# Chapter 1

# Overview

# 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 – “the Internet”

# 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

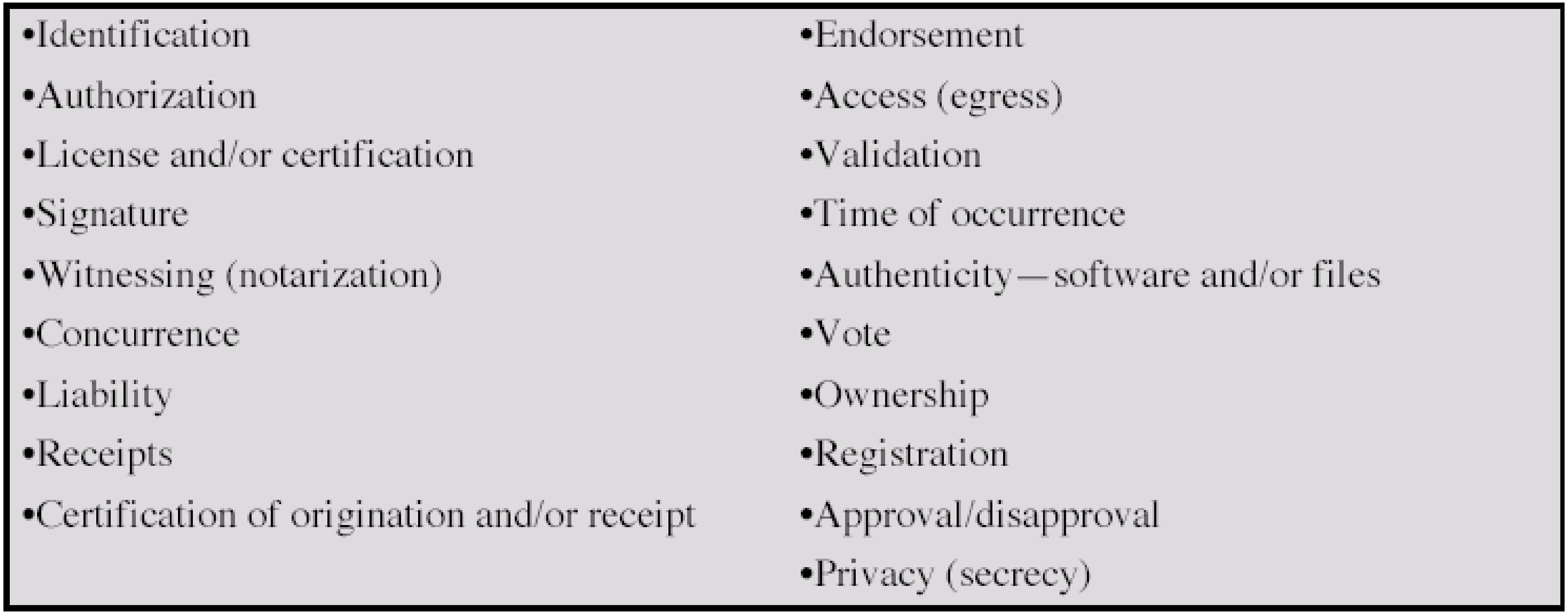
- need systematic way to define requirements
- consider three aspects of information security:
  - **security attack**
  - **security mechanism**
  - **security service**
- consider in reverse order

# Security Service

- is something that enhances the security of the data processing systems and the information transfers of an organization
- intended to counter security attacks
- make use of one or more security mechanisms to provide the service
- replicate functions normally associated with physical documents
  - eg. have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

# Information Integrity Functions

**Table 1.1 A Partial List of Common Information Integrity Functions [SIMM92]**



- Identification
- Authorization
- License and/or certification
- Signature
- Witnessing (notarization)
- Concurrence
- Liability
- Receipts
- Certification of origination and/or receipt
- Endorsement
- Access (egress)
- Validation
- Time of occurrence
- Authenticity—software and/or files
- Vote
- Ownership
- Registration
- Approval/disapproval
- Privacy (secrecy)

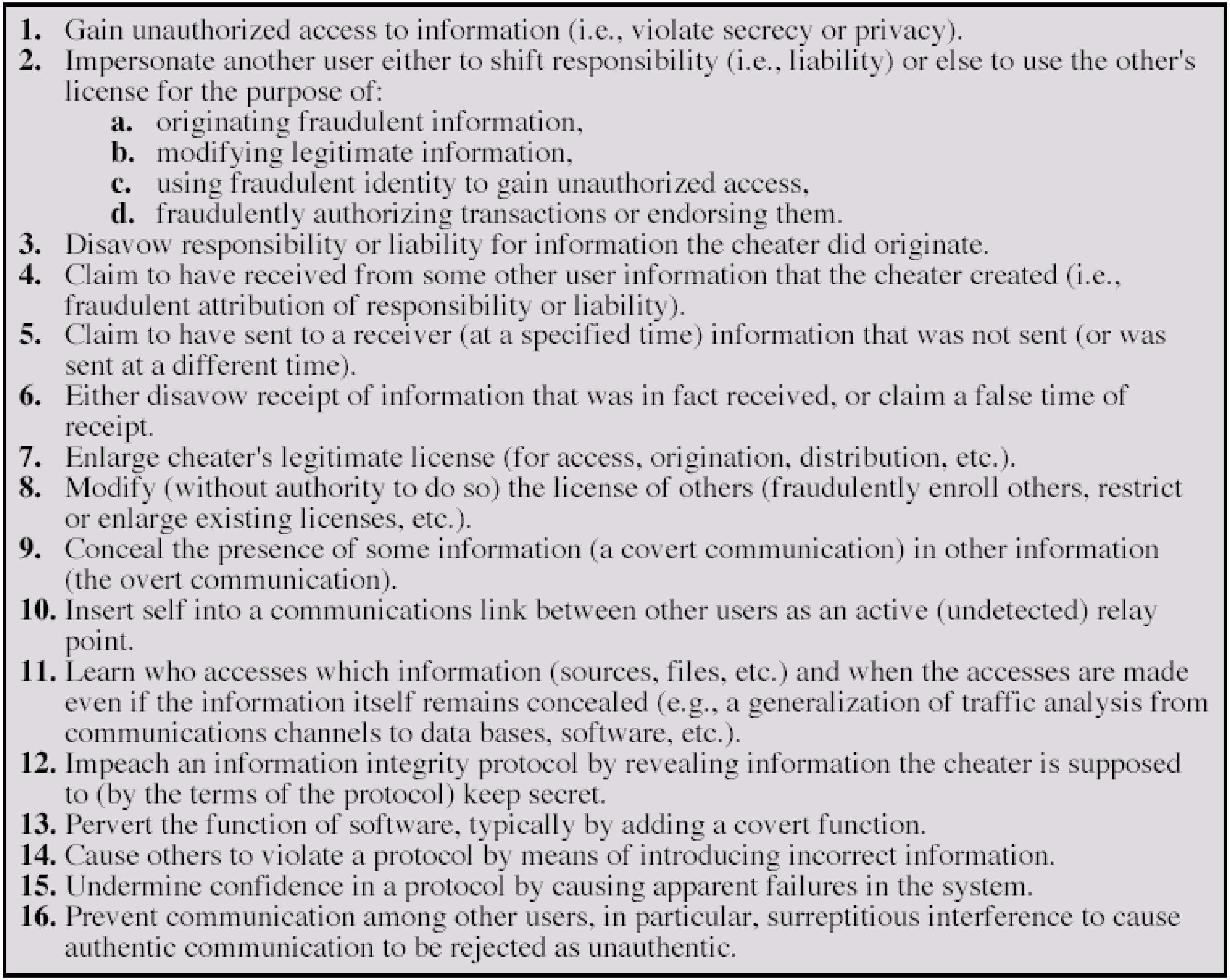
# Security Mechanism

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

# Security Attack

- any action that compromises the security of information owned by an organization
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- have a wide range of attacks
- can focus of generic types of attacks
- note: often *threat* & *attack* mean same

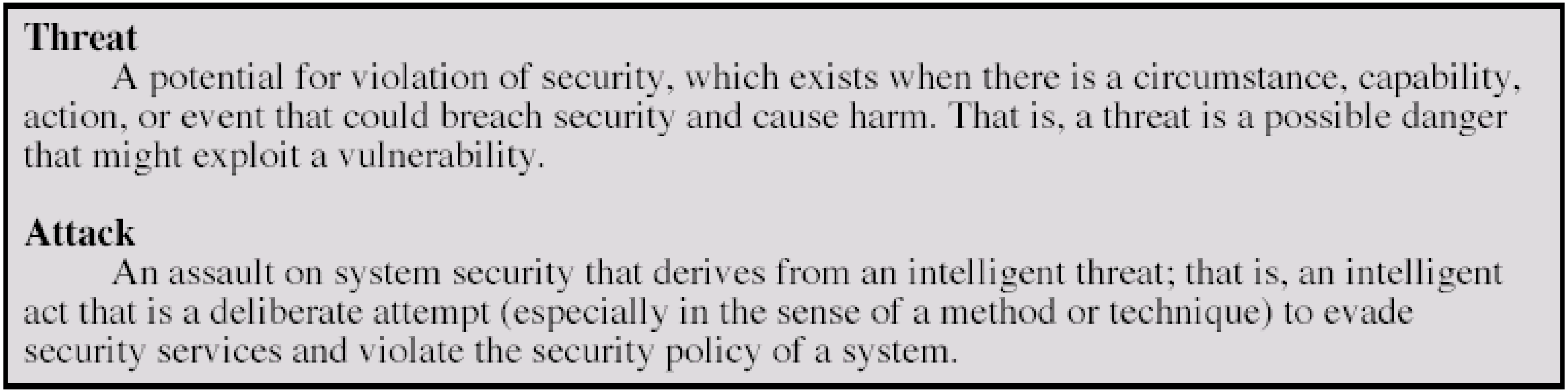
# Table 1.2 Examples of Security Attacks [SIMM92]



1. Gain unauthorized access to information (i.e., violate secrecy or privacy).
2. Impersonate another user either to shift responsibility (i.e., liability) or else to use the other's license for the purpose of:
   - a. originating fraudulent information,
   - b. modifying legitimate information,
   - c. using fraudulent identity to gain unauthorized access,
   - d. fraudulently authorizing transactions or endorsing them.
3. Disavow responsibility or liability for information the cheater did originate.
4. Claim to have received from some other user information that the cheater created (i.e., fraudulent attribution of responsibility or liability).
5. Claim to have sent to a receiver (at a specified time) information that was not sent (or was sent at a different time).
6. Either disavow receipt of information that was in fact received, or claim a false time of receipt.
7. Enlarge cheater's legitimate license (for access, origination, distribution, etc.).
8. Modify (without authority to do so) the license of others (fraudulently enroll others, restrict or enlarge existing licenses, etc.).
9. Conceal the presence of some information (a covert communication) in other information (the overt communication).
10. Insert self into a communications link between other users as an active (undetected) relay point.
11. Learn who accesses which information (sources, files, etc.) and when the accesses are made even if the information itself remains concealed (e.g., a generalization of traffic analysis from communications channels to data bases, software, etc.).
12. Impeach an information integrity protocol by revealing information the cheater is supposed to (by the terms of the protocol) keep secret.
13. Pervert the function of software, typically by adding a covert function.
14. Cause others to violate a protocol by means of introducing incorrect information.
15. Undermine confidence in a protocol by causing apparent failures in the system.
16. Prevent communication among other users, in particular, surreptitious interference to cause authentic communication to be rejected as unauthentic.

# Threats and Attacks

**Table 1.3 Threats and Attacks (RFC 2828)**



**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.

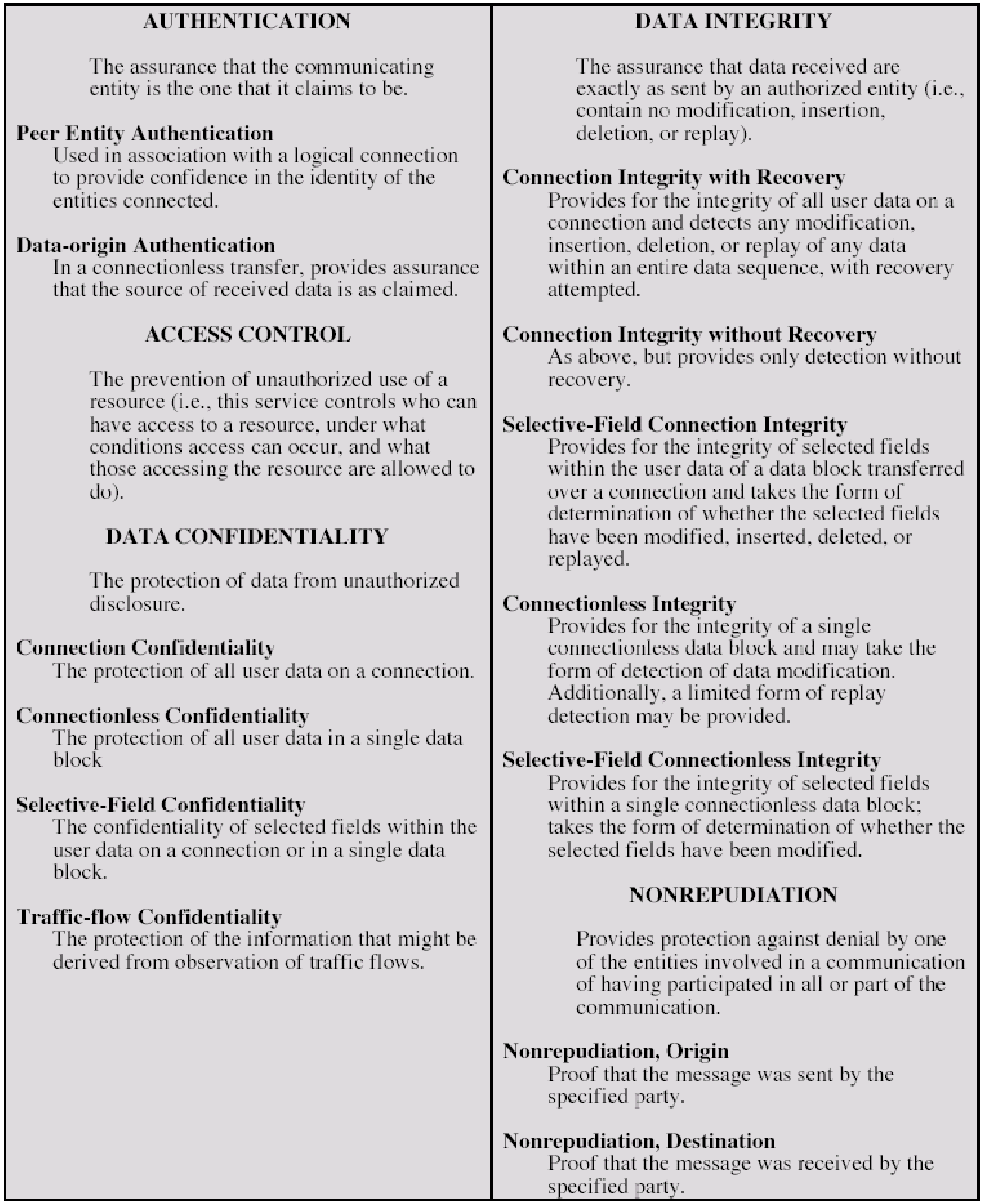
# OSI Security Architecture

- ITU-T X.800 Security Architecture for OSI
- systematically defines security requirements and characterises the approaches to satisfying those requirements
- for us it provides a useful, if abstract, overview of concepts we will study

# Security Services

- X.800 defines it as: a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers
- Internet Society RFC 2828 defines it as: a processing or communication service provided by a system to give a specific kind of protection to system resources
- X.800 defines it in 5 major categories

Table 1.4 Security Services (X.800)



### AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

**Peer Entity Authentication**
Used in association with a logical connection to provide confidence in the identity of the entities connected.

**Data-origin Authentication**
In a connectionless transfer, provides assurance that the source of received data is as claimed.

### ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

### DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

**Connection Confidentiality**
The protection of all user data on a connection.

**Connectionless Confidentiality**
The protection of all user data in a single data block

**Selective-Field Confidentiality**
The confidentiality of selected fields within the user data on a connection or in a single data block.

**Traffic-flow Confidentiality**
The protection of the information that might be derived from observation of traffic flows.

### DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

**Connection Integrity with Recovery**
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

**Connection Integrity without Recovery**
As above, but provides only detection without recovery.

**Selective-Field Connection Integrity**
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

**Connectionless Integrity**
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

**Selective-Field Connectionless Integrity**
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

### NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

**Nonrepudiation, Origin**
Proof that the message was sent by the specified party.

**Nonrepudiation, Destination**
Proof that the message was received by the specified party.

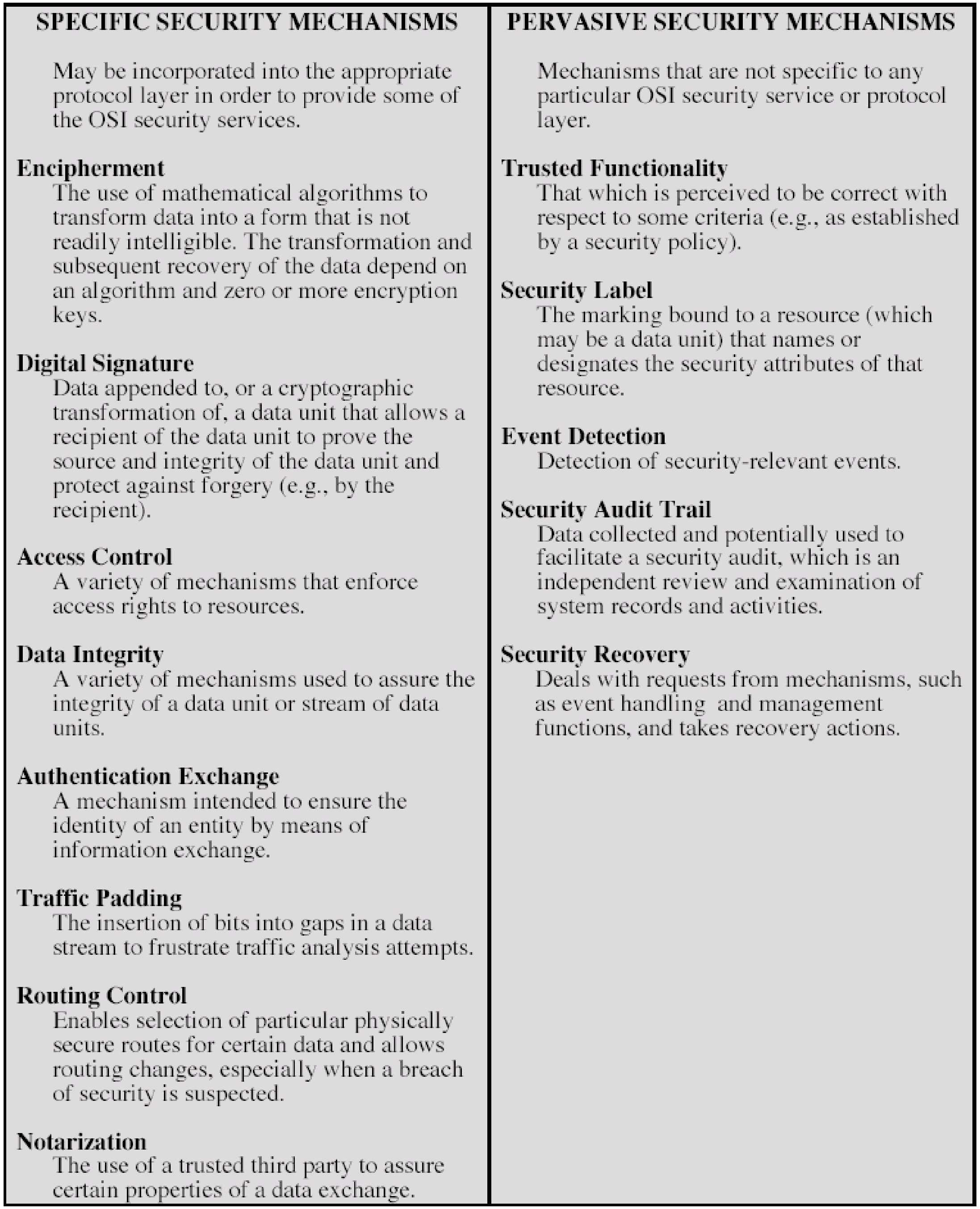
# Security Services (X.800)

- **Authentication -** assurance that the communicating entity is the one claimed
- **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 Service** – to ensure availability

# 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

## Table 1.5 Security Mechanisms (X.800)



| SPECIFIC SECURITY MECHANISMS | PERVASIVE SECURITY MECHANISMS |
|---|---|
| May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services. | Mechanisms that are not specific to any particular OSI security service or protocol layer. |
| **Encipherment**<br>The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys. | **Trusted Functionality**<br>That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy). |
| **Digital Signature**<br>Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient). | **Security Label**<br>The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource. |
| **Access Control**<br>A variety of mechanisms that enforce access rights to resources. | **Event Detection**<br>Detection of security-relevant events. |
| **Data Integrity**<br>A variety of mechanisms used to assure the integrity of a data unit or stream of data units. | **Security Audit Trail**<br>Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities. |
| **Authentication Exchange**<br>A mechanism intended to ensure the identity of an entity by means of information exchange. | **Security Recovery**<br>Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions. |
| **Traffic Padding**<br>The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts. | |
| **Routing Control**<br>Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected. | |
| **Notarization**<br>The use of a trusted third party to assure certain properties of a data exchange. | |

# Security Services and Mechanisms

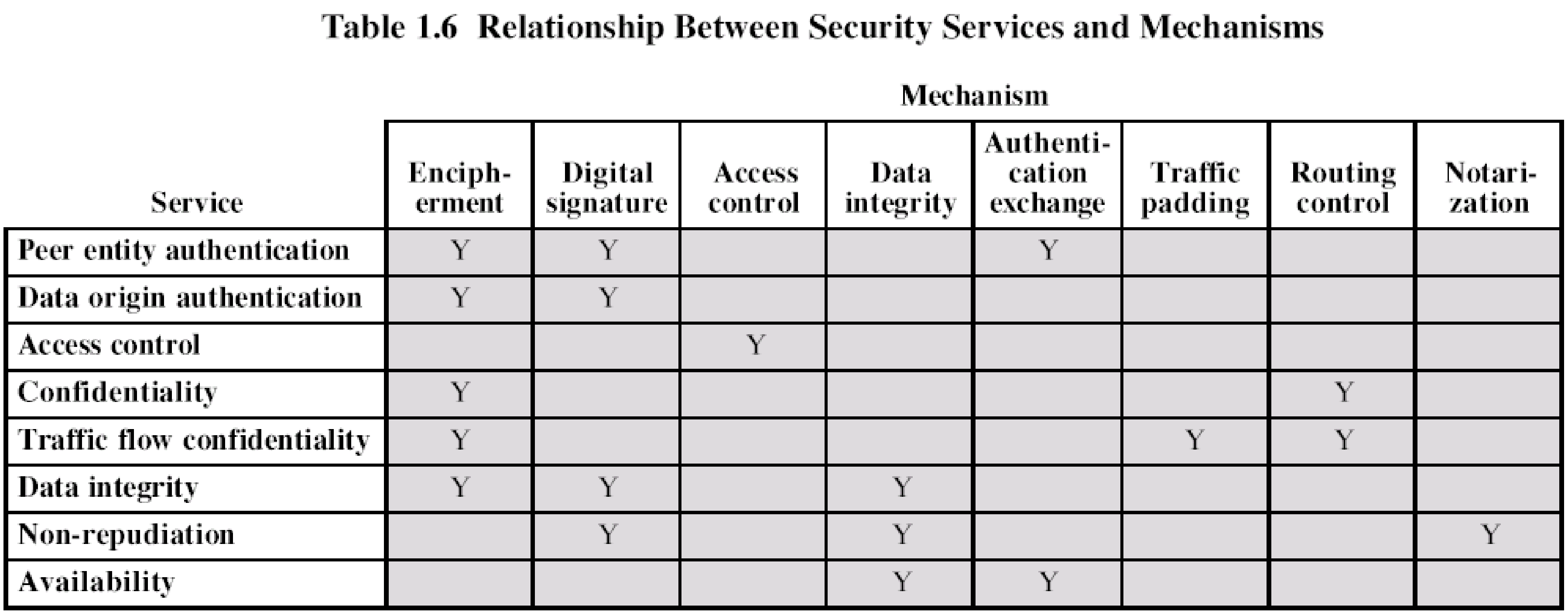


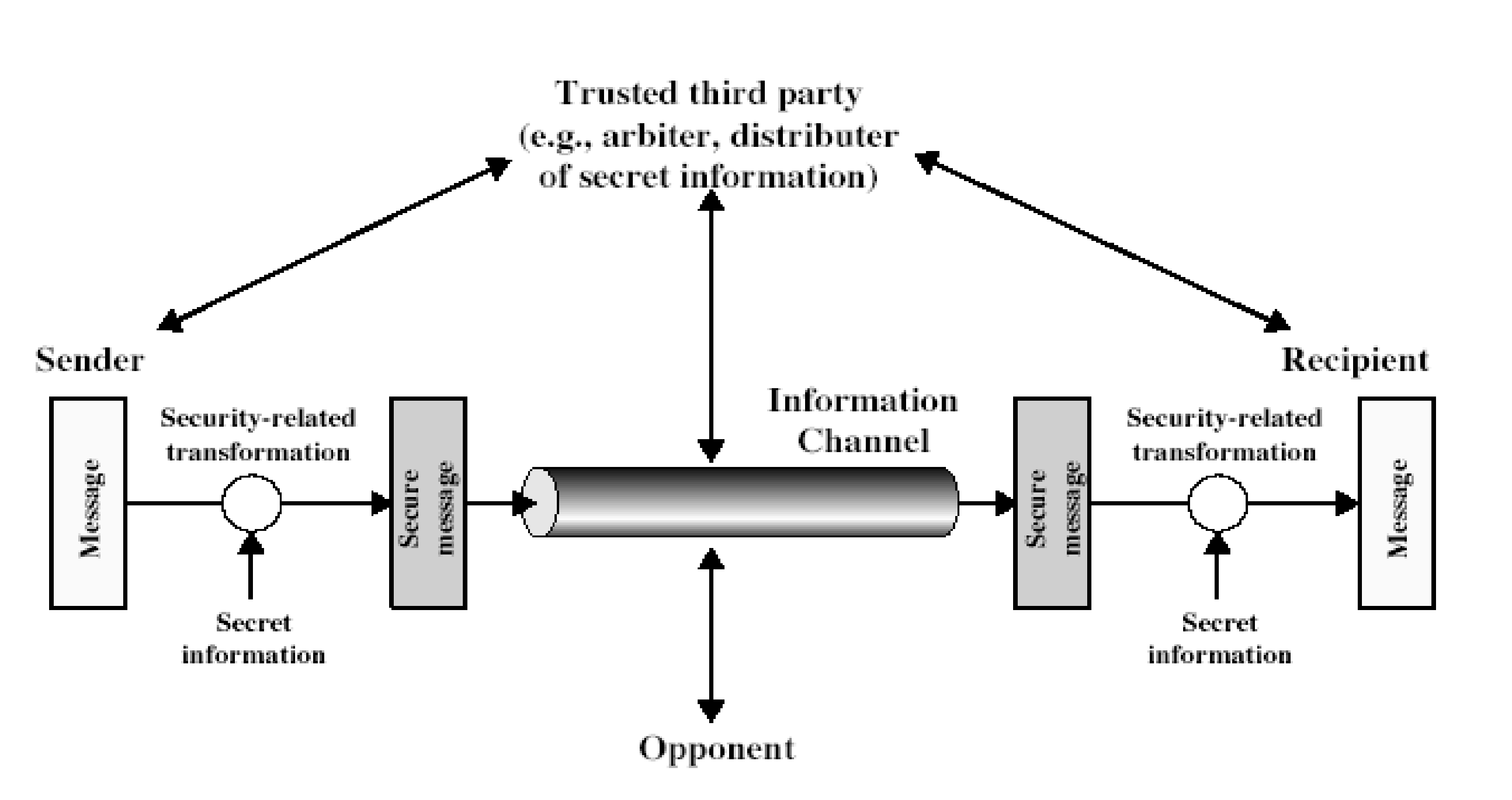
Table 1.6 Relationship Between Security Services and Mechanisms

| | 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 | | | | |
| Non-repudiation | | Y | | Y | | | | Y |
| Availability | | | | Y | Y | | | |

# 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

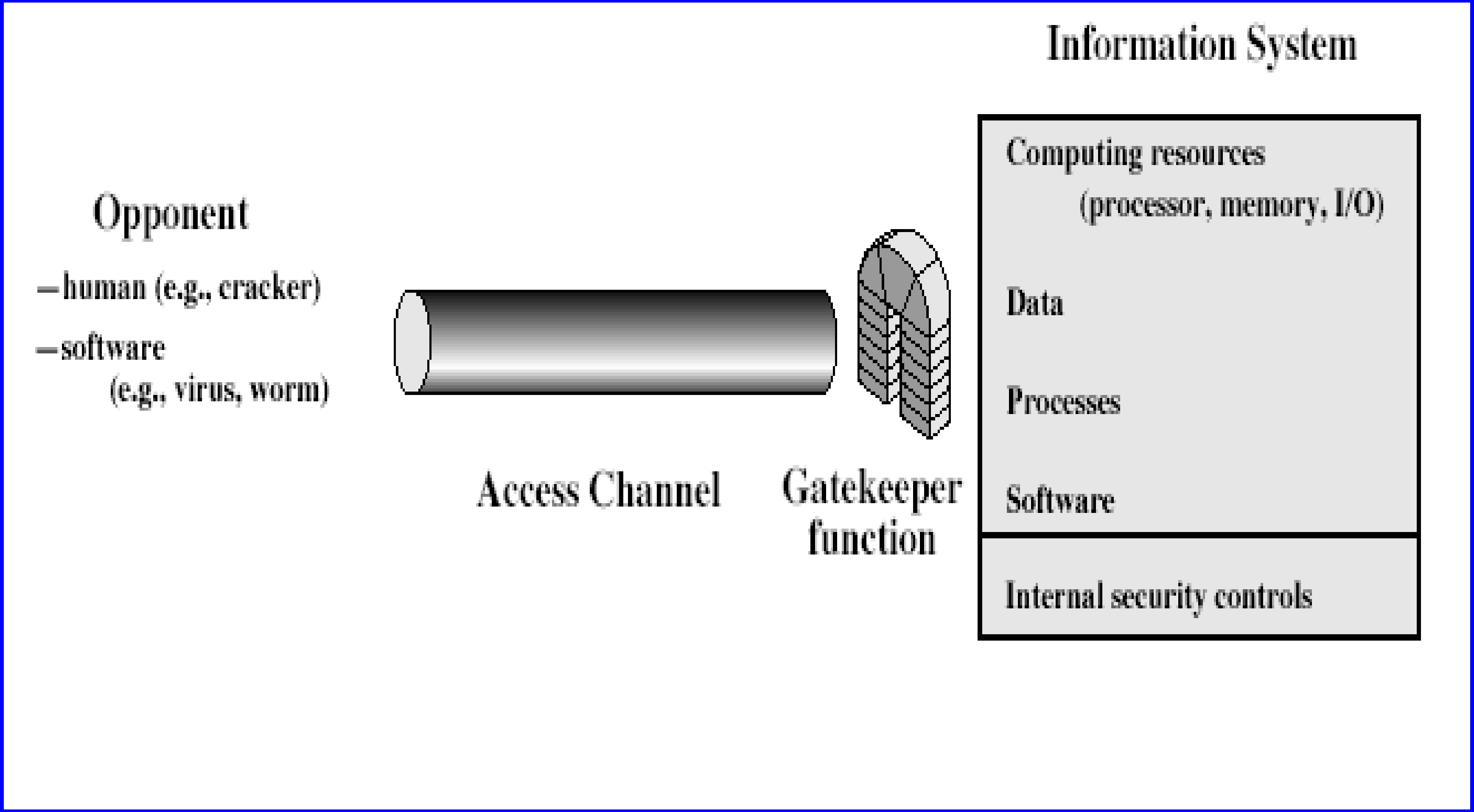
# Model for Network Security



# 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

# Model for Network Access Security



# Model for Network Access Security

- using this model requires us to:
  - select appropriate gatekeeper functions to identify users
  - implement security controls to monitor system activity and to detect intruders
- trusted computer systems can be used to implement this model

# Summary

- have considered:
  - computer, network, internet security def’s
  - security services, mechanisms, attacks
  - X.800 standard
  - models for network (access) security