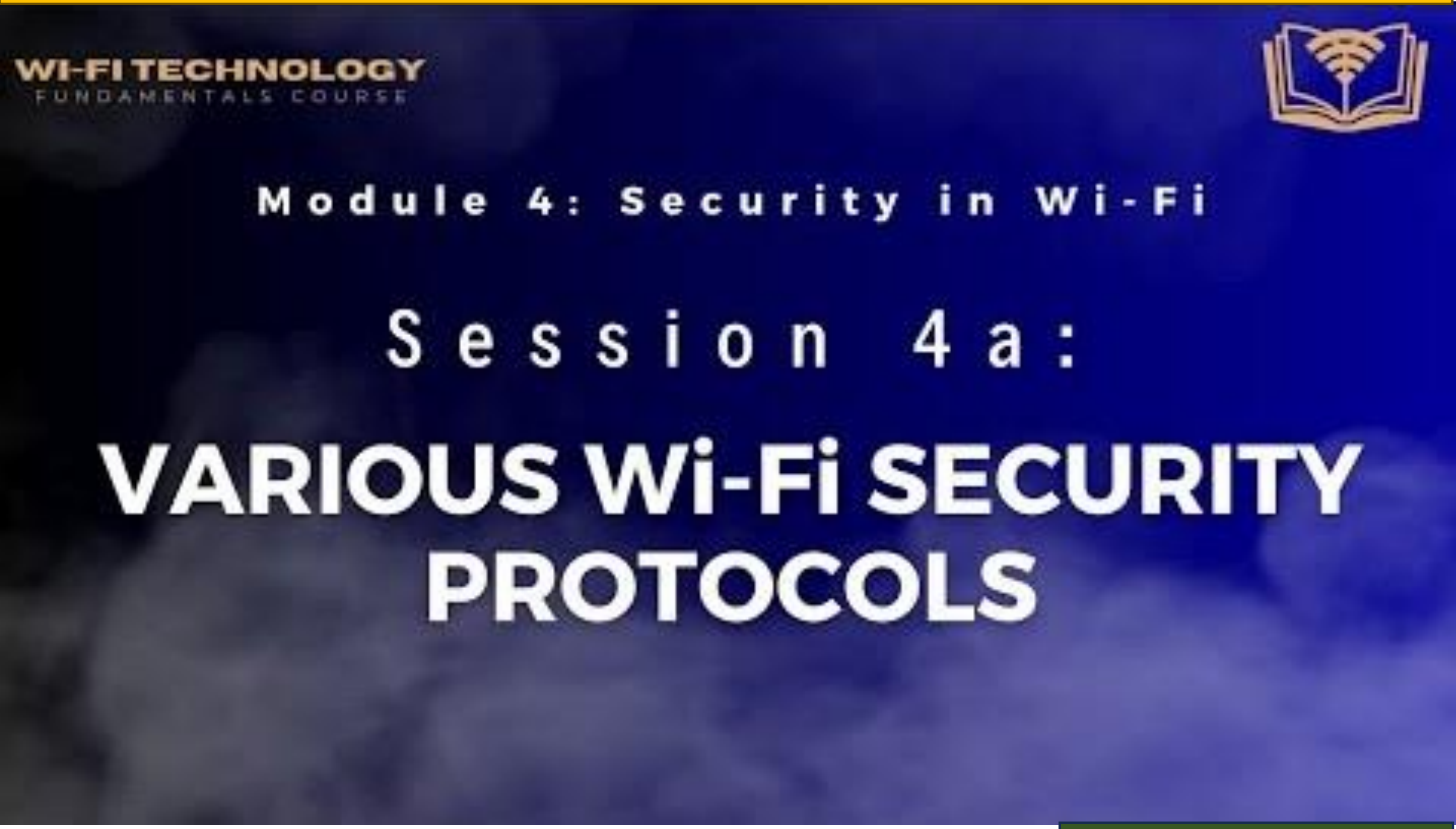


WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

Module 4: Security in Wi-Fi

Session 4a:

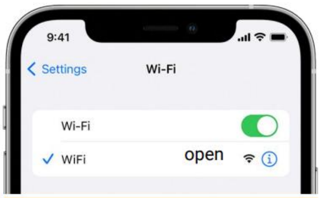
VARIOUS Wi-Fi SECURITY PROTOCOLS

Need of security in Wi-Fi?

If the user use Wi-Fi without security, then the information being accessed by the user can be easily seen by anyone. This is risky as someone hacker nearby us can easily know any of our confidential information like passwords, any account credentials etc. So, to avoid this it is important make sure that we have security in Wi-Fi.

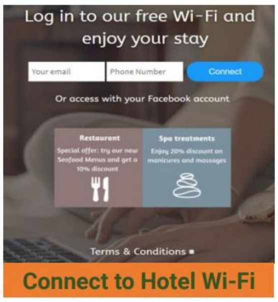
Methods of connecting to a Network:

1. Open Network: Connecting to any available open networks available but not secured.
2. Wi-Fi at Home: Connecting to Wi-Fi at home which generally uses some encryption and connecting to it by using the same passphrase as configured.
3. Hotel Wi-Fi: Connecting to a network at hotels or restaurants which we visit by entering some credentials in the captive portal like name or any required credentials to check if you're a valid user etc but still the connection is an open security.
4. Airport Wi-Fi: Connecting to Wi-Fi at airport where the network is very little secured.
5. Office Wi-Fi: Connecting to Wi-Fi at office which might be a secured network as the office Wi-Fi may have securities and the devices has the required certificates to connect to the Wi-Fi networks available.



Wi-Fi ●
✓ WiFi open

Connect to Open Networks


Log in to our free Wi-Fi and enjoy your stay

Your email | Phone Number | Connect

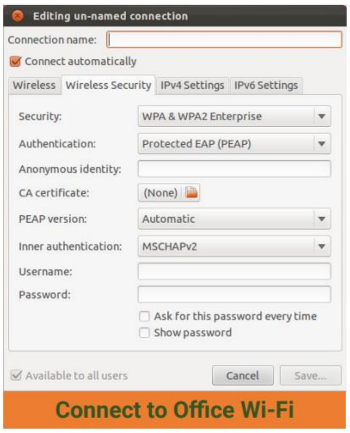
Or access with your Facebook account

Restaurant
Special offer: try our new Seafood Menus and get a 10% discount

Spa treatments
Enjoy 20% discount on manicures and massages

Terms & Conditions

Connect to Hotel Wi-Fi


Editing un-named connection

Connection name:

☑ Connect automatically

Security: WPA & WPA2 Enterprise

Authentication: Protected EAP (PEAP)

Anonymous identity:

CA certificate: (None)

PEAP version: Automatic

Inner authentication: MSCHAPv2

Username:

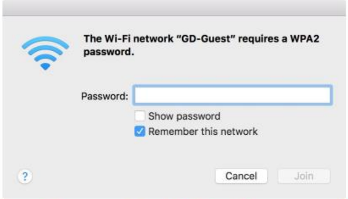
Password:

□ Ask for this password every time

□ Show password

☑ Available to all users

Connect to Office Wi-Fi

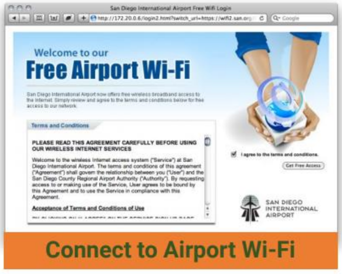

The Wi-Fi network "GD-Guest" requires a WPA2 password.

Password:

□ Show password

☑ Remember this network

Connect to WiFi at Home


San Diego International Airport Free Wifi Login

http://172.20.0.6/login2.html?switch_url=https://wifi2.san.org

Welcome to our

Free Airport Wi-Fi

San Diego International Airport now offers free wireless broadband access to the Internet. Simply review and agree to the terms and conditions below for free access to our network.

Terms and Conditions

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING OUR WIRELESS INTERNET SERVICES

Welcome to the wireless Internet access system ("Service") at San Diego International Airport. The terms and conditions of this agreement ("Agreement") shall govern the relationship between you ("User") and the San Diego County Regional Airport Authority ("Authority"). By requesting access to or making use of the Service, User agrees to be bound by this Agreement and to use the Service in compliance with this Agreement.

Acceptance of Terms and Conditions of Use

☑ I agree to the terms and conditions.

Connect to Airport Wi-Fi

How can we secure a communication?

Analogy:

Two users who are unknown to each other would like to communicate with each other. Then the two essential steps to secure a communication can be

Authentication: To communicate with each other initially both the users need to know if the other one is the right user to communicate that is they need to authenticate to each other that they are right users to communicate with.

Encryption: If the users communicate the actual message, then the message might be known to others. The users in this case can use code messages to share information so that if any intruder would like to know what is the communication, they are unable to know the actual information but can only see the code messages.

Enigma Machine Example:

The encryption is really important when it comes to the war zones as the information should not be known by the enemies. At the point of World War II Nazis used the Enigma Machine in the warfare. The Enigma Machine was an initial way of using keys to encrypt the data

The Enigma has an electromechanical rotor mechanism that scrambles the 26 letters of the alphabet. In typical use, if one person enters text on the Enigma's keyboard and another person writes down which of the 26 lights above the keyboard illuminated at each key press.

If plain text is entered, the illuminated letters are the coded text i.e., cipher text. Entering ciphertext transforms it back into readable plaintext. The rotor mechanism changes the electrical connections between the keys and the lights with each keypress

The security of the system depends on machine settings that were generally changed daily, based on secret key lists distributed in advance, and on other settings that were changed for each message. The receiving station would have to know and use the exact settings employed by the transmitting station to successfully decrypt an encoded message.

Three Pillars of Wi-Fi Security:

1. Authentication
2. Confidentiality
3. Integrity

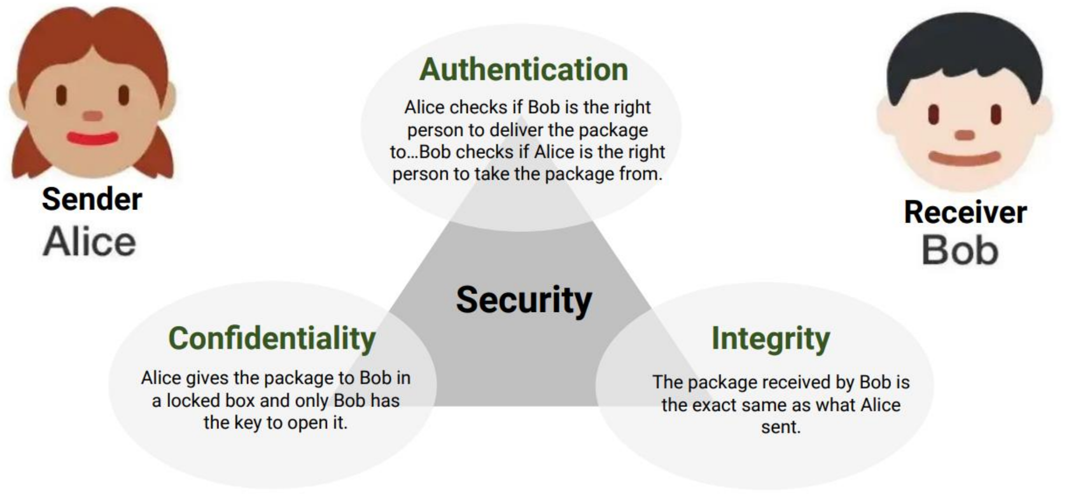
Analogy:

Consider two users Alice and Bob, the three pillars of Wi-Fi Security work as:

Authentication: Alice checks if Bob is the right user to send the information to and similarly Bob checks if Alice is the user from whom the information is to be taken.

Confidentiality: The information sent by Alice should not be understandable for anyone and Bob who is the valid user only should be able to know the actual information using some encryption

Integrity: The information received by Bob should be the exact same data sent by Alice.


Sender
Alice
Authentication
Alice checks if Bob is the right person to deliver the package to...Bob checks if Alice is the right person to take the package from.
Receiver
Bob
Security
Confidentiality
Alice gives the package to Bob in a locked box and only Bob has the key to open it.
Integrity
The package received by Bob is the exact same as what Alice sent.

The Three Enforcements of Wi-Fi security:

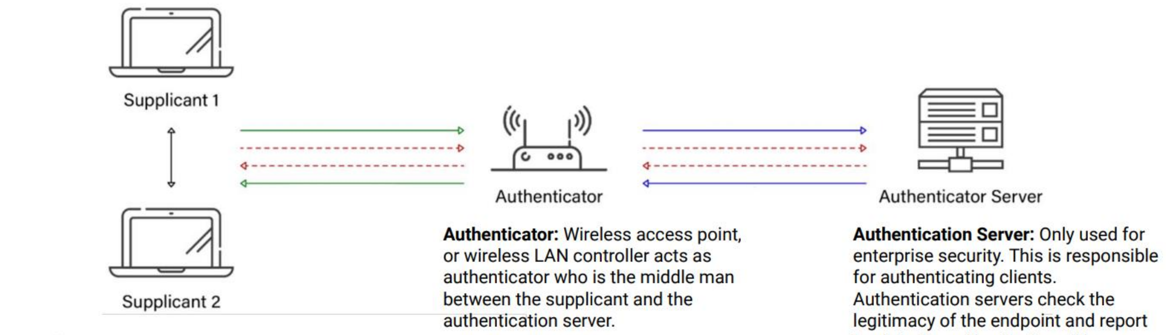
The three enforcements or entities that make sure the network is secured:

1. Supplicant: The supplicant is a software or application on our device that does the authentication and encryption part from the user side.
2. Authenticator: An access point or an wireless LAN controller that acts as authenticator in middle of authentication server and the supplicant
3. Authentication Server: Authenticates if the clients are valid users and sends and approval or denial to the authenticator.

In Residential Wi-Fi, the two components Supplicant and the Authenticator can only be used where the Authenticator can authenticate is the supplicant is a valid user or not.

But in case of Enterprise security, where there may be multiple access points in same network but each having different keys then it would be difficult where one authentication server (generally a radius server or ACS server) can be used as a central entity for all

Authenticators so that the it will be authenticating the supplicants and sending the approval or denial responses to the access points (Authenticators).



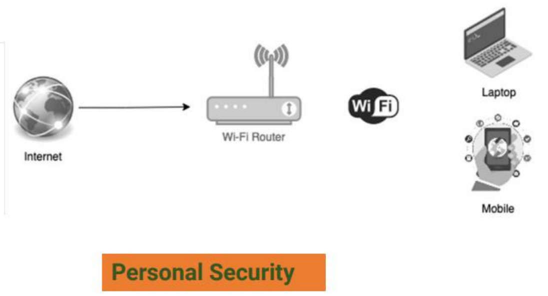
Authenticator: Wireless access point, or wireless LAN controller acts as authenticator who is the middle man between the supplicant and the authentication server.

Authentication Server: Only used for enterprise security. This is responsible for authenticating clients. Authentication servers check the legitimacy of the endpoint and report back to the authenticator with approval or denial.

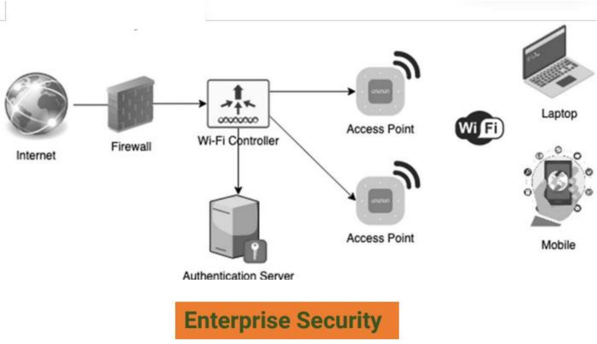
Supplicant: This is the application running on the endpoint or the client's device. It exchanges messages with the authenticator for authentication and encryption

Personal vs Enterprise Security:

1. Personal Security:
   a. Uses a pre-shared key.
   b. The Authenticator authenticates the user using the same pre-shared key and the supplicant gets connected to the network.
2. Enterprise Security:
   a. In Enterprise security, an authentication server (like a radius server) is used.
   b. The authenticator (i.e., the access points) act just as a relay between the authentication server and the supplicant but not doing any actual authentication.



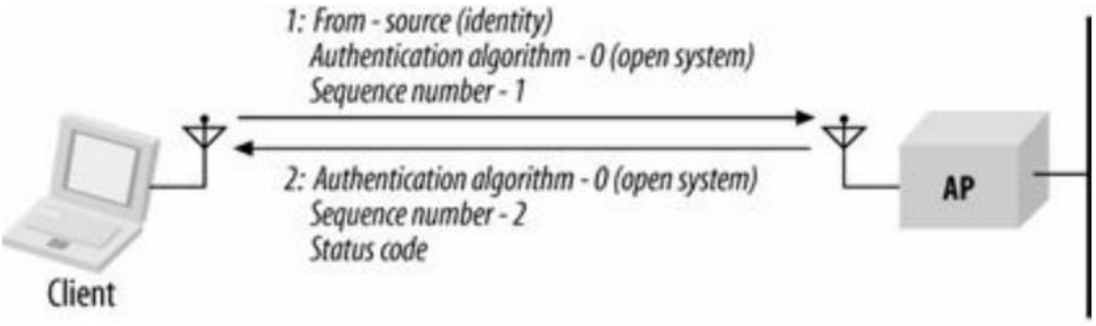
- Uses Pre Shared Keys (PSK)
- All security handshakes relating to Authentication are only between the Router and the Station.
- The security keys are manually entered in both the router and the station.



- Uses 802.1X/EAP
- The authentication aspect is handles by the authentication server on the enterprise network with the APs acting as relays.
- Usually the authentication is tied up with other IT systems like Active Directory services, authorization and accounting operations.
- Authentication is user based and there is no need to manually enter any security keys in the AP or the station.
- Is easily extensible to large scale deployments.

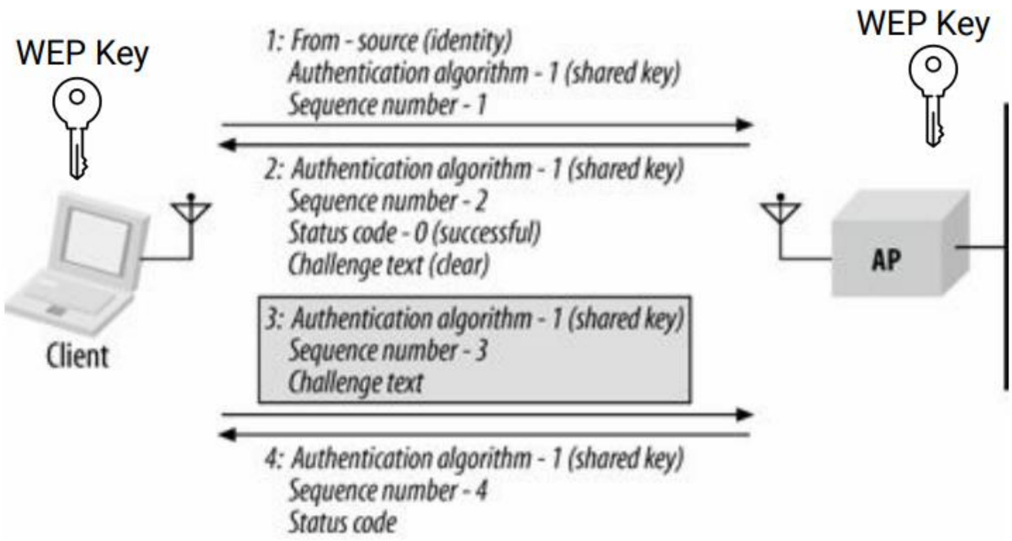
Base 802.11 Security: Open and Shared Key Authentication

1. Open System Authentication:
   a. The supplicant will send an Authentication request with Open security
   b. The AP acknowledge with an authentication response and then after associating the client, the data is transferred in plain text without any security.


1: From - source (identity)
Authentication algorithm - 0 (open system)
Sequence number - 1
2: Authentication algorithm - 0 (open system)
Sequence number - 2
Status code
Client
AP

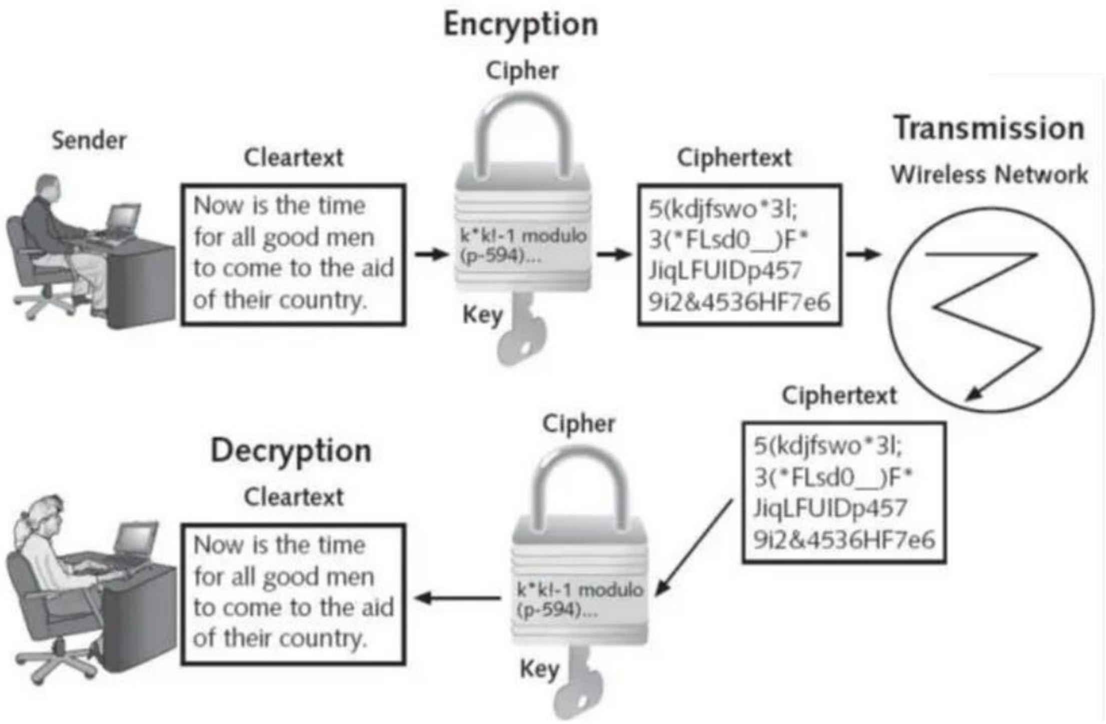
2. Shared Key Authentication – Uses WEP
   Wired networks are generally more secure than wireless networks because in wired setups, clients are physically connected and share data through that connection. In wireless networks, data can be intercepted by intruders within the network range. To address this, WEP (Wired Equivalent Privacy) was introduced to provide a level of privacy comparable to wired networks.

   Authentication and Encryption process:
   a. Both the client and the access point initially have the WEP key. The client then sends an authentication request with the algorithm set to 1, indicating shared key authentication.
   b. The access point responds by sending a challenge text to the client. The client uses its key to encrypt the challenge text sent by the access point and transmits it back to the access point.
   c. The access point decrypts the text using its own key. If the decrypted text matches the text previously sent by the access point, an acknowledgment is sent, and the client is authenticated.
   d. Subsequently, the transmitted data will be encrypted using the same key between the access point and the client.


WEP Key
1: From - source (identity)
Authentication algorithm - 1 (shared key)
Sequence number - 1
WEP Key
2: Authentication algorithm - 1 (shared key)
Sequence number - 2
Status code - 0 (successful)
Challenge text (clear)
AP
Client
3: Authentication algorithm - 1 (shared key)
Sequence number - 3
Challenge text
4: Authentication algorithm - 1 (shared key)
Sequence number - 4
Status code

What is a Key?

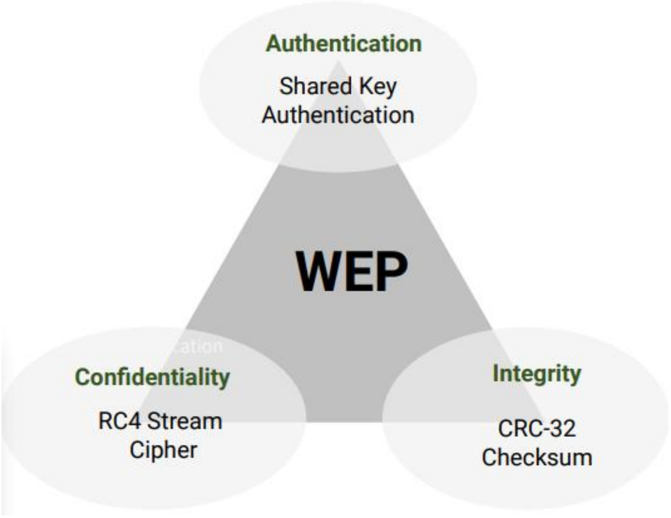
- A key is a sequence of bits/numbers that allows the user to encrypt and decrypt information.
- The key is only known to the sender and the receiver so the data transmitted cannot be understood by the intruder if he doesn't know the key to decrypt the data.


Encryption
Cipher
Sender
Cleartext
Now is the time for all good men to come to the aid of their country.
k*kl-1 modulo (p-594)...
Key
Ciphertext
5(kdjfswo*3l; 3(*FLsd0__)F* JiqLFUIDp457 9i2&4536HF7e6
Transmission
Wireless Network
Ciphertext
5(kdjfswo*3l; 3(*FLsd0__)F* JiqLFUIDp457 9i2&4536HF7e6
Cipher
Decryption
Cleartext
Now is the time for all good men to come to the aid of their country.
k*kl-1 modulo (p-594)...
Key

Wired Equivalent Privacy (WEP):

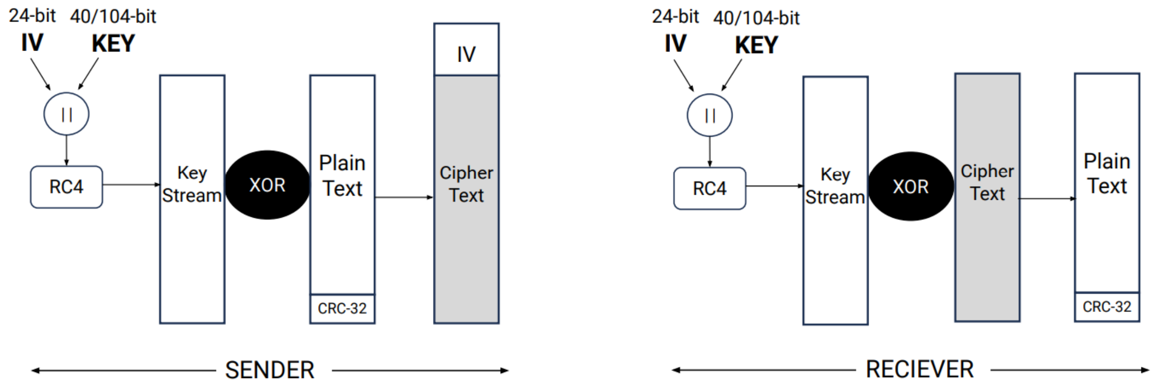
- Introduced in the base 802.11 standard to provide data confidentiality (encryption)
- It uses Encryption Keys to encrypt the data.

- A key is a sequence of bit of length that can be 40 or 104 bit long represented by 10 or 26 hex digits:
  - If 40-bit key is used then a 24 bit of Initialization vector is added and 64 bit is used (24 bit IV + 40 bit Key)
  - Similarly for 104-bit key a 24 bit of IV is added i.e., 128 bit is used (24 bit IV + 104 bit Key)
- IV (Initialization vector) is a random stream of 24 bits that is changed for each packet transmission and its primary purpose is to ensure that two packets don't have the same key stream so that the intruder doesn't be able to decrypt the packets easily.



WEP Encryption and Decryption Procedure:

1. The sender and receiver should have same base WEP key.
2. Initially to check the integrity of text, the CRC or checksum of the plain text is calculated and appended to the plain text, so that at the receiver the client can do reverse process and check the CRC to ensure the right message is received.
3. Then the encryption starts where the 24 bit that is unique for each packet and the 40 bit/ 104 bit base key are concatenated and run through an RC4 algorithm which is an encryption algorithm.
4. The RC4 algorithm creates a key stream which is in same length as the plain text including the CRC. The ex-or operation is done for key stream and the plain text that results in cipher text.
5. The cipher text and the IV in the plain text are sent to the receiver.
6. The receiver will take the IV from the packet received from the sender and as already it has the 40 bit /104 bit base key, it will concatenate and run through the RC4 algorithm to generate the key stream.
7. The ex-or operation is done for key stream and the cipher text received from the sender, resulting in the plain text including CRC.
8. The receiver will compute CRC and to check the integrity i.e., if the message received is correct.

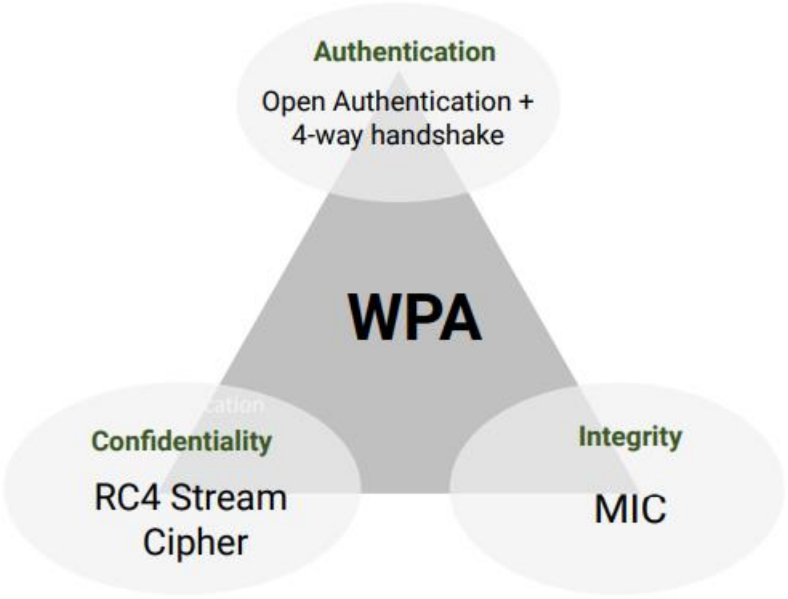


WEP Flaws:

1. Weak encryption: WEP uses a stream cipher called RC4, which is relatively weak and easy to crack.
2. Key reuse: WEP reuses the same encryption key for all packets, which makes it easier for attackers to crack the key.
3. Initialization vector (IV) gets reused for multiple packets over time, which can also be exploited by attackers.
4. For a 24-bit IV, there is 50% probability the same IV will repeat after 5,000 packets.
5. All the clients connecting to the access point have the same WEP key, so any other client can easily access the information of this client.

Wi-Fi Protected Access (WPA) – Personal:

1. WPA is intended to provide better security over WEP.
2. It was released as an intermediate solution and as a patchwork to overcome WEP weak securities.
3. Uses TKIP (Temporal Key Integrity Protocol) based on RC4 algorithm only but is a more robust technique compared to WEP.
4. Uses 48-bit IV, 64-bit key for authentication and 128-bit key for encryption so that cracking it would be more difficult.
5. Firmware upgrade is enough to use WPA instead of WEP and the user can enter a 8-64 bit ASCII value as the key.



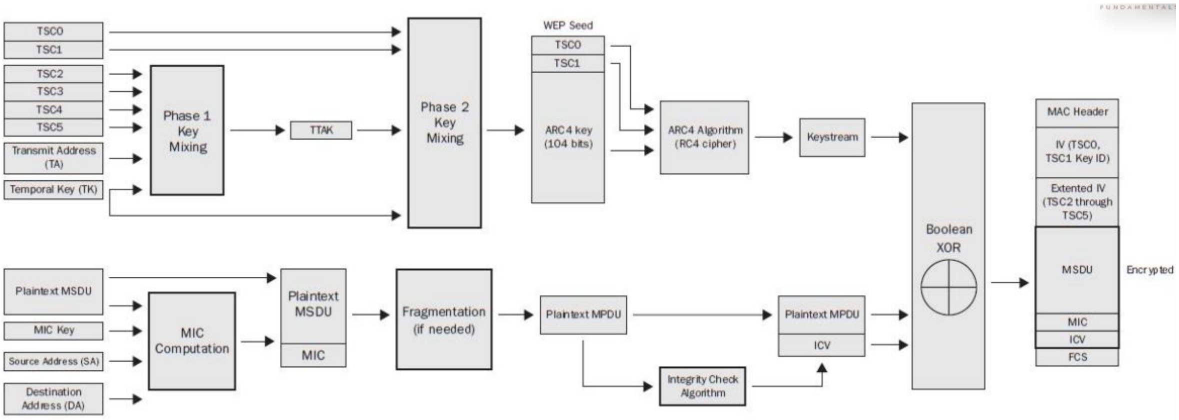
Improvements over WEP:

1. Unique per packet encryption keys is generated.
2. 48-bit Initialization Vector (IV) instead of 24 bit IV which removes the chance of repetition of IV.
3. Used Transmitter MAC as a part of the key to make the key unique for each Tx/Rx pair so each user connecting to same access point will have a different key generated while sharing information.
4. MIC (Message Integrity Check): MIC verifies the integrity of data packets to prevent attackers from modifying them and is more robust than CRC-32.

WPA Encryption Procedure:

1. TKIP use 2 phase key mixing process.
2. 48-bit TKIP Sequence Counter (TSC) is generated & broken into 6 octets (TSC0-TSC5)
3. Phase 1 key mixing us 128-bit temporal key (TK) with TSC2-TSC5 as well as Transmit Address (TA)
4. Output of phase 1 is known as TKIP-mixed transmit address & key (TTAK)
5. Phase 2 key mixing combines, TTAK with TSC0-TSC1 with 128-bit TK.
6. Output of the phase 2 is known as “WEP seed”.
7. WEP seed is then run through ARC4 algorithm & key stream is created.
8. WEP seed is represented as WEP Initialization Vector (IV) & 104-bit WEP keys.
9. Extend IV created by TSC2-5 of key mixing phase2.
10. IV & Extended IV (8 byte in total) called TKIP header.
11. TKIP uses Message Integrity Code (MIC) also named as “Michael”.
12. MIC is computed using Destination Address (DA), Source Address (SA), MSDU priority and plaintext Data.
13. TKIP MIC does not replace WEP ICV (32bit) but augments it.

14. WEP ICV helps prevent false detection of MIC failures that would cause TKIP countermeasure to be invoked.
15. MPDU+MIC+ICV used to perform XOR with Keystream to generated encrypted payload.
16. Frame Check Sequence (FCS) is calculated over all the header & entire frame body resulting 32bit CRC placed in FCS field.
17. Before MIC verification, receiving STA check FCS, ICV & TSC of all MPDU.

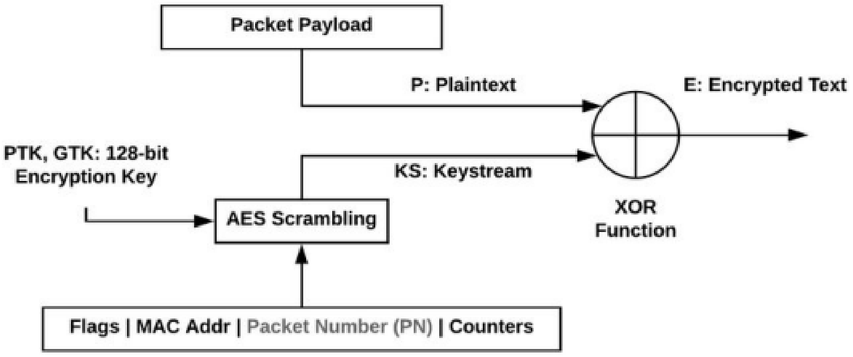


Wi-Fi Protected Access2 (WPA2) Personal:

1. Uses Advanced Encryption Standard (AES) for encryption.
2. Unlike WPA, this needs hardware support and uses 128-bit key for data encryption.
3. CBC-MAC (Cipher Block Chaining Message Authentication Code) mode is used to calculate the MIC.
4. Packet Number is used to prevent replay attacks.
5. CCM use new temporal key for each session.
6. APs can support WPA+WPA2 modes for backward compatibility.

In APs the Encryption type can be selected as the WPA2-PSK i.e., WPA2 Pre-Shared Key which is used for residential Wi-Fi. The passphrase (i.e., the base key) is to be given which is used to create the temporal keys, session keys. WPA2 APs mostly support backward compatible i.e., the clients that doesn't support WPA2 connect to WPA.

WPA2 Encryption Procedure:

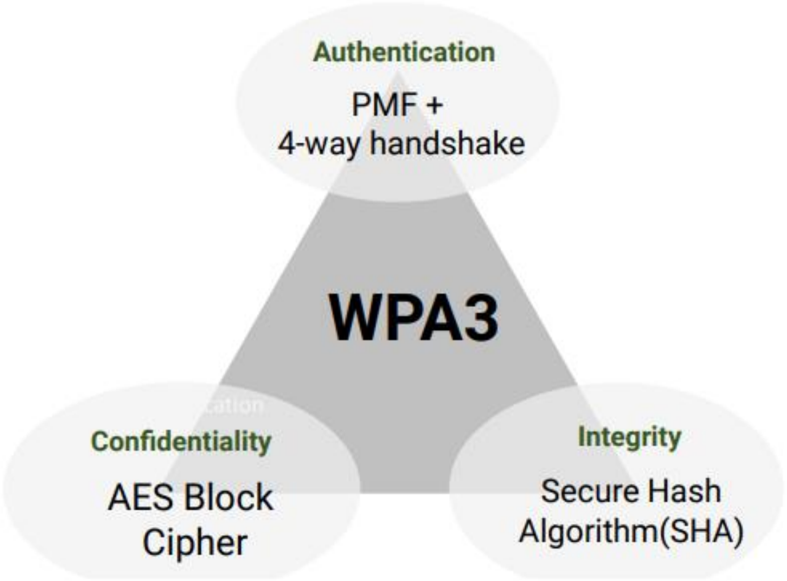


1. Passphrase (the base key) is known to both AP and supplicant. And then the client and the AP get authenticated to each other.
2. PSK Gets generated from the Passphrase and the SSID, then PMK (Pairwise Master Key) will be generated by some function using PSK, SSID etc.
3. A 4-way handshake procedure is done to generate the PTK, MTK, GTK keys that will be used for encryption.
4. Then PTK (Pairwise Transient Key) is generated with some pseudo random function using PMK, ANonce, SNonce, supplicant (client) MAC address and the Authenticator (Access Point) MAC address.
5. The ANonce and Snonce are shared by AP and client during a 4-way handshake procedure to derive the PTK.

Wi-Fi Protected Access3 (WPA3) Personal:

After a long time of WPA2 implementation, WPA3 was introduced which used more advanced algorithms to provide better security.

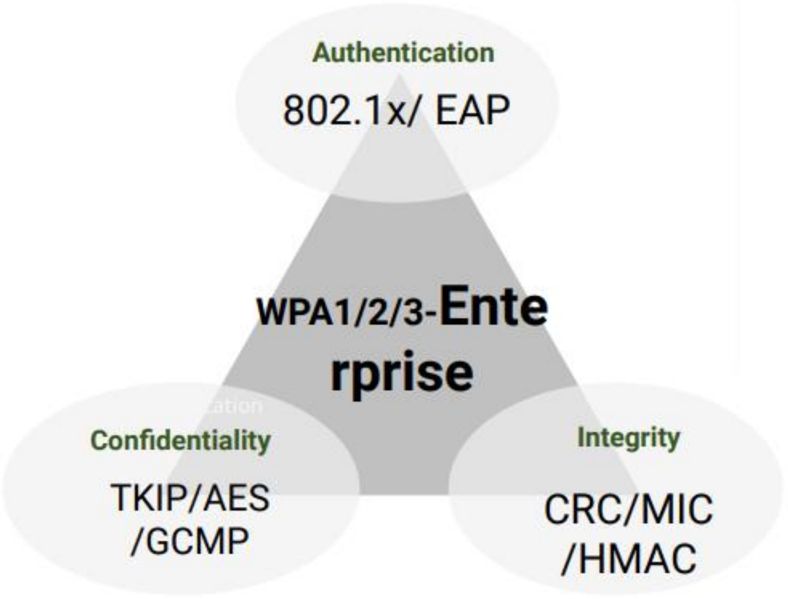
1. It uses GCMP (Galois/Counter Mode Protocol)
2. It uses 128/192/256-bit keys for data encryption and 384-bit Hashed-based Message Authentication Code (HMAC)
3. 256-bit Broadcast/Multicast Integrity Protocol (BIP-GMAC-256) is used.
4. A unique session key is generated for every individual session a user initiates.
5. As a part of WPA3 there is a mechanism called OWE which also helps in encrypting data in open networks i.e., providing enhanced open security with OWE.



Key features of WPA3:

1. Mandates PMF (Protected Management Frames) for protecting Management frames from other users that can avoid few attacks like Denial of Service attacks etc.
2. Replaces PSK (Pre-Shared Key) with SAE (Simultaneous Authentication of Equals) which is more secure to offline dictionary attacks.
3. Transition mode is a mixed mode that enables the use of WPA2 to connect clients that don't support WPA3.

Personal to Enterprise security:

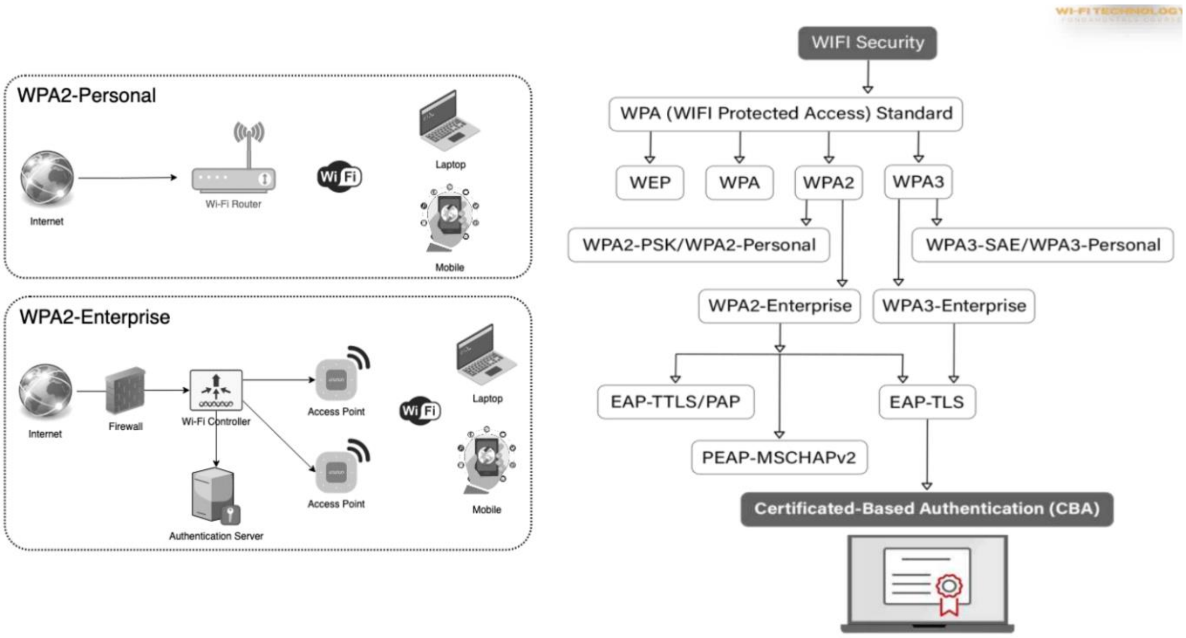


1. The encryption used will be WPA, WPA2 and WPA3 but the authentication will be done by the authentication server which involves auto-generation of keys etc.

2. The authentication aspect is handles by the authentication server on the enterprise network with the APs acting as relays.
3. Usually, the authentication is tied up with other IT systems like Active Directory services, authorization, and accounting operations.
4. Authentication is user based and there is no need to manually enter any security keys in the AP or the station.
5. Enterprise security is easily extensible to large scale deployments.

Summary of various authentication / encryption methods:

1. Initially WEP was used for encryption, later on WPA was introduced to make the network more secure compared to WEP but still used same RC4 algorithm as WEP.
2. Later years to provide more robust security WPA2, and WPA3 were introduced with more advanced algorithms which supported both personal and enterprise networks.



	WEP	WPA	WPA2	WPA3
Release Year	1999	2003	2004	2018
Encryption Method	Rivest Cipher 4 (RC4)	Temporal Key Integrity Protocol with RC4	CCMP and Standard Encryption Standard	Advanced Encryption Standard (AES)
Session Key Size	40-bit	128-bit	128-bit	128-bit (WPA3-Personal) 192-bit (WPA3-Enterprise)

Cipher Type	Stream	Stream	Block	Block
Data Integrity	CRC-32	Message Integrity Code	CBC-MAC	Secure Hash algorithm
Key Management	Not provided	4-way handshaking mechanism	4-way handshaking mechanism	Simultaneous Authentication of Equals handshake
Authentication	WPE-Open WPE- Shared	Pre-Shared key (PSK) & 802.1x with EAP variant	Pre-Shared key (PSK) & 802.1x with EAP variant	Simultaneous Authentication of Equals (SAE) with EAP variant