GOD + Desire = MAN
Man - Desire = GOD
...Bhagwan Sri Sathya Sai Baba

unit-4

Q) what is SSL ? explain TLS functionalities.

SSL (Secure socket layer) :-

→ It is a security protocol developed by Netscape to secure data exchange over internet

→ It protects data between browser and server by encrypting it, so that no one can read or modify it during transmission

→ provides security, privacy & data integrity

→ used in HTTPS

TLS (Transport layer security):

→ It is an improved & secure version of SSL

→ It is currently used in websites, email, online banking etc

→ more secure than SSL

→ used in HTTPS

→ works b/w transport layer & application layer

Functionalities of TLS :-

TLS uses 4 main protocol to provide security:

1. Handshake protocol:
   → establishes a secure connection
   → verifies identity (server) and sets encryption keys
2. Record protocol
   → encrypts & protect data before sending
3. Change cipher spec protocol:
   → tells both sides to start using the new encryption settings
4. Alert protocol:
   → sends error or warning messages

Differences between SSL & TLS

Feature	SSL	TLS
definition	older security protocol	new & improved version of SSL
security level	less secure	more secure
status	deprecated	currently used
data integrity	uses MAC	uses HMAC
Handshake	less efficient	more secure and faster
Encryption algorithms	Fewer	supports stronger modern algorithms
performance	slower	better performance
vulnerability	prone to attacks	improved security patches
who uses it	no longer used	widely used today
Key exchange	RSA, Diffie-Hellman	RSA, Diffie-Hellman, ECC

Hash functions	MD5, SHA-1	SHA-256 SHA-384 SHA 512
	~~Stands for~~	

Q) Difference between TKIP and CCMP

TKIP	CCMP
→ stands for Temporal key integrity protocol	→ stands for counter mode CBC-MAC protocol
→ It has moderate security level	→ It has high security level
→ uses RC4 encryption algorithm	→ uses AES encryption algorithm
→ introduced in WPA	→ introduced in WPA2 & WPA3
→ It has 128 bit key length	→ It has 128 bit (AES) key length
→ faster in performance but less secure	→ More secure, slightly heavier in performance

→ currently not recommended	→ currently widely used
→ data integrity uses michael MIC	→ uses CBC-MAC in data integrity
→ vulnerable to message modification, replay attacks	→ vulnerable to much stronger resistance

TKIP → temporary security solution

CCMP → advanced & secure protocol

Q) List & define SSH protocols

SSH (Secure shell) uses three main protocols to provide secure communication:

① Transport layer protocol:

→ establishes secure & encrypted connection b/w client & server

→ Handles encryption, compression,

integrity checking and session key exchange

→ Also responsible for host authentication

(2) User Authentication protocol:

→ verifies the identity of the user trying to connect.

→ Authentication methods:
- password-based
- public key authentication
- Host-based authentication

→ Ensures only authorized users gain access.

(3) Connection protocol:

→ manages the actual communication sessions (channels)

→ Allows multiple operations (like command execution, file transfer, port forwarding) over a single SSH connection

→ Handles session management and data forwarding

HPL

Q) Applications of SSH:

SSH is mainly used to securely access and manage remote systems over an unsecured network.

applications are:-

① Remote Login & command execution:

→ allows users to log in to a remote computer & execute commands securely

→ commonly used by system administrators

② Secure File Transfer:

→ Used to transfer files b/w systems securely using
- SCP (secure copy protocol)
- SFTP (SSH file transfer protocol)

③ Port Forwarding / Tunneling:

→ SSH can securely forward network ports to protect data

→ used for secure database access or bypassing firewalls

④ Remote Server management:

→ Used to manage Linux / Unix-based servers securely

→ Helps in tasks like software installations, system updates & monitoring

⑤ Secure Automation & scripting:

→ used in automated scripts for remote backups, updates & deployments
→ popular in DevOps & cloud environments

⑥ Access to remote network services:

→ SSH allows secure access to applications hosted on remote machines

→ Eg: connecting to remote Git repository using SSH

HPL

Q) purpose of HTTPS:

HTTPS (Hyper text transfer protocol secure)

→ It is used to securely transfer data between a web browser & web server

→ It protects sensitive information during online communication.

purposes:

① Data Encryption:

→ converts data into unreadable format (encrypts it)

→ prevents hackers from seeing the data (eg: passwords, credit card details)

② Authentication

→ ensures the user is connected to the real website, not a fake one

→ uses SSL/TLS certificates.

③ Data Integrity:

→ ensures the data is not modified or tampered during transmission

④ Secure online transactions:

→ used in banking, shopping, login pages etc

Q) What protocol conveys SSL alerts? Draw protocol format.

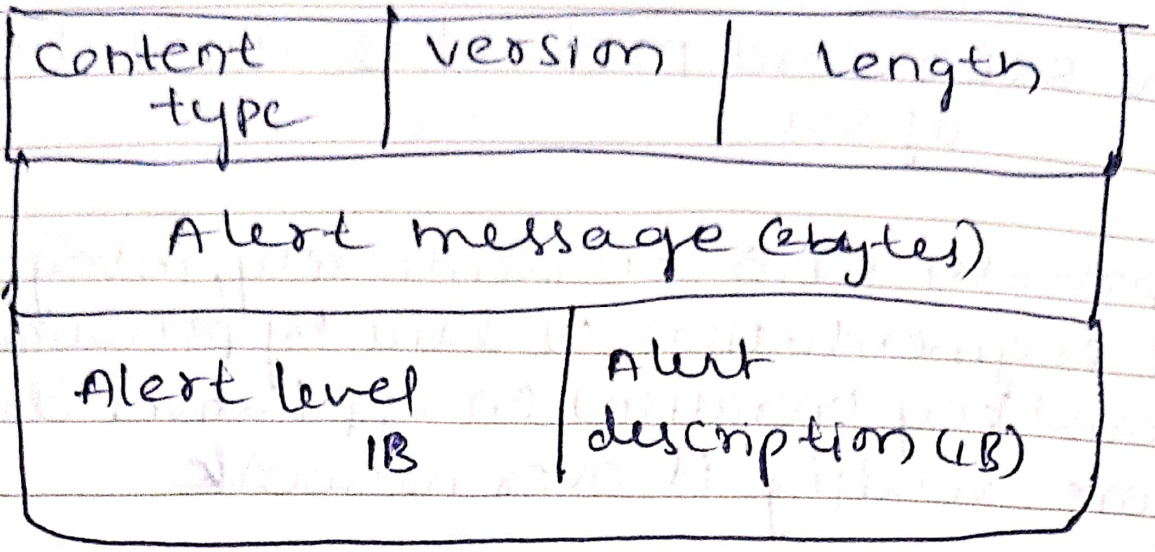
The SSL Alert protocol is responsible for conveying (sending) alert messages in SSL.

→ It is one of three SSL sub protocols.

→ The alert protocol notifies the peer (client/server) about errors or important event such as
- close connection
- warning messages
- Fatal errors

→ Each alert message contains 2 bytes:
- alert level
- alert description

SSL alert protocol format



Fields:

① Content type
→ identifies this is an alert protocol message (value = 21)

② version:
→ SSL/TLS protocol version

③ Length:
→ Size of alert message

④ Alert level
- 1 = warning
- 2 = Fatal (connection mut be closed)

⑤ Alert description:

Eg: • 0 – close_notify
• 10 – unexpected message
• 40 – handshake failure
• 42 – bad certificate

Q) Explain SSL Record Protocol operations.

→ The SSL record protocol is foundation of SSL

→ provides confidentiality, integrity and segmentation of data by performing several key operations on application data before sending it over network

SSL record protocol performs 4 major operations:

1) Fragmentation:

→ Application data is divided into manageable block

→ each fragment is usually ≤ 16kB

→ it prevents large data from overwhelming the network

2) Compression:

→ the fragmented data may be compressed to reduce size

→ depends on negotiated parameters

→ Help reduce redundancy & improve efficiency

3) MAC Generation

→ It is computed over:
MAC = Hash (MAC key, Sequence Number, Header, Data)

→ SSL uses HMAC with MD5 or SHA-1

purpose: Integrity protection

4) Encryption:
↓
fragment + MAC is encrypted.

eg: AES, DES, 3DES, RC4

→ ensures confidentiality of data

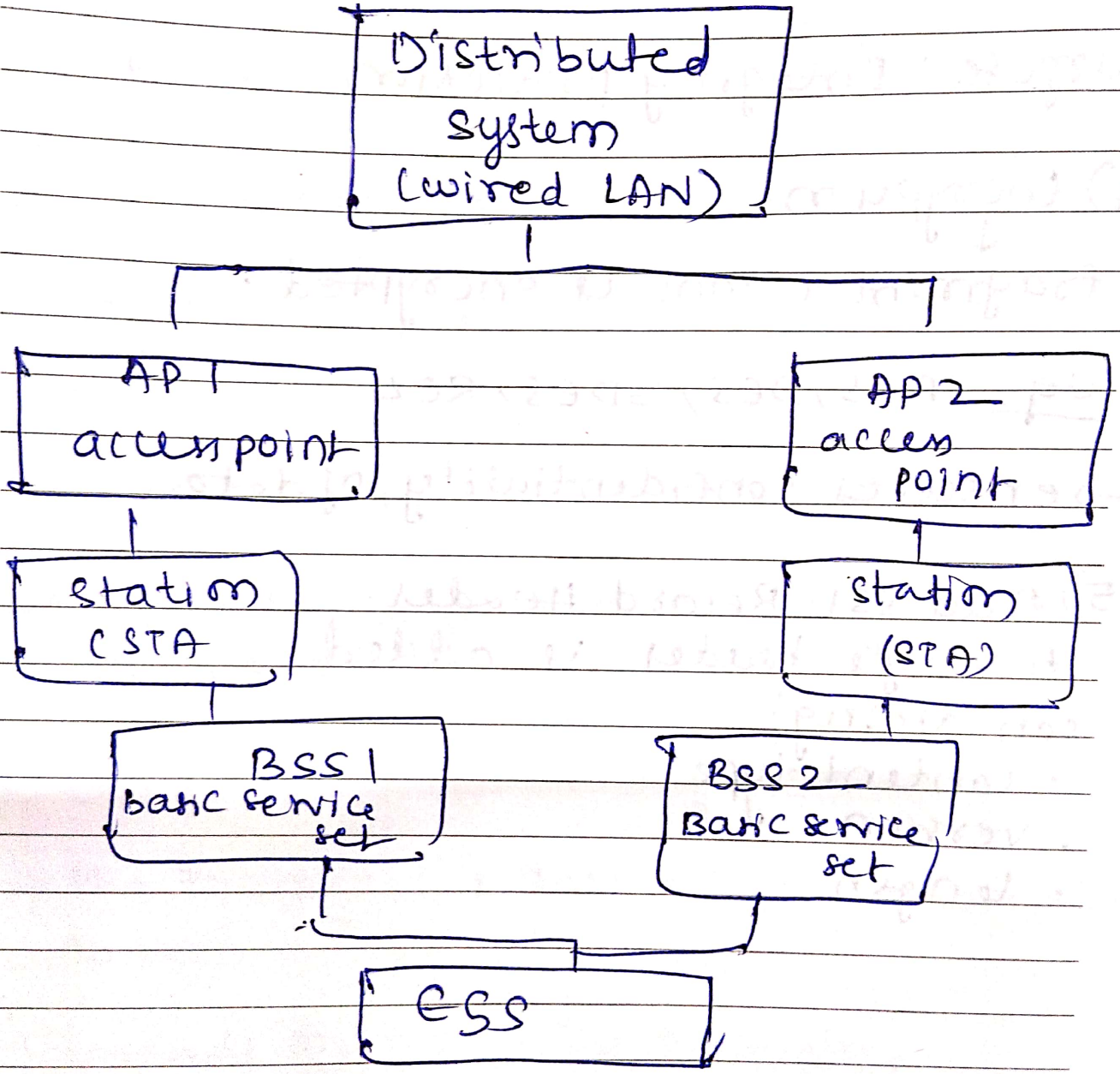
5) Add SSL Record Header.
A 5-byte header is added containing:
- content-type
- version
- length

Define Extended service set (ESS)

→ It is group of multiple basic service sets that are interconnected through a distributed system.

(OR)

→ Two or more Wi-Fi access points connected together to form a larger wireless network with continous coverage



Features :

→ Multiple BSSs connected :-
ESS is formed by connecting two or more BSSs through DS

→ Common SSID
all access points in ESS use same SSID, creating one large wireless n/w.

→ Seamless Roaming :
Stations can move b/w APs without losing connectivity

→ Large covering Area :
coverage beyond a single access point. Ideal for campuses, offices & buildings

→ Uses DS :
interconnects all APs & manage data transfer among BSS.

→ Support more users :
because multiple APs exist ESS can handle a large number of devices effectively.

Adv	Disadv
→ wider coverage	→ complex setup
→ supports mobility	→ Higher cost
→ scalability	→ potential interference

Q) What security areas are addressed by IEEE 802.11i?

IEEE 802.11i enhances security in Wi-Fi networks by improving authentication, encryption and key management

→ It mainly addresses four major security areas:

1) Authentication:
→ provides strong, mutual authentication between client and access point

→ Uses 802.1X, EAP and RADIUS for secure network access

2) Encryption (confidentiality):

→ introduces AES based CCMP encryption metho
→ replaces WEP encryption
→ Ensures data privacy over wireless medium

3) Integrity Protection:

→ Uses Message Integrity Code (MIC) in CCMP

→ prevents data tampering & replay attacks

→ Ensures packets are not modified in transit.

4) Key Management:

→ defines strong key generation & distribution methods

→ Introduces 4 way handshake for secure session key creation

→ Ensures keys are refreshed & protected

Q) List & Define IEEE 802.11i services

① Authentication service
② Access control
③ Data confidentiality
④ Data integrity
⑤ Key management
⑥ Replay protection
⑦ Robust security Network (RSN)

Q) Steps for packet exchange in SSH.

SSH communication happens in four main steps:

① TCP connection setup:
→ clients open TCP connection to server on port 22.

→ Basic transport channel is created

② SSH Handshake
→ client & server exchange protocol versions
→ perform Diffie-Hellman key exchange to generate a shared secret
→ server sends its host key → client verifies server identity.

③ User Authentication:

→ clients authenticates using
- password
- public key
- keyboard-interactive

→ If authentication succeeds, secure session starts

④ Secure Data Transfer.

→ Application data is exchanged through encrypted SSH packets.

→ A packet consist of:
- payload
- padding
- MAC

---

9) Explain SSH protocol stack

- SSH protocol stack is organized into three main layers
- Each layer has distinct role in ensuring secure communication over an insecure network

Layers of SSH protocol stack:

1) Transport layer:

→ runs on top of TCP/IP
→ provides confidentiality, integrity and server authentication
→ handles initial key exchange and sets up encryption algorithms
→ ensures that all communication is encrypted & protected from eavesdropping

2) Authentication Layer:

→ authenticates the client (user) to server.

→ supports multiple methods: passwords, public key cryptography, Kerbos or host based authentication

→ ensures only authorized users gain access to remote systems

3) Connection layer:

→ manages multiple logical channel over secure transport

→ provides services like remote shell access, file transfer (SCP/SFTP) & port tunneling

6) wireless LAN principles (IEEE 802.11, mobile security)

Wireless LANs (WLANs) based on IEEE 802.11 use radio waves to connect devices and mobile security is ensured through standards like IEEE 802.11i, which introduced strong authentication and encryption mechanisms

principles of IEEE 802.11 WLAN

1) wireless medium — uses radiowaves
2) Access method
3) Infrastructure mode
4) Ad-hoc mode
5) mobility support
6) security support
7) Power management

mobile security principles in WLAN

1. User authentication
2. Device authentication
3. confidentiality
4. Integrity protection

5) secure key mechanism
6) Replay attack protection
7) physical layer security
8) Firewall + VPN