Date: / /

CNS unit 6 IMP Notes

1] Draw and explain model for network security.

→ A model for network security involves multi lagered approch to protect computer networks from various threats.

- Here is a overview of brief key components

① create a logical information channel between source and destination

② source and destination cooperate using communication protocal like (TCP, IP) to data exchange.

③ Apply security related transformations to ensure confidentiality and authenticity.

④ share secret information between soure & destination, unknown to potential opponents.

⑤ Involve a trusted third party for tasks like dispute resolution which enhance the security of the transmission.

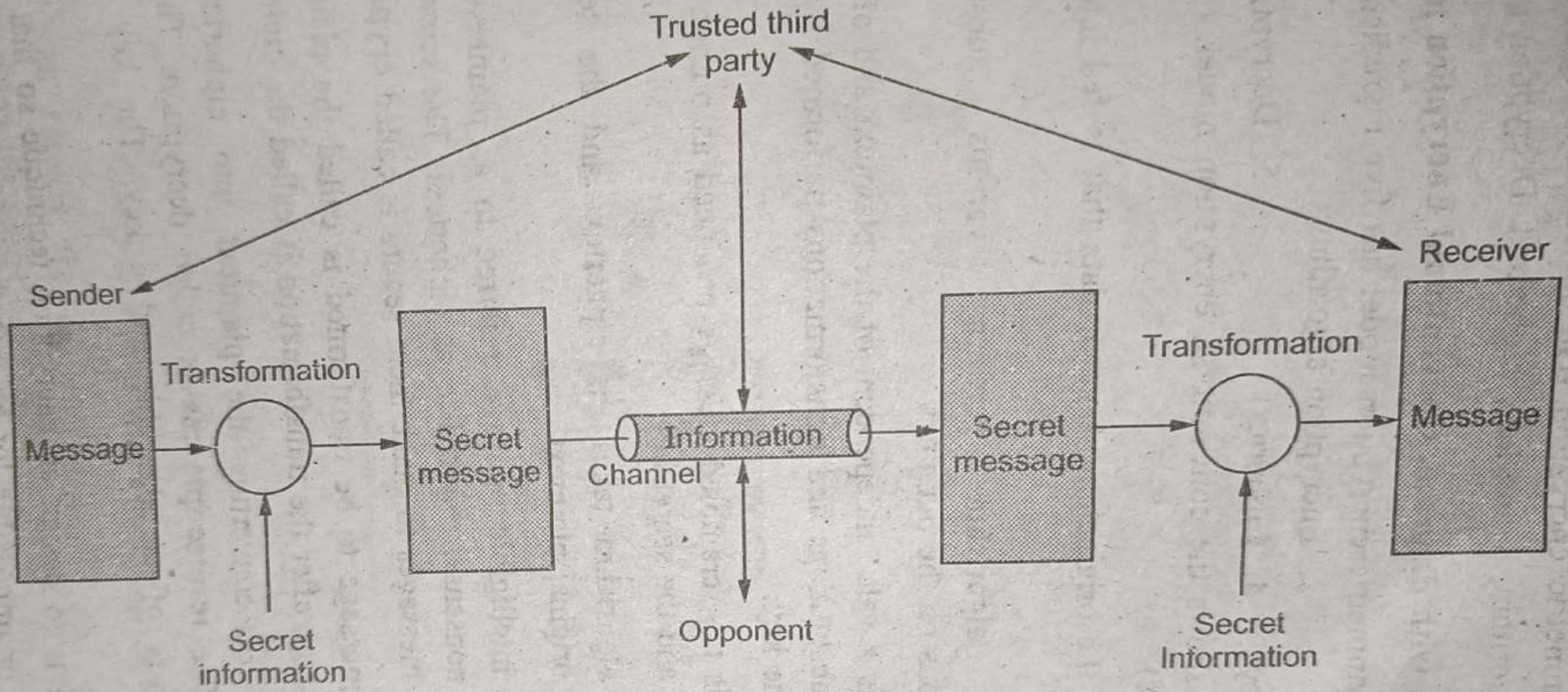


Fig. Q.19.1 Network security model

Page No.:
Date: / /

2] What is IPSec? What are different security services provided by IP Sec?

→ - IPsec means Internet Protocal security
- It provides security services to enhance the security of IP communications.
- The main security services offered by IPsec are

① Encryption
Protects the contents of communication from unauthorized access.

② Hashing
ensures that transmitted data has not been tampered during transit

③ Authentication
verifies identity of communication parties

④ Access control
controls who can or cannot access the network

These services contribute to overall security of IP communications.

Page No.:
Date: / /

3] Compare active attacks and Passive Attacks

Active Attack	Passive Attacks
① In active attack modification in information takes place	① In Passive attack, modification in the information does not take place
② In active attack, attention is on prevention	② In Passive attack attention is on detection
③ In active attack, victim get informed about attack	③ In Passive attack victim does not get informed about attack
④ In active attack system resources can be changed	④ In Passive attack System resources are not changing
⑤ can be easily detected	⑤ very difficult to detect
⑥ Purpose of active attack is to harm ecosystem	⑥ Purpose of Passive attack is to lear about the ecosystem
⑦ Prevention possibility - high	⑦ Prevention possibility - low.

Page No.:
Date: / /

4] Types of Network attacks

→ A Active Attacks -

① DDS Attack -
Overloads a network to make it unavailable for users

② Man in middle Attack -
Intercepting and altering communication between two parties

③ Malware
~~Phishing~~ Attacks -
Installing malicious software on target system to compromise its functionality

④ Brute force Attack
Gaining unauthorized access by ~~try~~ trying all possible combinations of passwords.

A Passive Attacks

① Packet Shilling
Analyzing & intercepting network traffic to capture INFO...

② monitoring
observing network activities without altering data

③ Passive Password Attacks
Gaining unauthorized access without actively interacting with system.

Page No.:
Date: / /

5] IDS

- IDS (Intrusion detection system)
- Design to monitor detect and respond to security threats
- Types - IDS (NIDS)
  IDS (HIDS)
- NIDS for monitoring network traffic
- HIDS for operating on individual devices
- works with Firewall & security system, provides information for incident investigation

6] ~~Firewall~~ S/MIME

- S/MIME enables email authentication through digital signatures, ensures message integrity
- Supports encryption for securing email content during transmission
- Depends on public-key infrastructure to manage digital certificates.
- Widely supported across email clients like mozila, outlook, thunderbird etc.
- Widely used by corporate, government, and personal fields people

3. When host-based IDSs operate on OS audit trails; they can help detect Trojan horse or other attacks that involve software integrity breaches.

Disadvantages :

1. Host-based IDSs are harder to manage, as information must be configured and managed for every host monitored.
2. Since at least the information sources for host-based IDSs reside on the host targeted by attacks, the IDS may be attacked and disabled as part of the attack.
3. Host-based IDSs are not well suited for detecting network scans or other such surveillance that targets an entire network.
4. Host-based IDSs can be disabled by certain denial-of-service attacks.

Q49 What is firewall ? Explain capabilities and limitation of firewall.

Ans. : A firewall is inserted between the Internet and LAN for security purpose. The firewall protects the LAN from Internet-based attacks and also provides security and audits.

A firewall may be a hardware or a software program running on a secure host computer. A firewall is placed at junction or gateway between the two networks.

- A firewall must have at least two network interfaces one for the network it is intended to protect and one for the network and other for the network it is exposed to. A firewall placed between a private or corporate network and a public network (Internet) is shown in Fig. Q.49.1.
- The term firewall comes from the fact that by segmenting a network into different physical subnetwork, they limit the damage that could spread from one subnet to other just like firedoors or firewalls.

Capabilites of firewall

- A firewall examines all traffic routed between the two networks to see if it meets the certain criteria. If it does, it is routed between the networks, otherwise it is stopped.
- A firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications.

Limitation :- Traditional firewalls may struggle to inspect and control specific application or services can't handle advanced threats.

6.10 : SSL

Q.41 What is SSL? List its feature.

Ans. : • SSL protocol is an internet protocol for secure exchange of information between a web browser and a web server.

- SSL is designed to make use of TCP to provide a reliable end to end secure service.
- Secure Socket Layer (SSL) provides security services between TCP and applications that use TCP. The SSL protocol is an internet protocol for secure exchange of information between a web browser and a web server.

Features of SSL

1. SSL server authentication, allowing a user to confirm a server's identity.
2. SSL client authentication, allowing a server to confirm a user's identity.
3. An encrypted SSL session, in which all information sent between browser and server is encrypted by a sending software and decrypted by the receiving software.
4. SSL supports multiple cryptographic algorithms.

Q.42 Compare IPSec and SSL.

Ans. :

Q.43 Explain SSL handshake protocol.

Ans. : • Handshake protocol allows the server and client to authenticate each other and to negotiate an encryption before transmitting application data various massages are used in protocol. Table Q.43.1 enlist these messages and there associated function.

Phase	Message type	Function
1.	Hello - request	Null
	Client - hello	Version, session id, cipher, compression
	Server - hellow	Version, session id, cipher, compression.
2.	Certificate	Chain of X.509 V3 certificates.
	Server - key - exchange	Parameters, signature.
	Certificate - request	Type, authorities.
	Server - done	Null
3.	Certificate - verify	Signature
4.	Client - key - exchange finished.	Parameters, signature hash value.

Table Q.43.1 SSL handshake protocol message types

action. (Refer Fig. Q.43.1 on

7] Security Mechanism & elements of Information Security.

→

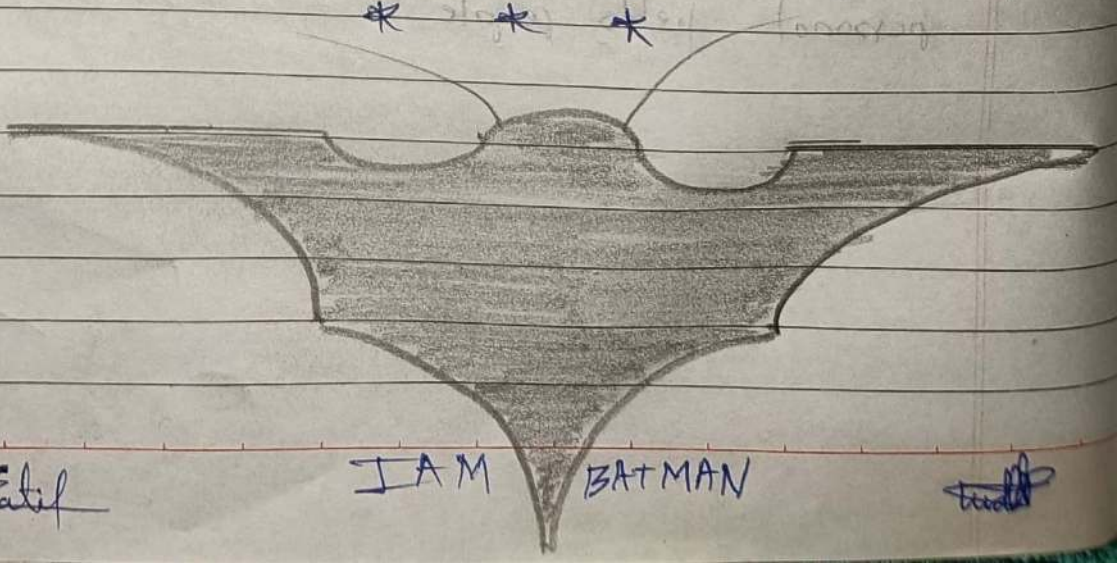
Security Mechanism

- They are technical methods enforcing security policies ex- firewall, encryption, access control.
- Aims for prevention, detection, correction
- security mechanism implement technical safeguards for security policies
- example : Password Policies that Specifies password requirement for user authentication.

elements of Information Security.

- Protects information from unauthorized access
- ensures accuracy of data.
- Guarantees accessibility to authorized users.
- Limits access to authorized parties.
- elements of Information Security provides protecting confidential information, integrity of data.

* * *



Fatil