Assignment – 6

1 Pillars of wifi security:

1. Authentication : To ensure only legitimate users are connecting to wifi network .Eg: Open System Authentication, WPA2-PSK , 802.1X authentication , WPA3-SAE etc.
2. Encryption: to ensure only trustworthy receiver can only see the message
3. Ensuring integrity in the transmitted message.
4. Efficient and safe derivation and transmission of session keys.
5. Restricting the access to wifi network based on Authorization.
6. Ensuring forward secrecy

2. Authentication vs encryption:

1. Authentication:

- To confirm who is accessing wifi network

- happens before getting access to wifi

- to ensure only legitimate users can access the network

- happens before getting IP in wifi network

- Eg: WPA2 personal PSK, 802.1x authentication

- prevents Man in the middle attack

2. Encryption:

- To protect the transmitted content from tampering in the channel

- happens after getting access to wifi network

- protected with session keys

- Eg: AES-CCMP

3. Differences between WEP, WPA, WPA2, WPA3 :

WEP:

* Works with static key and uses RC4 with 24 bit IV
* Easy to find IV by capturing enough packets
* Vulnerable for attacks since static keys are used
* With Pre shared key. So deprecated

WPA:

* To overcome issues on WEP, TKIP – RC4 based encryption is introduced
* Periodic key changes got introduced
* Per packet key mixing with MIC
* Still uses RC4 so deprecated

WPA2:

* Used 128 bit key
* Used AES-CCMP
* Strong if strong password is used
* KRACK attack is possible
* But still used in wifi network

WPA3:

* Uses AES-CCMP
* Uses 196 bit keys
* Uses 802.1x authentication , SAE for advanced protection.

PMK:

* Pairwise Master Key.
* It determines the entire protection of wifi network
* PMK is derived from the shared passphrase with SSID via some hashing algorithms
* PMK will be used by both AP and client since both have PMK to derive PTK.
* PMK will not be transmitted in air. But to be maintained secretly.
* Other than PMK, while deriving PTK , all others are known details.

4 way handshake:

* To prove both entities (AP, client) are legitimate and know PMK without sharing it.
* At first, AP initiates by creating Anonce and sends to client
* Client already generates Snonce and with the help of nonces, MAC, SSID,PMK, it generates PTK
* But client sends only Snonce with MIC generated from PTK
* Now AP can compute same PTK and verifies it with sent MIC
* Now AP sends GTK encrypted with PTK with MIC for client to decrypt it and verify.
* Client decrypts GTK with available PTK and verifies the sent MIC
* Client sends ACK with MIC for integrity
* If wrong passphrase is entered, then message 2 will get affected since it is the first point at which MIC is involved and will get failed in comparison.

802.1x Authentication:

- it is the port based access control protocol that lets Users get authenticated individually.

- It uses external RADIUS server for authentication.

- It uses individual digital certificates, passwords for authentication.

- Each user then derives different PMK for enhanced security

- whenever client tries to associate with AP, it blocks until authenticated

- now clients sends EAPOP start message to AP

- AP requests for EAP request identity message to client

- client responds with credentials

- AP forwards the response to RADIUS server for authentication

- Server presents the challenge based on the EAP protocol used.

-Once identify proven, via RADIUS accept message , MSK will sent and this will be followed by conventional 4 way handshake with derived PMK from MSK.