

Assignment No : 1

Q.1 Explain different services and mechanisms of security.

⇒ servizio chiavi e sbloccaggio dei laboratori

- Security Services are placed above each other.
⇒ Security services are safeguard controls recommended to be placed at the various OSI layers.
 - The various security services are listed as shown in below figure:

Security Services		Protocol Layer				
		Authentication	Access control	Data confidentiality	Data integrity	Non-repudiation
- 1)	Peer entity authentication			- 1) Connection based	- 1) Connection integrity with recovery	- 1) Non-repudiation with proof of origin
- 2)	Data origin authentication			- 2) Connectionless		
				- 3) Selective field	- 2) Connectionless without integrity	- 2) Non-repudiation with proof of delivery
				- 4) Traffic flow control	- 3) Selective field	
						connection integrity
					- 4) Connectionless integrity	
					- B) Selective field	connectionless integrity.

Lesson 10: Security Mechanisms

- Security Mechanisms
- ⇒ Security mechanisms are various techniques recommended to provide security services at the various OS layers.
- The various security mechanisms that can be applied are as follows:

1) Encryption

- ⇒
 - Symmetric key used in most cases
 - Asymmetric

2) Digital signatures

- ⇒
 - Signing a data unit
 - Verifying a data unit

3) Access Control

- ⇒
 - Passwords
 - Lifetime of access
 - Duration of access
 - Access routes

4) Data Integrity

- ⇒
 - Ident quantity of data received / quantity of data
 - Sequencing of data units

Time stamping

B) Authentication

- ⇒ **Handshaking** or initial session setup
- i) Cryptographic techniques
- ii) Traffic padding
- iii) Routing control
- iv) Notarization
- v) Pervasive security
- vi) Security labels
- vii) Event detection
- viii) Security audit
- ix) Security recovery

Q. 2. What are various types of attacks? Explain with examples.

⇒ At high level, there are two broad categories of security attacks carried over the network - active attacks, and passive attacks

Types of Attacks

- 1) Active Attacks

- a) Replay Attack
- b) DDoS Attack
- c) Fabrication Attack

- 2) Passive Attacks

- a) Traffic Analysis
- b) Eavesdropping

1) Active Attacks

→ An active attack is defined as ~~both~~ an attack where the attacker actively participates in the communication or the attack mechanism and disrupts the system by sending several manipulated inputs.

2) Replay Attack

→ This is like a replaying a song! The attacker captures the real and specific communication packets and stores them with herself and then sends it at a later point in time as if she is sending the information for the first time like an authentic information.

For being out of context level find it ↗

Attackers can capture information from the victim's Username, Passwords

User
Access granted

Website

Attackers → Get a copy

Attackers → 2021

Attackers → Information, Username, Password

Attackers → 2021

Attackers → send the copy

Access granted

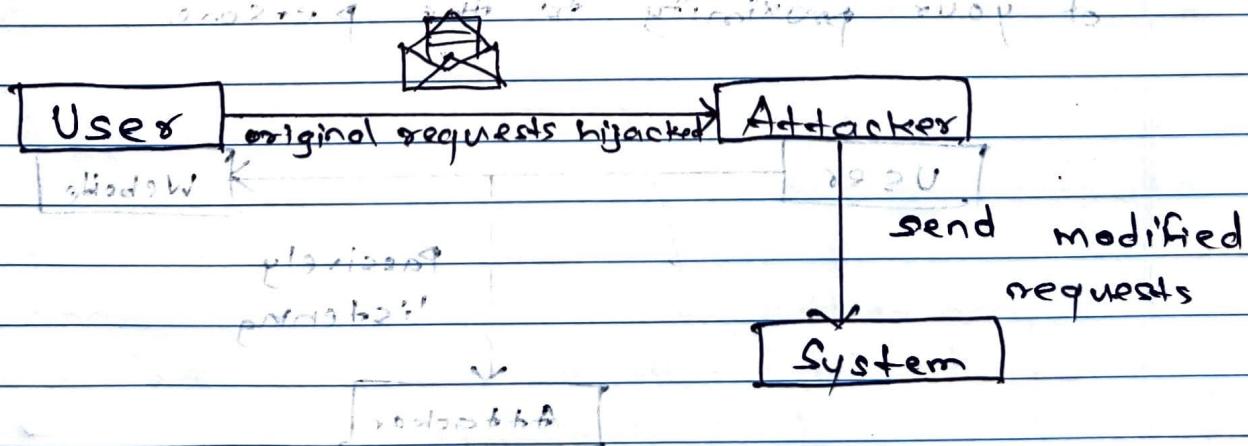
b) Denial of Service (DoS) Attack

⇒ DoS or DDoS variation in Distributed DoS refers to a category of attacks that can be aimed at various layers of network, operating system, application or other parts of information systems.

- For e.g., An application might be capable of processing a maximum of 100 requests per second. Attackers would typically send over ≥ 100 requests per second such that the application fails to cope up with it and crashes.

c) Fabrication Attacks

⇒ Fabrication attack is again a broad category of active attacks where the attacker deliberately modifies messages, parameters, properties, etc. of information system components and try to alter the behaviour of the system often by passing security controls.



2) Passive Attacks

⇒ A passive attack is defined as an attack where the attacker does not alter the behaviour of the information system and silently performs other malicious activities.

a) Traffic Analysis

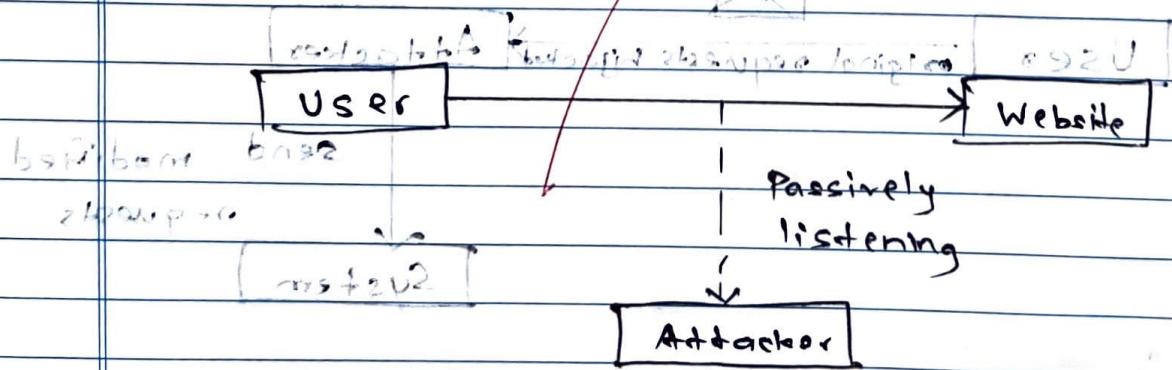
⇒ In traffic analysis, the network traffic and changes in patterns are monitored over a period of time to infer important information and guess possible activities.

- For e.g.,

Long communication between denote some emergency or situation monitored to establish contacts with nearby locations. In also, advertising, retransmission, segmentation, retransmission, etc.

b) Eavesdropping

⇒ Eavesdropping is very similar to over-hearing someone's telephonic conversation taking advantages of your proximity to the person.



Q.3 List few latest viruses on net and explain.

⇒ ~~Latest viruses on net and explain~~

⇒ ~~Latest viruses on net and explain~~

⇒ ~~How viruses are spread in network~~

1) Malware ~~is a program that can damage~~

2) Ransomware ~~is a type of malware~~

3) Trojans ~~are programs that can~~

a) AdBrot ~~malicious advertisements~~

b) Jokemo ~~malicious advertisements~~

1) Malware ~~is a term that includes~~

⇒ ~~Malware is a combined term that includes~~

more than computer viruses.

→ Worms, Trojans, adware and even ransomware may all be considered malware.

→ This is any computer code intentionally created to do damage to computer

systems, gain unauthorized access to computers or to steal information.

2) Ransomware ~~is a type of malware~~

⇒ ~~Ransomware disables access to computer files by encrypting data.~~

→ Demands for payment or other requests must be met before the offending software will be unlocked to restore access to servers or business files.

3) Trojans as a virus label with 2.7

- Trojans typically require the recipient to take some form of action, such as running a program or accessing a malicious website through a link passed by email.
- A common use of a Trojan attack is first to notify a computer user a virus has infected them.

4) CoBalt

- CoBalt is a virus that is one of the most recent viruses to be unleashed by hackers.
- It is not terribly sophisticated in its technology, but it can spread & harm just the same. It can infect, corrupt & randomize all the user's data.

5) Joker as a virus type 2.7

- Joker is a serious piece of malware in the form of ransomware that is offered on underground hacking sites for proliferation by other cyberthieves.

- It can be distributed through social media sites, including ~~Facebook~~ and others.

~~Facebook~~ and other social media sites, such as WhatsApp, are used to spread this malware. It has been sold for \$100,000 and is contained in a virus of 2.7.