OSI security architecture

*OSI security architecture – Attacks, Services and Mechanisms*

***INTRODUCTION*** *Computer data often travels from one computer to another, leaving the safety of  
its protected physical surroundings. Once the data is out of hand, people with bad  
intention could modify or forge your data, either for amusement or for their own benefit.  
Cryptography can reformat and transform our data, making it safer on its trip  
between computers. The technology is based on the essentials of secret codes, augmented  
by modern mathematics that protects our data in powerful ways.*

***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 OSI SECURITY ARCHITECTURE***

*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. The OSI security architecture was developed  
in the context of the OSI protocol architecture, which is described in Appendix H.  
However, for our purposes in this chapter, an understanding of the OSI protocol  
architecture is not required.

*For our purposes, the OSI security architecture provides a useful, if abstract, overview of  
many of the concepts. The OSI security architecture focuses on security attacks,  
mechanisms, and services. These can be defined briefly as follows:****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, Services and Mechanisms*** *To assess the security needs of an organization effectively, the manager  
responsible for security needs some systematic way of defining the requirements for*  
security and characterization of approaches to satisfy those requirements. One approach  
is to consider three aspects of information security:  
**Security attack** – Any action that compromises the security of information  
owned by an organization.  
**Security mechanism** – A mechanism that is designed to detect, prevent or  
recover from a security attack.  
**Security service** – A 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.

***SECURITY SERVICES*** *The classification of security services are as follows:*

***Confidentiality:****Ensures that the information in a computer system and  
transmitted information are accessible only for reading by authorized parties.  
Eg., printing, displaying and other forms of disclosure.*

***Authentication:****Ensures that the origin of a message or electronic document is  
correctly identified, with an assurance that the identity is not false.*

***Integrity:****Ensures that only authorized parties are able to modify computer  
system assets and transmitted information. Modification includes writing,  
changing status, deleting, creating and delaying or replaying of transmitted  
messages.*

***Non repudiation****: Requires that neither the sender nor the receiver of a message  
be able to deny the transmission.*

***Access control****: Requires that access to information resources may be controlled  
by or the target system.*

***Availability****: Requires that computer system assets be available to authorized  
parties when needed.*

***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***

***AUTHENTICATION***

*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.*

***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*** *One of the most specific security mechanisms in use is cryptographic techniques.  
Encryption or encryption-like transformations of information are the most common  
means of providing security. Some of the mechanisms are*

*Encipherment*

*Digital Signature*

*Access Control*

***SECURITY ATTACKS*** *There are four general categories of attack which are listed below.*

***Interruption*** *An asset of the system is destroyed or becomes unavailable or unusable. This is  
an attack on availability.  
e.g., destruction of piece of hardware, cutting of a communication line or  
disabling of file management system.*

***Interception***

*An unauthorized party gains access to an asset. This is an attack on  
confidentiality. Unauthorized party could be a person, a program or a  
computer.e.g., wire tapping to capture data in the network, illicit copying of files*

***Modification*** *An unauthorized party not only gains access to but tampers with an asset. This is  
an attack on integrity.  
e.g., changing values in data file, altering a program, modifying the contents of  
messages being transmitted in a network.*

***Fabrication*** *An unauthorized party inserts counterfeit objects into the system. This is an attack  
on authenticity.  
e.g., insertion of spurious message in a network or addition of records to a file.*

***Passive attack*** *Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.  
The goal of the opponent is to obtain information that is being transmitted. Passive  
attacks are of two types:*

***Release of message contents:****A telephone conversation, an e-mail message and a  
transferred file may contain sensitive or confidential information. We would like  
to prevent the opponent from learning the contents of these transmissions.*

***Traffic analysis****: If we had encryption protection in place, an opponent might still  
be able to observe the pattern of the message. The opponent could determine the  
location and identity of communication hosts and could observe the frequency  
and length of messages being exchanged. This information might be useful in  
guessing the nature of communication that was taking place.  
Passive attacks are very difficult to detect because they do not involve any alteration  
of data. However, it is feasible to prevent the success of these attacks.*

***Active attacks***

*These attacks involve some modification of the data stream or the creation of a false  
stream. These attacks can be classified in to four categories:*

***Masquerade****– One entity pretends to be a different entity.****Replay****– involves passive capture of a data unit and its subsequent transmission  
to produce an unauthorized effect.****Modification of messages****– Some portion of message is altered or the messages  
are delayed or recorded, to produce an unauthorized effect.****Denial of service****– Prevents or inhibits the normal use or management of  
communication facilities. Another form of service denial is the disruption of an  
entire network, either by disabling the network or overloading it with messages so  
as to degrade performance.  
It is quite difficult to prevent active attacks absolutely, because to do so would require  
physical protection of all communication facilities and paths at all times. Instead, the goal  
is to detect them and to recover from any disruption or delays caused by them.*

Specify the four categories of security threats?

Interruption

Interception

Modification

Fabrication

Explain active and passive attack with example?

*Passive attack:  
Monitoring the message during transmission. Eg: Interception  
Active attack:  
It involves the modification of data stream or creation of false data stream.  
E.g.: Fabrication, Modification, and Interruption*

Define integrity and no repudiation?

Integrity:

*Service that ensures that only authorized person able to modify the message.*

Non repudiation:

*This service helps to prove that the person who denies the transaction is true or false.*

Define security mechanism

*It is process that is designed to detect prevent, recover from a security attack.  
Example: Encryption algorithm, Digital signature, Authentication protocols.*

State why network need security.

*When systems are connected through the network, attacks are possible during ransmission time.*

Define confidentiality and authentication.

***Confidentiality:*** *It means how to maintain the secrecy of message. It ensures that the information in a computer system and transmitted information are accessible only for reading by autherised person.****Authentication:*** *It helps to prove that the source entity only has involved the transaction.*

Specify the basic task for security service

*A service that enhances the security of the data processing systems and the  
information transfer of an organization. The services are intended to counter  
security attack, and they make use of one or more security mechanism to provide  
the service.*

Define threat and 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 to evade security services and violate the security policy of a system.****16Marks***

Write short notes on  Security attacks .

Explain in detail Security services.

Explain OSI security architecture.

*Network Security Model  
Saturday, July 02, 2016  
3:51 PM*

***Symmetric and public key algorithms*** *Encryption/Decryption methods fall into two categories.*

*Symmetric key*

*Public key  
In symmetric key algorithms, the encryption and decryption keys are known both to  
sender and receiver. The encryption key is shared and the decryption key is easily  
calculated from it. In many cases, the encryption and decryption keys are the same.  
In public key cryptography, encryption key is made public, but it is  
computationally infeasible to find the decryption key without the information known to  
the receiver.*

***A MODEL FOR NETWORK SECURITY***

*A message is to be transferred from one party to another across some sort of internet. The  
two parties, who are the principals in this transaction, must cooperate for the exchange to  
take place. A logical information channel is established by defining a route through the  
internet from source to destination and by the cooperative use of communication  
protocols (e.g., TCP/IP) by the two principals.*

***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  
  referred conventional / private-key / single-key  
sender and recipient share a common key  
all classical encryption algorithms are private-key  
was only type prior to invention of public-key in 1970‟****plaintext****- the original  
message  
Some basic terminologies used :****ciphertext****- the coded message****cipher****- algorithm for transforming plaintext to ciphertext****key****- info used in cipher known only to sender/receiver****encipher (encrypt)****- converting plaintext to ciphertext****decipher (decrypt)****- recovering ciphertext from plaintext****cryptography****- study of encryption principles/methods*

***cryptanalysis (codebreaking)****- the study of principles/ methods of deciphering  
ciphertext without knowing key****cryptology****- the field of both cryptography and cryptanalysis*

*random nonsense, referred to as cipher text. The encryption process consists of an  
algorithm and a key. The key is a value independent of the plaintext. Changing the key  
changes the output of the algorithm. Once the cipher text is produced, it may be  
transmitted. Upon reception, the cipher text can be transformed back to the original  
plaintext by using a decryption algorithm and the same key that was used for encryption.  
The security depends on several factors. First, the encryption algorithm must be powerful  
enough that it is impractical to decrypt a message on the basis of cipher text alone.  
Beyond that, the security depends on the secrecy of the key, not the secrecy of the  
algorithm.  
·****Two requirements for secure use of symmetric encryption:*** *–  
–  
a strong encryption algorithm  
a secret key known only to sender / receiver  
Y = EK(X)  
X = DK(Y)*

***assume encryption algorithm is known******implies a secure channel to distribute key***

***MCQ***

An asymmetric-key (or public-key) cipher uses

*a. 1 Key        b. 2 Key        c. 3 Key        d. 4 Key  
Ans: B*

In Asymmetric-Key Cryptography, two keys, e and d, have a special relationship to

*a. Others        b. Data            c. Keys         d. Each other  
Ans: D*

In Cryptography, original message, before being transformed, is called

*a. Simple Text         b. Plain Text         c. Empty Text        d. Filled Text  
Ans: B*

An encryption algorithm transforms plaintext into

*a. Cipher text         b. Simple Text         c. Plain Text        d. Empty Text  
Ans: A*

Original message, before being transformed, is

Differentiate symmetric and asymmetric encryption

|  |  |
| --- | --- |
| *SYMMETRIC* | *ASYMMETRIC* |
| *It is a form of cryptosystem in which encryption and decryption performed using the same key. Eg: DES, AES* | *It is a form of cryptosystem in which encryption and decryption Performed using two keys. Eg: RSA, ECC* |

Compare stream cipher with block cipher with example.

*Stream cipher:  
Processes the input stream continuously and producing one element at a time.  
Example: caeser cipher.  
Block cipher:  
Processes the input one block of elements at a time producing an output block for each input block. Example: DES.*

Specify the components of encryption algorithm.

 Plaintext

 Encryption algorithm

 Secret key

 Cipher text

 Decryption algorithm

REFERENCES

<http://www.brainkart.com/article/Classical-Encryption-Techniques_8339/>

<https://www.tutorialspoint.com/cryptography/index.htm>

<https://www.geeksforgeeks.org/cryptography-introduction/>

[https://www.techopedia.com/definition/1770/cryptography#:~:text=Cryptography%20involves%20creating%20written%20or,information%20to%20be%20kept%20secret.&text=Information%20security%20uses%20cryptography%20on,transit%20and%20while%20being%20stored](https://www.techopedia.com/definition/1770/cryptography).

<https://www2.slideshare.net/lineking/classical-encryption-techniques-in-network-security?qid=e388c29f-793d-4f2b-bcaf-9d22e9ca07b5&v=&b=&from_search=1>

<https://www.researchgate.net/publication/334418542_A_Review_Paper_on_Cryptography>

<https://www.academia.edu/Documents/in/Cryptography>