Wi-Fi TRAINING - MODULE 6

Akash S, embedUR Systems

Qn 1:

What are the pillars of Wi-Fi security

Three Pillars of Wifi Security:

- **Authenticity**
- **Integrity**
- **Availability**

Authenticity:

- Authenticity ensures only authorized devices and users can access the Wi-Fi network securely
- It verifies identities through strong passwords or digital certificates to block unauthorized entry
- This prevents rogue devices from joining and potentially disrupting network operations
- Standards like 802.1X enforce authenticity by requiring proper credentials before connection

Integrity:

- Integrity guarantees that data sent over Wi-Fi remains unchanged during its journey
- It uses message authentication codes to detect any tampering or corruption in transit
- This ensures users receive accurate information without alterations by malicious actors
- Integrity mechanisms like those in WPA3 maintain trust in network communications

Confidentiality:

- Confidentiality protects data by encrypting it to prevent unauthorized access during transmission
- It ensures sensitive information like passwords or emails stays hidden from eavesdroppers
- WPA3 uses advanced encryption methods to secure data across the wireless network
- This pillar keeps user privacy intact even in public Wi-Fi environments

Summary:

- **Authenticity:** Verify that the sender is real
- **Integrity:** Verify the message is not modified
- **Confidentiality:** Proper encryption and decryption

Qn 2:

Describe the frame format of the 802.11 MAC header and explain the purpose of each field

Overview:

Authentication:

- Authentication confirms device or user identity
- It blocks unauthorized access to networks

Encryption:

- Encryption protects data from being read
- It ensures privacy during transmission

Comparison:

ASPECT	AUTHENTICATION	ENCRYPTION
Definition	Authentication verifies the identity of devices or users joining the WiFi network	Encryption protects data by converting it into an unreadable form for security
Process	It involves checking credentials like passwords or certificates before granting access	It scrambles data using algorithms like AES to ensure only authorized parties read it
Purpose	The goal is to ensure only trusted devices connect and block unauthorized access	The aim is to keep data private and safe from eavesdroppers during transmission
Example	802.1X uses EAP methods to authenticate users before they join the network	WPA3 applies encryption to secure data packets traveling between devices and access points

Qn 3:

Explain the differences between WEP, WPA, WPA2, and WPA3

ASPECT	WEP	WPA	WPA2	WPA3
Introduction	WEP was the first WiFi security standard introduced in 1999 for basic protection	WPA came in 2003 as an improvement over WEP with better security	WPA2 launched in 2004 as a stronger standard with robust encryption	WPA3 debuted in 2018 to address modern threats and enhance security
Encryption	Uses RC4 encryption which is weak and easily cracked by attackers	Employs TKIP for encryption, stronger than WEP but still vulnerable	Adopts AES encryption for secure data protection against most attacks	Uses AES with GCMP for faster and more secure data encryption
Key Management	Relies on static keys that remain unchanged, making it prone to hacking	Introduces dynamic keys with TKIP to improve key rotation and security	Enhances key management with pre-shared keys and better key exchange	Implements stronger key derivation with 192-bit security for enterprise use
Vulnerabilities	WEP has multiple flaws like IV reuse, easily exploited within minutes	WPA fixes some issues but TKIP can still be attacked over time	WPA2 is secure but vulnerable to KRACK attacks on handshake	WPA3 mitigates KRACK and adds forward secrecy for better protection

Qn 4:

Why is WEP considered insecure compared to WPA2 or WPA3

Weak Encryption in WEP:

- WEP uses RC4 encryption which is outdated and easily cracked by modern tools
- It relies on initialization vectors that repeat, making encryption patterns predictable
- Attackers can break WEP encryption in minutes using widely available software
- WPA2 and WPA3 use AES encryption, providing much stronger data protection

Static Key Vulnerability:

- WEP employs static keys that remain unchanged, allowing attackers to exploit them
- There’s no automatic key rotation, leaving the network open to repeated attacks
- WPA2 introduces dynamic key management with frequent updates for better security
- WPA3 enhances this with 192-bit security and forward secrecy for added protection

Lack of modern defenses:

- WEP lacks mechanisms to counter modern threats like packet sniffing or spoofing
- It doesn’t support secure key exchange, making data interception straightforward
- WPA2 defends against most attacks with robust handshake and encryption methods
- WPA3 adds features like protection against offline dictionary attacks for safety

Qn 5:

Why was WPA2 introduced

WPA2 development:

- WPA2 emerged to replace the vulnerable WEP standard in the early 2000s
- It responded to growing security concerns as Wi-Fi usage expanded rapidly worldwide
- The IEEE 802.11i task group focused on creating a robust security protocol
- WEP's flaws like static keys and weak encryption drove the need for change
- Released in 2004, WPA2 became the mandatory security standard for Wi-Fi networks

Purpose:

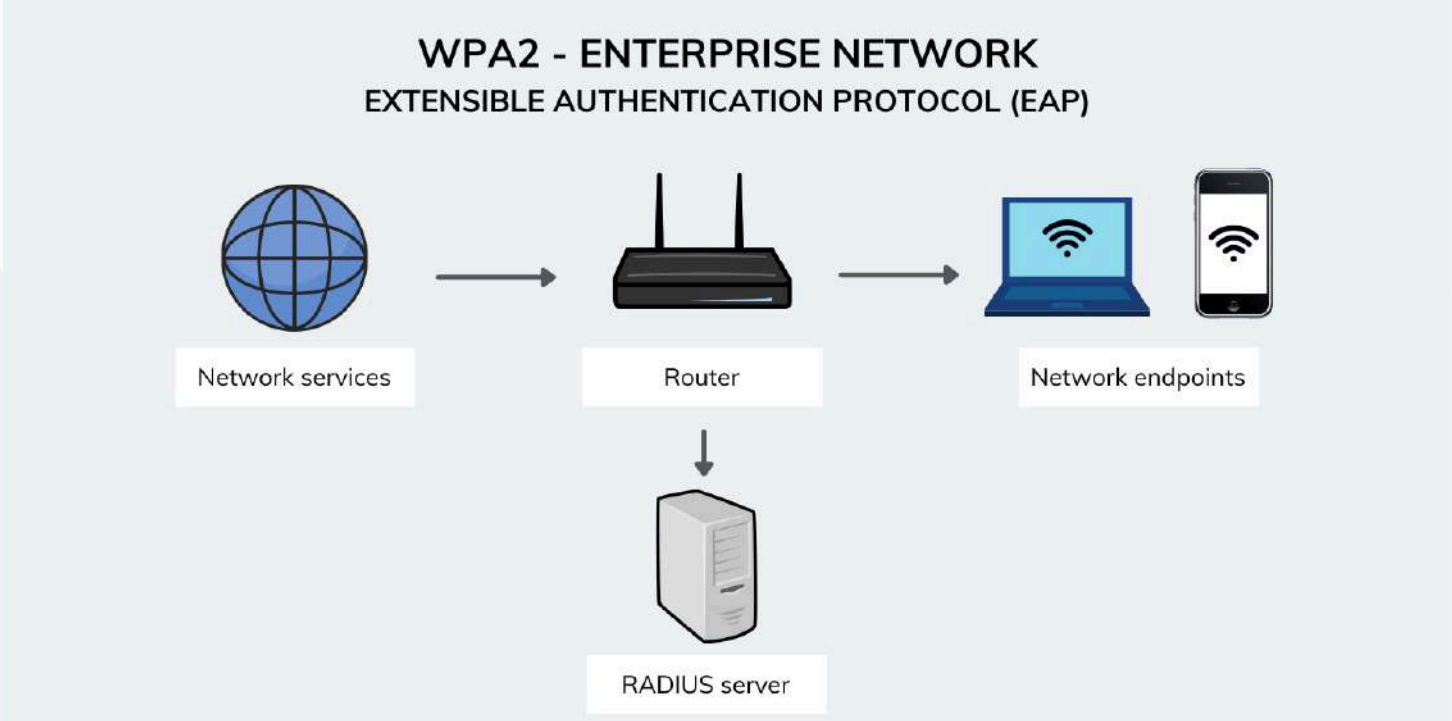
- WPA2 adopted AES encryption to provide strong protection against various cyber attacks
- It aimed to enhance key management with dynamic keys for improved network security
- The goal was to ensure data privacy and integrity during all wireless transmissions
- It sought to support enterprise networks with advanced authentication methods like 802.1X
- WPA2 intended to address vulnerabilities exploited in the earlier WPA security standard

Outcomes:

- WPA2 significantly reduced the risk of unauthorized access to Wi-Fi networks globally
- It became widely adopted, securing homes and businesses for over a decade
- The standard enabled faster and more reliable connections in high-density environments
- It laid a strong foundation for future security enhancements like WPA3 features
- Despite its strengths, WPA2 later faced challenges with attacks like KRACK

Impact on Wifi:

- WPA2 boosted user confidence in Wi-Fi by offering a more secure connection
- It enabled the growth of public Wi-Fi hotspots in cafes and airports
- The standard supported the rise of mobile devices needing reliable security
- It encouraged businesses to deploy larger wireless networks without fear of breaches
- WPA2's success paved the way for widespread Wi-Fi use globally



Qn 6:

What is the role of the Pairwise Master Key (PMK) in the 4-way handshake

PMK:

- Think of the PMK as the secret handshake between your device and the access point
- It’s created during authentication using a passphrase or 802.1X to start things off
- This key ensures both sides trust each other before sharing sensitive data
- Without the PMK, the 4-way handshake wouldn’t even get off the ground

Generating keys in handshake:

- The PMK helps create the Pairwise Transient Key during the 4-way handshake process
- It mixes with random numbers from both sides to make a unique key
- This new key handles encryption for all the data you send and receive
- It’s like the PMK unlocks a safe to protect your Wi-Fi conversations

Key insights:

- Both the device and Access point will have the **PMK**
- With the base as PMK, the ANonce and SNonce will start
- PMK lets the client and access point verify each other’s identity securely

Qn 7:

How does the 4-way handshake ensure mutual authentication between the client and the access point

Initial steps:

- The 4-way handshake begins with a shared Pairwise Master Key from authentication
- Both the client and access point use this key to start the process
- It’s like a secret code they both know to prove they’re legit
- This ensures no outsider can jump in and pretend to be either side

ANone and SNone random numbers:

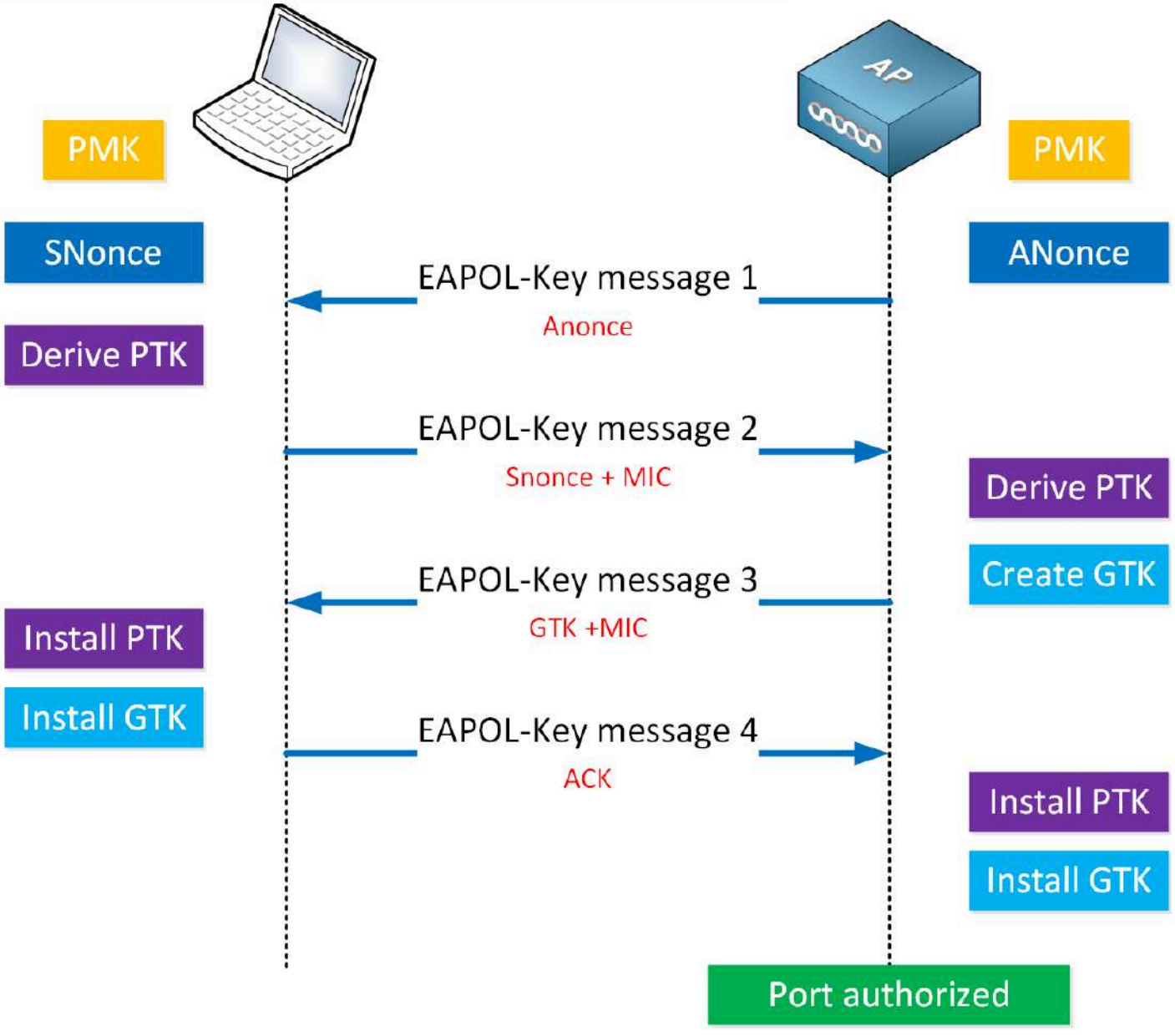
- The access point sends a random number called a nonce to the client first
- The client replies with its own nonce, creating a unique pair of numbers
- They use these nonces with the PMK to generate a fresh session key
- This step confirms both sides are active and not replaying old messages

Verification:

- Both sides create the Pairwise Transient Key using the nonces and PMK together
- They exchange messages with a code to check the key matches perfectly
- If the codes don’t match, the handshake fails, blocking fake devices
- This mutual check proves they both have the right key and identity

Secure Connection:

- The handshake ends with both agreeing on the session key for encryption
- They confirm the keys are installed, ready to protect all future data
- This process keeps your Wi-Fi safe from eavesdroppers or imposters
- It’s a teamwork effort to make sure you’re connected to the real network



Qn 8:

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

Handshake will fail:

- **It will stop at Message 2**
- Entering a wrong passphrase means the client can’t generate the correct Pairwise Master Key
- The 4-way handshake starts but quickly hits a roadblock due to mismatched keys
- Both the client and access point will fail to agree on the session key

Authentication will fail:

- The access point checks the message integrity code and finds it doesn’t match
- It realizes the client’s key doesn’t align with its own, stopping the process
- The client gets no confirmation, leaving it unable to connect to the network
- This mismatch proves the passphrase error, blocking any further communication attempts

Connection impact:

- The access point checks the message integrity code and finds it doesn’t match
- It realizes the client’s key doesn’t align with its own, stopping the process
- The client gets no confirmation, leaving it unable to connect to the network
- This mismatch proves the passphrase error, blocking any further communication attempts

Qn 9:

What problem does 802.1X solve in a network

Unauthorized access:

- 802.1X steps in to stop strangers from joining your network without permission
- It checks every device’s identity before letting it connect to the Wi-Fi
- This keeps unwanted users from sneaking into sensitive areas like offices
- Think of it as a security guard verifying IDs at the network door

It fixes weak authentication:

- Older systems relied on simple passwords that hackers could guess easily
- 802.1X uses strong methods like EAP to verify users more securely
- It replaces weak shared keys with individual credentials for each device
- This makes it tougher for attackers to break into the network

Scalability:

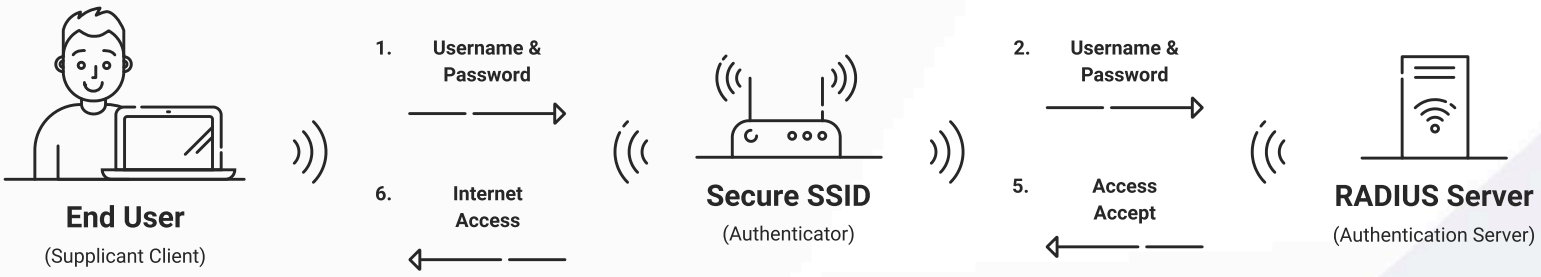
- In big networks, managing lots of devices becomes a headache without control
- 802.1X centralizes authentication through a server to handle the load
- It scales smoothly as more users or devices join the system
- This keeps everything organized even in large enterprise setups

Qn 10:

How does 802.1X enhance security over wireless networks

Strong User Verification:

- 802.1X requires each device to authenticate using EAP protocols
- It enforces credential checks like usernames and certificates for access
- This prevents unauthorized devices from connecting to the network
- It supports multiple authentication methods for robust verification



Centralized security:

- 802.1X uses a RADIUS server to centralize authentication processes
- The server maintains a database of authorized users and devices
- Administrators can update security policies across the network remotely
- This improves scalability and consistency in large deployments

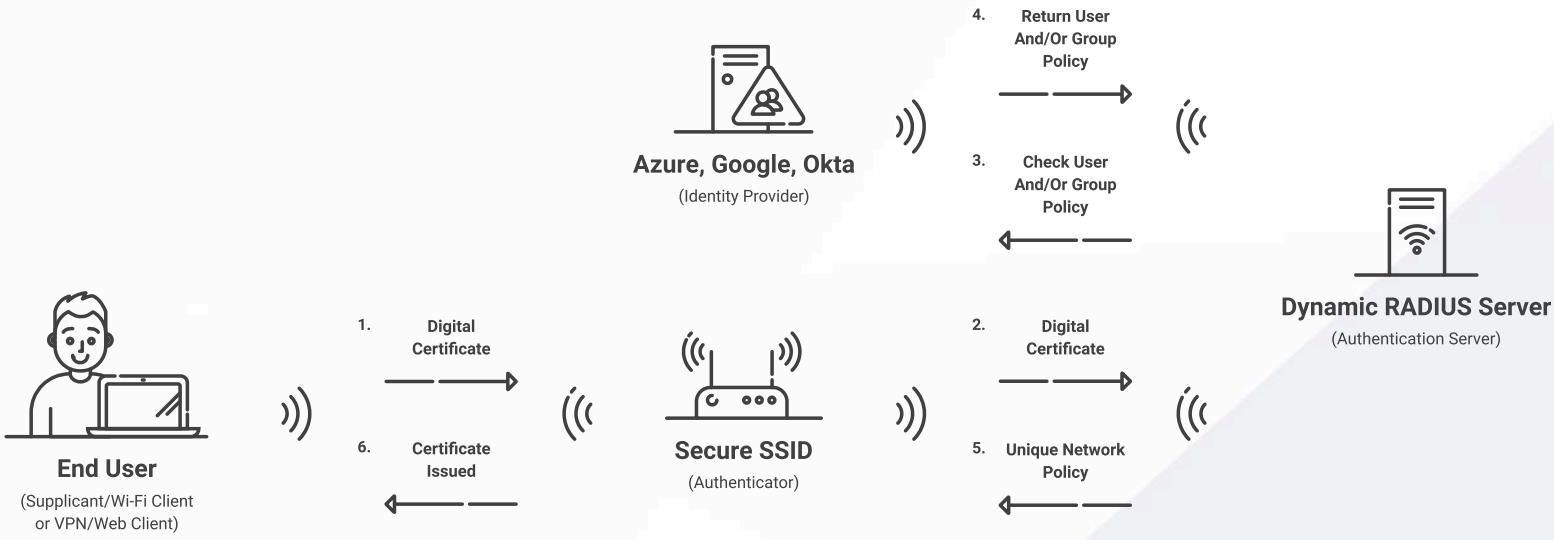
Dynamic key:

- 802.1X enables administrators to enforce strict access policies
- It blocks devices that fail to meet predefined security requirements

How 802.1x works:

Authentication flow:

- 802.1X requires each device to authenticate using EAP protocols
- It enforces credential checks like usernames and certificates for access
- This prevents unauthorized devices from connecting to the network
- It supports multiple authentication methods for robust verification



Post-authentication flow:

- The access point opens the port for the client after authentication
- Session keys are used to encrypt all data between client and AP
- The client can now communicate securely within the wireless network
- Periodic re-authentication ensures ongoing security throughout the session

THE END

AKASH S