Name: J Kevin Immanuel

College: VIT Chennai

WIFI TRAINING MODULE 6

Q1) What are the pillars of wifi security?

Authentication: This is to check if the sender is real. There are different authentication process like open authentication shared key auth, etc.

Integrity: This is to check if the content sent is unchanged and no other person has listened to it.

Confidentiality: This is to make sure that only the sender and receiver can see and understand the message and any third party can not check and understand the message.

Q2) Explain the difference between authentication and encryption in WIFI security.

Authentication is the process of verifying if the sender is real or not. This is mostly done in the initial stages of connectivity. There are many authentication process like open authentication, shared key authentication and so on.

Encryption is the process of encrypting and decrypting the messages shared between the sender and receiver are protected and are not visible and readable to third party listeners/attackers. This occurs after connection between the sender and receiver is established and every time a message is shared between the sender and receiver.

Q3) Explain the differences between WEP, WPA, WPA2 and WPA3.

Feature	WEP	WPA	WPA2	WPA3
Encryption	RC4	TKIP	AES	AES-GCMP
Handshake	Static key	4-way (TKIP)	4-way (AES)	SAE (more secure)
Security	Very weak	Weak	Secure	Very secure

Q4) Why is WEP considered insecure compared to WPA2/3?

WEP is done through the use of a shared key. Initially, the devices are connected through the use of a shared key. This key is common for ALL the devices.

The encryption stream cipher used is RC4. This is a weaker cipher and is easy to crack. So, the messages even though encrypted are easily able to be cracked.

The key is a combination of a 24bit initialization vector and a 40bit/104bit key. This IV is small in length and often easily be guessed. Also, the IV gets reused multiple times for different frames. So, if once it is guessed, the other frames are easily be cracked.

Q5) Why was WPA2 introduced?

WPA1 was an improvement over WEP, but it still used the same problematic techniques like RC4 encryption. This means that it can still be cracked easily. Also, Message Integrity Check (MIC), used for integrity checking was weak, so there was a need to create a stronger security protocol.

Q6) What is the role of Pairwise Master Key in 4 way handshake?

Pairwise Master Key is responsible for the derivation of the Pairwise Transient Key, which is in turn responsible for the encryption/decryption of unicast messages.

PTK includes the ANonce, SNonce, PMK, MAC of both devices.

Q7) How does 4 way handshake ensure mutual authentication between client and access point?

In a 4 way handshake, the following steps are occurred to ensure authentication:

1) The access point first sends a ANonce frame – a frame of random numbers generated – to the client requesting authentication
2) The client receives this ANonce and generates the Pairwise Transient Key using the Anonce, SNonce – random number generated by the client, the MAC address of both the devices and the PMK – Pairwise Master Key. The client now sends back the SNonce and MIC frames to the AP.
3) The AP then processes these frames and sends to the client the GTK – Group Temporal Key and other such necessary keys, and also instructions to install the keys. GTK allows client to send multicast and broadcast messages.
4) The client receives the message, installs the keys and finally sends a final EAPOL Key frame acknowledging the process.

Q8) What will happen if we put a wrong passphrase during a 4-way handshake?

If the wrong passphrase is entered, 2 out of the 4 messages are performed. The client will send the SNonce and MIC to access point, but since the passphrase is wrong, MIC check will fail, so the entire authentication process stops.

Q9) What problem does 802.1x solve in a network?

IEEE 802.1X solves the problem of unauthorized device access to a network, especially in enterprise or campus environments where controlling who can connect is crucial. 802.1X introduces RADIUS server in order to make Authentication, authorization and accounting centralized. This is done in order to reduce overhead on AP authenticating every client and managing records on the AP itself, now it is done on a remote RADIUS server. It also makes sure that the authentication process is now user based and not server based, meaning instead of a common PSK, users now have a username and password or a TLS/SSL certificate for authentication.

Q10) How does 802.1x enhance security over wireless networks?

1) 802.1x introduced the usage of user based authentication, meaning that only username and password or certification is required to authenticate a user, instead of a common pre shared key.
2) Mutual authentication: In 802.1xbased authentication, there is mutual authentication, meaning that both the client as well as AP/RADIUS server has to share their credentials to each other to verify their authenticity.
3) Encrypted tunnel: EAP-PEAP has an encryption tunnel where the credentials shared are protected inside the TLS tunnel.
4) Authorization and VLAN assignment: Based on the RADIUS server criteria, different user can be allocated to different VLAN with different accessibility and priority.