OSI Security Architecture

B Tech CSE- IV Sem

TCS 491

Introduction to Cryptography

Jan- Jun 2022

THE OSI SECURITY ARCHITECTURE

ITU-T[3] Recommendation X.800, Security Architecture for OSI, defines a systematic approach to assess effectively the security needs of an organization and to evaluate and choose various security products and policies…

The OSI security architecture focuses on security attacks, mechanisms, and services:

- These can be defined briefly as:
- 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.

NOTE: In the literature, the terms threat and attack are commonly used to mean more or less the same thing.

- But here we provide definitions taken from RFC 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

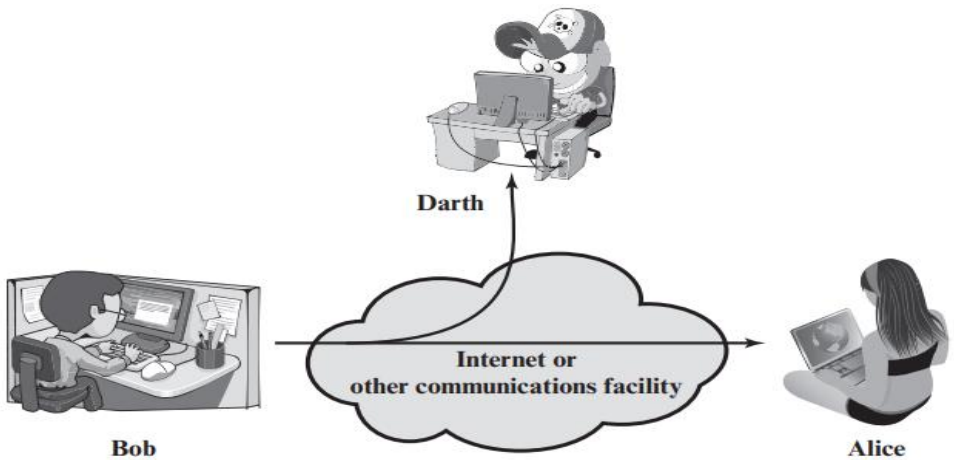
- A useful means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of passive attacks and active attacks.

Passive Attacks: A passive attack attempts to learn or make use of information from the system but does not affect system resources

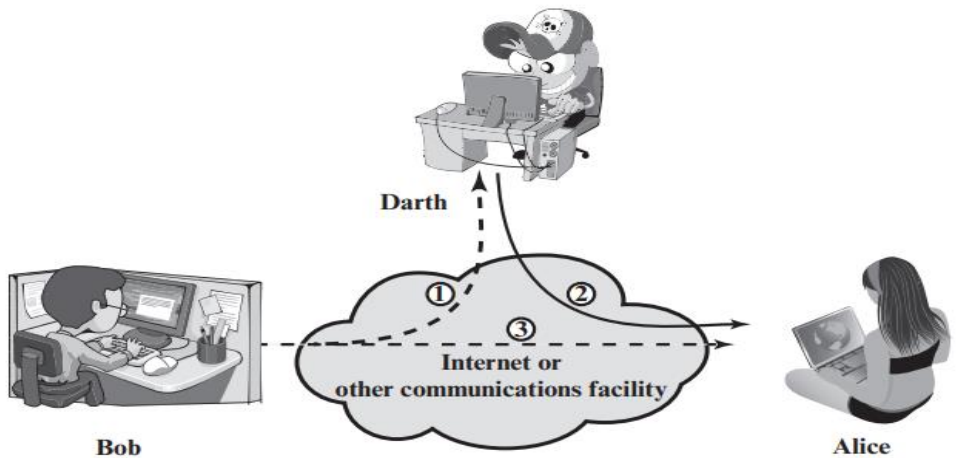
- Passive attacks are in the nature of eavesdropping on transmissions, or monitoring of transmissions. The goal of the opponent is to obtain information that is being transmitted.
- Two types of passive attacks are the release of message contents and traffic analysis.
- The release of message contents is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.
- A second type of passive attack, traffic analysis, is subtler. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.
- 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: 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
- Replay
- Modification of messages, and
- Denial of service.
- A masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.
- Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (paths 1 and 2 active). For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."
- The denial of service prevents or inhibits the normal use or management of communications facilities (path 3 active). This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.
- Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely because of the wide variety of potential physical, software, and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them. If the detection has a deterrent effect, it may also contribute to prevention.



(a) Passive attacks



(b) Active attacks

SECURITY SERVICES

- X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers. Perhaps a clearer definition is found in RFC 4949, which provides the following definition: a processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.
- X.800 divides these services into five categories and fourteen specific services (Table 1.2). We look at each category in turn.5

X.800 divides these services into five categories and fourteen specific services as shown below:

- CATEGORY 1:
- 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.

- CATEGORY 2:
- 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).

- CATEGORY 3:Confidentiality is the protection of transmitted data from passive attacks. With respect to the content of a data transmission, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. For example, when a TCP connection is set up between two systems, this broad protection prevents the release of any user data transmitted over the TCP connection. Narrower forms of this service can also be defined, including the protection of a single message or even specific fields within a message. These refinements are less useful than the broad approach and may even be more complex and expensive to implement. The other aspect of confidentiality is 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 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.

- CATEGORY 4:
- 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.

- CATEGORY 5:
- 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

- The mechanisms are divided into those that are implemented in a specific protocol layer, such as TCP or an application-layer protocol, and those that are not specific to any particular protocol layer or security service…

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

SPECIFIC SECURITY MECHANISMS….. Contd…..

- 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.

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.

SECURITY MECHANISMS

- X.800 distinguishes between reversible encipherment mechanisms and irreversible encipherment mechanisms. A reversible encipherment mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted. Irreversible encipherment mechanisms include hash algorithms and message authentication codes, which are used in digital signature and message authentication applications

Table 1.4 Relationship Between Security Services and Mechanisms

SERVICE \ MECHANISM	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			

Thank You
&
Best Wishes