Wireless Network Security Overview

Chun-Jen (James) Chung

Arizona State University

Outline

- Describe the basic IEEE 802.11 wireless security protections
- Define the vulnerabilities of open system authentication, WEP, and device authentication
- Describe the WPA and WPA2 personal security models
- Explain how enterprises can implement wireless security

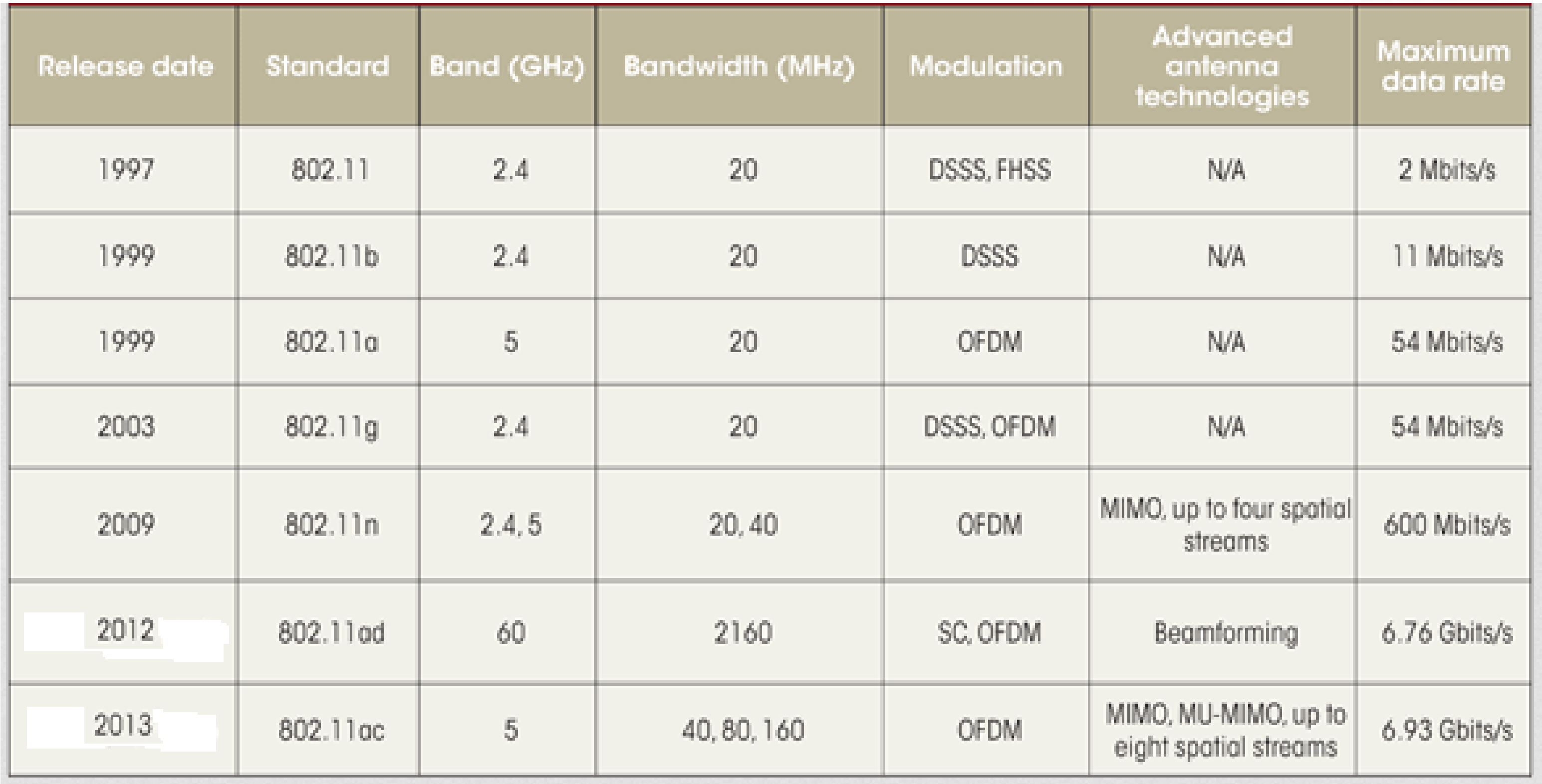
IEEE 802.11 Wireless Security Protections

IEEE 802

- In the early 1980s, the IEEE (Institute of Electrical and Electronics Engineers) began work on developing computer network architecture standards
  - This work was called Project 802, and maintained by the IEEE 802 LAN/MAN Standards Committee (LMSC)
  - The standards dealing with LANs and MANs
    - Such as Ethernet family, Token Ring, WLAN, Bridging
- In 1990, the IEEE formed a committee to develop standards for WLANs (Wireless Local Area Networks)
  - The 802.11 family consists of a series of *half-duplex* over-the-air modulation techniques that use the same basic protocol.

IEEE 802.11 WLAN Standard

- In 1997, the IEEE approved the IEEE 802.11 WLAN standard



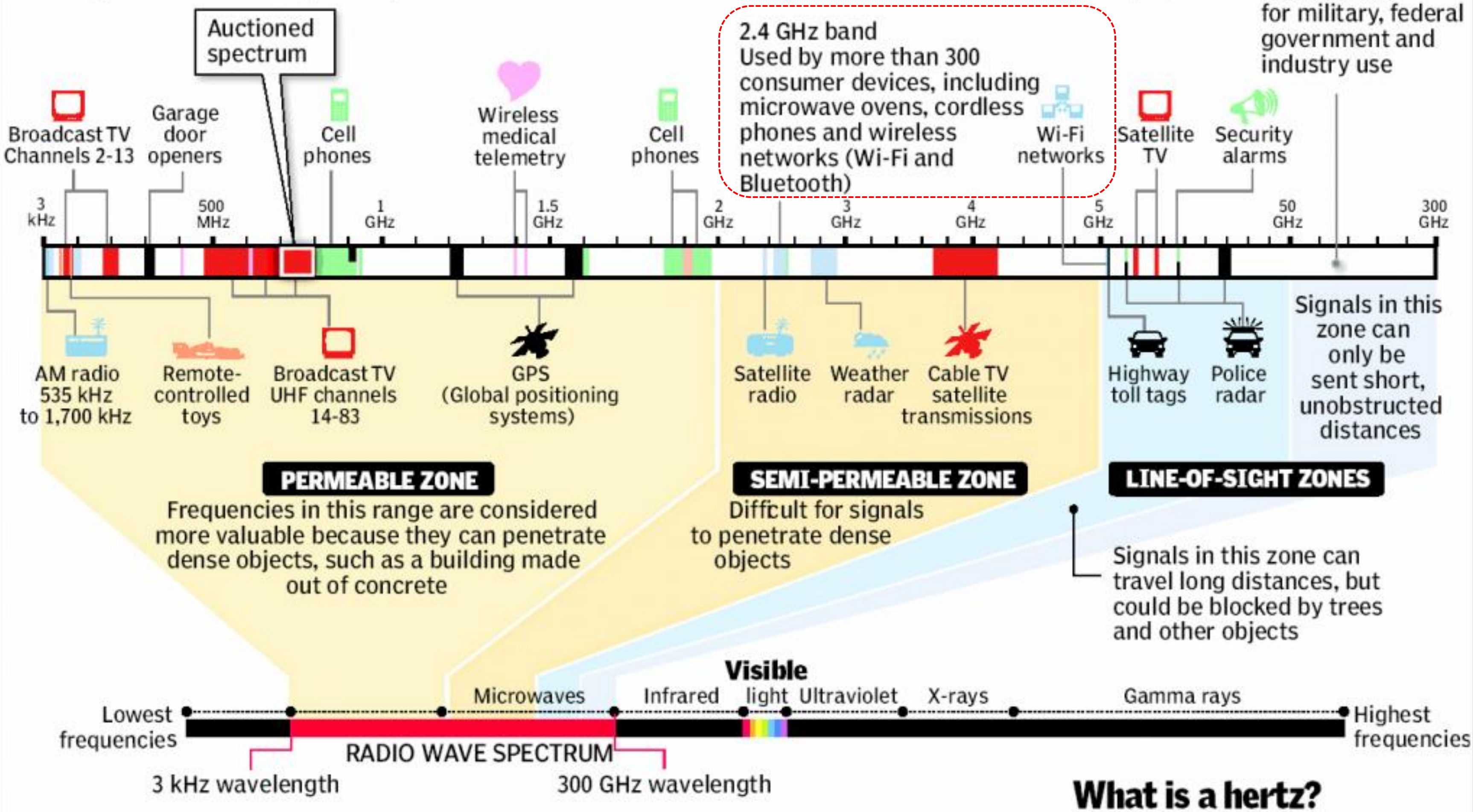
Release date	Standard	Band (GHz)	Bandwidth (MHz)	Modulation	Advanced antenna technologies	Maximum data rate
1997	802.11	2.4	20	DSSS, FHSS	N/A	2 Mbits/s
1999	802.11b	2.4	20	DSSS	N/A	11 Mbits/s
1999	802.11a	5	20	OFDM	N/A	54 Mbits/s
2003	802.11g	2.4	20	DSSS, OFDM	N/A	54 Mbits/s
2009	802.11n	2.4, 5	20, 40	OFDM	MIMO, up to four spatial streams	600 Mbits/s
2012	802.11ad	60	2160	SC, OFDM	Beamforming	6.76 Gbits/s
2013	802.11ac	5	40, 80, 160	OFDM	MIMO, MU-MIMO, up to eight spatial streams	6.93 Gbits/s

Information about 802.11 family. http://en.wikipedia.org/wiki/802.11

Inside the radio wave spectrum

Almost every wireless technology – from cell phones to garage door openers – uses radio waves to communicate. Some services, such as TV and radio broadcasts, have exclusive use of their frequency within a geographic area. But many devices share frequencies, which can cause interference. Examples of radio waves used by everyday devices:

Most of the white areas on this chart are reserved for military, federal government and industry use



2.4 GHz band
Used by more than 300 consumer devices, including microwave ovens, cordless phones and wireless networks (Wi-Fi and Bluetooth)

Signals in this zone can only be sent short, unobstructed distances

PERMEABLE ZONE

Frequencies in this range are considered more valuable because they can penetrate dense objects, such as a building made out of concrete

SEMI-PERMEABLE ZONE

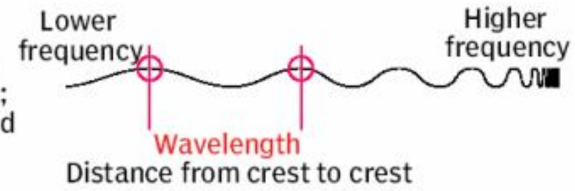
Difficult for signals to penetrate dense objects

LINE-OF-SIGHT ZONES

Signals in this zone can travel long distances, but could be blocked by trees and other objects

The electromagnetic spectrum

Radio waves occupy part of the electromagnetic spectrum, a range of electric and magnetic waves of different lengths that travel at the speed of light; other parts of the spectrum include visible light and x-rays; the shortest wavelengths have the highest frequency, measured in hertz



What is a hertz?

One hertz is one cycle per second. For radio waves, a cycle is the distance from wave crest to crest

1 kilohertz (kHz) = 1,000 hertz

1 megahertz (MHz) = 1 million hertz

1 gigahertz (GHz) = 1 billion hertz

Source: New America Foundation, MCT, Howstuffworks.com
Graphic: Nathaniel Levine, Sacramento Bee

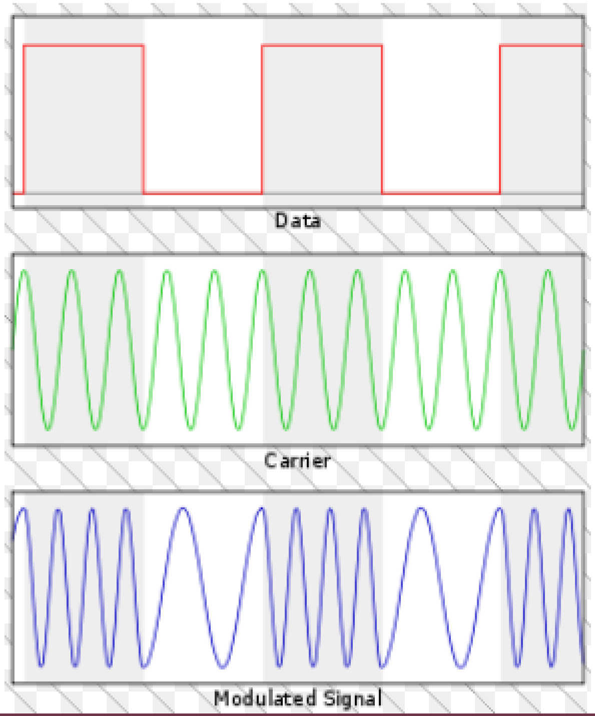
Modulation

- The process of impressing the data (0/1) to be transmitted on the radio carrier.
- The goal of modulation is to squeeze as much data into the least amount of spectrum possible.

Basdband signal pulse (0 and 1)

Carrier radio-frequency signal
(a sine wave)

Modulating the amplitude, frequency, and phase of the carrier



Digital Modulation Techniques

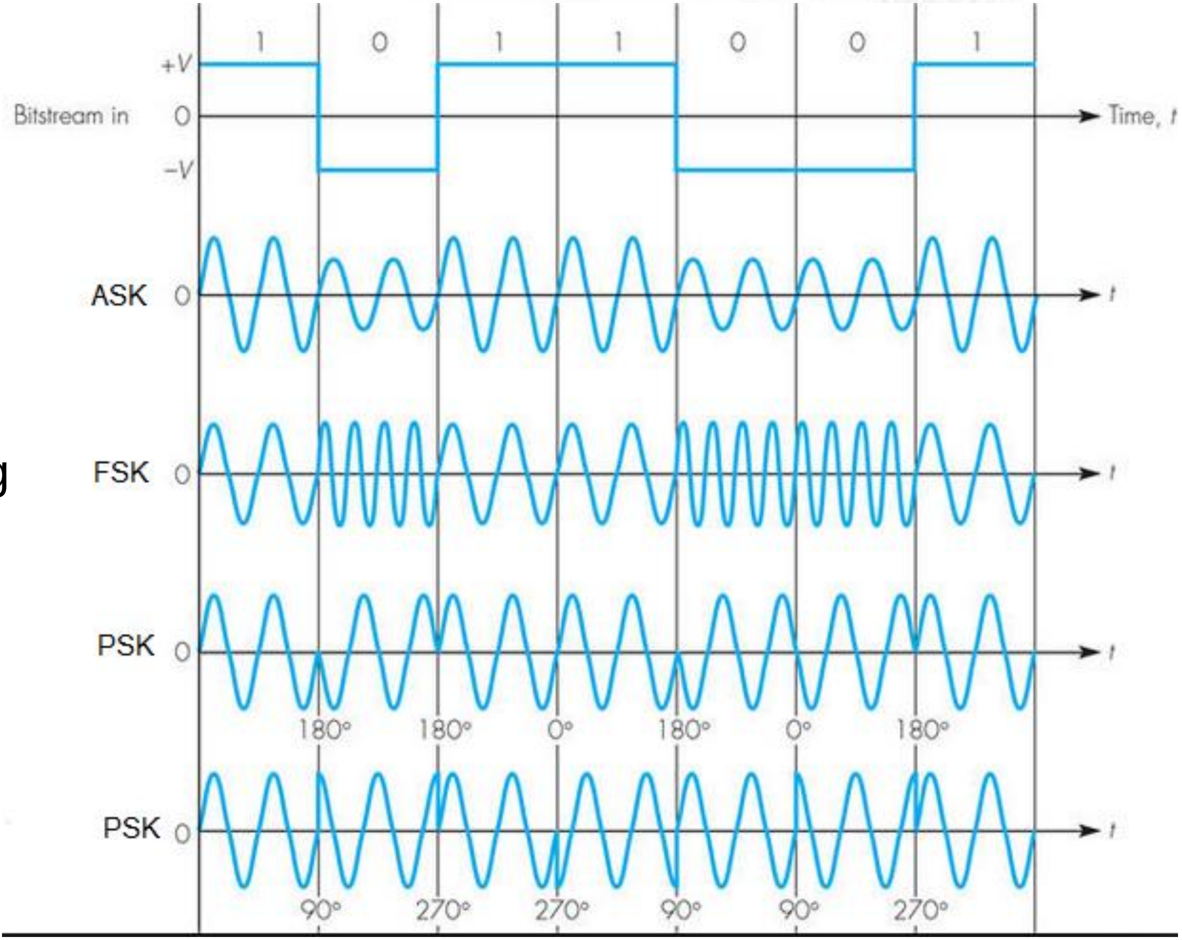
A sine wave:

$A\cos(\omega t + \theta)$

Amplitude Shifting Keying

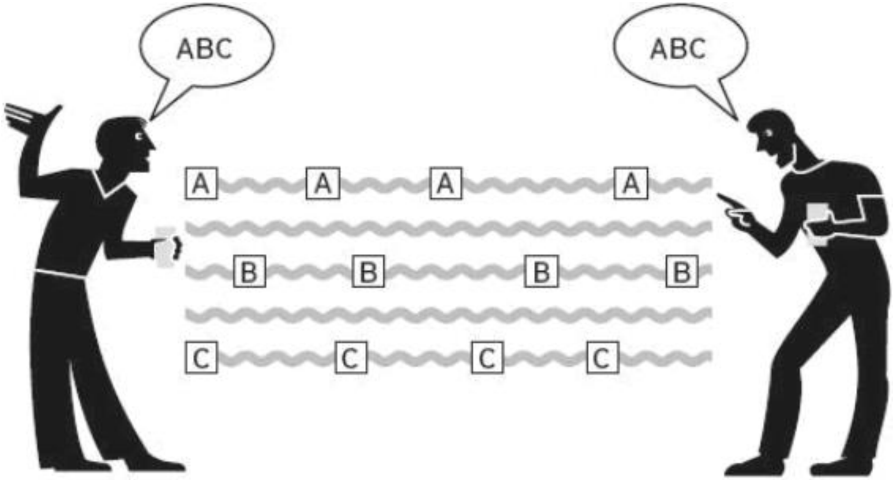
Frequency Shifting Keying

Phase Shifting Keying



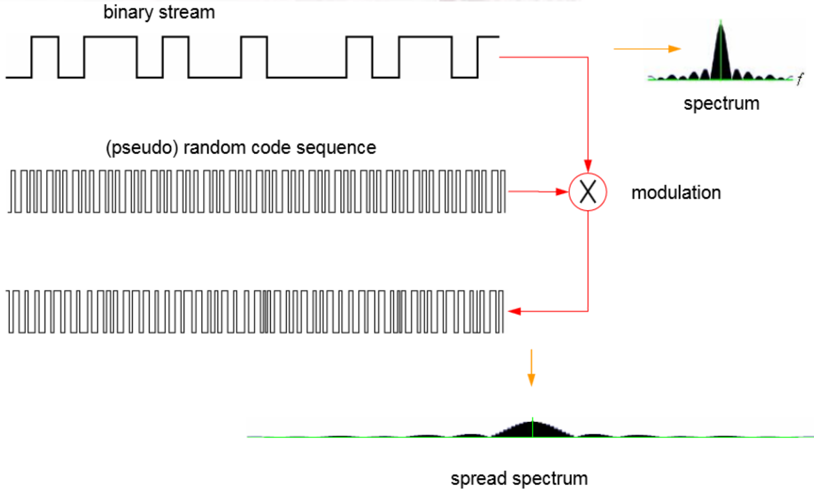
Spread Spectrum (SS)

- A signal (e.g. an electrical, electromagnetic, or acoustic signal) generated with a particular bandwidth is *deliberately* ***spread*** in the frequency domain, resulting in a signal with *a wider bandwidth*.
- These techniques are used for a variety of reasons
  - establishing secure communications
  - increasing resistance to natural interference, noise and jamming
  - preventing the detection
  - multiplexing



In spread-spectrum communication, low-power radio transmitters divide their signals into coded packets across a range of frequencies and receivers reconstruct the message.

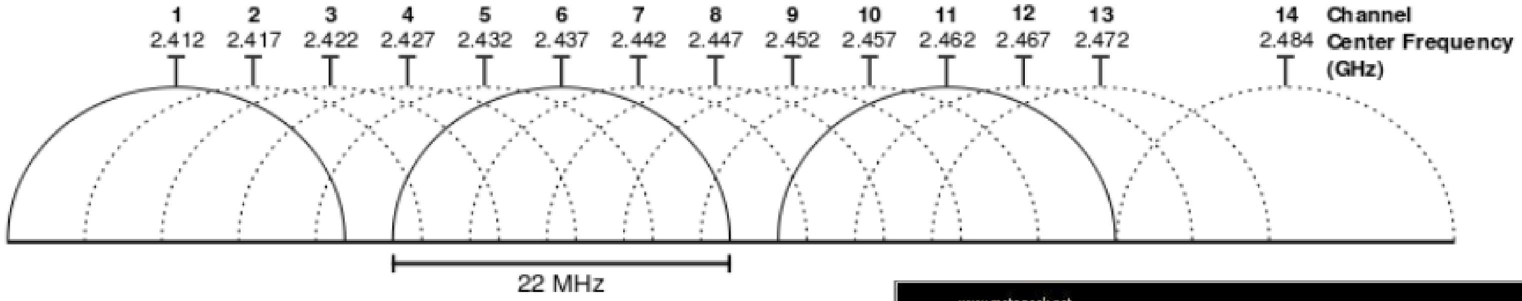
Spread Spectrum Modulation

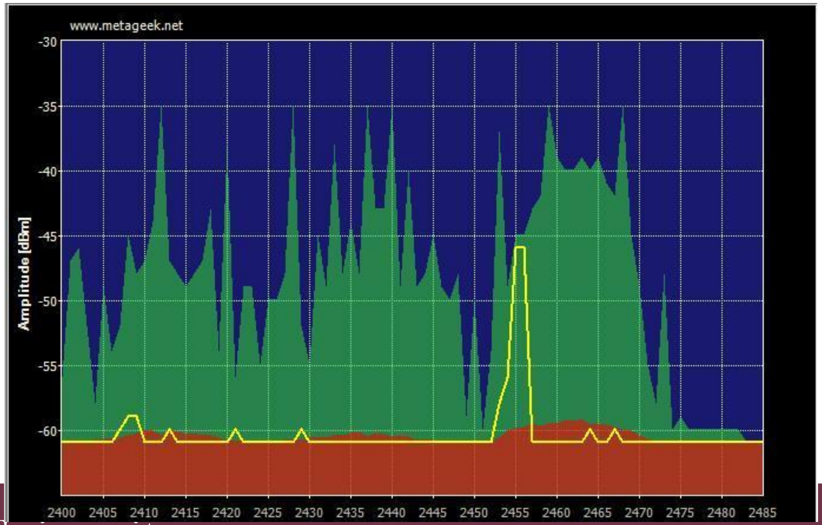


- Direct-Sequence Spread Spectrum (DSSS)
  - multiply the data being transmitted by a "noise" signal.
  - This noise signal is a *pseudorandom sequence* of 1 and −1 values, at a frequency much higher than that of the original signal.
- Frequency-Hopping Spread Spectrum (FHSS)
  - use a small frequency bandwidth to communicate and then *hop* to another frequency and then another until a hopping pattern known as a hopping sequence has been completed.
- Orthogonal Frequency-Division Multiplexing (OFDM)
  - splits a high speed information signal into multiple lower speed information signals and then transmits these lower speed signals in parallel.
- Time-Hopping Spread Spectrum (THSS)

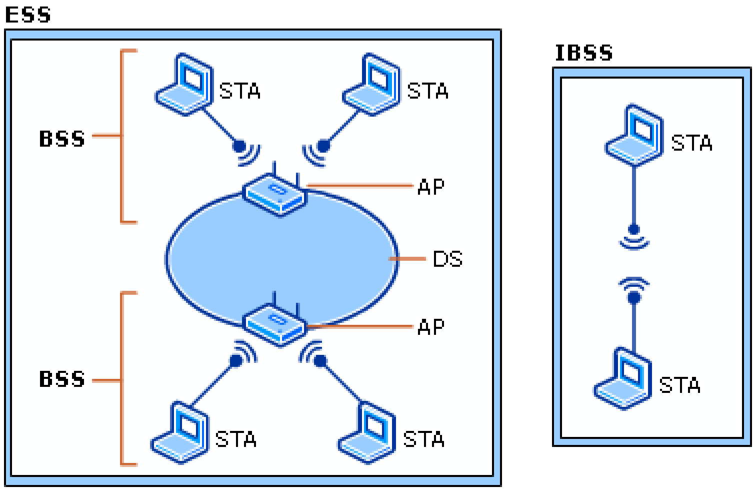
WLAN Channels & Frequencies

- Each spectrum is sub-divided into channels with a center frequency and bandwidth, analogous to the way radio and TV broadcast bands are sub-divided.





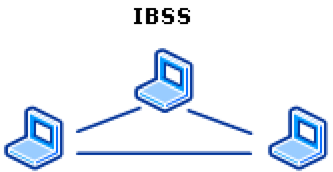
IEEE 802.11 Architecture

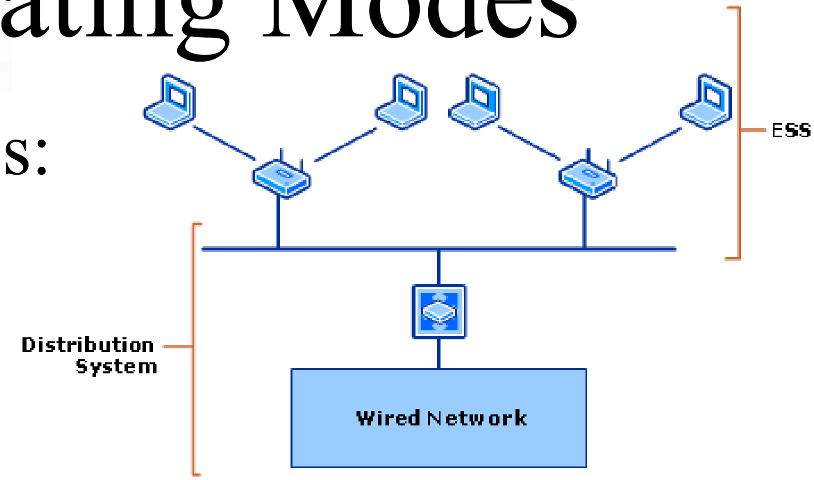


- *Station (STA)*: an adapter card, PC Card, or an embedded device to provide wireless connectivity.
- *Wireless Access Point (AP)*: functions as a bridge between wireless STAs and existing network backbone for network access.
- *Basic Service Set (BSS)*: a wireless network, consisting of a *single wireless AP* supporting one or multiple wireless clients.
- *Extended Service Set (ESS)*: a set of two or more wireless APs connected to the same wired network that bounded by a router (also known as a *subnet*).
- *Distribution System (DS)*: a logical component used to interconnect BSSs.
- *Independent Basic Service set (IBSS)*: a wireless network, consisting of at least two STAs, used where no access to a DS is available. An IBSS is also sometimes referred to as an *ad hoc wireless network*.

IEEE 802.11 Operating Modes

- IEEE 802.11 two operating modes:
  - Infrastructure mode
  - Ad hoc mode

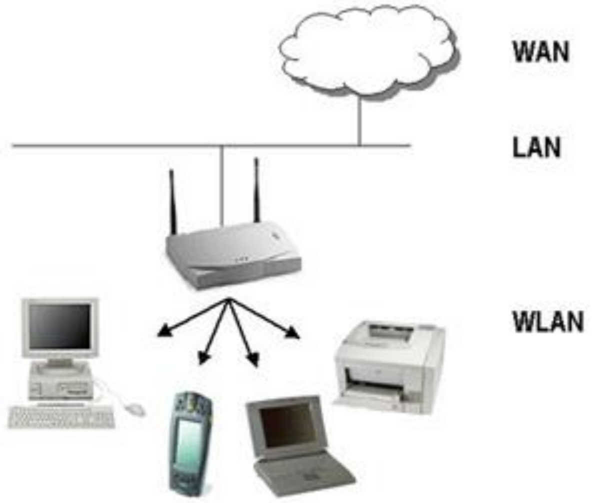




- In both operating modes,
  - Service Set Identifier (SSID), also known as the *wireless network name*, identifies the wireless network.
    - The *SSID* is a name configured on the wireless AP (for infrastructure mode) or an initial wireless client (for ad hoc mode) that identifies the wireless network.
    - The SSID is periodically advertised by the wireless AP or the initial wireless client using a special 802.11 MAC management frame known as a *beacon frame*.

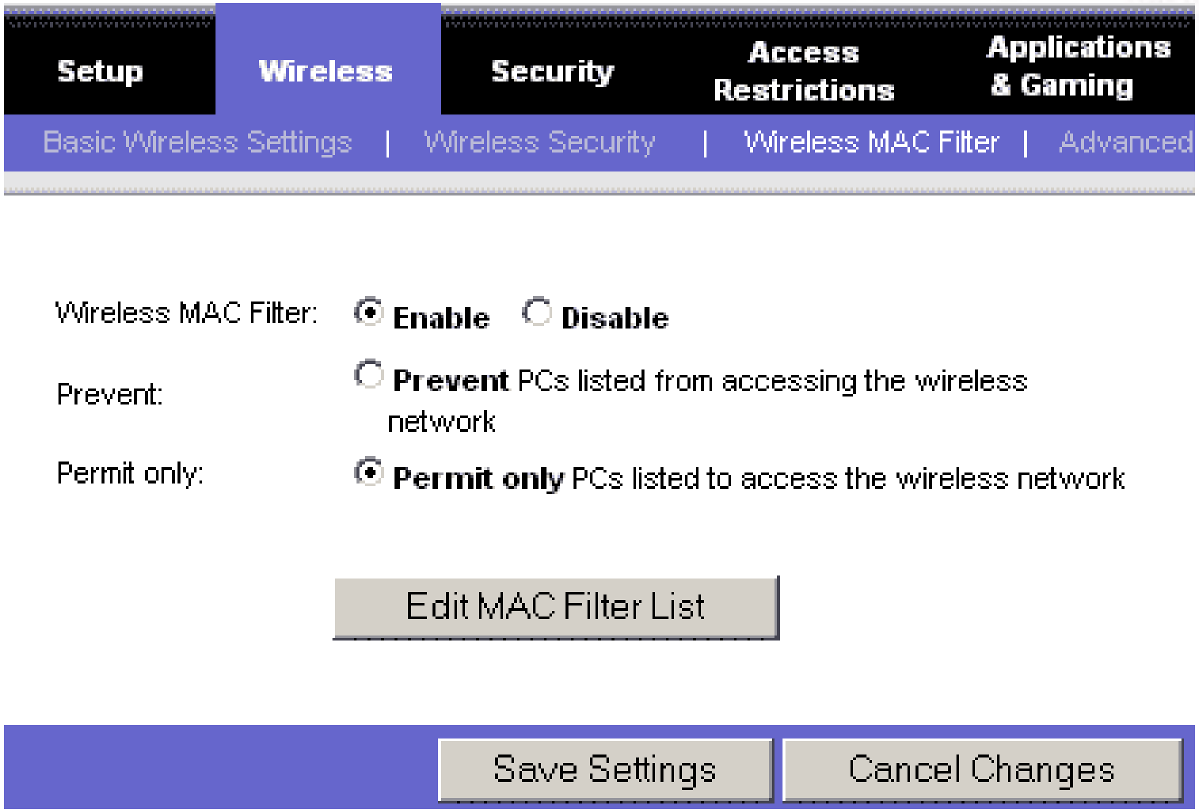
Controlling Access to a WLAN

- Access is controlled by limiting a device's access to the *access point (AP)*
- Only devices that are authorized can connect to the AP
  - Media Access Control (MAC) address filtering
  - Shared key for mutual authentication.



Access points wirelessly transmit data to and from network devices, connect wireless devices to the wired LAN, and the internet.

MAC Address Filtering



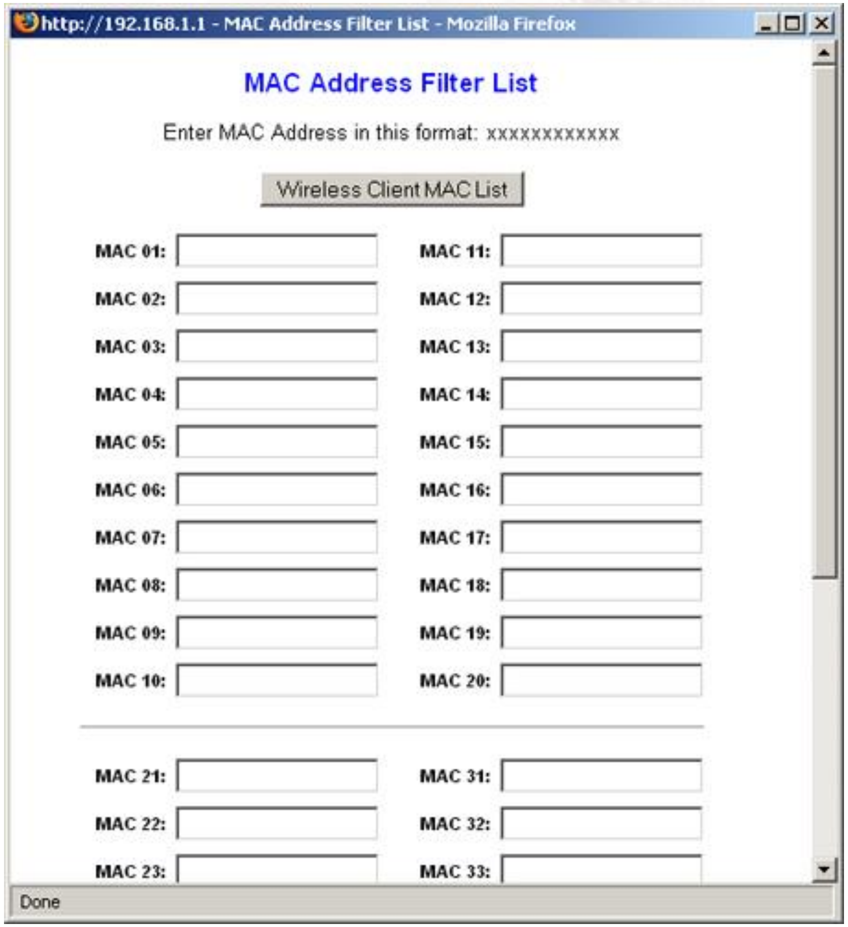
Wireless MAC Filter: ● **Enable** ○ **Disable**

Prevent: ○ **Prevent** PCs listed from accessing the wireless network

Permit only: ● **Permit only** PCs listed to access the wireless network

MAC Address Filtering

- Usually implemented by *permitting* instead of preventing



http://192.168.1.1 - MAC Address Filter List - Mozilla Firefox

MAC Address Filter List

Enter MAC Address in this format: xxxxxxxxxxxx

MAC 01:		MAC 11:	
MAC 02:		MAC 12:	
MAC 03:		MAC 13:	
MAC 04:		MAC 14:	
MAC 05:		MAC 15:	
MAC 06:		MAC 16:	
MAC 07:		MAC 17:	
MAC 08:		MAC 18:	
MAC 09:		MAC 19:	
MAC 10:		MAC 20:	
MAC 21:		MAC 31:	
MAC 22:		MAC 32:	
MAC 23:		MAC 33:	

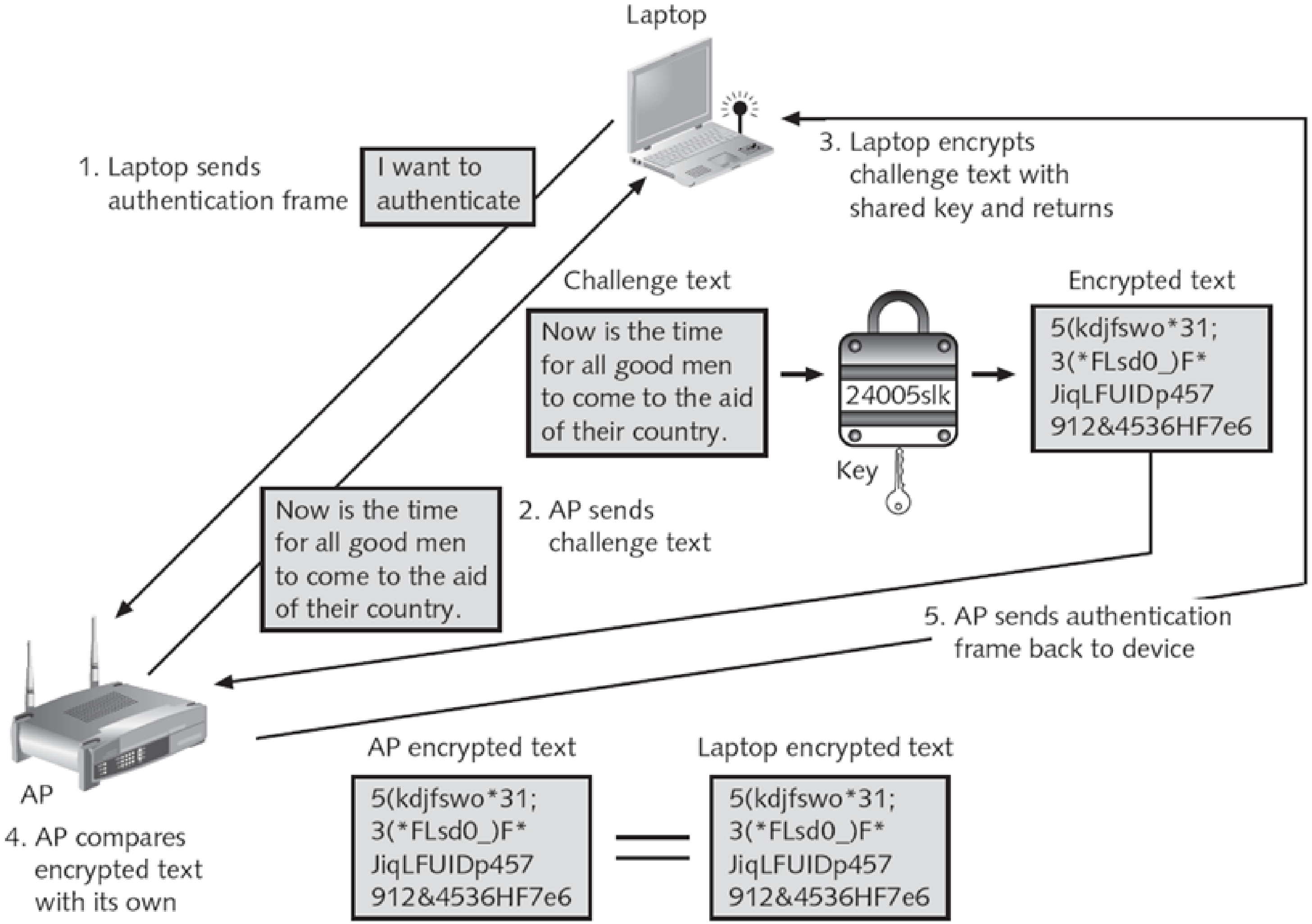
MAC Address Filtering Weaknesses

- MAC addresses are transmitted in the *clear text*
  - An attacker can just sniff for MACs
- Managing a large number of MAC addresses is difficult
- MAC address filtering does not provide a means to *temporarily* allow a guest user to access the network
  - Other than manually entering the user's MAC address into the access point

Device Authentication

- Before a computer can connect to a WLAN, it must be ***authenticated***
- Types of authentication in 802.11
  - **Shared key authentication**
    - Only lets computers in if they know the **shared key**
    - Through challenge/response messages exchange
  - **Open system authentication**
    - Lets everyone in
    - Do not involve challenge/response

Shared Key Authentication



Laptop

1. Laptop sends authentication frame

I want to authenticate

2. AP sends challenge text

Now is the time for all good men to come to the aid of their country.

3. Laptop encrypts challenge text with shared key and returns

Challenge text

Now is the time for all good men to come to the aid of their country.

24005slk

Key

Encrypted text

5(kdjfswo*31;
3(*FLsd0_)F*
JiqLFUIDp457
912&4536HF7e6

4. AP compares encrypted text with its own

AP

AP encrypted text

5(kdjfswo*31;
3(*FLsd0_)F*
JiqLFUIDp457
912&4536HF7e6

=

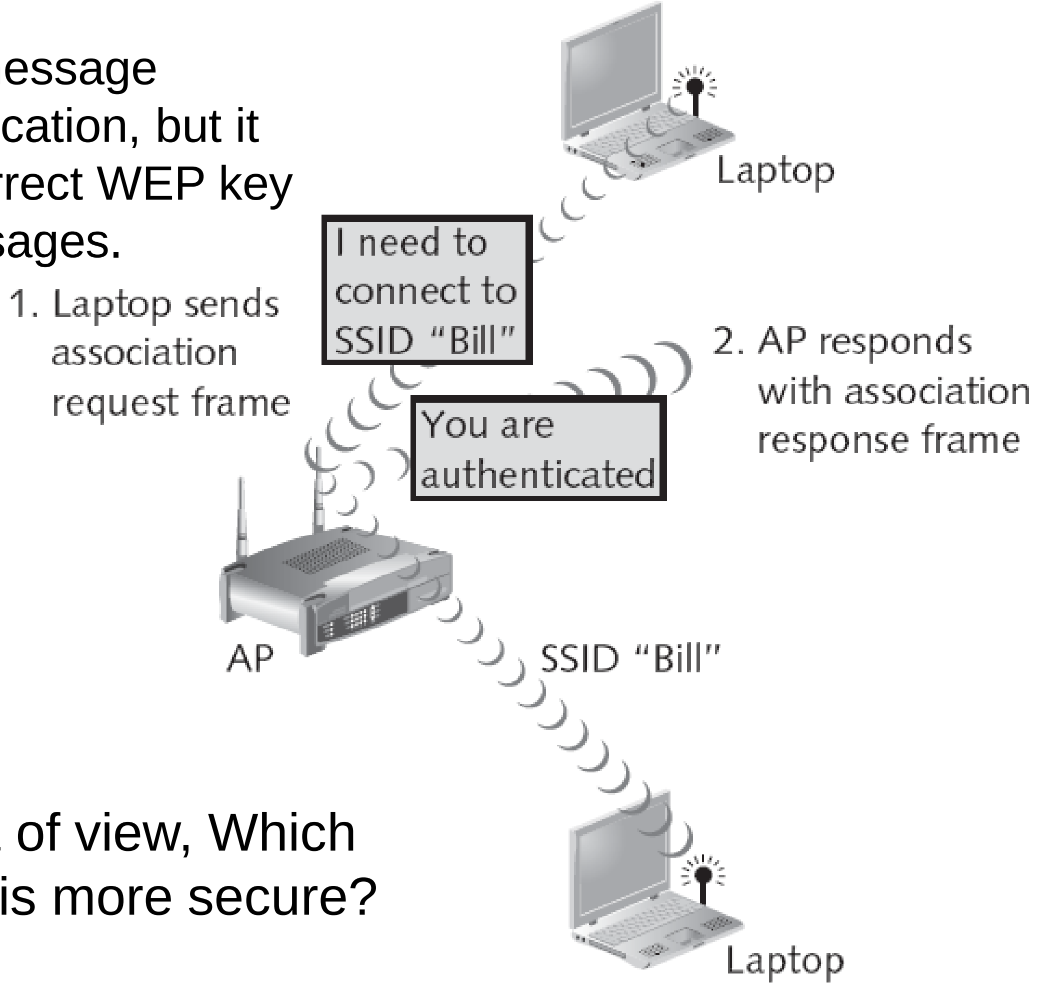
Laptop encrypted text

5(kdjfswo*31;
3(*FLsd0_)F*
JiqLFUIDp457
912&4536HF7e6

5. AP sends authentication frame back to device

Open System Authentication

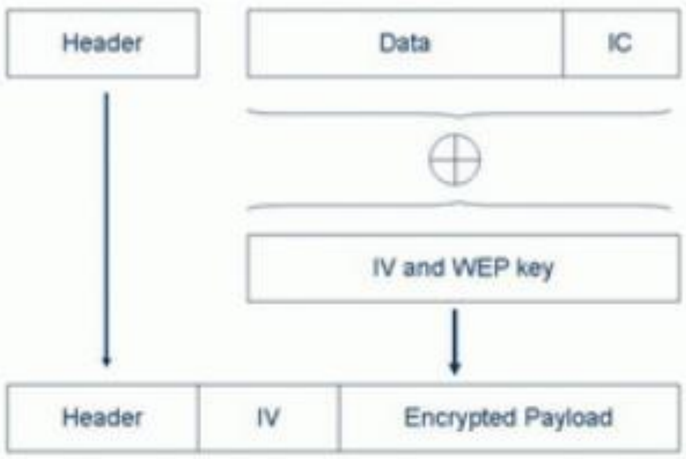
No challenge/response message exchange for the authentication, but it still needs to have the correct WEP key to send and receive messages.


Laptop
I need to connect to SSID "Bill"
1. Laptop sends association request frame
2. AP responds with association response frame
You are authenticated
AP
SSID "Bill"
Laptop

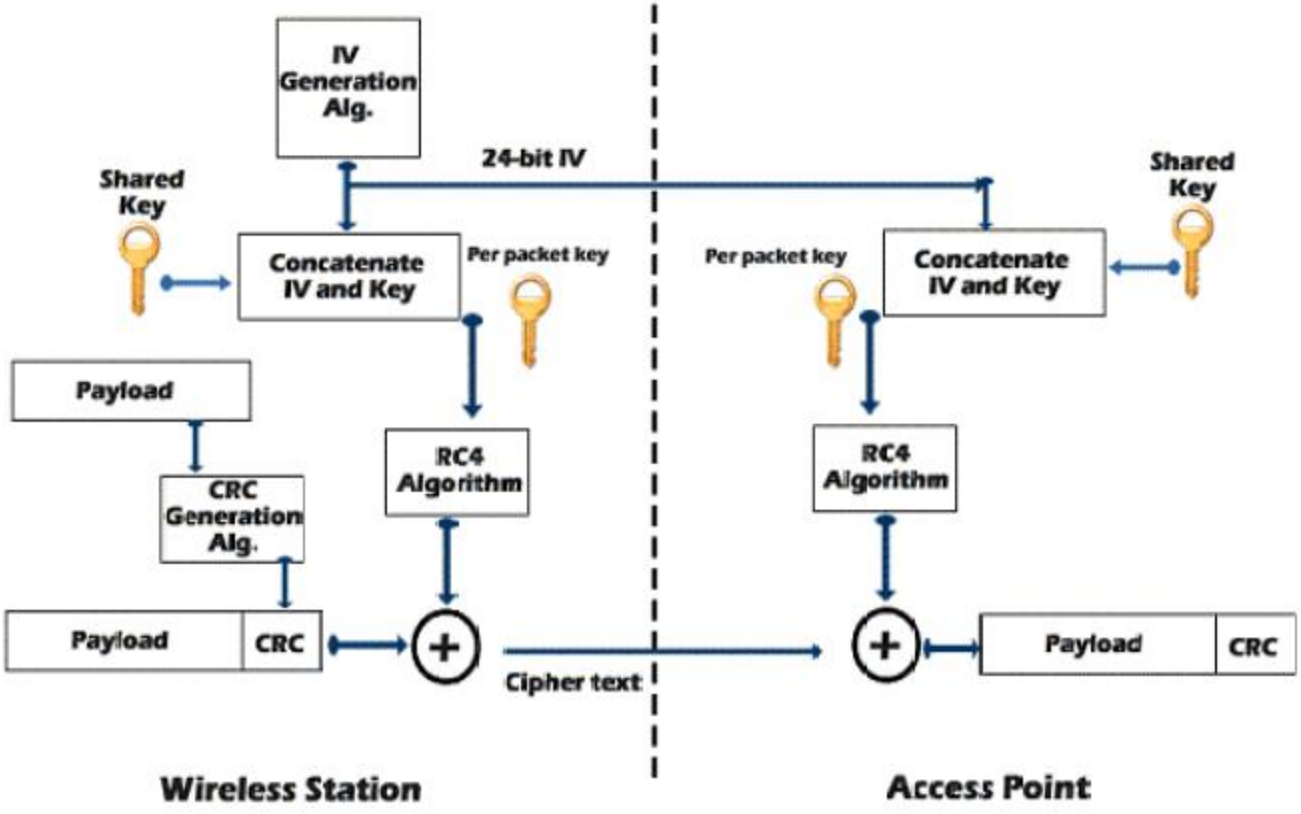
From the security point of view, Which authentication method is more secure?

Wired Equivalent Privacy (WEP)

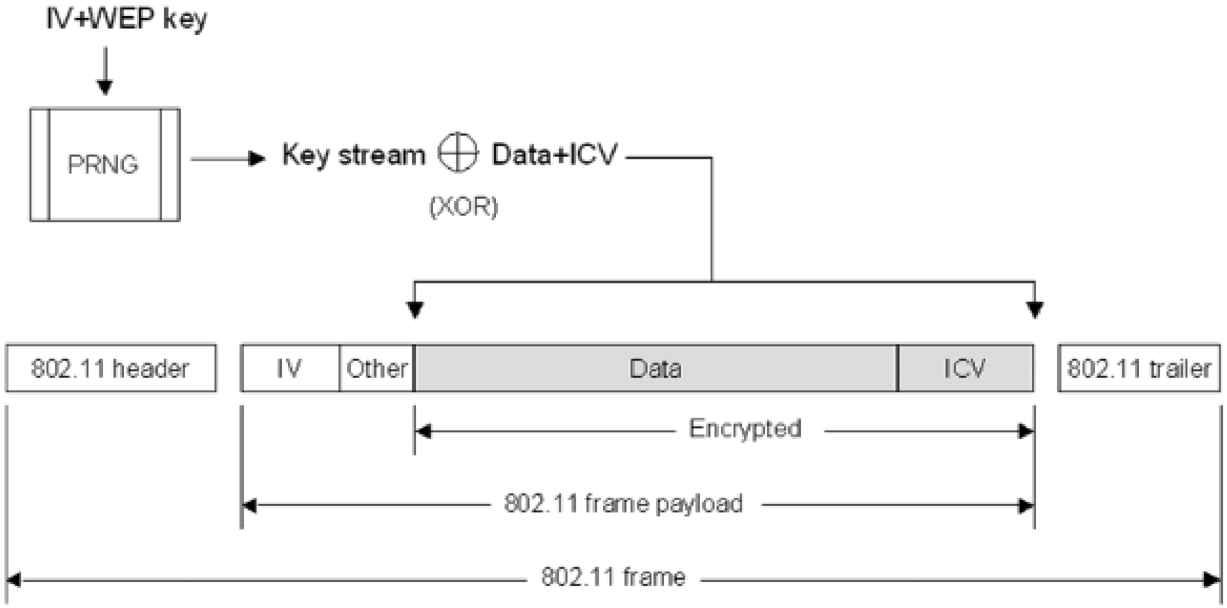
- Designed to ensure that *only authorized parties* can view transmitted wireless information
- Uses *encryption* to protect traffic and provide confidentiality
- WEP uses RC4 (stream cipher) for the encryption purposes.
  - Require a seed value (Initialization Vector, IV) to start its key stream generator.
  - The IV and the shared WEP key are used to encrypt/decrypt transferred packets.



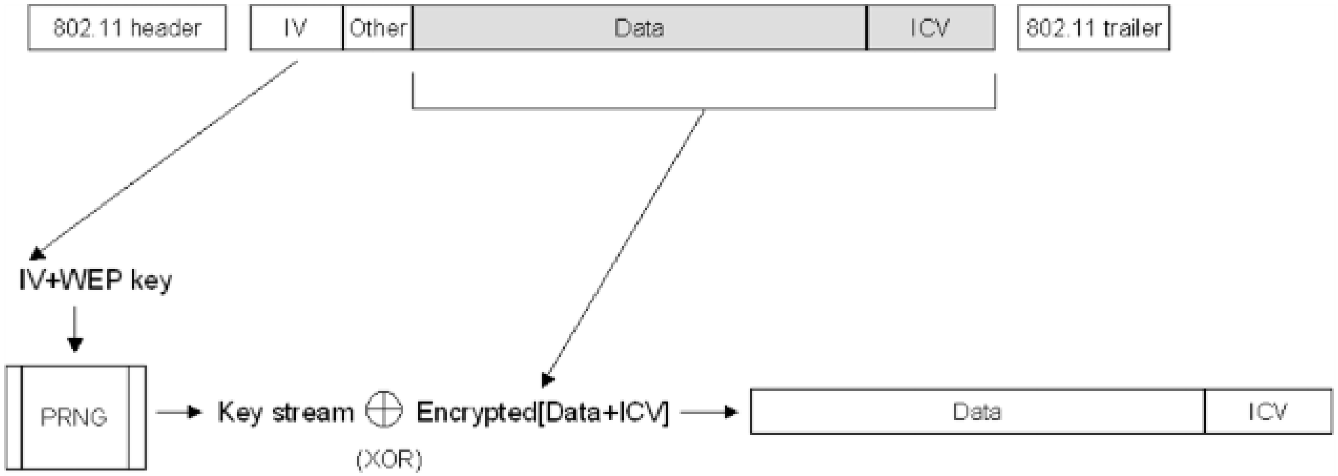
WEP Encryption Process



WEP Encryption

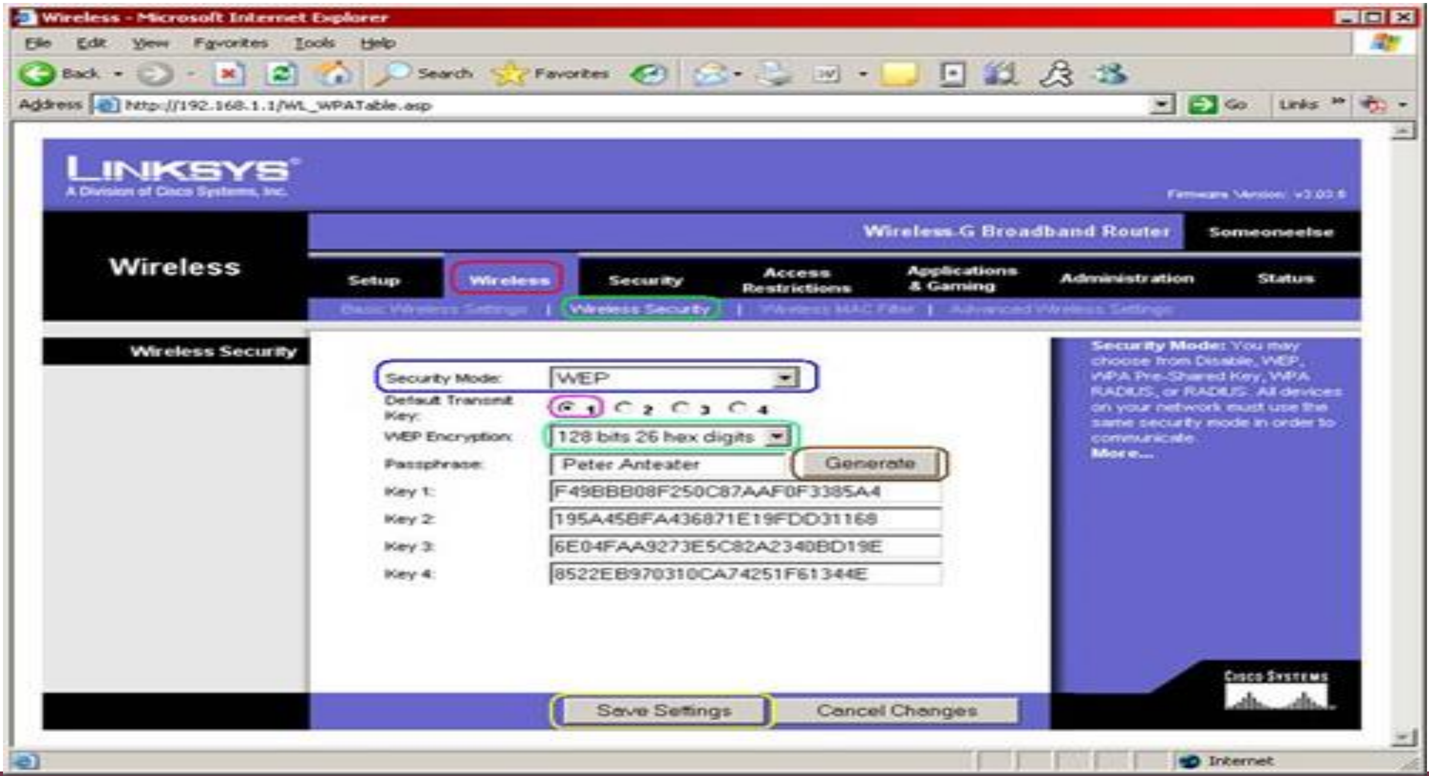


WEP Decryption



WEP Keys

- WEP secret keys can be 64 or 128 bits long
- The AP and devices can hold up to *four* shared secret keys
  - One of which must be designated as the *default key*


Wireless - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.1/WL_WPATable.asp
Go Links
LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: v3.03.6
Wireless-G Broadband Router
Someoneelse
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings
Wireless Security
Generate
Save Settings
Cancel Changes
Cisco Systems
Internet

Security Mode: WEP

Default Transmit Key: ● 1 ○ 2 ○ 3 ○ 4

WEP Encryption: 128 bits 26 hex digits

Passphrase: Peter Anteater

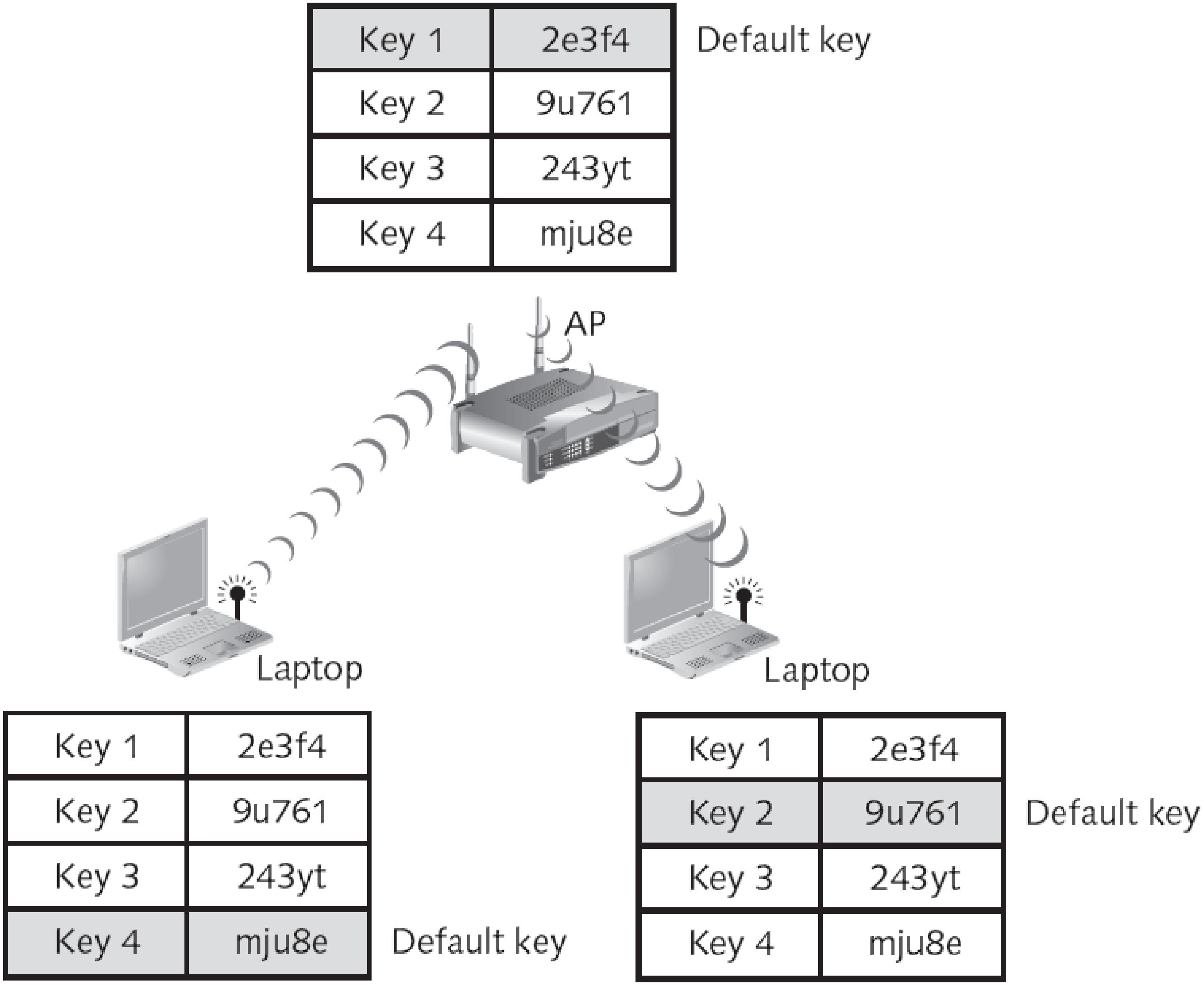
Key 1: F49BBB08F250C87AAF0F3385A4

Key 2: 195A45BFA436871E19FDD31168

Key 3: 6E04FAA9273E5C82A2340BD19E

Key 4: 8522EB970310CA74251F61344E

Security Mode: You may choose from Disable, WEP, WPA Pre-Shared Key, WPA RADIUS, or RADIUS. All devices on your network must use the same security mode in order to communicate.
More...



Key 1	2e3f4	Default key
Key 2	9u761	
Key 3	243yt	
Key 4	mju8e	

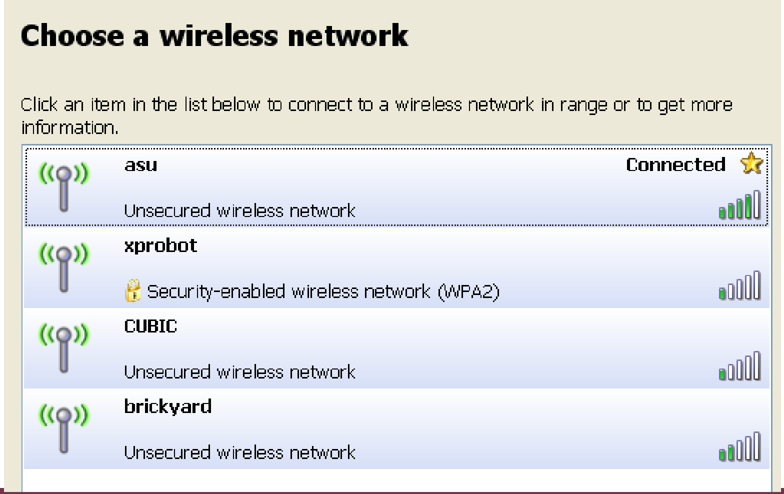
Key 1	2e3f4	
Key 2	9u761	
Key 3	243yt	
Key 4	mju8e	Default key

Key 1	2e3f4	
Key 2	9u761	Default key
Key 3	243yt	
Key 4	mju8e	

Figure 6-3 Default WEP key

SSID Vulnerabilities

- To connect, a computer needs a SSID (network name)
  - SSID is short for *service set **identifier***.
  - SSID is a case sensitive, 32 alphanumeric character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the basic service set (BSS)
- Routers normally send out ***beacon frames*** announcing the SSID
  - A management frames in IEEE 802.11
  - Contains all the information about the network
- Passive scanning
  - A wireless device listens for a beacon frame



Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

asu — Connected ☆
Unsecured wireless network

xprobot
Security-enabled wireless network (WPA2)

CUBIC
Unsecured wireless network

brickyard
Unsecured wireless network

Turning Off Beaconing

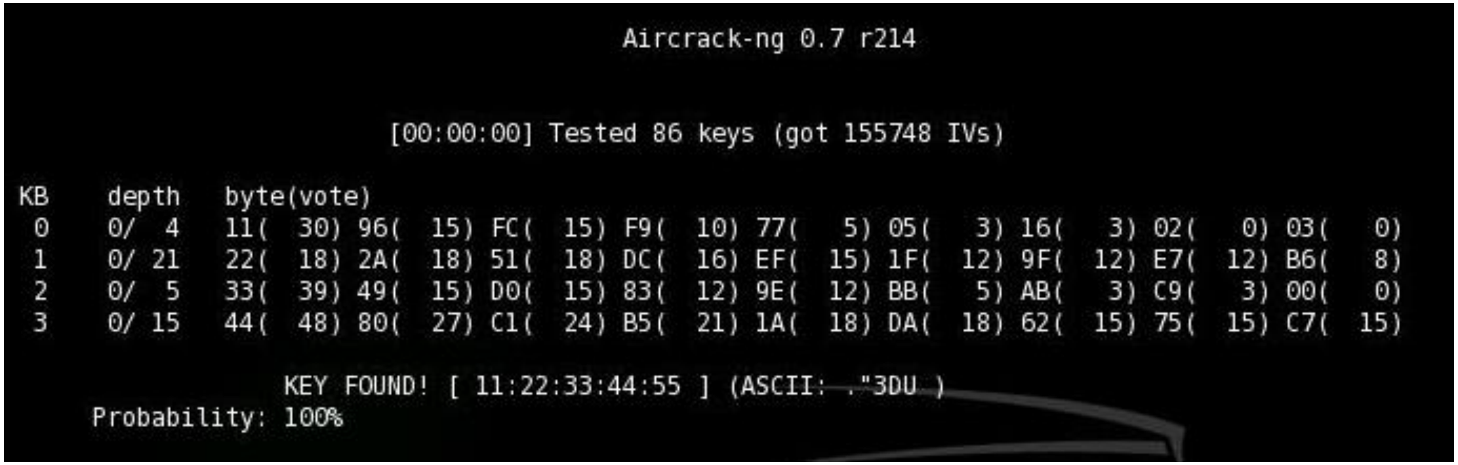
- For the "security" concern, some people turn off beacons
  - This annoys your legitimate users, who must now type in the SSID to connect
  - It doesn’t stop intruders, because the SSID is sent out in management frames anyway
  - It can also affect *roaming*
  - Windows XP prefers networks that broadcast

Vulnerabilities in WEP

- Key length
  - WEP can use only a 64-bit or a 128-bit (WEP2) key, which including 24-bit initialization vector (IV) and a 40-bit or 104-bit default key.
  - The 24-bit IV is *too short* and *repeats*. The 40-bit default key is also easily to be broken. Packets can be *replayed* to force the AP to pump out IVs
  - A 32-bit CRC is added as “Integrity check value” (ICV) to the packet in clear. ICV is a linear sum, it’s easy to be resolved by induction.
- MITM attack
  - The process of exchanging the challenge text occurs over the wireless link and is vulnerable to a man-in-the-middle attack.
  - The key stream created by performing *XOR function* on plaintext and the encrypted challenge is easily to be broken.
- Rouge AP attacks
  - WEP does not support *mutual authentication*. It only authenticates the client, making it open to rouge AP attacks.

Cracking WEP

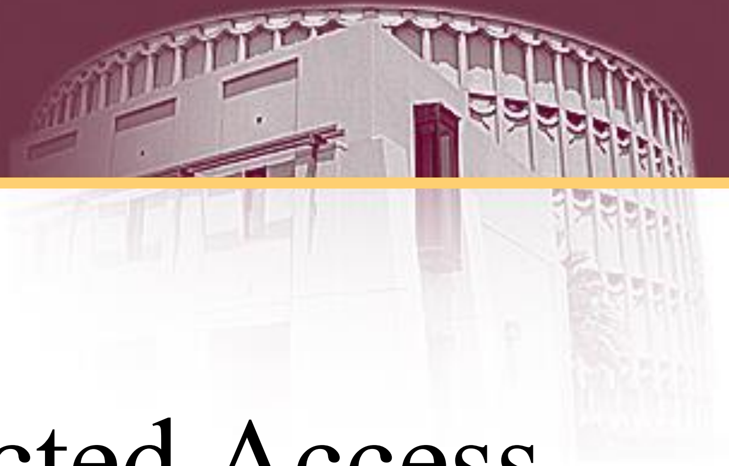
- With the right equipment, WEP can be cracked in just a few minutes
  - You need a special wireless card (driver support *raw-monitor mode*)



```
                                 Aircrack-ng 0.7 r214


                      [00:00:00] Tested 86 keys (got 155748 IVs)

KB    depth   byte(vote)
 0    0/  4   11(  30) 96(  15) FC(  15) F9(  10) 77(   5) 05(   3) 16(   3) 02(   0) 03(   0)
 1    0/ 21   22(  18) 2A(  18) 51(  18) DC(  16) EF(  15) 1F(  12) 9F(  12) E7(  12) B6(   8)
 2    0/  5   33(  39) 49(  15) D0(  15) 83(  12) 9E(  12) BB(   5) AB(   3) C9(   3) 00(   0)
 3    0/ 15   44(  48) 80(  27) C1(  24) B5(  21) 1A(  18) DA(  18) 62(  15) 75(  15) C7(  15)

                KEY FOUND! [ 11:22:33:44:55 ] (ASCII: ."3DU )
     Probability: 100%
```

Summary of WEP Problems

- IV value is too short, no protection for reuse
- Weak integrity check (CRC is predictable)
- No mutual authentication
- No user management
- No centralized key management
  - Manual key distribution => hard to change keys
- Single set of keys shared by all
  - Require frequently change
- Directly uses master key (pre-share key)
- No protection against replay



Wi-Fi Protected Access

WPA Security

WPA2 Security

WPA Security

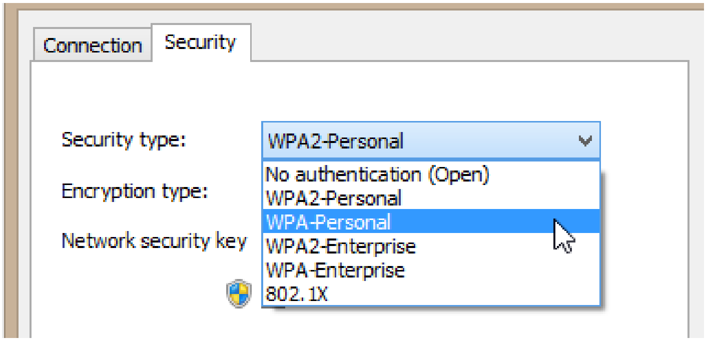
- Wireless Ethernet Compatibility Alliance (WECA)
  - A consortium of wireless equipment manufacturers and software providers
- WECA's goals:
  - To encourage wireless manufacturers to use the IEEE 802.11 technologies
  - To promote and market these technologies
  - To test and certify that wireless products adhere to the IEEE 802.11 standards to ensure product interoperability

WPA Security

- In 2002, the WECA organization changed its name to **Wi-Fi (Wireless Fidelity) Alliance**
- In October 2003 the Wi-Fi Alliance introduced **Wi-Fi Protected Access (WPA)**
  - WPA had the design goal to protect both present and future wireless devices, addresses both *wireless authentication* and *encryption*
- WPA adapts
  - *Preshared key* (PSK) addresses authentication
  - *Temporal Key Integrity Protocol* (TKIP) addresses encryption

WPA – Personal

- **Preshared key (PSK)** authentication
  - Uses a *passphrase* to generate the 256-bit encryption key
  - Also known as ***WPA Personal***
  - Designed for home and small office networks and doesn't require an authentication server



Security type: WPA2-Personal

- Key must be entered into both the *access point* and *all wireless devices*
  - Prior to the devices communicating with the AP
- The PSK is not used for encryption
  - Instead, it serves as the starting point (*seed*) for mathematically generating the encryption keys

WPA Improvement

- Extended 48-bit Initialization Vector (IV) and IV Sequencing Rules
  - 2^48 possible IVs and key/IV combinations
  - Prevents reuse and collision of IV
  - Implements advanced sequencing rules
- Key Derivation and Distribution
- TKIP generates per-packet keys
- A Message Integrity Code (MIC)
- WPA provides a *Transition Security Network* (TSN)

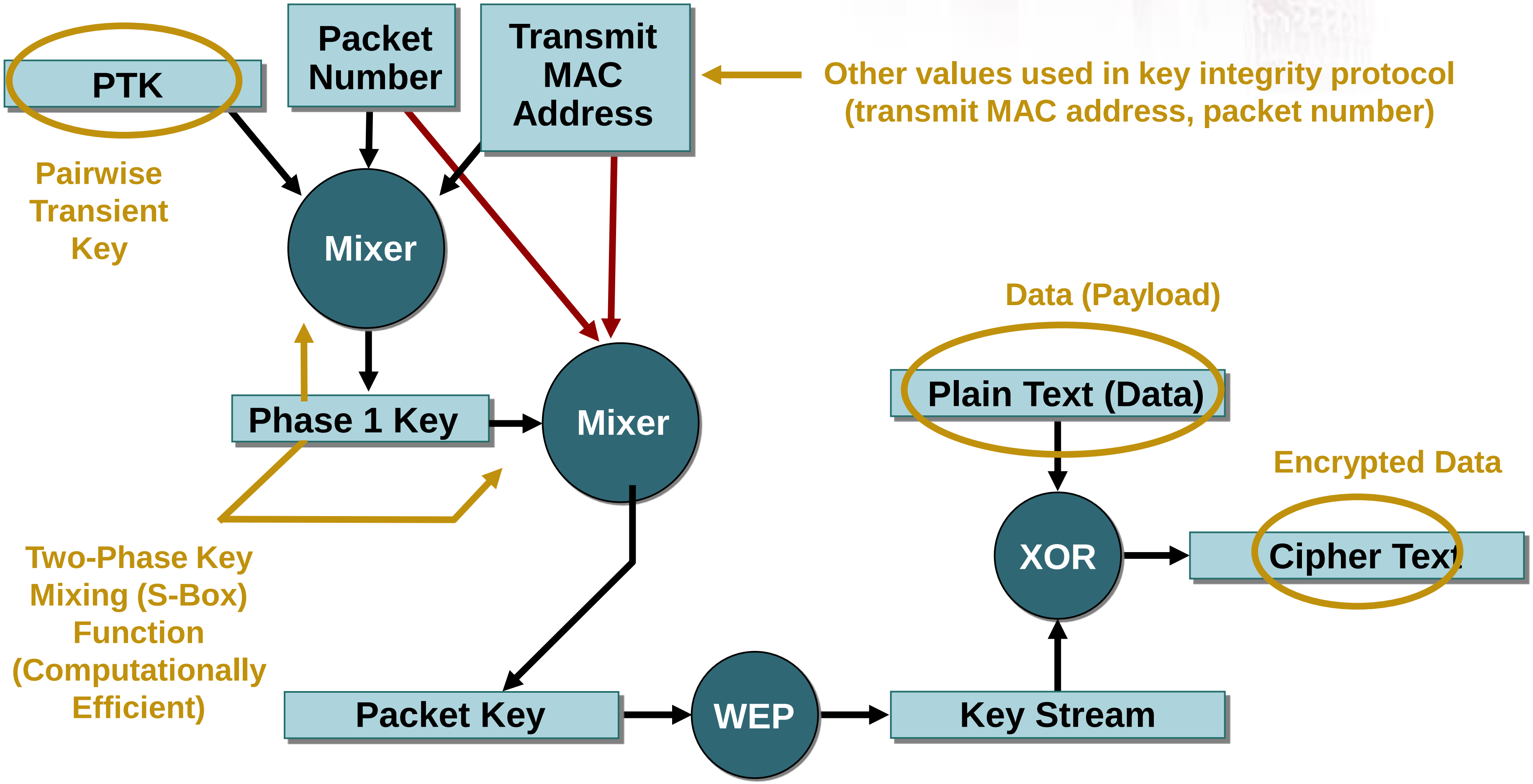
Key Derivation and Distribution

- Separate keys for authentication, encryption and integrity
- Password-based key derivation
  - Using passphrase and a salt (SSID) to derive keys for encryption
- Keys are distributed
  - Using a four-way handshake
  - Using *Pairwise Master Key*, Client Random number, Client MAC address, AP random number, and AP MAC address
  - Gives 4 values
    - Data encryption key, Data Integrity Key, Key exchange encryption key, and Key exchange integrity key

Temporal Key Integrity Protocol (TKIP)

- WPA replaces WEP with *TKIP*
- TKIP advantages:
  - TKIP uses a longer 128-bit key
  - TKIP uses a *new key* for each packet

TKIP: Per-Packet Key Mixing



Other values used in key integrity protocol (transmit MAC address, packet number)

Pairwise Transient Key

Data (Payload)

Encrypted Data

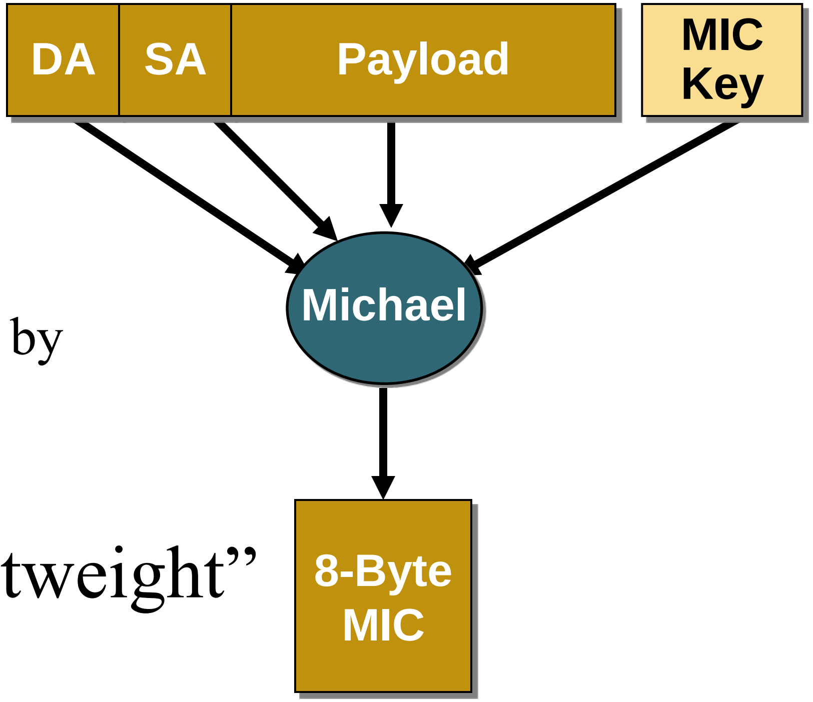
Two-Phase Key Mixing (S-Box) Function (Computationally Efficient)

Message Integrity Check (MIC)

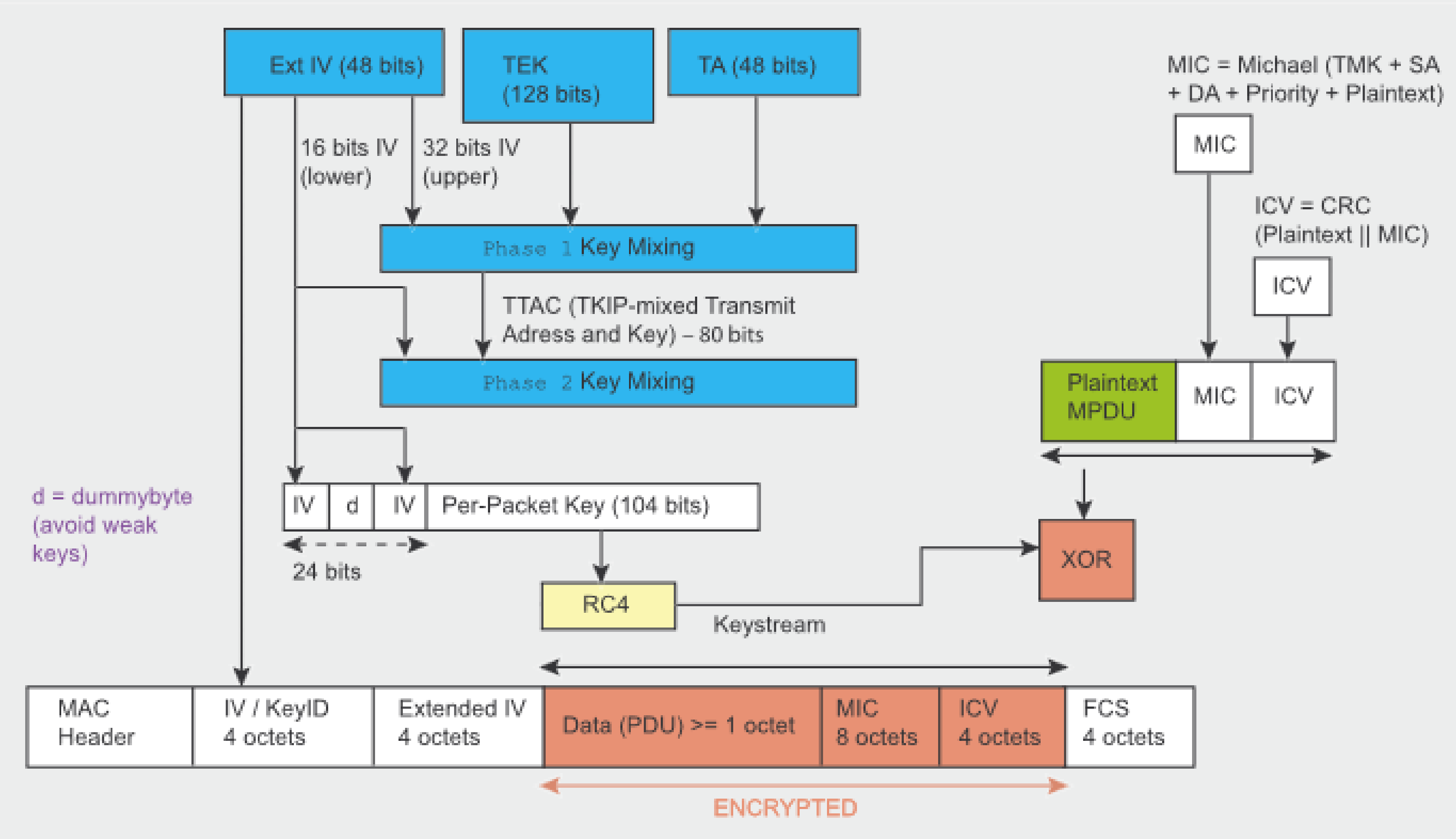
- WPA also replaces the (CRC) function in WEP with the **Message Integrity Check (MIC, a.k.a., Michael)**
  - Designed to prevent an attacker from capturing, altering, and resending data packets
  - With 802.11 and WEP, data integrity is provided by a 32-bit *integrity check value* (ICV) that is appended to the 802.11 payload and encrypted with WEP. Although the ICV is encrypted, you can use cryptanalysis to change bits in the encrypted payload and update the encrypted ICV without being detected by the receiver.
  - With WPA, a method known as *Michael* specifies a new algorithm that calculates an 8-byte *message integrity code* (MIC) using the calculation facilities available on existing wireless devices. The MIC is placed between the data portion of the IEEE 802.11 frame and the 4-byte ICV. The MIC field is encrypted together with the frame data and the ICV.
  - Michael also provides *replay protection*. A new frame counter in the IEEE 802.11 frame is used to prevent replay attacks.

Message Integrity Check

- MIC is calculated from:
  - A 64-bit MIC key (derived from the master session key)
  - Destination MAC address
  - Source MAC address
  - Data payload
- Uses Michael algorithm
  - A non-linear integrity check invented by Neil Furguson. Designed for WPA.
  - Has its own key
- Algorithm is relatively "lightweight"
  - Computationally inexpensive
  - Can be implemented in firmware on NIC cards

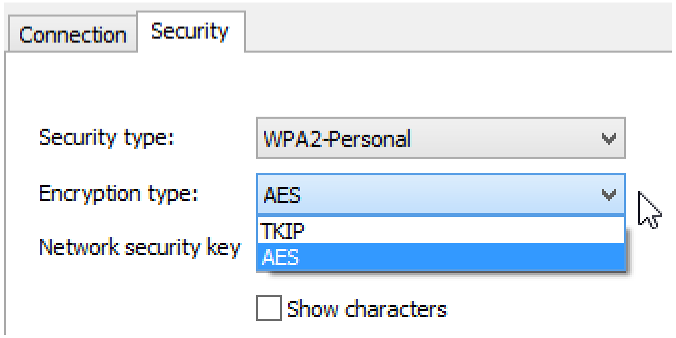


TKIP Key-Mixing Scheme and encryption



IEEE 802.11i

- 802.11i – wireless network security mechanism standards
  - Ratified in June 2004, and Standardizes
    - 802.1X for authentication
    - AES to be used for encryption
    - Key management
- WPA2 – the full implementation of IEEE 802.11i
  - Supplement to WPA1 (a subset of IEEE 802.11i), which uses TKIP encryption
  - Provides for *AES encryption* to be used
  - Third-party testing and certification for WLAN device compatibility



Security type: WPA2-Personal

Encryption type: AES

Network security key

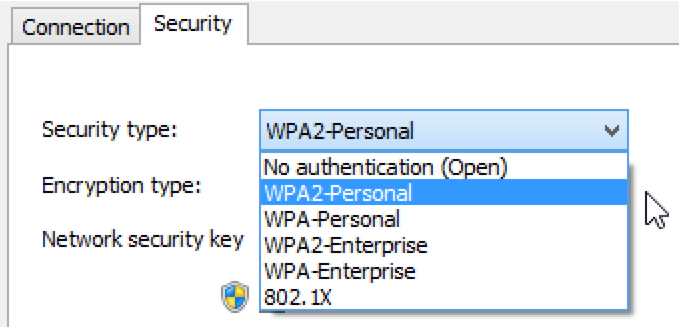
□ Show characters

Wi-Fi Protected Access 2 (WPA2)

- Introduced by the Wi-Fi Alliance in September 2004
- WPA2 provides a *Robust Security Network* (**RSN**) with two new protocols for the *key derivation and distribution*:
  - 4-way handshake
  - Group key handshake
- RSN only allows the creation of RSN associations (RSNAs)
  - A type of association used by a pair of STAs if they use 4-way handshake
- Two RSNA data *confidentiality* and *integrity* protocols
  - TKIP
  - Counter Mode CBC-MAC or simply **CCMP** (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)

WPA2 – Personal

- PSK Authentication
  - Uses PSK (Pre-Shared Key) for authentication
  - Intended for personal and small office home office users who do not have advanced server capabilities
  - PSK keys are automatically changed and authenticated between devices after a specified period of time known as *the rekey interval*


Connection | Security

Security type: WPA2-Personal

Encryption type:

Network security key

No authentication (Open)
WPA2-Personal
WPA-Personal
WPA2-Enterprise
WPA-Enterprise
802.1X

PSK Key Management Weaknesses

- People may send the key by e-mail or another insecure method
- *Changing* the PSK key is difficult
  - Must type new key on every wireless device and on all access points
  - In order to allow a guest user to have access to a PSK WLAN, the key must be given to that guest

Pre-Shared Key Weakness

- A PSK is a 64-bit hexadecimal number
  - Usually generated from a *passphrase*
    - Consisting of letters, digits, punctuation, etc. that is between 8 and 63 characters in length
- If the passphrase is a common word, it can be found with a ***dictionary attack.***

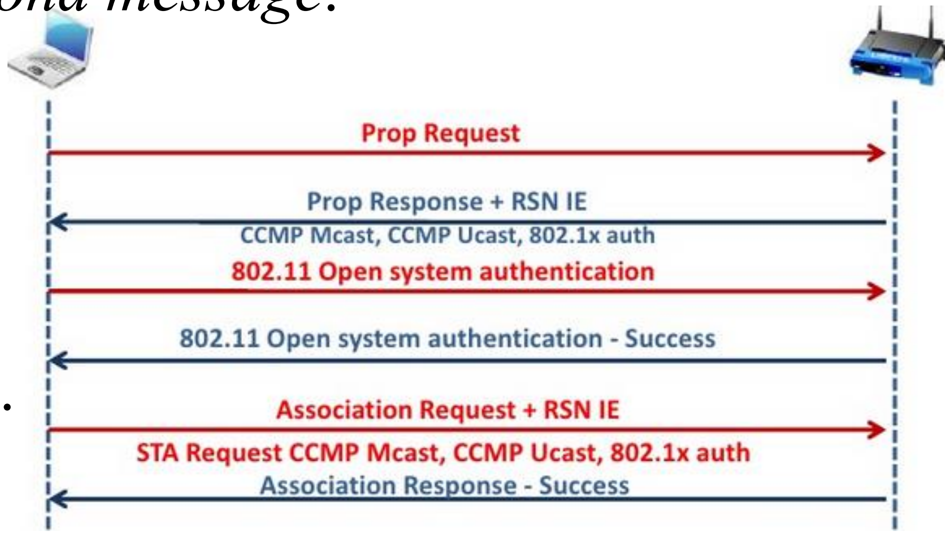
WPA2 Process

WPA2 establishes a secure communication channel in 4 phases:

- Phase 1: Agreeing on the security policy
  - The AP and the client will agree on the *security policy* (authentication and pre-authentication method)
- Phase 2: Authentication
  - Generate *master key* for WPA2-Enterprise (802.1X authentication)
- Phase 3: Key derivation and distribution
  - Creating *temporary keys* followed by 4-way handshake and group key handshake
- Phase 4: data confidentiality and integrity
  - All keys generated in phase 3 will be used by the CCMP protocol to provide data confidentiality and integrity

WPA2 Process – Phase 1

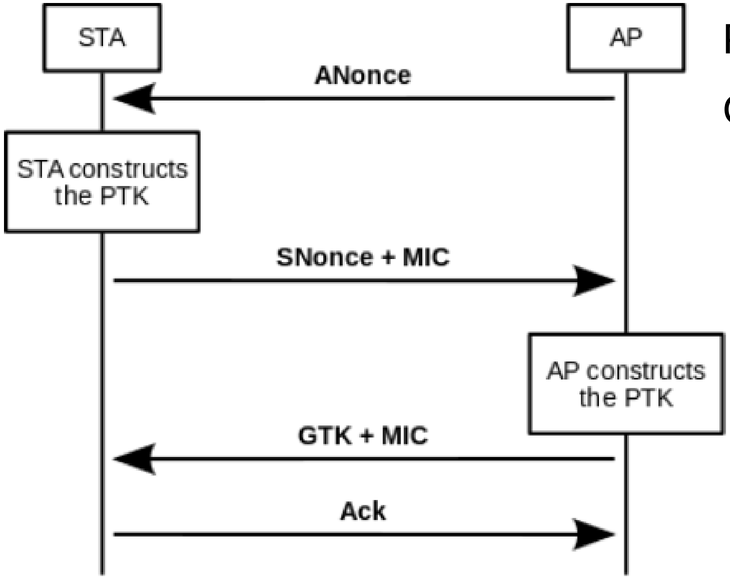
- AP advertises the *security policies* which it supports through the *Beacon* or through the *probe respond message*.
- After the *open authentication*, the client sends his response in the *association request message* which will be validated by an *association response* from the AP.
- The security policy information is included in the RSN IE (Information Element), and it contains:
  - *Authentication* methods (802.1X or PSK)
  - Security protocols for *unicast* (CCMP, TKIP, etc.)
  - Security protocols for *multicast* (CCMP, TKIP, etc.)


Prop Request
Prop Response + RSN IE
CCMP Mcast, CCMP Ucast, 802.1x auth
802.11 Open system authentication
802.11 Open system authentication - Success
Association Request + RSN IE
STA Request CCMP Mcast, CCMP Ucast, 802.1x auth
Association Response - Success

WPA2 Phase 3
4-way handshake in WPA2-PSK

- WPA2-PSK (or WPA-PSK) provides the 256-bits shared secret key **PMK** (*Pairwise Master Key*) in both ends to maintain the entire session.
- **PTK** (*Pairwise Transient Key*) in both ends are generated by concatenating:
  - PMK, AP nonce (ANonce), STA nonce (SNonce), AP MAC address, STA MAC address
  - The product is then put through a cryptographic hash function.

PMK



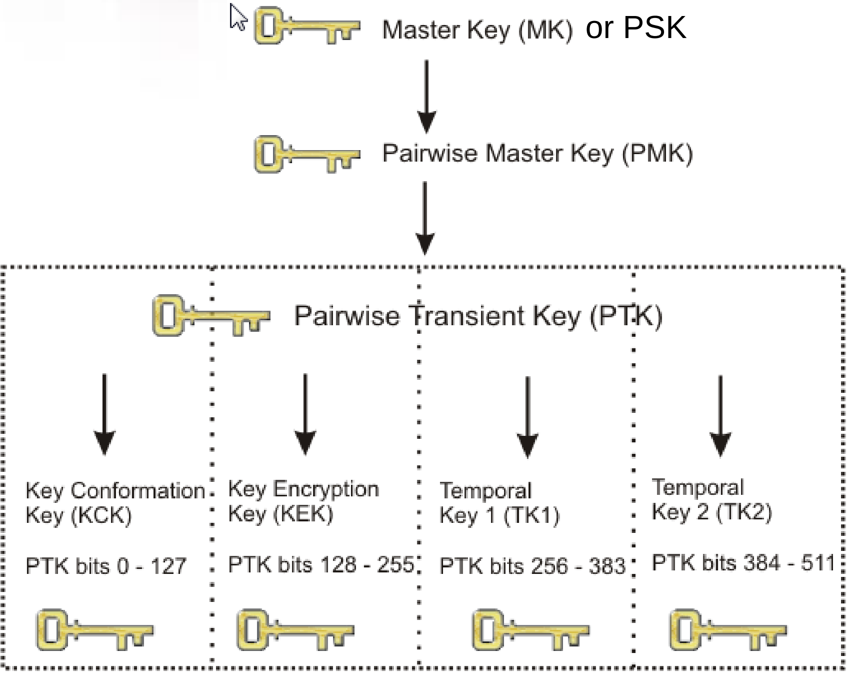
PMK

Generate ANonce

Generate SNonce and Message Integrity Code

GTK (Group Temporal Key) uses for decrypt multicast and broadcast traffic

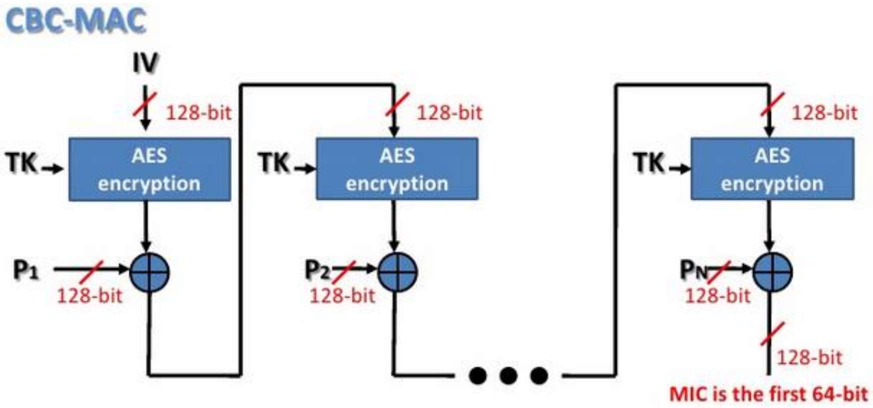
Pairwise Transient Key (PTK)

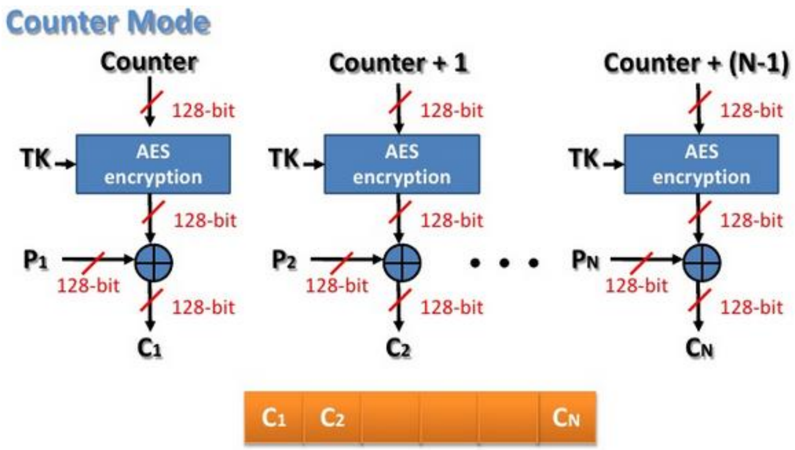


- PTK has 64 bytes long for TKIP
  - 16 bytes of *Key Confirmation Key* (KCK)
    - Used to compute MIC on WPA Key message
  - 16 bytes of *Key Encryption Key* (KEK)
    - AP uses this key to encrypt additional data sent (in the 'Key Data' field) to the client (for example, the RSN IE or the GTK)
  - 16 bytes of *Temporal Key* (TK or TEK)
    - Used to encrypt/decrypt Unicast data packets
  - 8 bytes of Michael MIC Authenticator Tx Key
    - Used to compute MIC on unicast data packets transmitted by the AP
  - 8 bytes of Michael MIC Authenticator Rx Key
    - Used to compute MIC on unicast data packets transmitted by the station

WPA2 Encryption

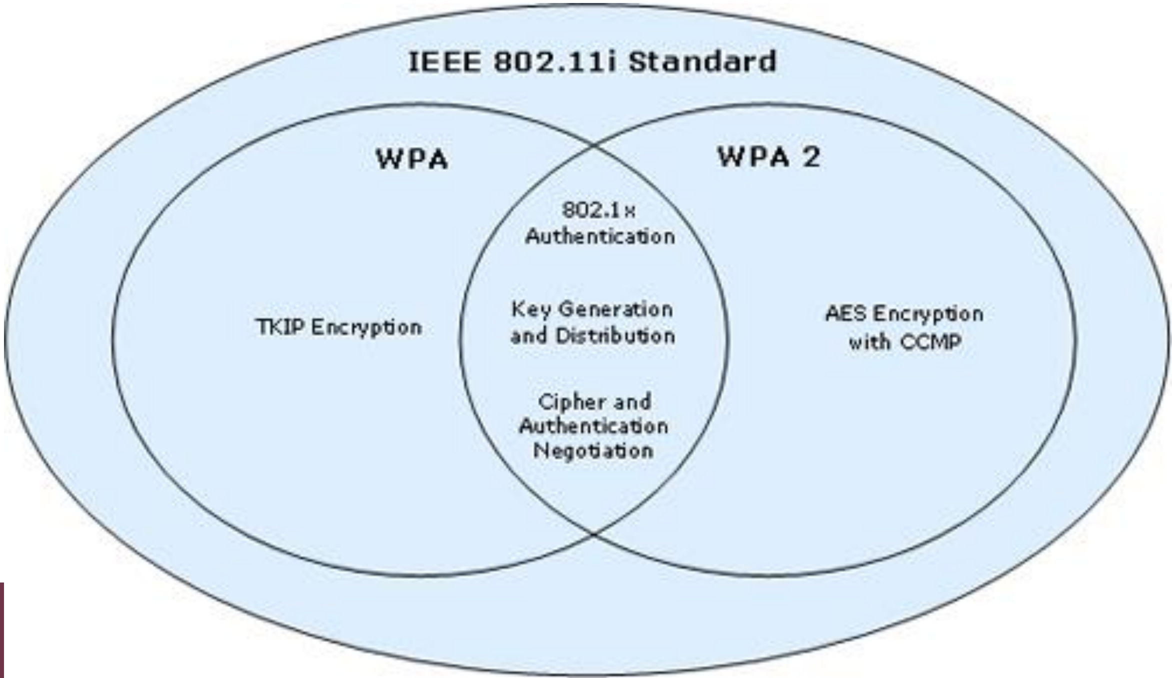
- WPA2 uses AES with key length of 128 bit to encrypt the data.
- The AES uses the Counter-Mode/CBC-MAC Protocol (CCMP)
- The AES-CCMP uses the same key for both encryption and authentication, but with different IVs.





WPA-PSK vs.WPA2-PSK

Security Model	Category	Security Mechanism	Security Level
WPA Personal Security	Authentication	PSK	Low-Medium (depends on length of passphrase)
WPA Personal Security	Encryption	TKIP	Medium
WPA2 Personal Security	Authentication	PSK	Medium
WPA2 Personal Security	Encryption	AES-CCMP	High

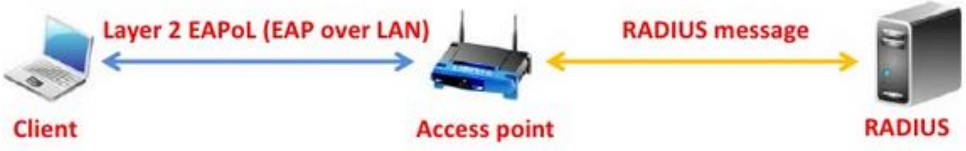


WEP vs. WPA vs. WPA2

	WEP	**WPA-PSK**	**WPA2-PSK**	**WPA-Enterprise**	**WPA2-Enterprise**
Authentication	none	PSK	PSK	**802.1X**	**802.1X**
Encryption	RC4	TKIP (RC4)	AES-CCMP	TKIP (RC4)	AES-CCMP
Key Size	40 (128) bits	128 bits	128 bits	128 bits	128 bits
IV size	24 bits	48 bits	48 bits	48 bits	48 bits
Integrity	CRC-32	Michael	CCM	Michael	CCM
Key Management	none	PSK	PSK	**EAP-based**	**EAP-based**
Security level	poor	medium	high	medium	high

WPA2-Enterprise

- WPA2 Enterprise mode consists of 3 components:
  - Supplicant (client)
  - Authenticator (AP)
  - Authentication Server (RADIUS)
    - RADIUS (Remote authentication Dial In User Service) was primarily used by ISPs who authenticated username and password before the user got authorized to use the ISP's network



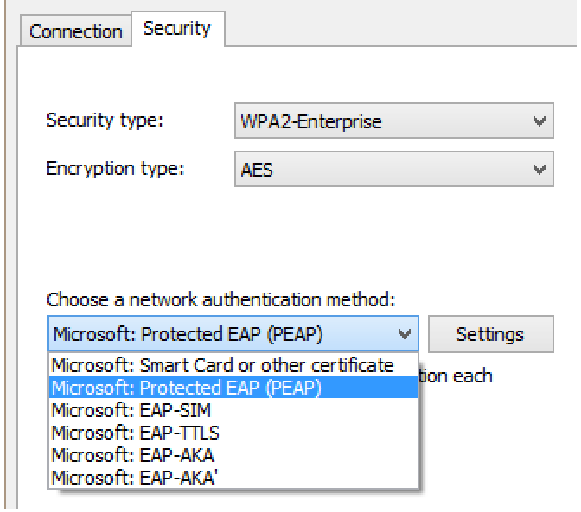
- The AP makes the **PAE** (*Port Access Entity*) by dividing each virtual port into two logical ports:
  - One for service: only open to allow the successful authenticators
  - One for authentication: open to allow any authentication frames
- It requires the users to be separately authenticated by using the Extended EAP (*Extensible Authentication Protocol*)
  - EAPOL: EAP over LAN

IEEE 802.1X for WLANs

- IEEE 802.1X is an IEEE Standard for *Port-based Network Access Control* (PNAC), and provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.
- Mutual authentication
  - Server is authenticated by client, and client is authenticated by server
  - Using Extensible Authentication Protocol (EAP)
- Encryption keys derived *dynamically*
- Ability to refresh encryption keys
  - RADIUS session timeout is used to give a fixed “validity” window for a user’s WLAN session key
- *Centralized* user and key management
  - EAP-based

EAP Authentication Methods (802.1X)

EAP is an *authentication framework* which supports multiple authentication methods. EAP typically runs directly over data link layers without requiring IP.



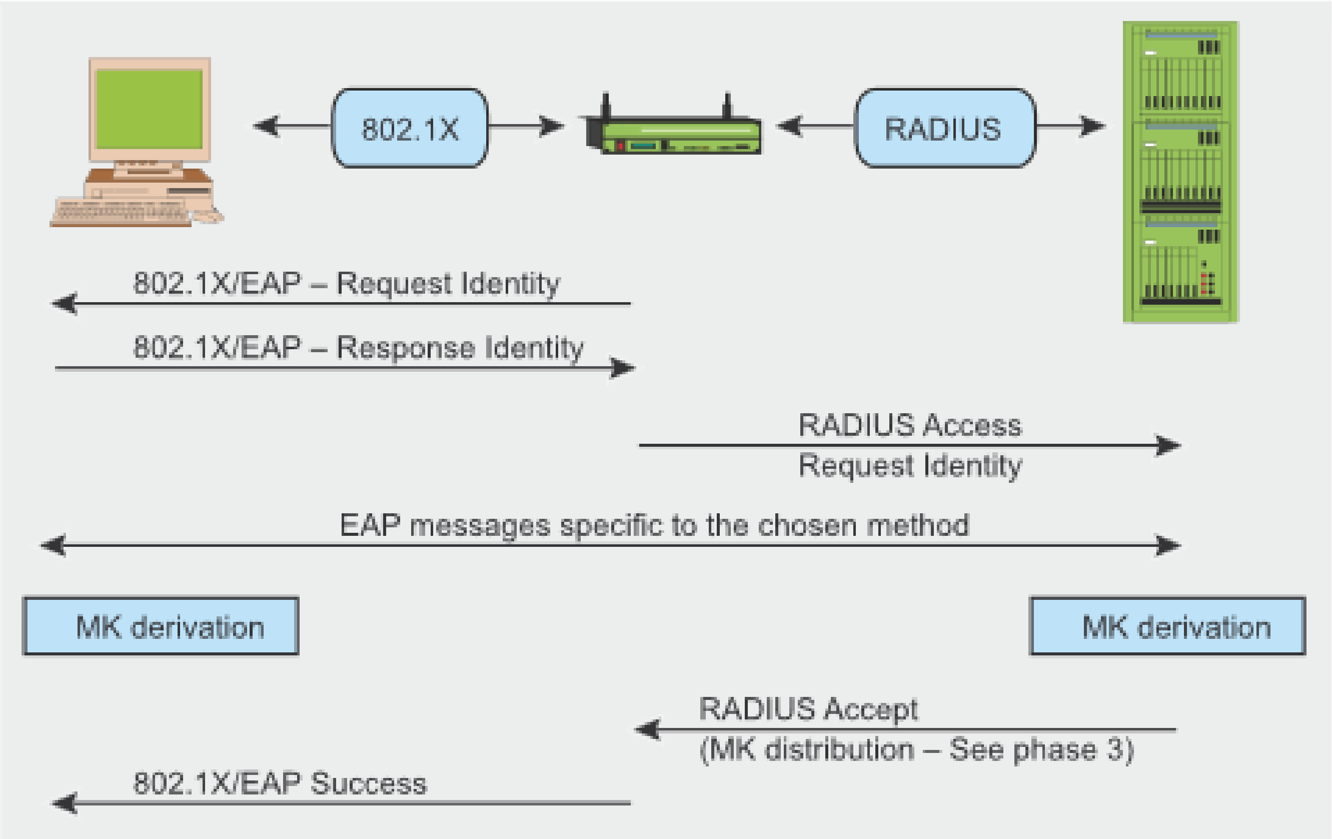
Security type: WPA2-Enterprise

Encryption type: AES

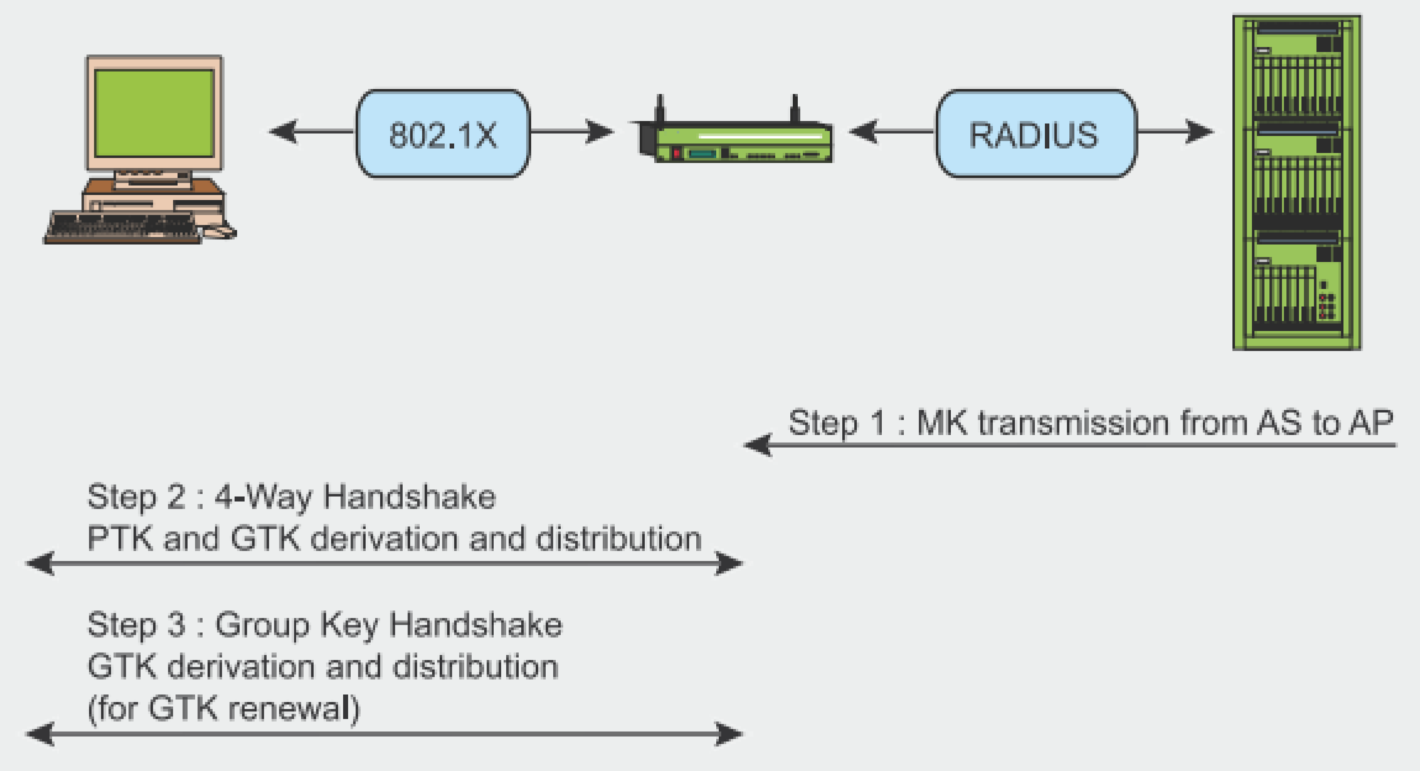
Choose a network authentication method: Microsoft: Protected EAP (PEAP)

- Cisco Lightweight EAP (LEAP)
  - User authentication via user ID and password
- EAP-FAST
  - User authentication via *username/password*
  - Uses a per-user PAC (analogous to a certificate) to authenticate server
- Protected EAP (PEAP)
  - User authentication via *One-Time Password (OTP)* or *static password* (PAP or MS-CHAPv2)
  - Same CA certificate used to validate server to all users
- EAP-TLS
  - User authentication with *digital certificate* (certificate installed per user)

WPA2-Enterprise Process Phase 2 IEEE 802.1X Authentication


802.1X
RADIUS
802.1X/EAP – Request Identity
802.1X/EAP – Response Identity
RADIUS Access
Request Identity
EAP messages specific to the chosen method
MK derivation
MK derivation
RADIUS Accept
(MK distribution – See phase 3)
802.1X/EAP Success

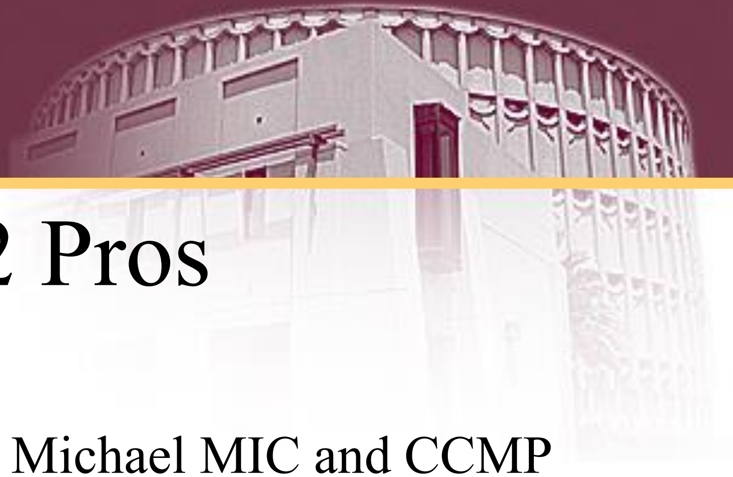
WPA2-Enterprise Process Phase 3 Key derivation and distribution



Step 1 : MK transmission from AS to AP

Step 2 : 4-Way Handshake
PTK and GTK derivation and distribution

Step 3 : Group Key Handshake
GTK derivation and distribution
(for GTK renewal)



WAP2 Pros

- No MAC address spoofing
  - MAC address included in both Michael MIC and CCMP
- No replay attack
  - Each message has a sequence number (TSC in TKIP and PN in CCMP)
- No key collision and weak key problems
- No dictionary based key recovery
  - All keys are computer generated binary numbers
- No keystream recovery
  - Each key is used only once in TKIP. No keystream in CCMP
- No rouge Aps
  - Mutual authentication optional

WPA2 other features

- **Key-caching for PMK**
  - Remembers a client, so if a user roams away from a wireless access point and later returns, she does not need to re-enter her credentials (no need to re-authenticate)
- **Pre-authentication**
  - Allows a device to become authenticated to an AP before moving into range of the AP (roaming)
  - Authentication packet is sent ahead

WPA2 vs. WPA

- WPA2 is based on the Robust Security Network (RSN) which make it support all the features available in WPA (transition security network, TSN).
- WPA2 supports strong encryption and authentication for both *infrastructure* and an *ad-hoc* network; in contrast WPA just supports the *infrastructure* networks.
- WPA2 reduced the overhead of the key derivation process.

WPA2 Cons

- Like all Wi-Fi security standard, the WPA2 can’t stand in front of the physical layer attacks like:
  - RF jamming
  - Data flooding
  - AP points failure
- Also, it can’t protect against layer 2 session hijacking
- It is vulnerable for the DoS attack.
- It is vulnerable to the MAC address spoofing and the mass de-authentication attacks.