Chapter 1 – Introduction

Background

- Information Security requirements have changed in recent times.
- Traditionally provided by physical and administrative mechanisms.
- Computer use requires automated tools to protect files and other stored information.
- Use of networks and communications links requires measures to protect data during transmission.

Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers.
- **Network Security** - measures to protect data during their transmission.
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks.

Aim of Course

- Our focus is on Internet Security.
- Consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information.

Services, Mechanisms, Attacks

- Need systematic way to define requirements.
- Consider three aspects of information security:
    - **security service.**

- **security mechanism.**
- **security attack.**

Security Service

is something that enhances the security of the data processing systems and the information transfers of an organization**.**

Security Mechanism

- a mechanism that is designed to detect, prevent, or recover from a security attack.
- use: cryptographic techniques.

Security Attack

- any action that compromises the security of information owned by an organization.
- note: often *threat* & *attack* mean same.

Security Services (X.800)

- **Authentication -** assurance that the communicating entity is the one claimed (authorized one).
- **Access Control -** prevention of the unauthorized use of a resource.
- **Data Confidentiality** –protection of data from unauthorized disclosure (access).
- **Data Integrity -** assurance that data received is as sent by an authorized entity.

- **Non-Repudiation** - protection against denial by one of the parties in a communication.

Security Mechanisms (X.800)

- specific security mechanisms:
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization.
- pervasive security mechanisms:
  - trusted functionality, security labels, event detection, security audit trails, security recovery.

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.

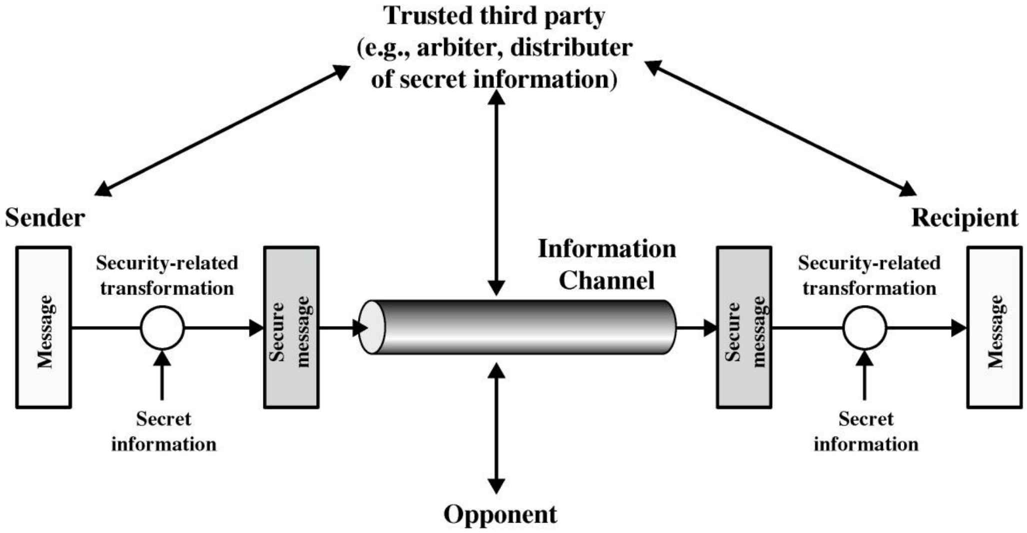

Figure 1.1 Model for Network Security

Model for Network Security

- Using this model requires us to:
  - design a suitable algorithm for the security transformation.
  - generate the secret information (keys) used by the algorithm.
  - develop methods to distribute and share the secret information.
  - specify a protocol enabling the principals to use the transformation and secret information for a security service.