



Chapter 1

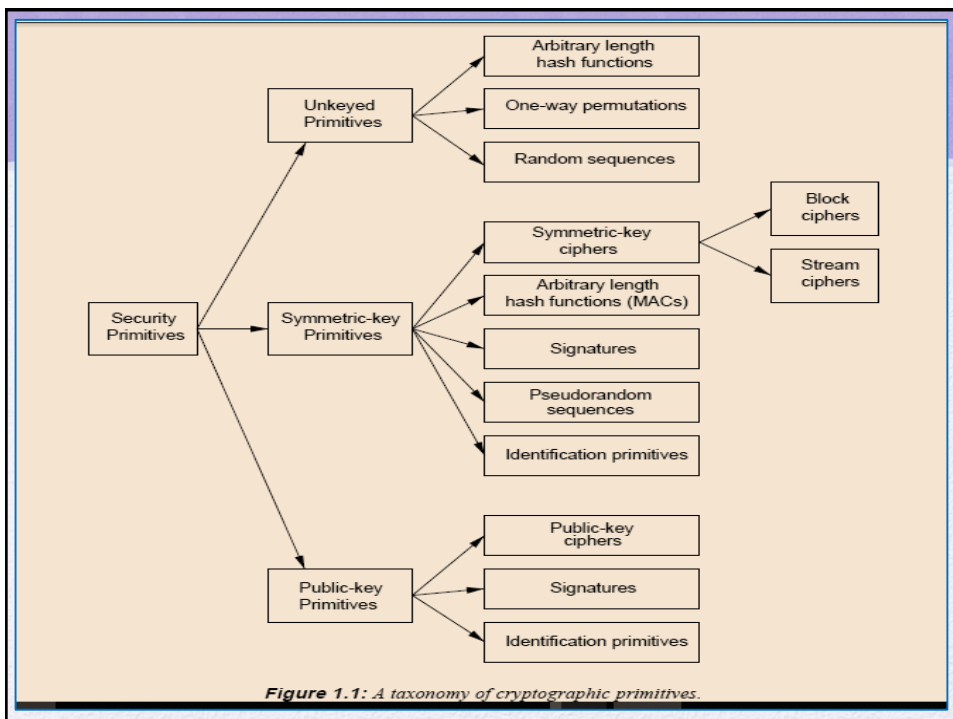
Overview

“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

| | |
|---|--|
| privacy or confidentiality | keeping information secret from all but those who are authorized to see it. |
| data integrity | ensuring information has not been altered by unauthorized or unknown means. |
| entity authentication or identification | corroboration of the identity of an entity (e.g., a person, a computer terminal, a credit card, etc.). |
| message authentication | corroborating the source of information; also known as data origin authentication. |
| signature | a means to bind information to an entity. |
| authorization | conveyance, to another entity, of official sanction to do or be something. |
| validation | a means to provide timeliness of authorization to use or manipulate information or resources. |
| access control | restricting access to resources to privileged entities. |
| certification | endorsement of information by a trusted entity. |
| timestamping | recording the time of creation or existence of information. |
| witnessing | verifying the creation or existence of information by an entity other than the creator. |
| receipt | acknowledgement that information has been received. |
| confirmation | acknowledgement that services have been provided. |
| ownership | a means to provide an entity with the legal right to use or transfer a resource to others. |
| anonymity | concealing the identity of an entity involved in some process. |
| non-repudiation | preventing the denial of previous commitments or actions. |
| revocation | retraction of certification or authorization. |



Cryptographic algorithms and protocols can be grouped into four main areas:

Symmetric encryption

- Used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords

Asymmetric encryption

- Used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures

Data integrity algorithms

- Used to protect blocks of data, such as messages, from alteration

Authentication protocols

- Schemes based on the use of cryptographic algorithms designed to authenticate the identity of entities

The field of network and Internet security consists of:



measures to deter, prevent, detect, and correct security violations that involve the transmission of information

Computer Security

- The NIST *Computer Security Handbook* defines the term computer security as:

“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)

Computer Security Objectives

Confidentiality

- Data confidentiality
 - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
 - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

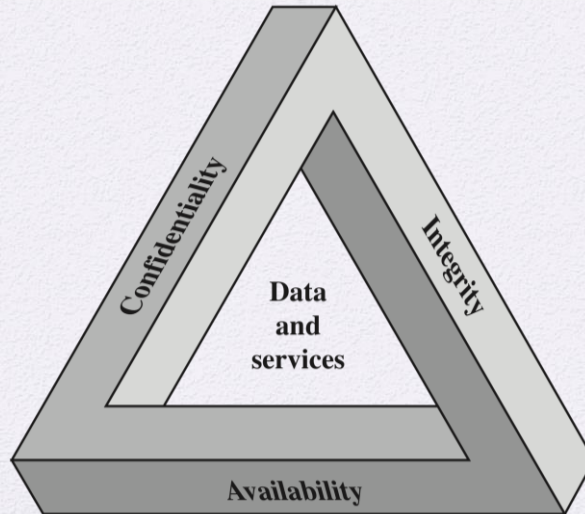
Integrity

- Data integrity
 - Assures that information and programs are changed only in a specified and authorized manner
- System integrity
 - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability

- Assures that systems work promptly and service is not denied to authorized users

CIA Triad



Possible additional concepts:

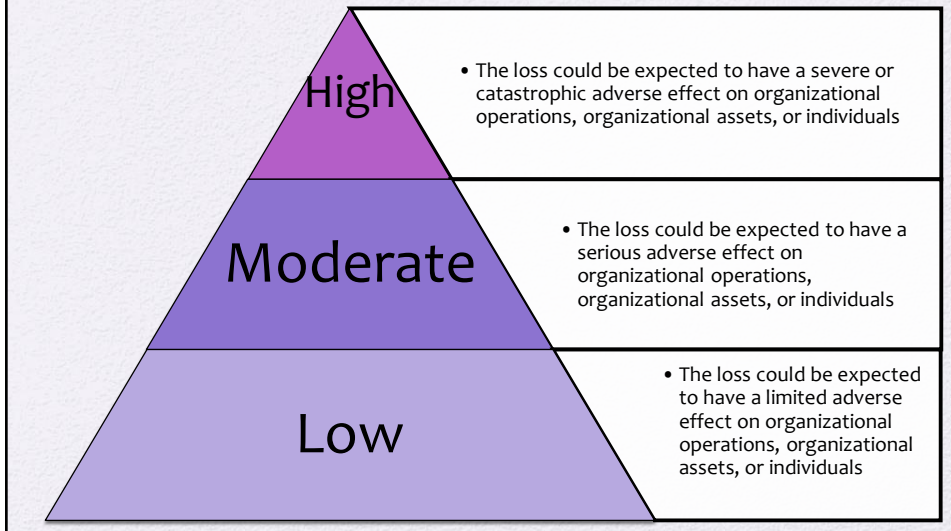
Authenticity

- Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity

Breach of Security Levels of Impact



Computer Security Challenges

- Security is not simple
- Potential attacks on the security features need to be considered
- Procedures used to provide particular services are often counter-intuitive
- It is necessary to decide where to use the various security mechanisms
- Requires constant monitoring
- Is too often an afterthought
- Security mechanisms typically involve more than a particular algorithm or protocol
- Security is essentially a battle of wits between a perpetrator and the designer
- Little benefit from security investment is perceived until a security failure occurs
- Strong security is often viewed as an impediment to efficient and user-friendly operation

OSI Security Architecture

- **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 processing or communication service that enhances the security of the data processing systems and the information transfers of an organization
 - Intended to counter security attacks, and they make use of one or more security mechanisms to provide the service

Table 1.1 Threats and Attacks (RFC 4949)



RFC= Reference For Comment 4949 = Internet Security Glossary

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.

Security Attacks

- A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of *passive attacks* and *active attacks*

- A *passive attack* attempts to learn or make use of information from the system but does not affect system resources

- An *active attack* attempts to alter system resources or affect their operation

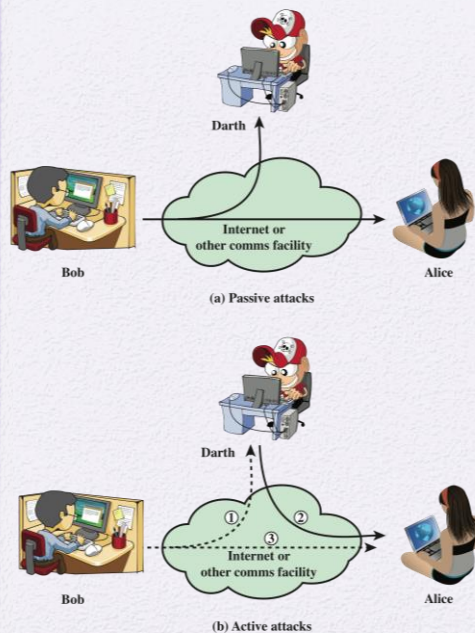


Figure 1.1 Security Attacks

Passive Attacks

- Are in the nature of eavesdropping on, or monitoring of, transmissions

- Goal of the opponent is to obtain information that is being transmitted



- **Two types of passive attacks are:**

- *The release of message contents*
- *Traffic analysis*

Active Attacks

- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them



Masquerade

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

Modification of messages

- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

Denial of service

- Prevents or inhibits the normal use or management of communications facilities

Security Services

- **Defined by X.800 as:**
 - A service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.
- **Defined by RFC 4949 as:**
 - A processing or communication service provided by a system to give a specific kind of protection to system resources

X.800 Service Categories

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Nonrepudiation



Authentication

- Concerned with assuring that a communication is authentic
 - In the case of a single message, assures the recipient that the message is from the source that it claims to be from
 - In the case of ongoing interaction, assures the two entities are authentic and that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties

Two specific authentication services are defined in X.800:

- Peer entity authentication
- Data origin authentication

Access Control

- The ability to limit and control the access to host systems and applications via communications links
- To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual



Data Confidentiality

- The protection of transmitted data from passive attacks
 - Broadest service protects all user data transmitted between two users over a period of time
 - Narrower forms of service includes the protection of a single message or even specific fields within a message
- The protection of traffic flow from analysis
 - This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility

Data Integrity



Can apply to a stream of messages, a single message, or selected fields within a message

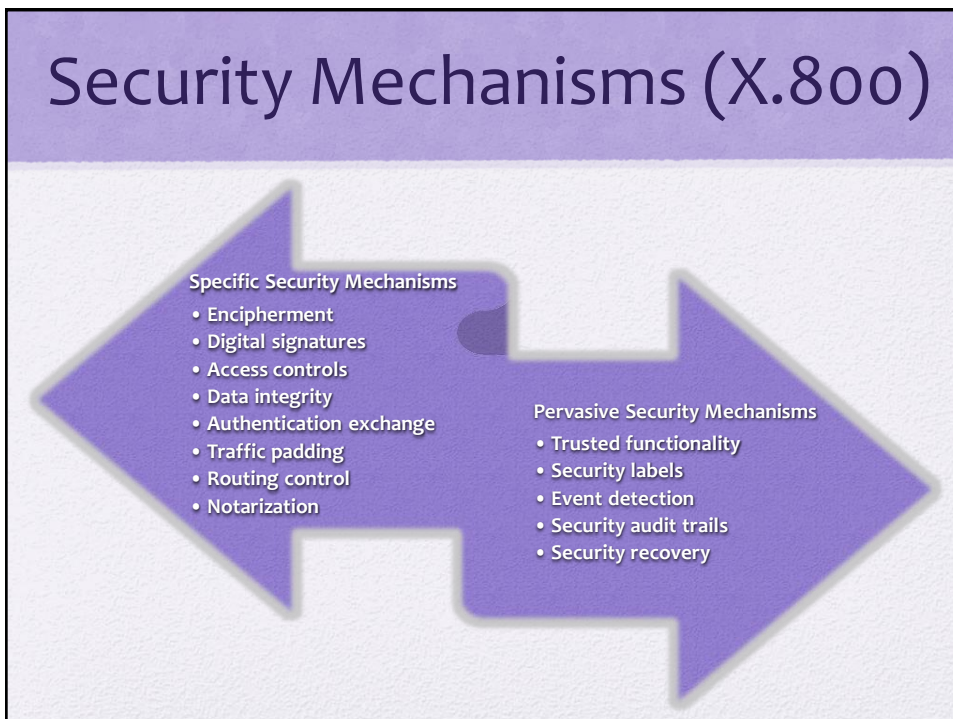
Connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays

A connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only

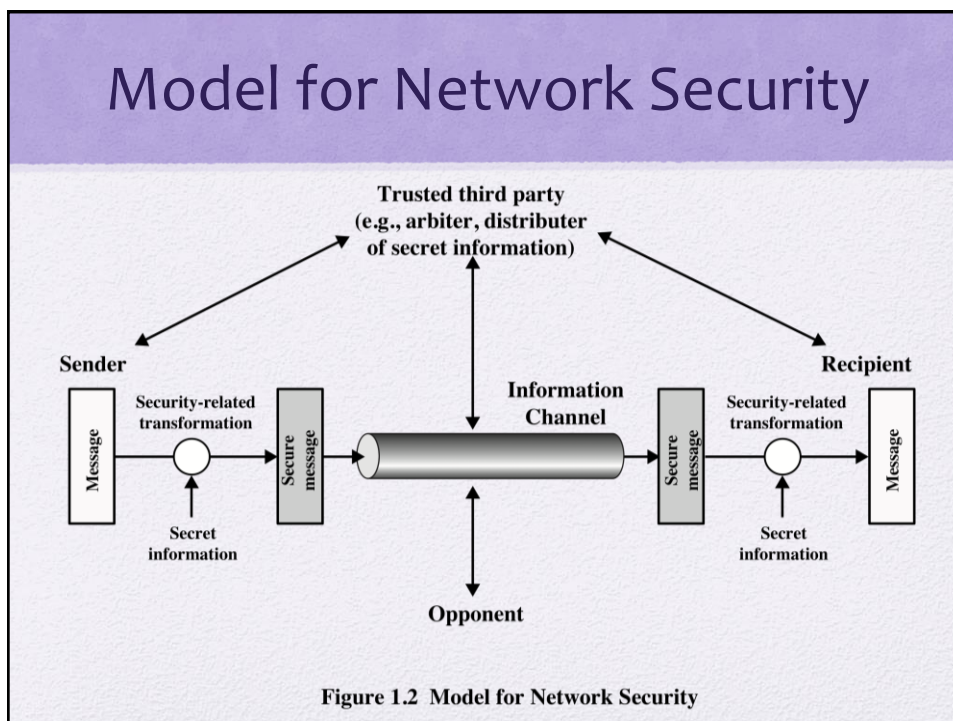
Nonrepudiation

- Prevents either sender or receiver from denying a transmitted message
- When a message is sent, the receiver can prove that the alleged sender in fact sent the message
- When a message is received, the sender can prove that the alleged receiver in fact received the message

| | | |
|--|---|---|
| <p>AUTHENTICATION</p> <p>The assurance that the communicating entity is the one that it claims to be.</p> <p>Peer Entity Authentication</p> <p>Used in association with a logical connection to provide confidence in the identity of the entities connected.</p> <p>Data-Origin Authentication</p> <p>In a connectionless transfer, provides assurance that the source of received data is as claimed.</p> <p>ACCESS CONTROL</p> <p>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).</p> <p>DATA CONFIDENTIALITY</p> <p>The protection of data from unauthorized disclosure.</p> <p>Connection Confidentiality</p> <p>The protection of all user data on a connection.</p> <p>Connectionless Confidentiality</p> <p>The protection of all user data in a single data block.</p> <p>Selective-Field Confidentiality</p> <p>The confidentiality of selected fields within the user data on a connection or in a single data block.</p> <p>Traffic-Flow Confidentiality</p> <p>The protection of the information that might be derived from observation of traffic flows.</p> | <p>DATA INTEGRITY</p> <p>The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).</p> <p>Connection Integrity with Recovery</p> <p>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.</p> <p>Connection Integrity without Recovery</p> <p>As above, but provides only detection without recovery.</p> <p>Selective-Field Connection Integrity</p> <p>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.</p> <p>Connectionless Integrity</p> <p>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.</p> <p>Selective-Field Connectionless Integrity</p> <p>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.</p> <p>NONREPUDIATION</p> <p>Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.</p> <p>Nonrepudiation, Origin</p> <p>Proof that the message was sent by the specified party.</p> <p>Nonrepudiation, Destination</p> <p>Proof that the message was received by the specified party.</p> | <p>Table 1.2</p> <p>Security Services (X.800)</p> <p>(This table is found on page 18 in textbook)</p> |
|--|---|---|



| SPECIFIC SECURITY MECHANISMS | PERVASIVE SECURITY MECHANISMS | <h1>Table 1.3</h1> <h2>Security Mechanisms (X.800)</h2> <p>(This table is found on pages 20-21 in textbook)</p> |
|---|--|---|
| <p>May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.</p> <p>Encipherment 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.</p> <p>Digital Signature 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).</p> <p>Access Control A variety of mechanisms that enforce access rights to resources.</p> <p>Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.</p> <p>Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.</p> <p>Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.</p> <p>Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.</p> <p>Notarization The use of a trusted third party to assure certain properties of a data exchange.</p> | <p>Mechanisms that are not specific to any particular OSI security service or protocol layer.</p> <p>Trusted Functionality That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).</p> <p>Security Label The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.</p> <p>Event Detection Detection of security-relevant events.</p> <p>Security Audit Trail Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.</p> <p>Security Recovery Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.</p> | |



Network Access Security Model

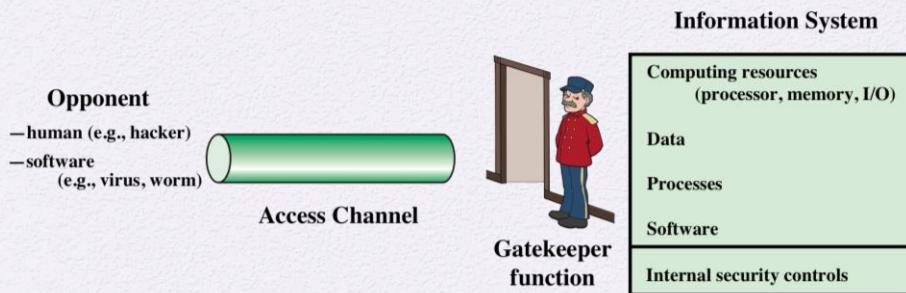


Figure 1.3 Network Access Security Model

Unwanted Access

- Placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs such as editors and compilers
- Programs can present two kinds of threats:
 - 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



Summary

- Computer security concepts
 - Definition
 - Examples
 - Challenges
- The OSI security architecture
- Security attacks
 - Passive attacks
 - Active attacks
- Security services
 - Authentication
 - Access control
 - Data confidentiality
 - Data integrity
 - Nonrepudiation
 - Availability service
- Security mechanisms

