Ransomware

- In recent years, ransomware has quickly become one of the most prevalent types of malware.
- The most common malware variants encrypt a system or specific files, pausing any work from being done until the victim pays a ransom to the attacker.
- Other forms of ransomware threaten to publicize sensitive information within the encrypted data.
- Ransomware is a form of malware that **encrypts a victim's files**. It is used by cybercriminals
- The attacker then demands a ransom from the victim to restore access to the data upon payment.
- Users are shown instructions for how to pay a fee to get the decryption key.

Ransomware

- Ransomware uses asymmetric encryption.
- It uses a pair of keys to encrypt and decrypt a file. The public-private pair of keys is uniquely generated by the attacker for the victim, with the private key to decrypt the files stored on the attacker's server.
- The attacker makes the private key available to the victim only after the ransom is paid, but that is not always the case.
- Without access to the private key, it is nearly impossible to decrypt the files that are being held for ransom.
- The WannaCry ransomware attack was a worldwide cyberattack in May 2017 by the WannaCry ransomware cryptoworm.
- which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.

Ransomware Cont..

- If a computer or network has been infected with ransomware, the ransomware **blocks access** to the system or **encrypts** its **data**.
- Cybercriminals demand **ransom money** from their victims in exchange for releasing the data.
- In order to protect **against ransomware infection**, a watchful eye and security software are recommended.
- Victims of malware attacks have three options **after an infection**: they can either **pay the ransom**, try to **remove the malware**, or **restart the device**.
- **Attack vectors** frequently used by extortion Trojans include the **Remote Desktop Protocol**, **phishing emails**, and **software vulnerabilities**.
- A ransomware attack can therefore target both **individuals** and **companies**.

Defend Against Ransomware

- Often organizations can mitigate ransomware attacks by having up-to-date backups.
- If their files become locked, they can simply wipe the system and reboot from an offline backup.
- Organizations should train users about the threat, patch their software as necessary and install all the usual security solutions.

Examples Of Ransomware Malware Attacks

- With vendors and organizations increasingly moving online, more data is at risk of exposure.
- Attackers know this and often take advantage of small to mid-sized organizations with weaker network security, requesting an amount they know the organization can afford.
- Notable examples from the 2010s included CryptoLocker, Locky, WannaCry, Hermes, GandCrab, and Ryuk.

Phishing

- **Phishing** is a type of deception designed to steal valuable personal data, such as credit card numbers, passwords, account data, or other information.
- Phishing is a type of email attack that attempts to trick users into divulging passwords, downloading an attachment or visiting a website that installs malware on their systems.
- More targeted efforts at specific users or organizations are known as spear phishing. Because the goal is to trick the user, attackers will research the victim to maximize trick potential, often using spoofing to make the email seem legit.
- Millions of fraudulent e-mail messages that appear to come from Web sites you trust, like your bank or credit card company, and request that you provide personal information.

Phishing Cont..

- As scam artists become more sophisticated, so do their phishing e-mail messages and pop-up windows.
- They often include official-looking logos from real organizations and other identifying information taken directly from legitimate Web sites.
- Phishing attacks are the **practice of sending fraudulent communications that appear to come from a reputable source**.
- It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

Defend Against Phishing

- Because phishing relies on social engineering — tricking users into doing something — employee training is one of the best defences against these attacks.
- Users should deploy anti-spam and anti-malware solutions, and staff should know not to divulge personal information or passwords in email messages.
- Training about downloading attachments or clicking website links in messages, even if they appear to come from a known source, is imperative given phishing attackers often pretend to be a company or person known to the victim.

Phishing Malware Attacks

- **Deceptive Phishing-**Most common type, using an email headline with a sense of urgency from a known contact. This attack blends legitimate links with malicious code, modifies brand logos, and evades detection with minimal content.
- **Spear Phishing-** Spear phishing targets specific users or organizations by exploring social media, recording out-of-office notifications, compromising API tokens, and housing malicious data in the cloud.
- **Whaling**-Even more targeted than spear phishing, whaling targets chief officers of an organization by infiltrating the network, exposing the supply chain, and following up the malicious email with a phone call to give it legitimacy.

Phishing Malware Attacks

- **Vishing**- Targeting victims over the phone, vishing is the use of Voice over Internet Protocol (VoIP), technical jargon, and ID spoofing to trick a caller into revealing sensitive information.
- **Smishing**-Smishing also targets phone users, but this one comes in the form of malicious text messages. Smishing attacks often include triggering the download of a malicious app, link to data-stealing forms, and faux tech support.
- **Pharming-**Moving away from trying to trick users, pharming leverages cache poisoning against the DNS, using malicious email code to target the server and compromise web users’ URL requests.

DoS attack

- A Denial-of-Service (DoS) attack is **an attack meant to shut down a machine or network, making it inaccessible to its intended users**.
- DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.
- A denial-of-service (DoS) attack is a malicious attempt to overwhelm a web property with traffic in order to disrupt its normal operations.
- DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users.
- A DoS attack is characterized by using a single computer to launch the attack.

DoS attack

- The primary focus of a DoS attack is to oversaturate the capacity of a targeted machine, resulting in denial-of-service to additional requests.
- The multiple attack vectors of DoS attacks can be grouped by their similarities.
- DoS attacks typically exploited security vulnerabilities present in network, software and hardware design.
- These attacks have become less prevalent as DDoS attacks have a greater disruptive capability and are relatively easy to create given the available tools.
- In reality, most DoS attacks can also be turned into DDoS attacks.
- DoS attacks fall in 2 categories:
  - **Buffer overflow attacks**
  - **Flood attacks**

Buffer overflow attacks

- An attack type in which a memory buffer overflow can cause a machine to consume all available hard disk space, memory, or CPU time.
- This form of exploit often results in sluggish behavior, system crashes, or other deleterious server behaviors, resulting in denial-of-service.

Flood attacks

- By saturating a targeted server with an overwhelming amount of packets, a malicious actor is able to oversaturate server capacity, resulting in denial-of-service.
- In order for most DoS flood attacks to be successful, the malicious actor must have more available bandwidth than the target.

DoS Attacks

- **Smurf attack** - a previously exploited DoS attack in which a malicious actor utilizes the broadcast address of vulnerable network by sending spoofed packets, resulting in the flooding of a targeted IP address.
- **Ping flood** - this simple denial-of-service attack is based on overwhelming a target with ICMP (ping) packets. By inundating a target with more pings than it is able to respond to efficiently, denial-of-service can occur. This attack can also be used as a DDoS attack.
- **Ping of Death** - often conflated with a ping flood attack, a ping of death attack involves sending a malformed packet to a targeted machine, resulting in deleterious behavior such as system crashes.

OSI Security Architecture

- OSI-Open System Interconnection
- The International Telecommunication Union-Telecommunication Standardization Sector (ITU-T)
- To assess effectively the security needs of an organization and to evaluate and choose various security products and policies, the manager responsible for security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements.
- This is difficult enough in a centralized data processing environment; with the use of local and wide area networks, the problems are compounded.

OSI Security Architecture

- The OSI security architecture focuses on security attacks, mechanisms, and services.
- **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. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

OSI Security Architecture

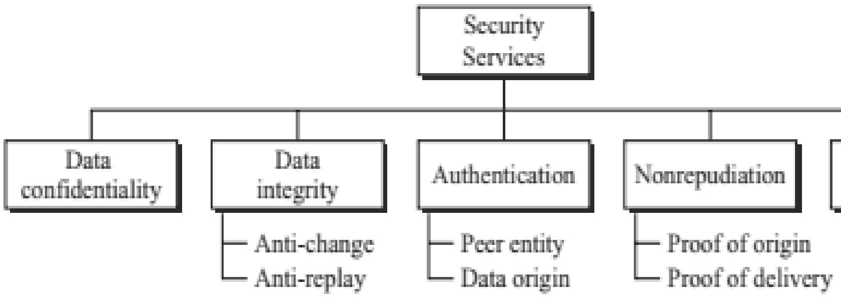
- Following provides definitions taken from RFC 4949(Request for Comments), *Internet Security Glossary*
- **Threat -** A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible 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 Services and Mechanisms

- The International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) provides some security services mechanisms to implement those services.
- Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service.
- A mechanism can be used in one or more services.

Security Services

Figure 1.3 *Security services*



Security Services Cont..

- It is easy to relate one or more of these services to one or more of the security goals. It has been designed to prevent the security attacks
- **Data Confidentiality**
  - Data confidentiality is designed to protect data from disclosure attack.
  - The service as defined by X.800 is very broad and encompasses confidentiality of the whole message or part of a message and also protection against traffic analysis.
  - It is designed to prevent snooping and traffic analysis attack.

Security Services Cont..

- **Data Integrity**
  - Data integrity is designed to protect data from modification, insertion, deletion, and replaying by an adversary.
  - It may protect the whole message or part of the message.
- **Authentication**
  - This service provides the authentication of the party at the other end of the line.
  - In connection-oriented communication, it provides authentication of the sender or receiver during the connection establishment (peer entity authentication).
  - In connectionless communication, it authenticates the source of the data (data origin authentication).

Security Services Cont..

- **Nonrepudiation**
  - Nonrepudiation service protects against repudiation by either the sender or the receiver of the data.
  - In nonrepudiation with proof of the origin, the receiver of the data can later prove the identity of the sender if denied.
  - In nonrepudiation with proof of delivery, the sender of data can later prove that data were delivered to the intended recipient.
- **Access Control**
  - Access control provides protection against unauthorized access to data.
  - The term access in this definition is very broad and can involve reading, writing, modifying, executing programs, and so on.

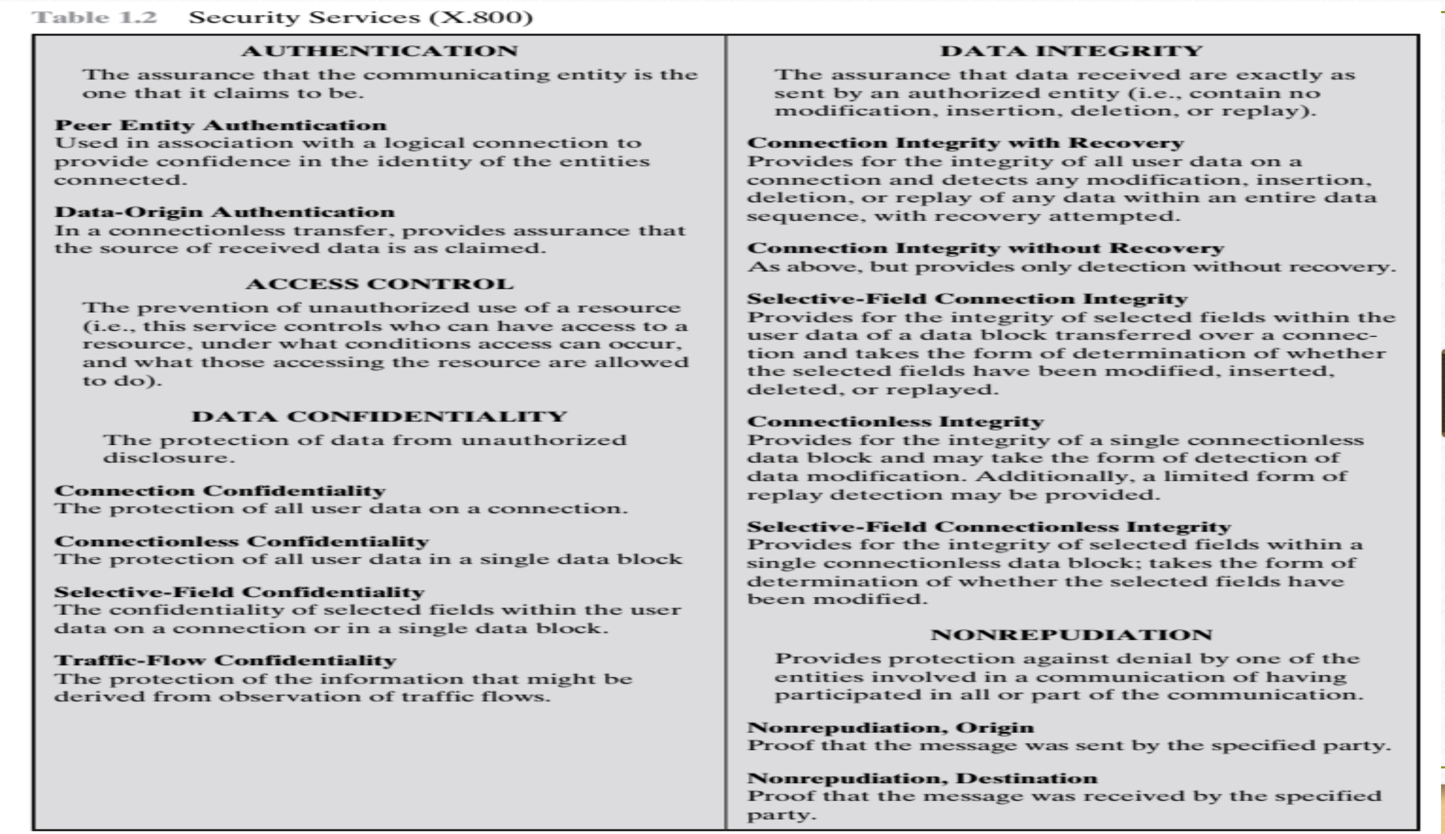


Table 1.2 Security Services (X.800)

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 Mechanisms

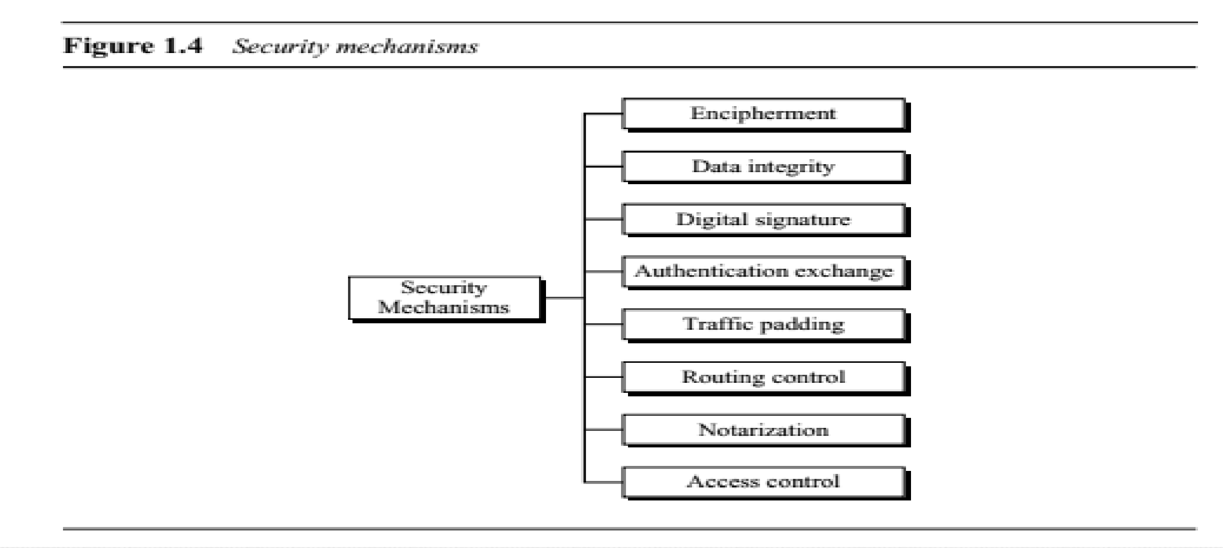


Figure 1.4 *Security mechanisms*

Security Mechanisms

- Encipherment
- Data integrity
- Digital signature
- Authentication exchange
- Traffic padding
- Routing control
- Notarization
- Access control

Security Mechanisms Cont..

- **Encipherment**
  - Encipherment, hiding or covering data, can provide confidentiality.
  - It can also be used to complement other mechanisms to provide other services.
  - Cryptography and steganography are used for enciphering.
- **Data Integrity**
  - The data integrity mechanism appends to the data a short checkvalue that has been created by a specific process from the data itself.
  - The receiver receives the data and the checkvalue.
  - He creates a new checkvalue from the received data and compares the newly created checkvalue with the one received. If the two checkvalues are the same, the integrity of data has been preserved.

Security Mechanisms Cont..

- **Digital Signature**
  - A digital signature is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature.
  - The sender uses a process that involves showing that she owns a private key related to the public key that she has announced publicly.
  - The receiver uses the sender's public key to prove that the message is indeed signed by the sender who claims to have sent the message.
- **Authentication Exchange**
  - In authentication exchange, two entities exchange some messages to prove their identity to each other. For example, one entity can prove that she knows a secret that only she is supposed to know.

Security Mechanisms Cont..

- **Traffic Padding**
  - Traffic padding means inserting some bogus data into the data traffic to thwart the adversary’s attempt to use the traffic analysis.
- **Routing Control**
  - Routing control means selecting and continuously changing different available routes between the sender and the receiver to prevent the opponent from eavesdropping on a particular route.
- **Access Control**
  - Access control uses methods to prove that a user has access right to the data or resources owned by a system. Examples of proofs are passwords and PINs.

Security Mechanisms Cont..

- **Notarization**
  - Notarization means selecting a third trusted party to control the communication between two entities. This can be done to prevent repudiation.
  - The receiver can involve a trusted party to store the sender request in order to prevent the sender from later denying that she has made such a request.
  - This security mechanism involves **use of trusted third party in communication**. It acts as mediator between sender and receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.

Security Services and Mechanisms

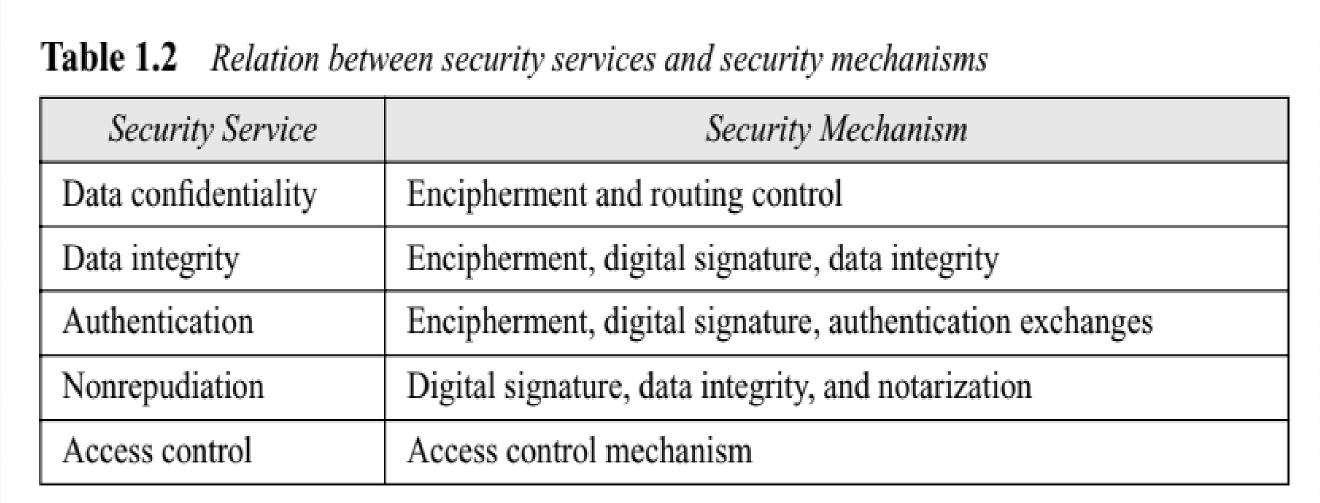


Table 1.2 *Relation between security services and security mechanisms*

Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

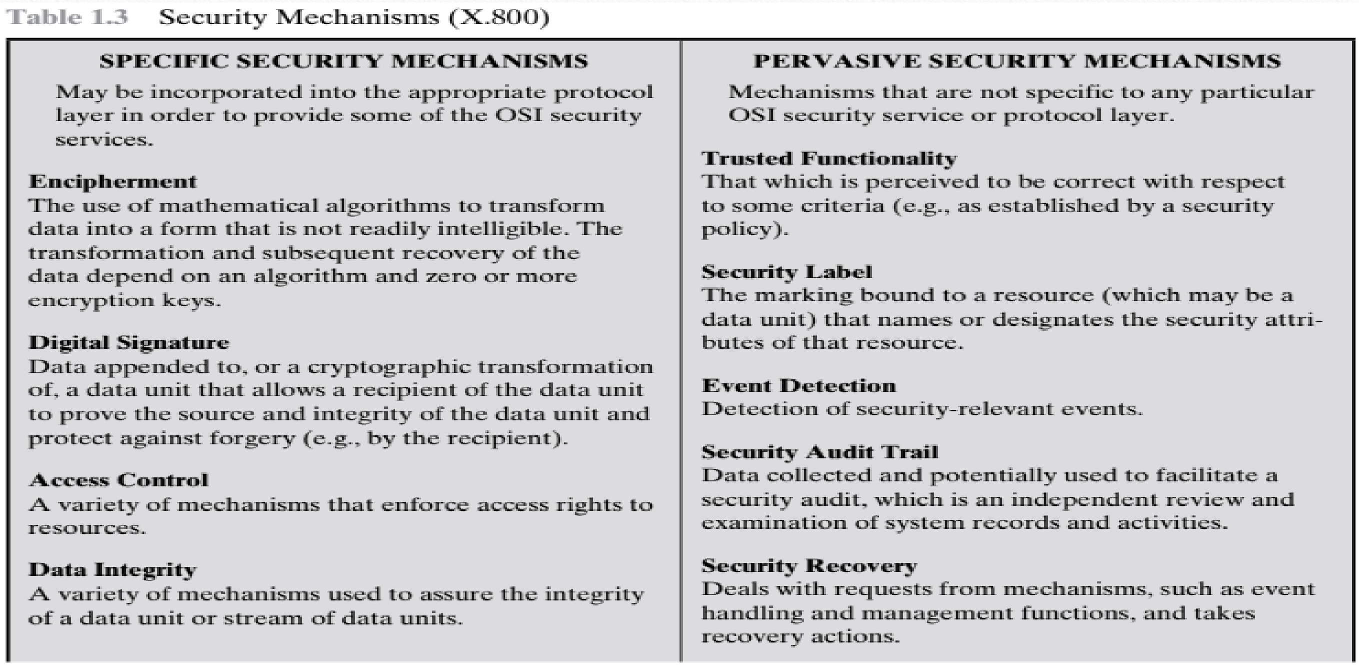


Table 1.3 Security Mechanisms (X.800)

SPECIFIC SECURITY MECHANISMS

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

Encipherment
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.

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).

Access Control
A variety of mechanisms that enforce access rights to resources.

Data Integrity
A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

PERVASIVE SECURITY MECHANISMS

Mechanisms that are not specific to any particular OSI security service or protocol layer.

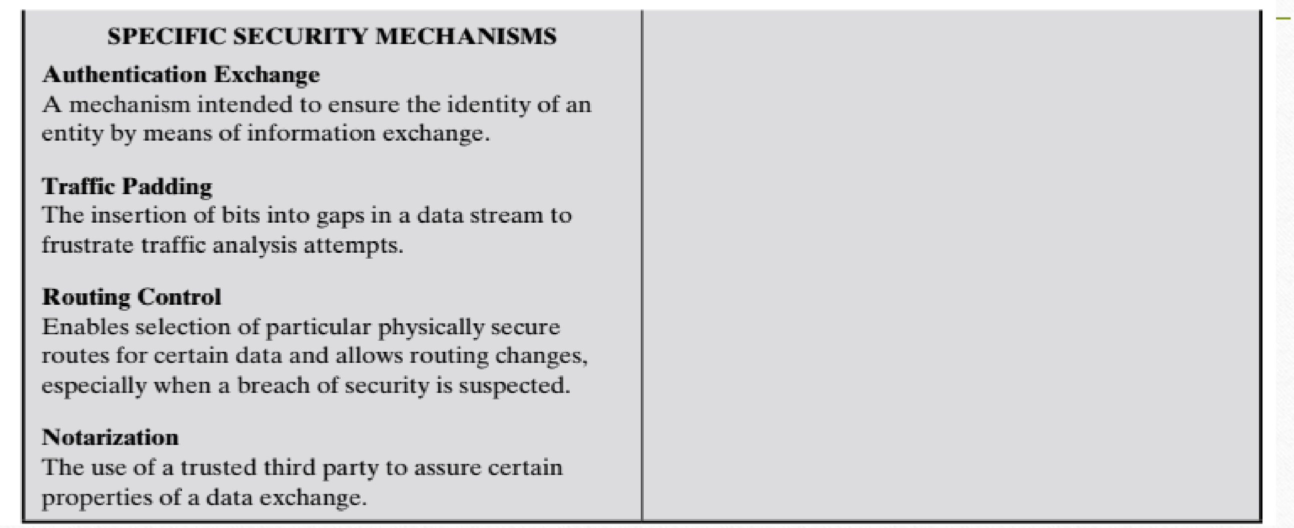
Trusted Functionality
That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

Security Label
The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Event Detection
Detection of security-relevant events.

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.

Security Recovery
Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.



SPECIFIC SECURITY MECHANISMS

Authentication Exchange
A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic Padding
The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Routing Control
Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

Notarization
The use of a trusted third party to assure certain properties of a data exchange.

Network Security Model

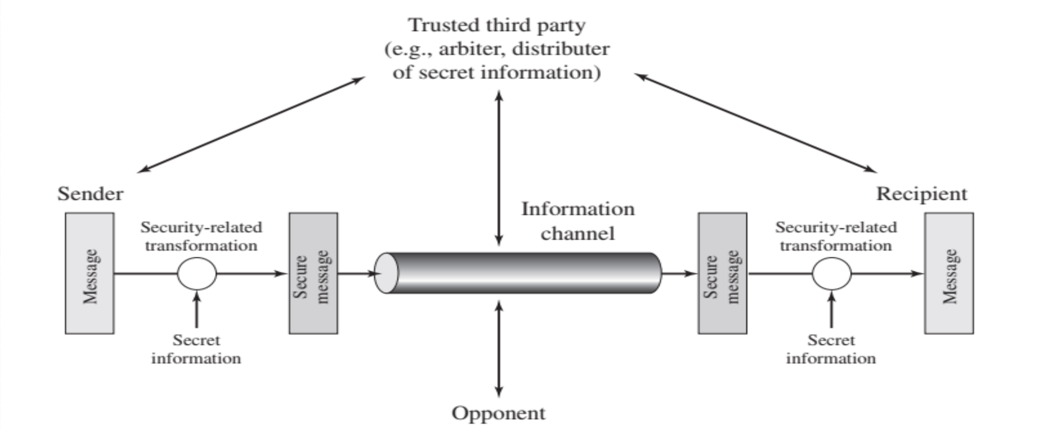


Figure 1.2 Model for Network Security

Network Security Model

- There are four basic tasks in designing a particular security service:
  - Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
  - Generate the secret information to be used with the algorithm.
  - Develop methods for the distribution and sharing of the secret information.
  - 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.