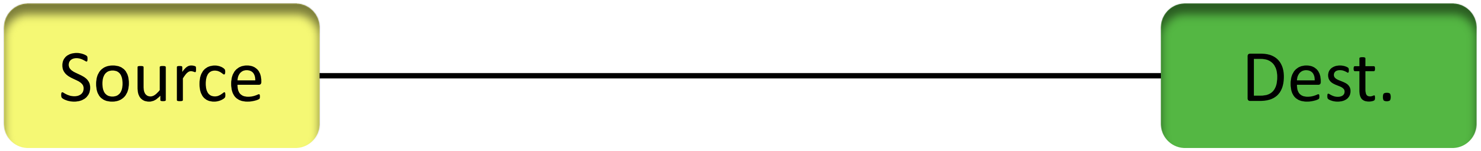
CS-8843
Data and Network Security

Lecture 2

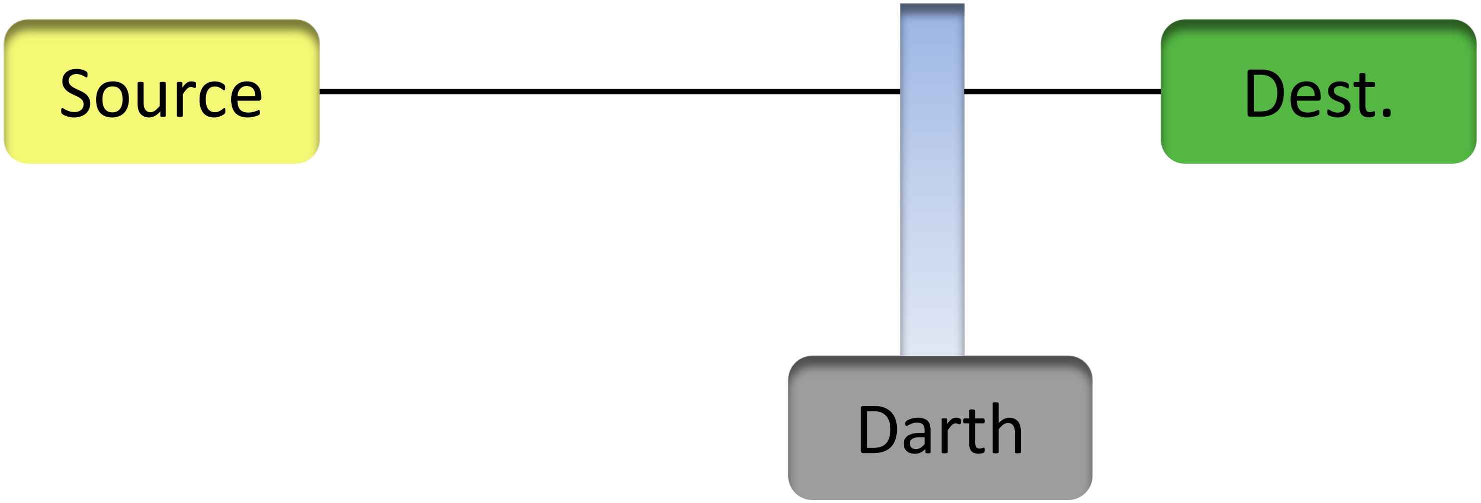
Attacks (for what?)

- **Interruption:** This is an attack on availability
- **Interception:** This is an attack on confidentiality
- **Modification:** This is an attack on integrity
- **Fabrication:** This is an attack on authenticity

Normal Flow

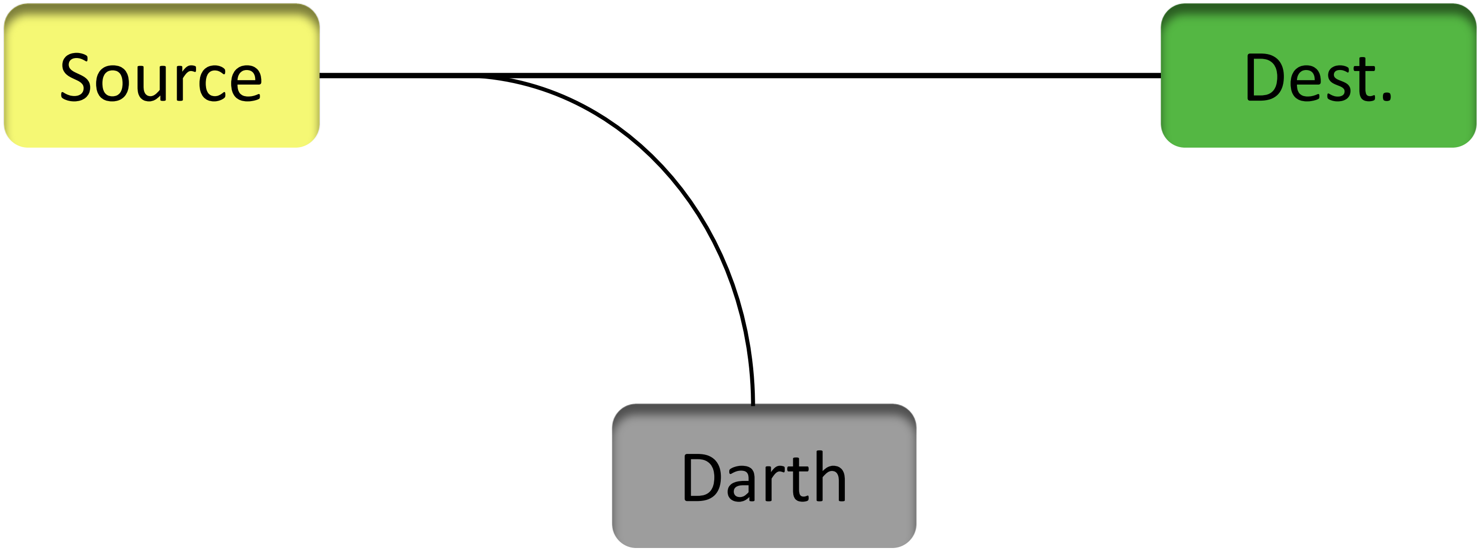


Interruption



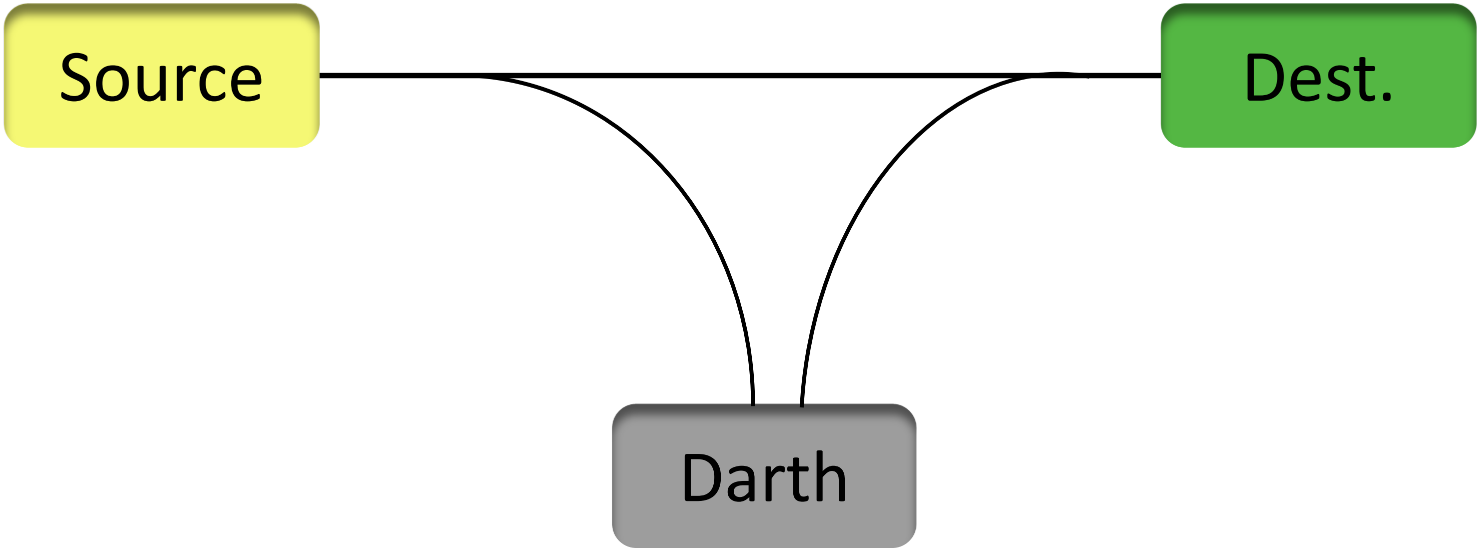
This is an attack on availability

Interception



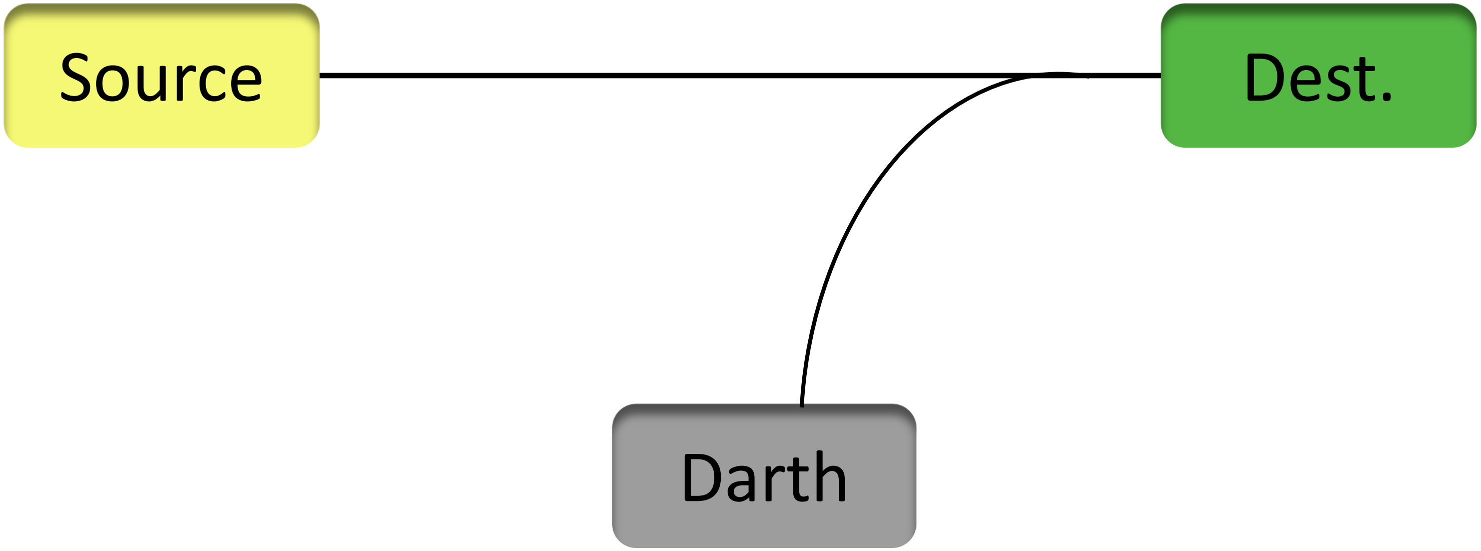
This is an attack on confidentiality

Modification



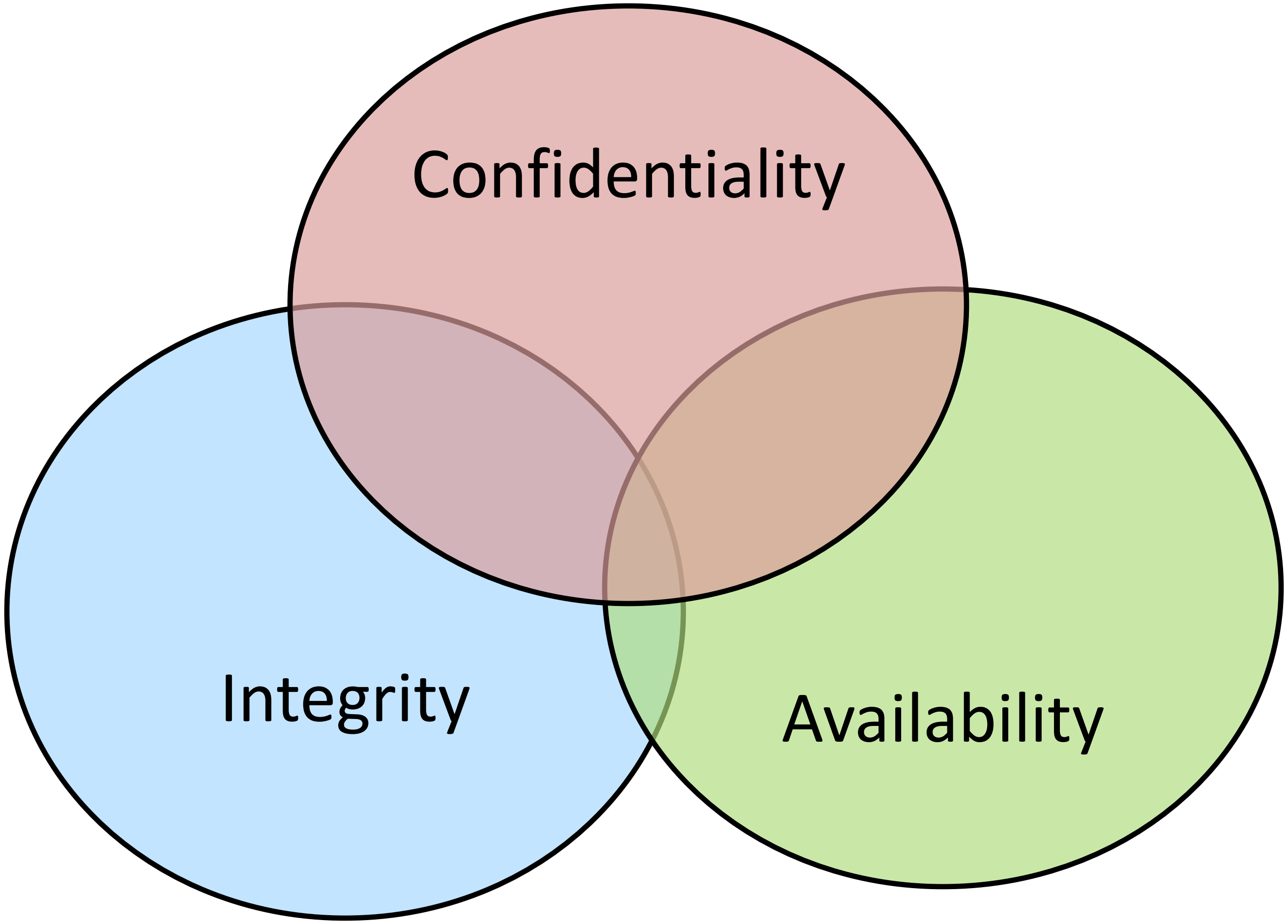
This is an attack on integrity

Fabrication



This is an attack on authenticity

Security Goals



Types of Attacks

- Broadly, two Types of attacks
  - Passive attacks and Active Attacks

- Passive attacks
  - Attempts to learn or make use of information from system.
  - Does not effect the system.
  - Goal is to obtained the information that is being transmitted.
  - Difficult to detect.
  - Feasible to prevent (prevention rather then detection).

Types of Attacks (cont….)

- Passive attacks (cont..)
  - Further divided into two type:
    1. **Release of message contents**:
       - e.g. Telephone conversation, attached file, email message.
    2. **Traffic analysis:**
       - If we can mask our communication.
       - Still attacker can learn location and identification of hosts.
       - Frequency and length of communication, helps to learn nature of communication.

Types of Attacks (cont..)

- Active Attacks
  - Involves modification of data stream or creation of false stream.
  - Divided into four types:

    1. **Replay**
       - Involves passive capture of data units
       - And its subsequent retransmission to produce an unauthorized access.

Types of Attacks (cont..)

- Active Attacks (cont..)

  2. **Masquerade:**
     - One entity pretends to be another entity.
     - Usually includes one from other active attacks.

       - e.g. authentication sequence captured and replayed to get unauthorized access privileges.

Types of Attacks (cont..)

- Active Attacks (cont..)

  3. **Modification of message:**
     - Some portion of a legitimate message is altered OR delayed OR re-ordered. To produce unauthorized effect.

       - e.g. Modify **Allow Ali** to *read confidential file accounts* to **Allow Adnan** to *read confidential file accounts*.

Types of Attacks (cont..)

- Active Attacks (cont..)

  4. **Denial of Service:**
     - Prevents normal use or management of communication facility.
     - May have a specific target (e.g. security audit service).
     - Another form is the disruption of an entire host or network.

Security Services

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files

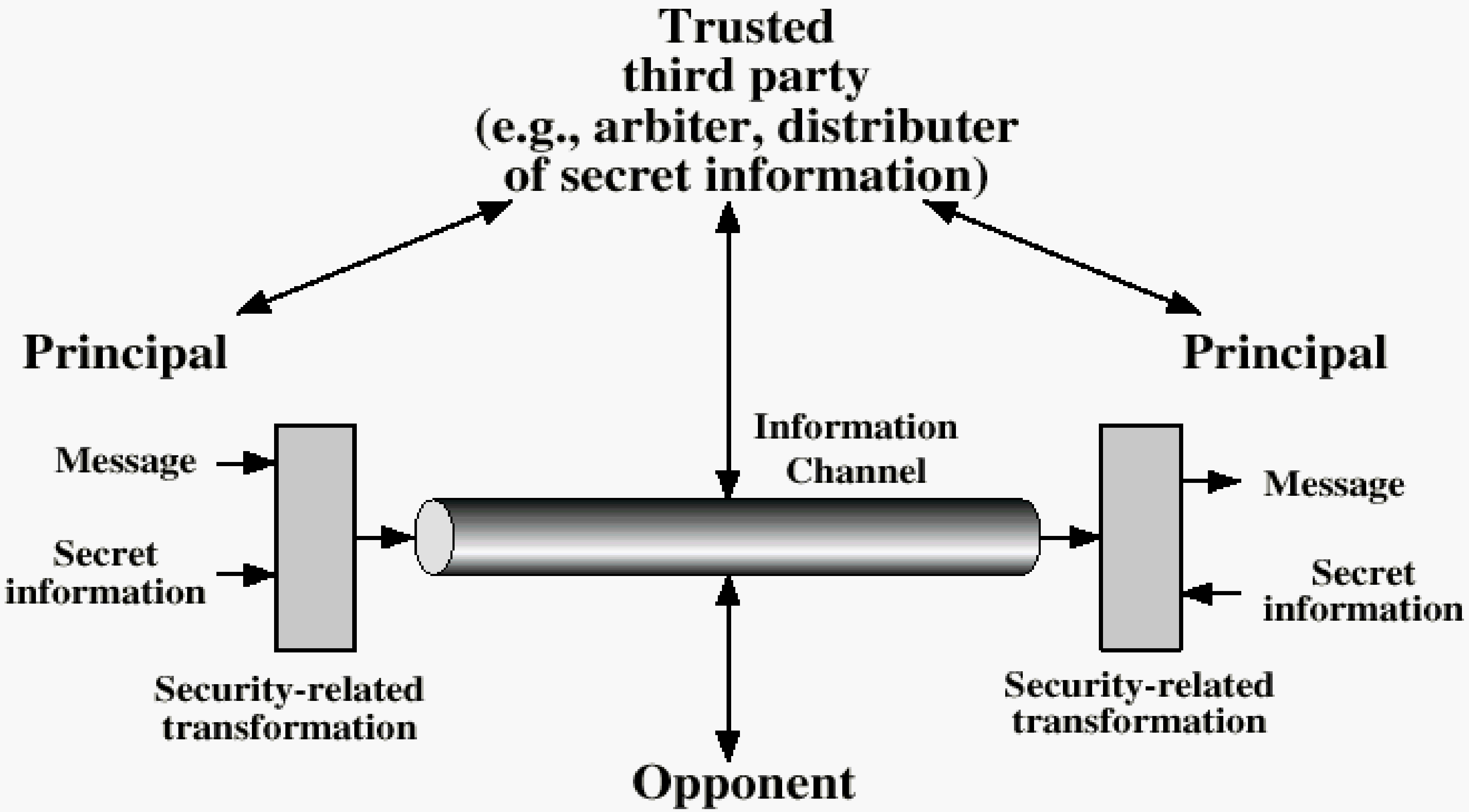


Figure 1.3 Model for Network Security

- This general model shows that there are four basic tasks in designing a particular security service:
  - 1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
  - 2. Generate the secret information to be used with the algorithm.
  - 3. Develop methods for the distribution and sharing of the secret information.
  - 4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

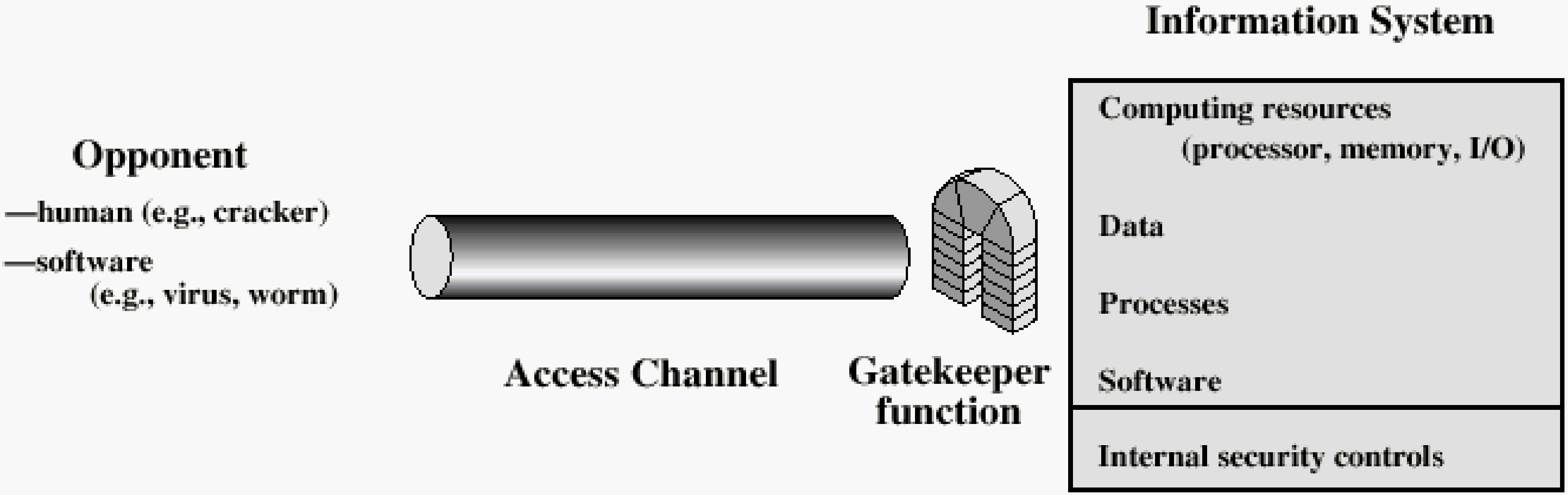
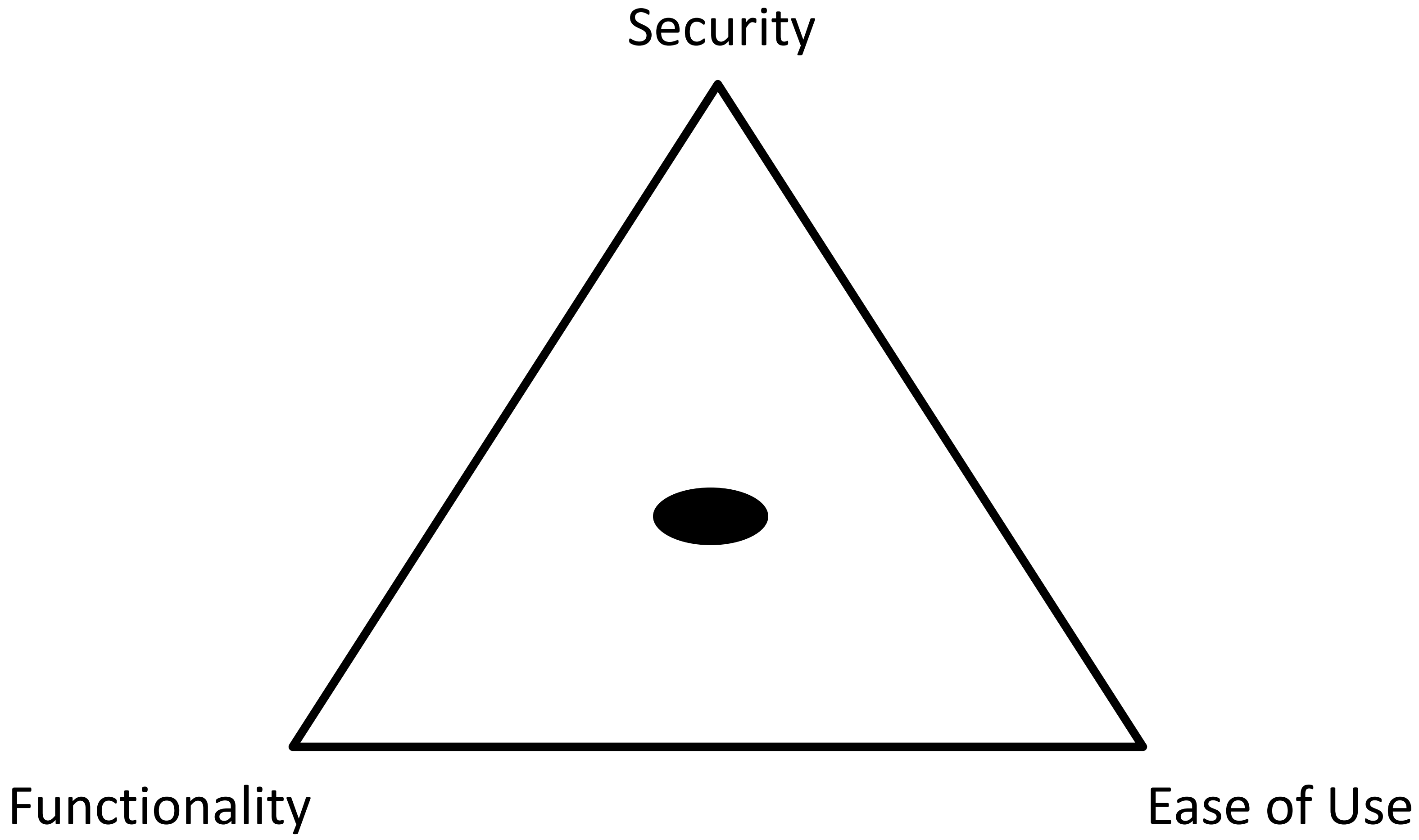


Figure 1.4 Network Access Security Model

Method of Defense

- Encryption
- Software Controls (access limitations in a data base, in operating system protect each user from other users)
- Hardware Controls (smartcard)
- Policies (frequent changes of passwords)
- Physical Controls

Security's impact on overall functionality



The End.