Cryptography and Network Security
Overview & Chapter 1

Sixth Edition

by William Stallings

Lecture slides by Lawrie Brown

DR: Hayam MOUSA

Chapter 0 – Reader’s Guide

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

—***The Art of War*, Sun Tzu**

Book Roadmap

- Cryptographic algorithms
  - symmetric ciphers
  - asymmetric encryption
  - hash functions
- Mutual Trust
- Network Security
- Computer Security

Chapter 1 – Introduction

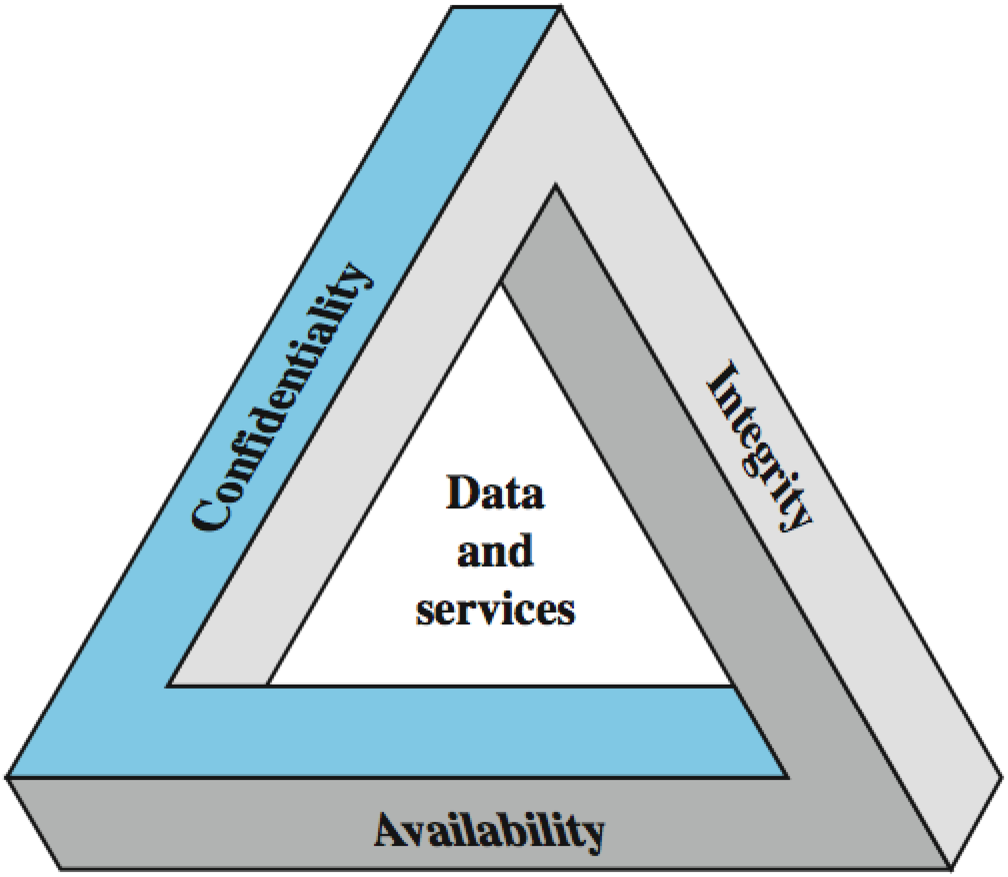
- *The combination of space, time, and strength that must be considered as the basic elements of this theory of defense makes this a fairly complicated matter. Consequently, it is not easy to find a fixed point of departure..*

  — On War, Carl Von Clausewitz

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 (includes hardware, software, firmware, information/data, and telecommunications)

Key Security Concepts



Standards Organizations

- National Institute of Standards & Technology (NIST)
- Internet Society (ISOC)
- International Telecommunication Union Telecommunication Standardization Sector (ITU-T)
- International Organization for Standardization (ISO)

Network and computer security Requirements CIA

- **Confidentiality**
  - **Data Confidentialit**y –protection of data from unauthorized disclosure
  - **Privacy**: Individuals control which data can be collected and stored and by whom and to whom
- **Integrity** –
  - **Data Integrity**: assurance that data received is as sent by an authorized entity
  - **System integrity**: System performs its intended function free from delibrate or inadvertent unauthorized manipulation.
- **Availability**
  - Systems work promptly and service is not denied to authorized users.(resource accessible/usable)

Additional Concepts

- **Accountability:**
  - The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after action recovery and legal action
- **Authenticity:**
  - The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.

Levels of Impact for Security Breaches

- Low
    - (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
- High
    - The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
    - (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

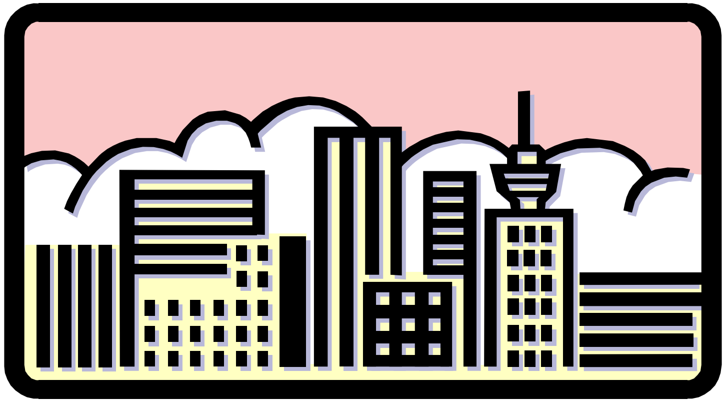
- Confidentiality – student grades
- Integrity – patient information
- Availability – authentication service

Computer Security Challenges

1. not simple
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
9. too often an after-thought
10. regarded as impediment to using system

OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study



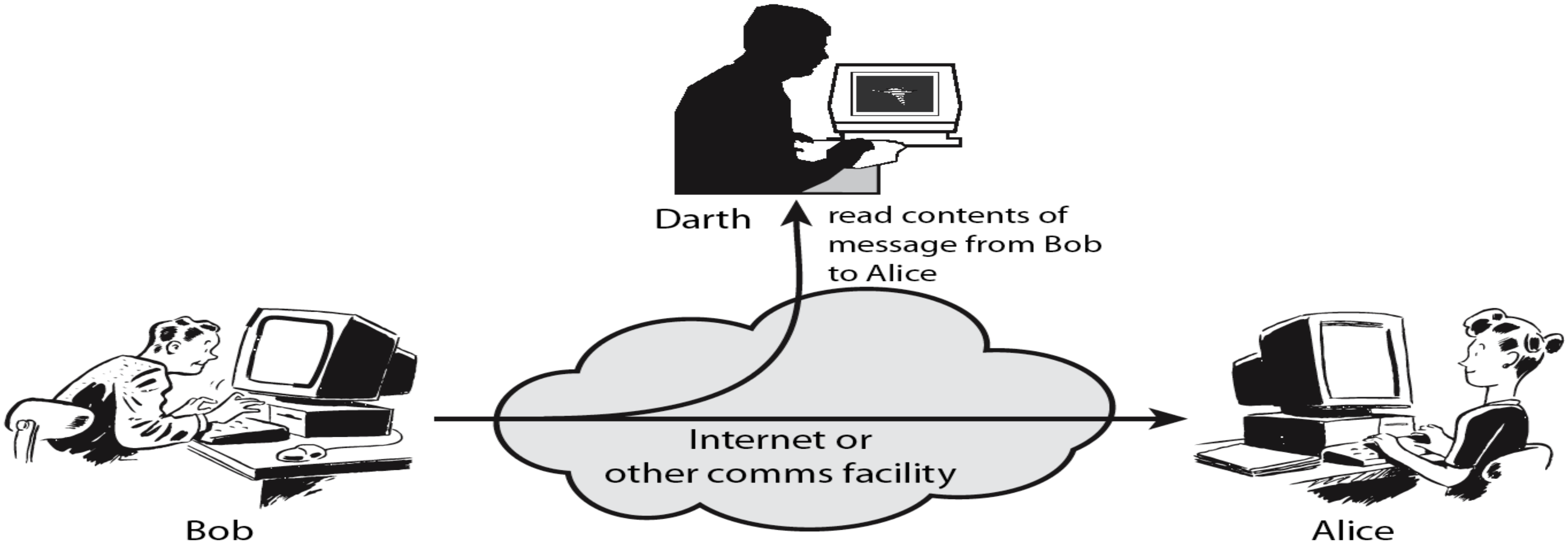
Aspects of Security

- **security attack**
  - Any action that compromises the security of information owned by an organization.
- **security mechanism**
  - A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- **security service**
  - A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

Threat VS. Attack

- **Threat**
  - A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.
- **Attack**
  - An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

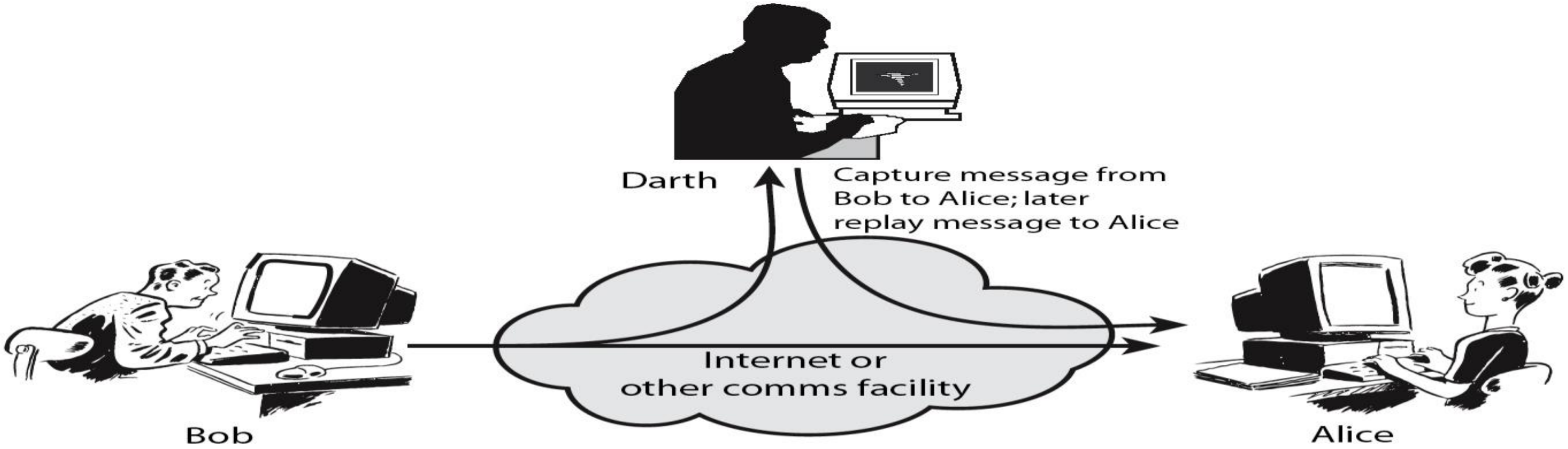
Passive Attacks


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

- A passive attack attempts to learn or make use of information from the system but does not affect system resources.
  - Release message contents
  - Traffic Analysis

Passive attacks are very difficult to detect, because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

Active Attacks


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

- An active attack attempts to alter system resources or affect their operation. Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories:
  - Masquerade,(takes place when one entity pretends to be a different entity)
  - Replay,
  - Modification of messages,
  - Denial of service.

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:

  “a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers”

- RFC 2828:

  “a processing or communication service provided by a system to give a specific kind of protection to system resources”

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

- 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

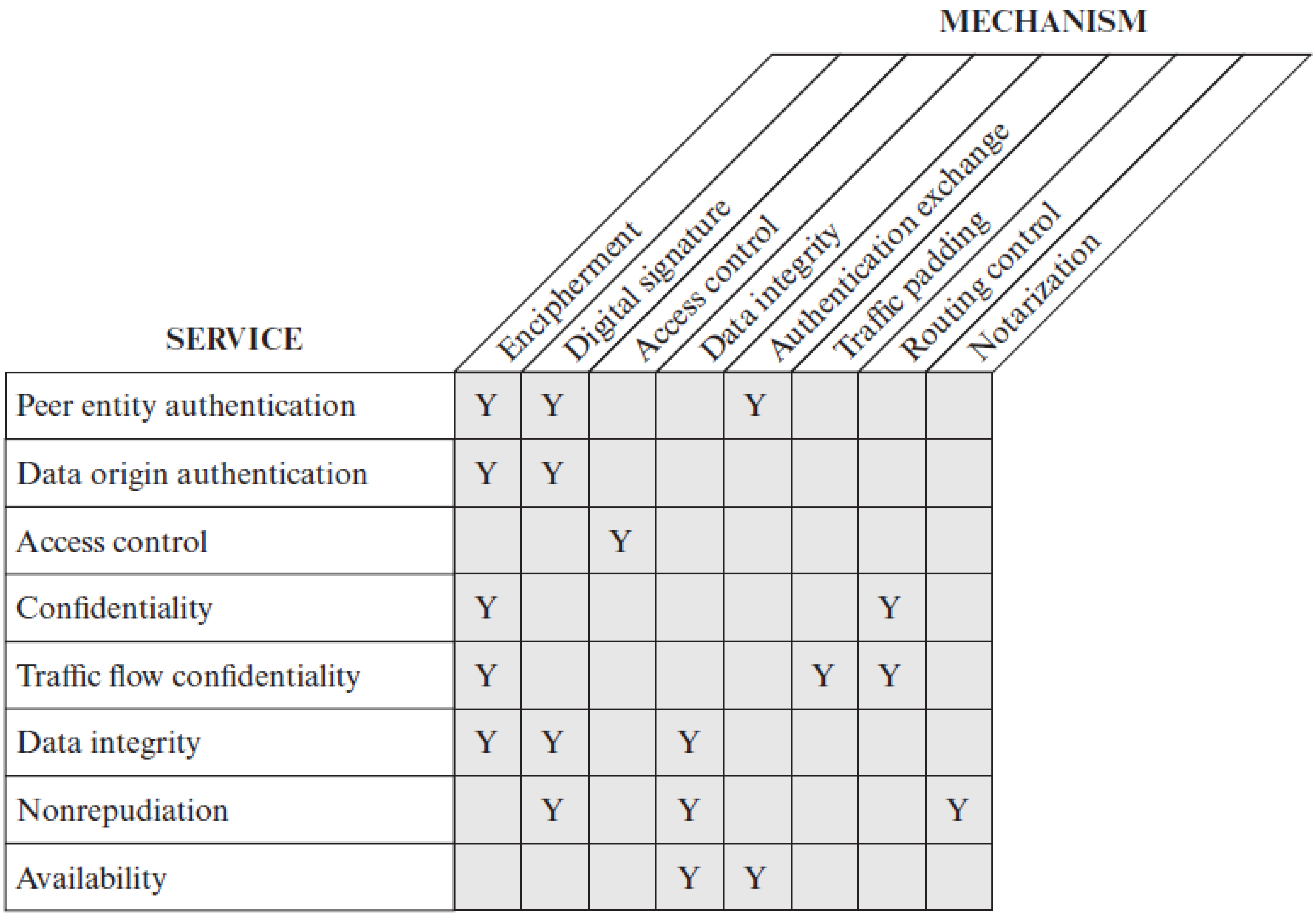
Security Mechanisms (X.800)

- Specific security mechanisms:
  - May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.
    - Encipherment
    - Digital signatures
    - Access controls,
    - Data integrity,
    - Authentication exchange,
    - Traffic padding,
    - Routing control,
    - Notarization

Security Mechanisms (X.800)

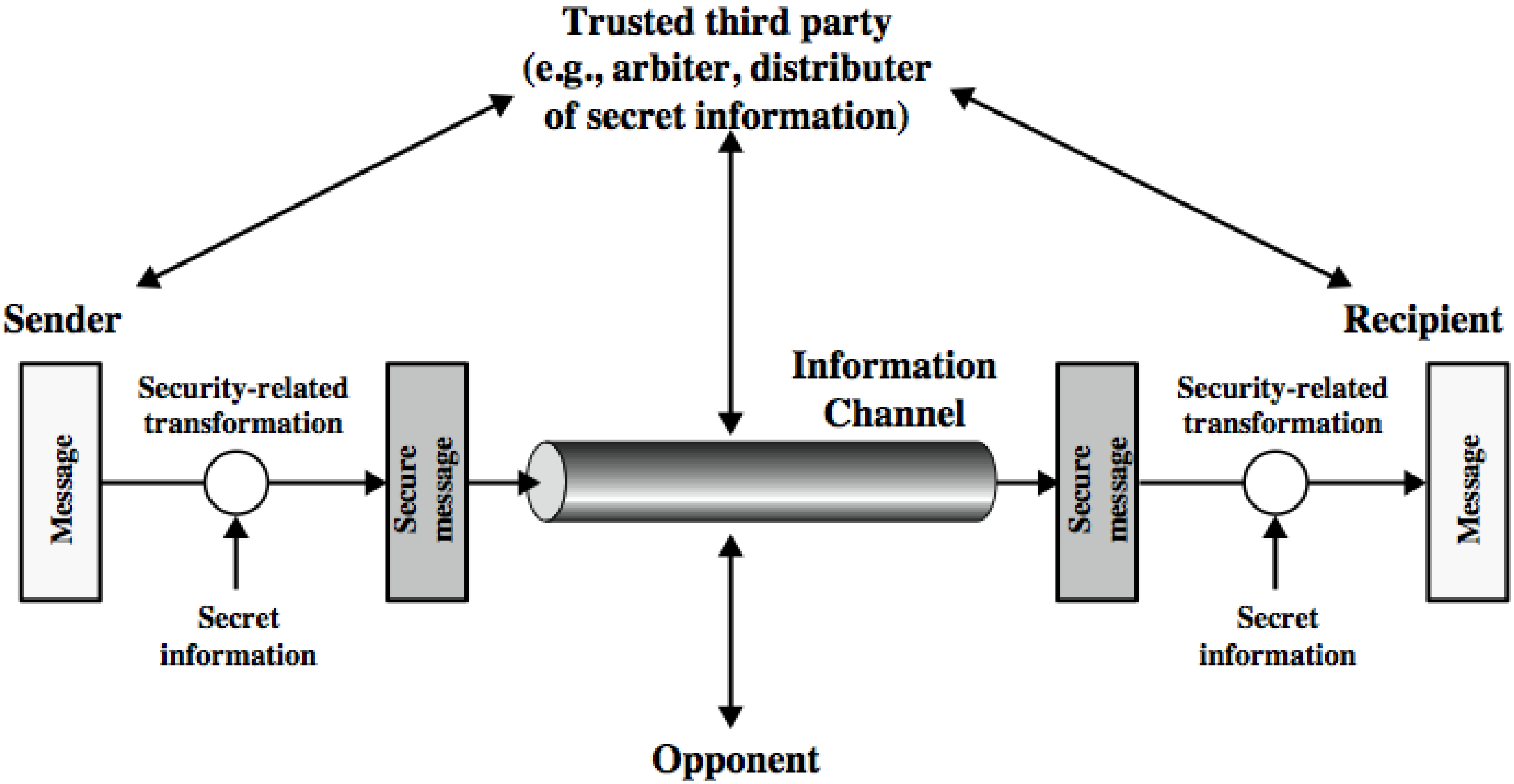
- Pervasive security mechanisms:
  - Mechanisms that are not specific to any particular OSI security service or protocol layer.
    - Trusted functionality,
    - Security labels,
    - Event detection,
    - Security audit trails,
    - Security recovery

Security Services VS. Mechanisms



	MECHANISM							
SERVICE	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Model for Network Security



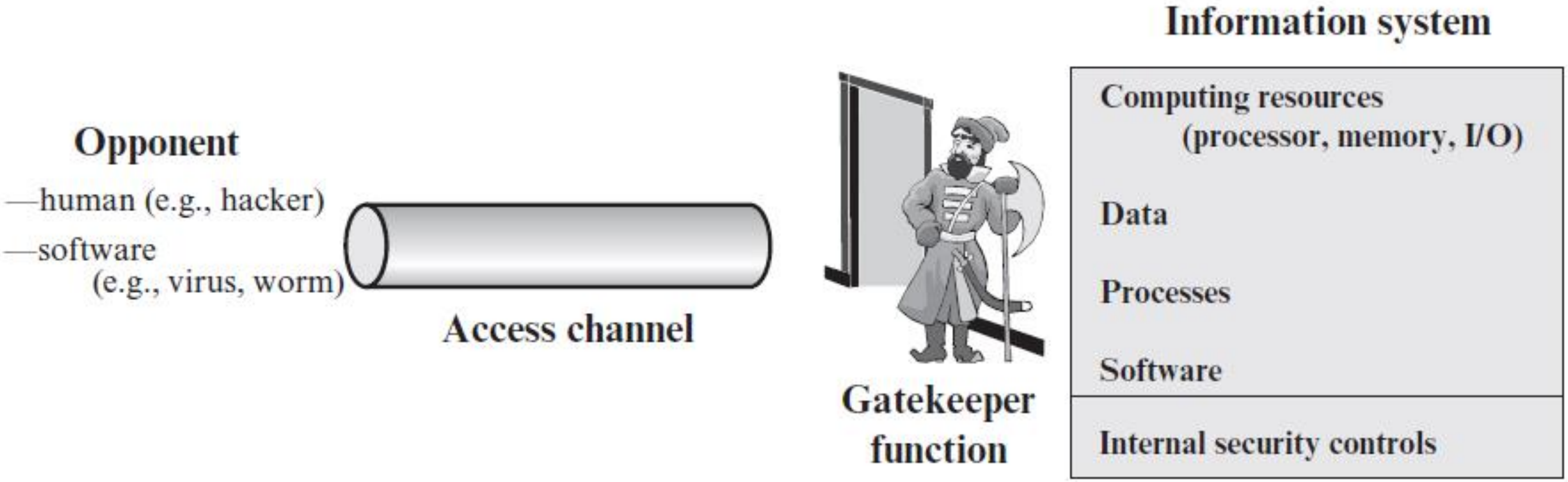
Model for Network Security

- 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

- **Information access threats**: Intercept or modify data on behalf of users who should not have access to that data.
- **Service threats**: Exploit service flaws in computers to inhibit use by legitimate users.



Model for Network Access Security

- using this model requires us to:
  1. Select appropriate gatekeeper functions to identify users
  2. Implement security controls to ensure only authorised users access designated information or resources.

Summary

- topic roadmap & standards organizations
- security concepts:
  - confidentiality, integrity, availability
- X.800 security architecture
- security attacks, services, mechanisms
- models for network (access) security