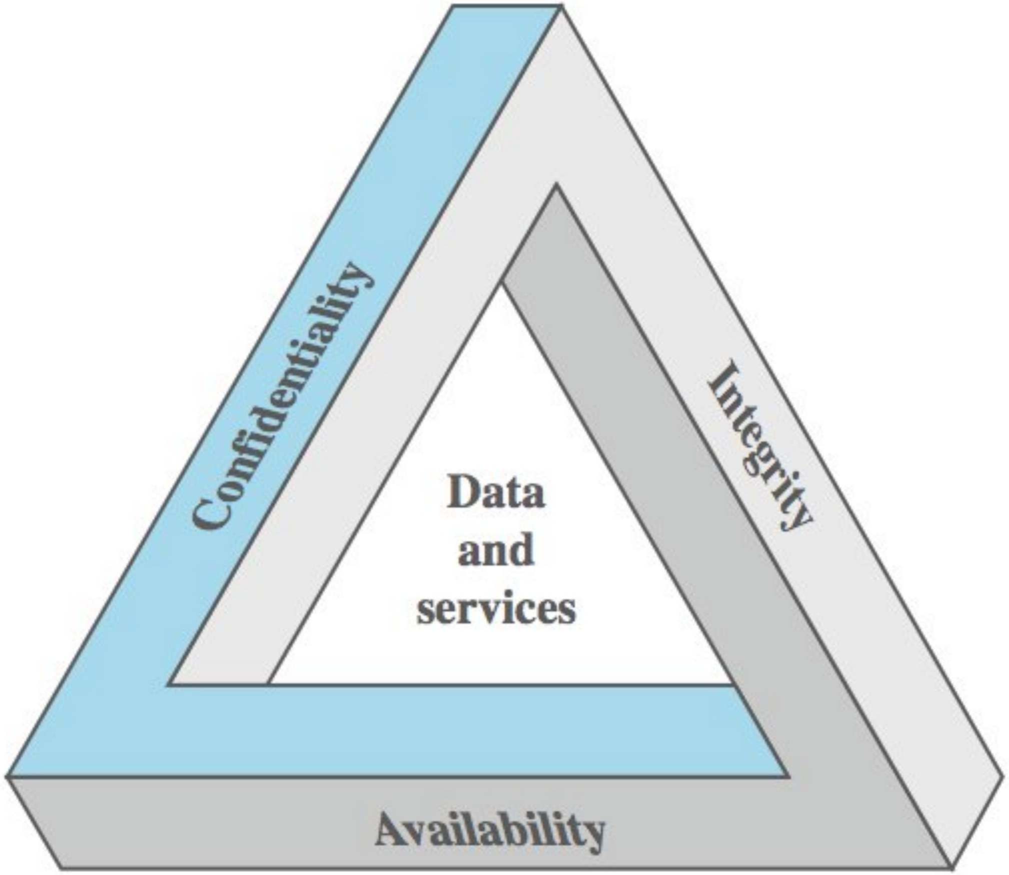
Cryptography and Network Security

Dr. Rafiqul Islam

Computer Security

- The protection afforded to an automated information system in order to attain-
  - the applicable objectives of preserving the integrity, availability and confidentiality of information system resources
- That includes hardware, software, firmware, information/data, and telecommunications.

Key Security Concepts



Levels of Impact

- Can define 3 levels of impact from a security breach
  - Low
  - Moderate
  - High

Low Impact

- The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
- A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might

  (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;

  (ii) result in minor damage to organizational assets;

  (iii) result in minor financial loss; or

  (iv) result in minor harm to individuals.

Moderate Impact

- The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- A serious adverse effect means that, for example, the loss might

  (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;

  (ii) result in significant damage to organizational assets;

  (iii) result in significant financial loss; or

  (iv) result in significant harm to individuals that does not involve loss of life or serious, life-threatening injuries.

High Impact

- The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
- A severe or catastrophic adverse effect means that, for example, the loss might

  (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;

  (ii) result in major damage to organizational assets;

  (iii) result in major financial loss; or

  (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Examples of Security Requirements

- confidentiality – student grades
- integrity – patient information
- availability – authentication servicetim

Computer Security Challenges

1. Not simple – easy to get it wrong
2. Must consider potential attacks
3. Procedures used counter-intuitive
4. Involve algorithms and secret info
5. Must decide where to deploy mechanisms
6. Battle of wits between attacker / admin
7. Not perceived on benefit until fails
8. Requires regular monitoring a process, not an event
9. Too often an after-thought
10. Regarded as impediment to using system

    “Unusable security is not secure”

Aspects of Security

- Consider 3 aspects of information security:
  - security attack
  - security mechanism (control)
  - security service
- Note terms
  - *threat* – a potential for violation of security
  - *vulnerability* – a way by which loss can happen
  - *attack* – an assault on system security, a deliberate attempt to evade security services

Handling Attacks

- Passive attacks – focus on Prevention
  - Easy to stop
  - Hard to detect
- Active attacks – focus on Detection and Recovery
  - Hard to stop
  - Easy to detect

Security Service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
    - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Services (X.800)

- **Authentication** - assurance that communicating entity is the one claimed
  - have both peer-entity & data origin authentication
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **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
- **Availability** – resource accessible/usable

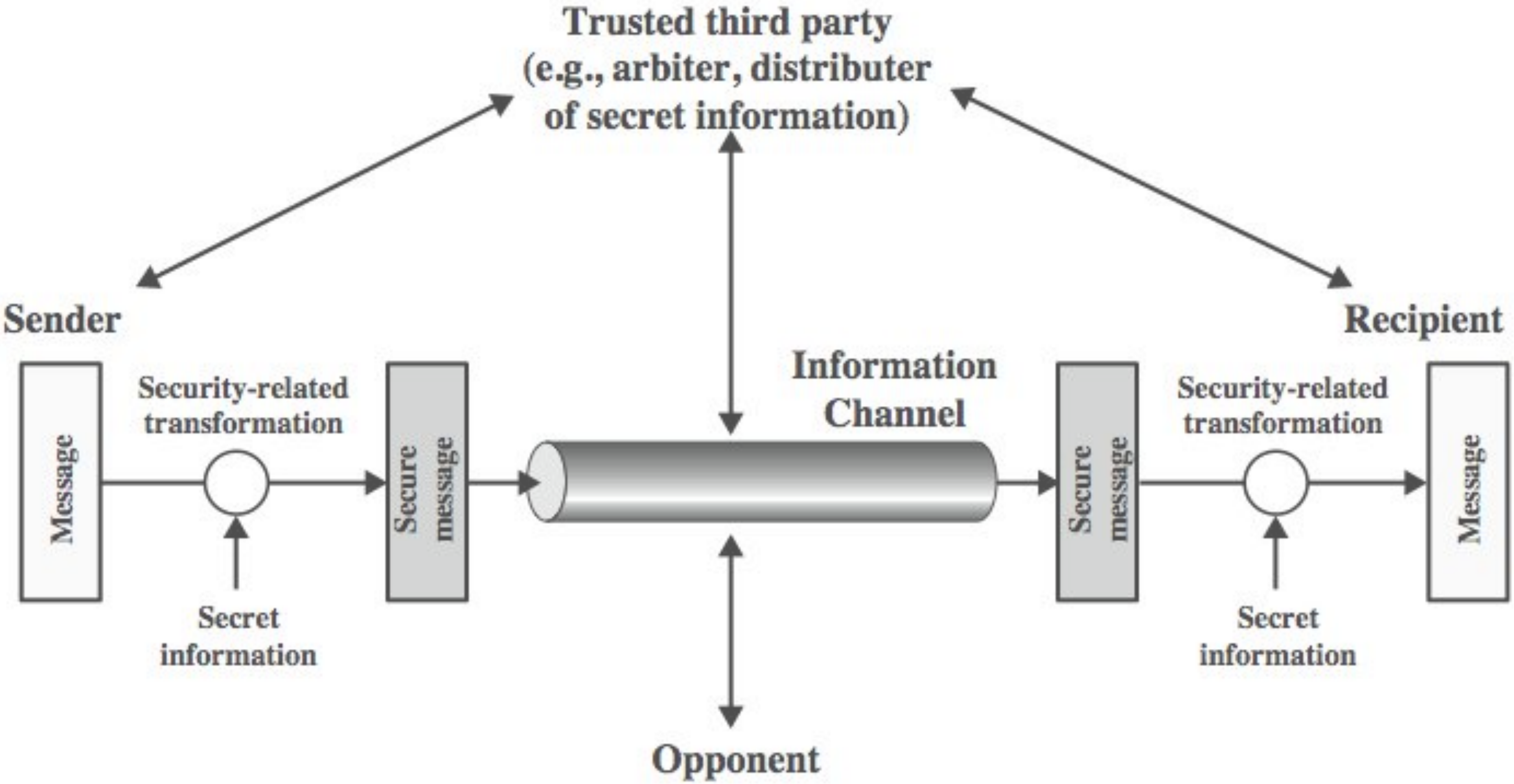
Security Mechanism

- a.k.a. control
- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
  - **cryptographic techniques**
- hence our focus on this topic

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

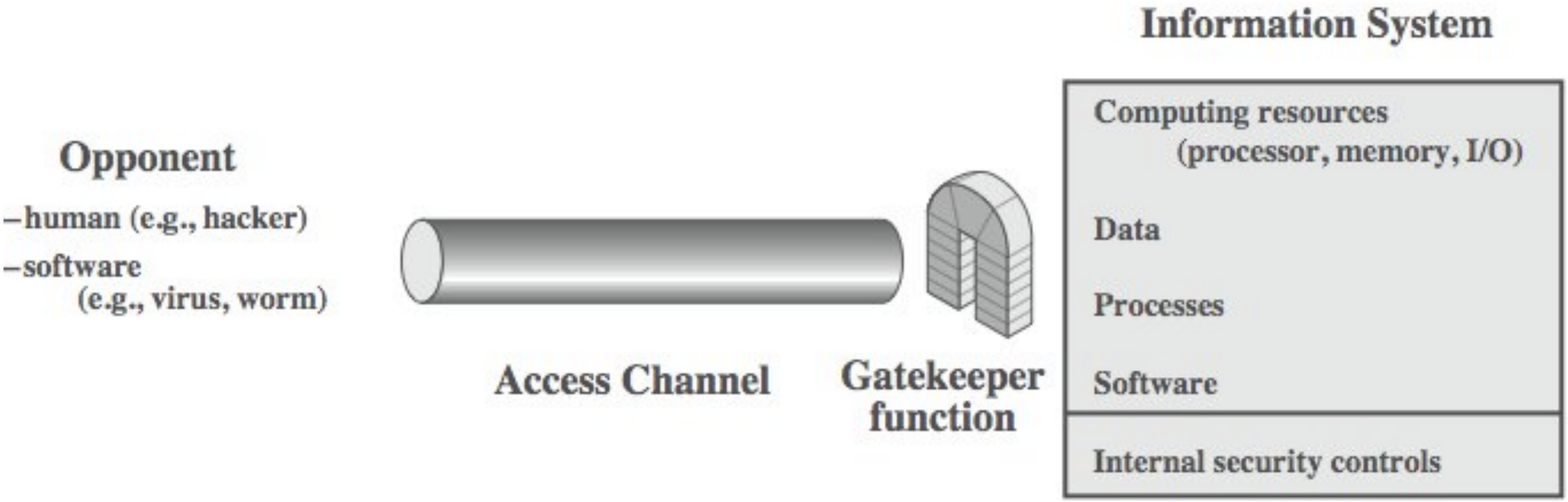
Model for Network Security



Model for Network Security

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

Model for Network Access Security



End Chapter-1

- Questions??