Chapter One

Introduction

What is Internet?

- The Internet is a worldwide IP network, that links collection of different networks from various sources, governmental, educational and commercial.

Preliminaries

Information security: protection of information and its system from unauthorized access.

Network security means information security within a network and during their transmission.

So, we shall start with the information security.

Definitions

Computer Security: measures to protect data within a computer and during its processing.

Internet Security: measures to protect data during their transmission over a collection of interconnected networks.

Preliminaries [Cont..]

Vulnerability: It is a weakness that can be used to cause loss or harm to an information system. Vulnerable points of a system are used to attack the system to breach its security.

Threat: It can be seen as potential violation of security of a system. Of course violation of security will be done to cause harm or loss. Threats exist because of vulnerabilities in a system.

Preliminaries [Cont..]

Attack: It is an **action** performed by an entity with the intention to violate security. Examples of attacks are destruction, modification, fabrication, interruption or interception of data.

Control: It is a **protective measure** (an action, procedure, technique or device) that attempts to prevent exploitation of the vulnerabilities of a system.

Preliminaries [Cont..]

Logical Control : It uses software and data to monitor and control access to data (information) of a system. As for example, password authentication schemes, access control schemes, firewalls to network, network intrusion detection systems, and encryption methods are types of logical controls.

Physical Control: It monitors and controls the surrounding place *i.e.* the environment of the systems. For example: doors and locks, cameras, barricades, fencing, security guards etc.

Services and Mechanisms

- **Security Mechanism:** A mechanism that is designed to detect, prevent, or recover from a security attack.

- **Security Service:** A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

Security Services

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Access control (prevent misuse of resources)
- Availability:
  - Denial of Service Attacks
  - Virus that deletes files

The Basic Components

Confidentiality: is the concealment of information or resources. It means to prevent disclosure of information to unauthorized users.

- □ E.g., only sender, intended receiver should “understand” message contents

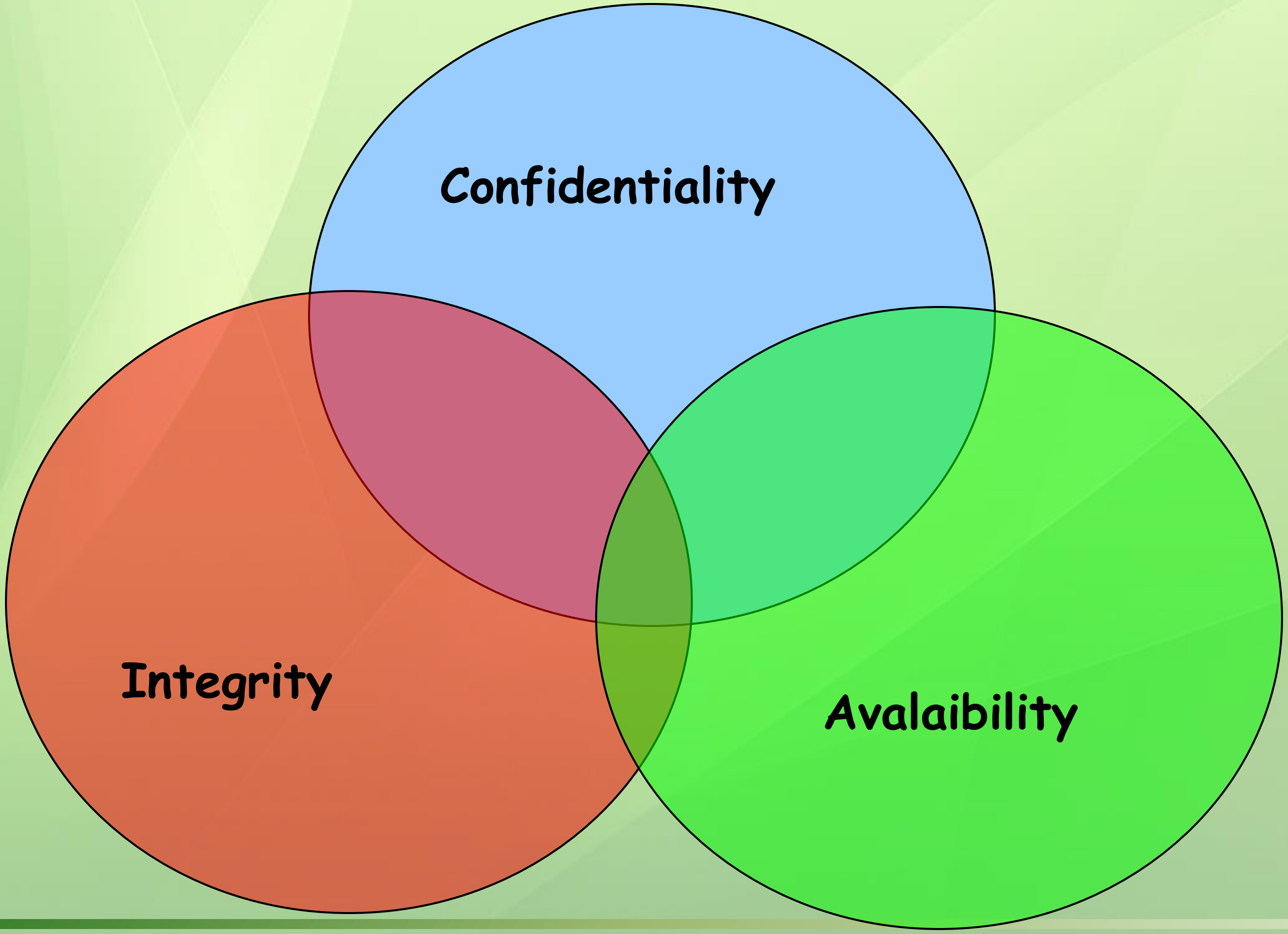
Authenticity: is the identification and assurance of the origin of information.

Integrity: refers to the trustworthiness of data or resources in terms of preventing improper and unauthorized modifications or changes. It refers data consistency.

The basic components [Cont..]

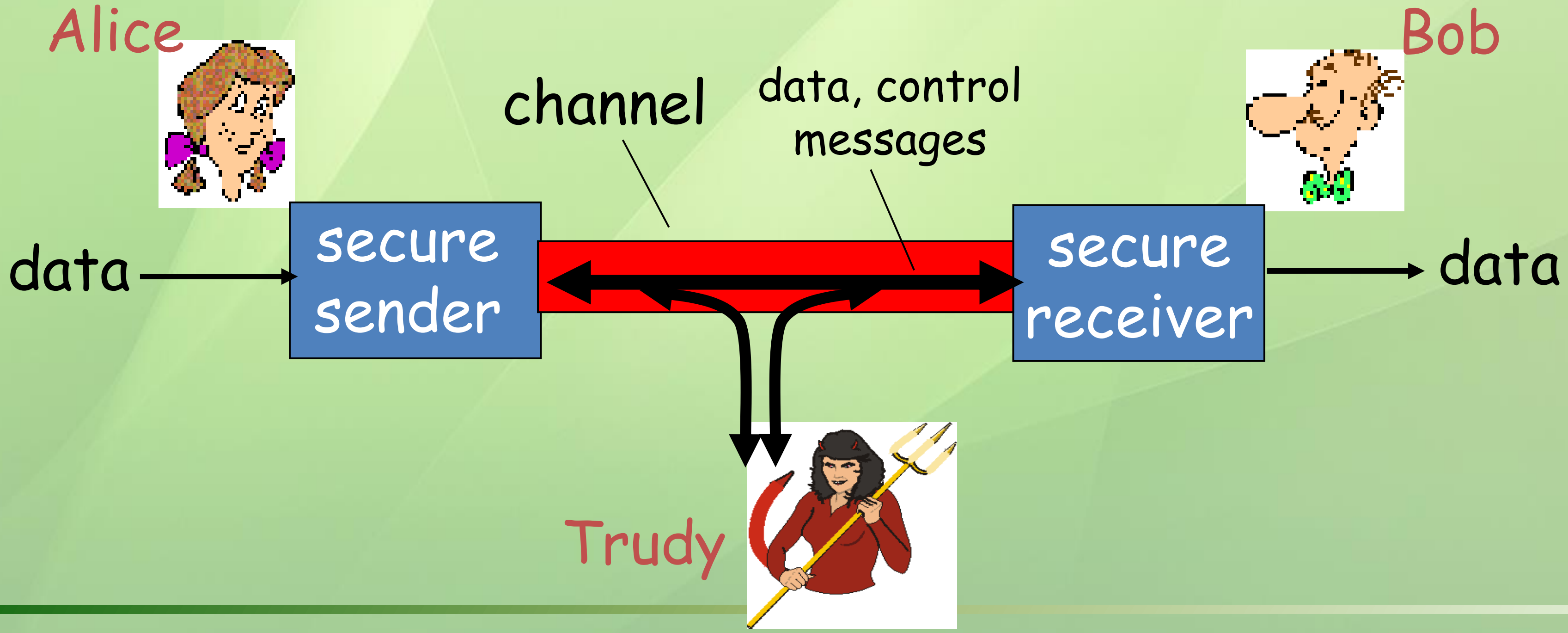
Availability: refers to the ability to use the information or resource desired. It means information must be accessible to authorized users or information must be available when it is needed to authorized user. In other words an authorized user should not be prevented from accessing information, data or objects to which he has legitimate access.

Security Goals



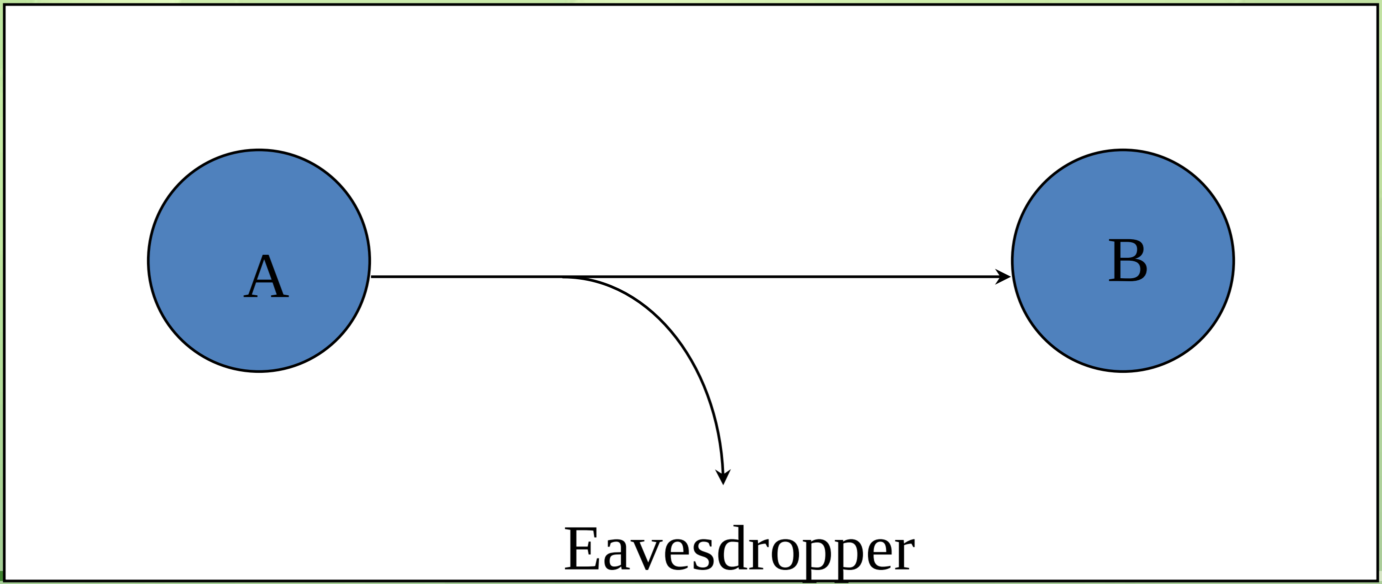
Friends and enemies: Alice, Bob, Trudy

- ❑ well-known in network security world
- ❑ Bob, Alice want to communicate “securely”
- ❑ Trudy (intruder) may intercept, delete, add messages



Eavesdropping - Message Interception (Attack on Confidentiality)

- ❑ Unauthorized access to information
- ❑ Wiretappers and Packet sniffers
- ❑ Illicit copying of files and programs



Attack on confidentiality [cont..]

Wiretapping: means to intercepts communications. A wiretap can be done in such a way that neither the sender nor the receiver of a communication knows that the contents have been intercepted.

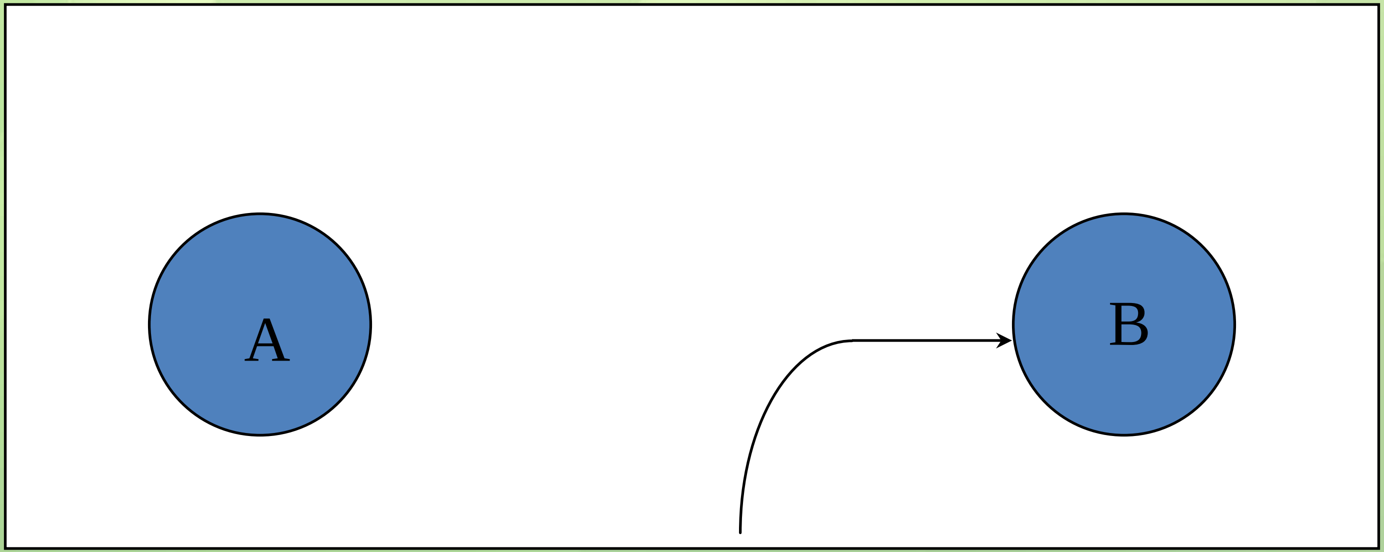
Passive wiretapping is just listening or reading.

Active wiretapping means injecting something into the communication.

Packet sniffer: software used by intruder to analyze packet.

Authenticity Attack - Fabrication

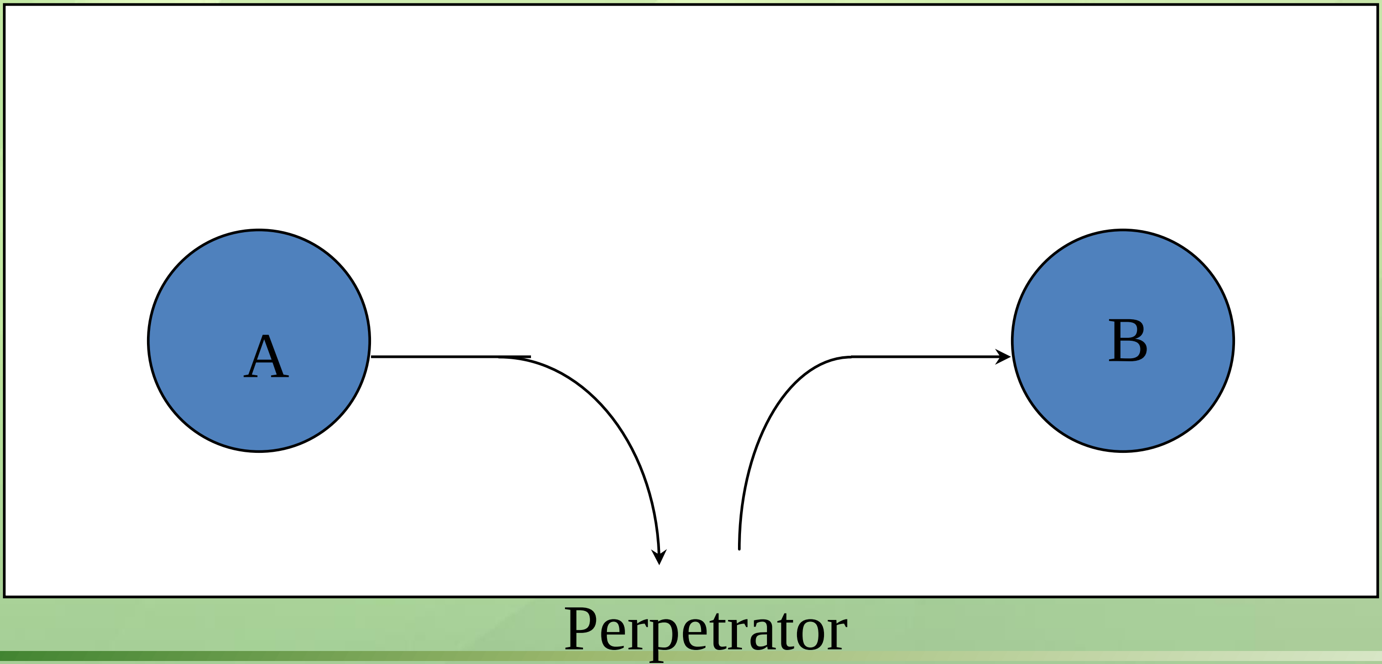
- Unauthorized assumption of other’s identity
- Generate and distribute objects under this identity



Masquerader: from A

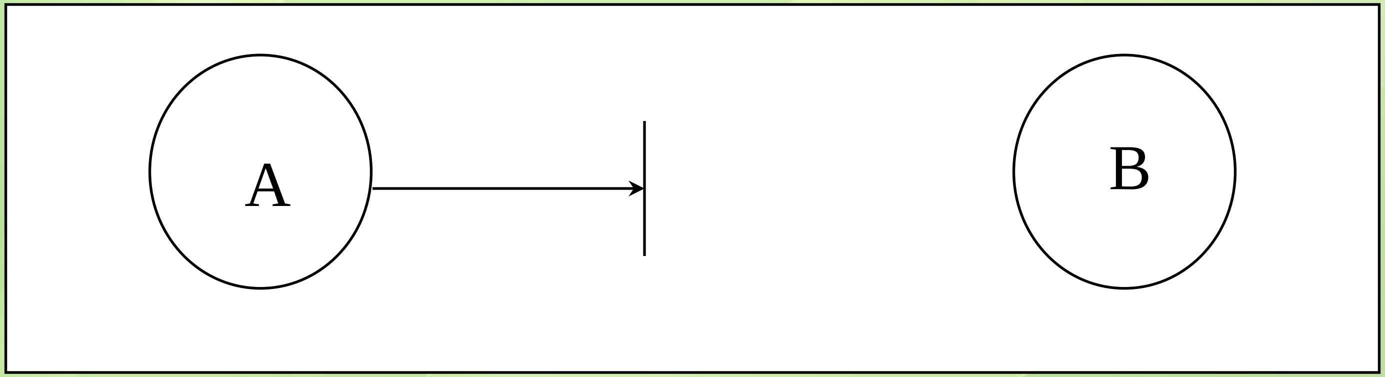
Integrity Attack - Tampering With Messages

- ❑ Stop the flow of the message
- ❑ Delay and optionally modify the message
- ❑ Release the message again



Attack on Availability

- ❑ Destroy hardware (cutting fiber) or software
- ❑ Modify software in a subtle way (alias commands)
- ❑ Corrupt packets in transit



- ❑ Blatant *denial of service* (DoS):
  - □ Crashing the server
  - □ Overwhelm the server (use up its resource)

Classify Security Attacks as

- **Passive attacks** - eavesdropping on, or monitoring of, transmissions to:
  - obtain message contents, or
  - monitor traffic flows
- **Active attacks** – modification of data stream to:
  - masquerade of one entity as some other
  - replay previous messages
  - modify messages in transit
  - denial of service

Security policy and mechanism

Threat analysis: A threat analysis is a process where all possible threats to a system are identified. It is an important aid for defining the security policy. A list containing these threats and the severity of each threat is created. This list is then used as a basis for defining the security policy.

Security policy: It is a set of rules stating what is permitted and what is not permitted in a system during normal operation. It is written in general terms and describes the security requirements for a system.

Security Policy and Mechanism

Mechanism: a procedure, tool, or method of enforcing a policy.

Security mechanisms implement functions that help *prevent*, *detect*, *and respond to recovery from* security attacks.

Security functions are typically made available to users as a set of security services through integrated interfaces.

Cryptography underlies many security mechanisms.

How to Make a System Trustworthy

- Specification
  - A statement of desired functions.
- Design
  - A translation of specifications to a set of components.
- Implementation
  - Realization of a system that satisfies the design.
- Assurance
  - The process to insure that the above steps are carried out correctly.
  - Inspections, proofs, testing, etc.

The Security Life Cycle

- The *iterations* of
  - Threats analysis
  - Policy
  - Specification
  - Design
  - Implementation
  - Operation and maintenance

Security mechanism

This is the end

Of

Introduction

Thank You.