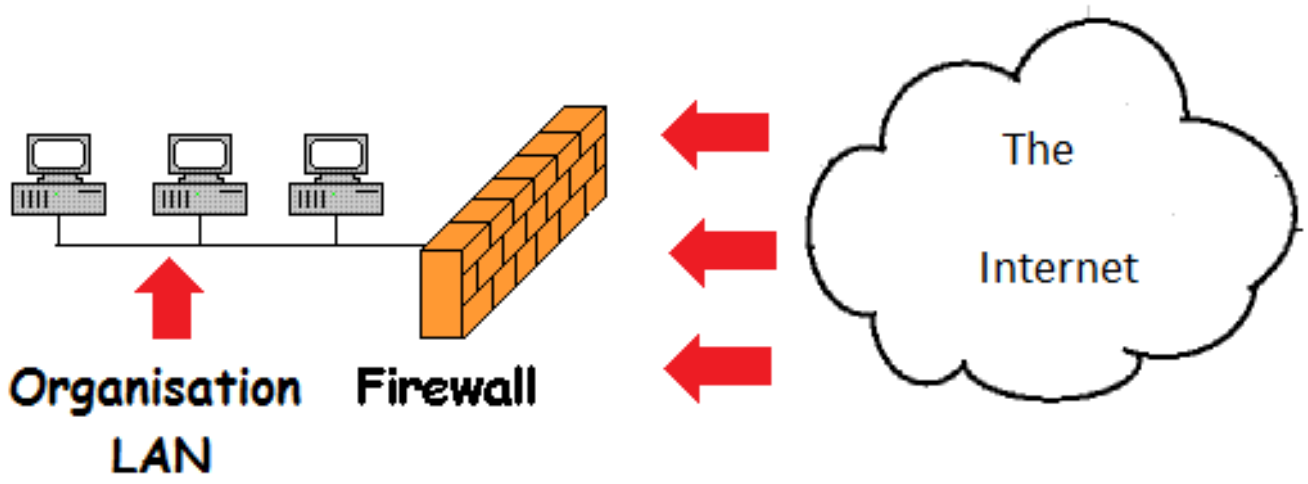
Parties involved in Network Security Businesses and other organisations

- Businesses providing Security Services
  - Many businesses provide security services of one sort or another and some are also active in research. Two well known examples are RSA Security and Counterpane.
- Non profit Security Organizations
  - These provide free advice on computer security and in some cases training and formal certifications. Example organizations are CERT (Computer Emergency Response Team) and I2SC (Internet Information Security Council)

Parties involved in Network Security Malfeasors

- This term refers to individuals who breach one or more of the security goals outlined in the first part of the lecture. It includes a wide range of individuals, goals and motives. There is not always a clear delineation between the different groups.
- Script Kiddies : usually young. Use scripts downloaded from internet. Main motive is curiosity.
- Crackers/Hackers : More knowledgeable than script kiddies. Main motive is status with fellow crackers.
- Career Criminals : May have some knowledge, but often use services of crackers. Main motive is making money through illegal computer related activities.
- Terrorists : Various terrorist groups may use cyber attacks as an adjunct to more conventional terrorist activities. Main motive is disruption of computer activities of those they are opposed to.
- Governments: Governments sponsor hacking (Cyber warfare). This is more common than is generally thought. Naturally, all governments will deny or minimize their own activities in this area. Main motive is political e.g. attacking network resources of states or organizations they dislike.

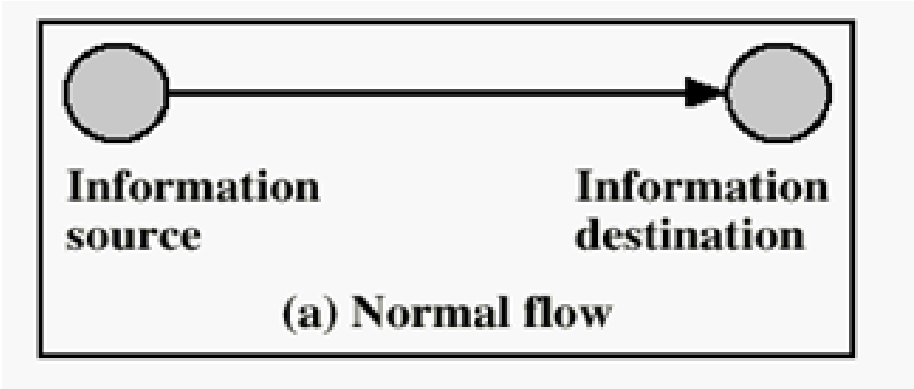
Attacks (threats) and Vulnerabilities



Threats (or attacks) on a system and its network connections (symbolised by red arrows) can come from external or internal sources.

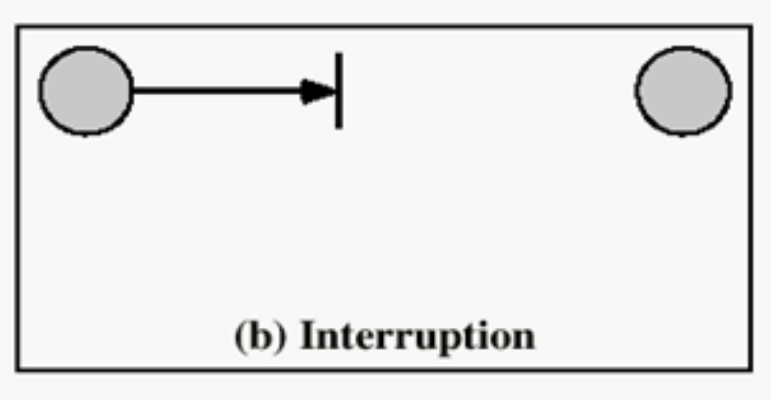
Vulnerabilities (or weaknesses) in the system are weak points in the system that can potentially be exploited.

Type of Security Attacks



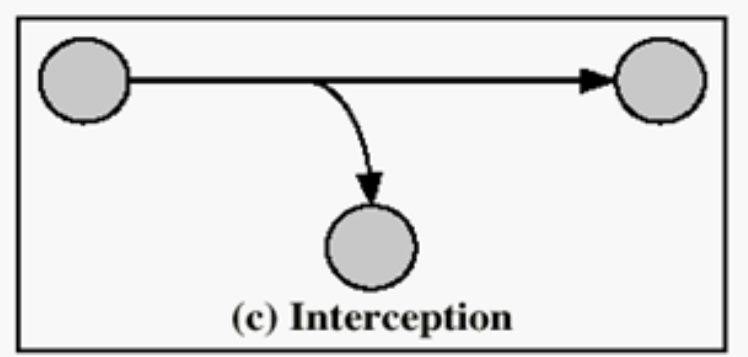
- **Security Attack: Any action that compromises the security of information.**
- Let's see four common type of attacks:

Security Attack (1): Interruption



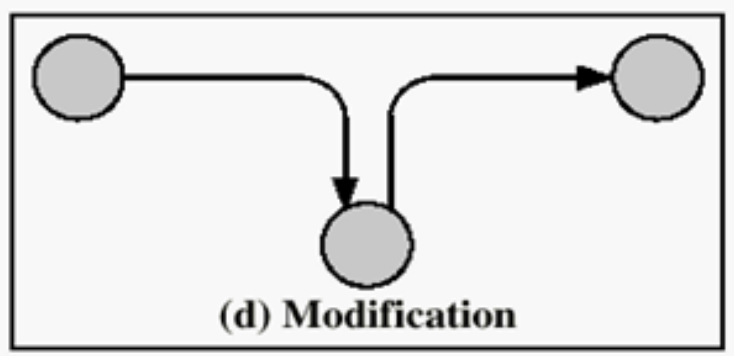
- **Interruption: resources not made available - This is an attack on**
- Availability

Security Attack (2): Interception



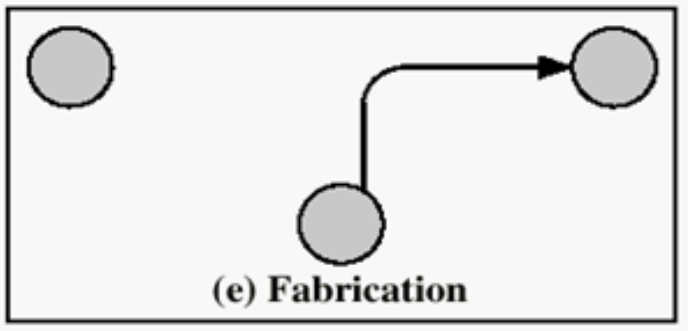
- **Interception:data is read by unauthorized people -This is an attack on**
- confidentiality

Security Attack (3): Modification



- **Modification:existing data is changed by unauthorized people -This is an attack on**
- integrity

Security Attack (4): Fabrication



- **Fabrication: false data is created -This is an attack on**
- message origin authentication

Vulnerabilities

- Vulnerabilities are weaknesses in computers and networks that can potentially be attacked. Vulnerabilities can be classified as:

1. Technological Vulnerabilities : Weaknesses in networking protocols, operating systems, software and network equipment.
2. Configuration Weaknesses : Weaknesses that come about because of human error in the configuration of hardware and software
3. Policy Weaknesses : These are shortcomings in the security policy (or even a total lack of a security policy) that lead to inconsistencies and weaknesses in networks, computers and security systems.