Module 17
Wireless Hacking

Ansh Bhawnani

Wireless Concepts

Module 17

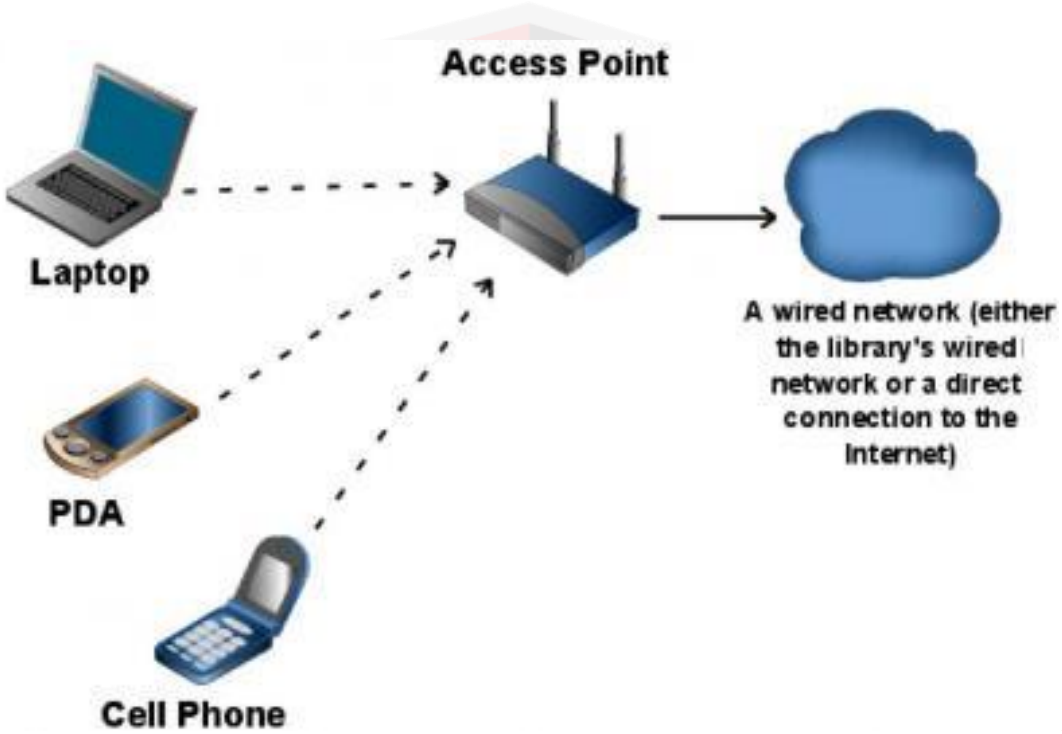
1. Wireless Networks

Module 17

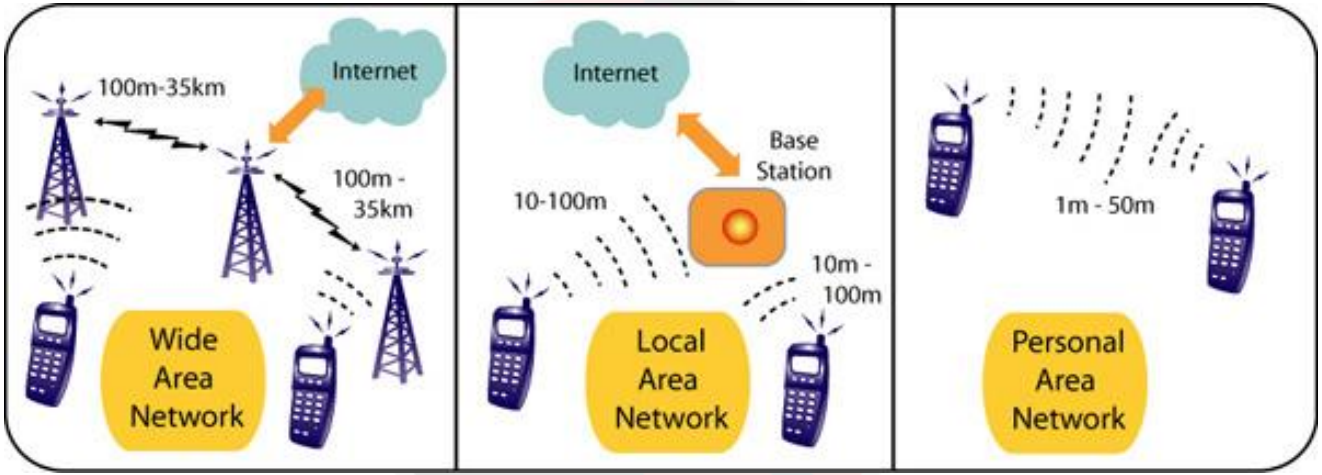
Wireless Concepts

- Wireless networks are computer networks that are not connected by cables of any kind.
- The basis of wireless systems are radio waves.
- A **wireless network** is a computer network that uses wireless data connections between network nodes.
- Examples of wireless networks include cell phone networks, wireless local area networks (WLANs), wireless sensor networks, satellite communication networks, and terrestrial microwave networks
- Homes, telecommunications networks and business installations avoid the costly process of introducing cables into a building.
- This implementation takes place at the physical level (layer) of the OSI model network structure.

Wireless Concepts



Wireless Concepts



Wireless Concepts

History

- **1973** – Ethernet 802.3
- **1991** – 2G cell phone network
- June **1997** – 802.11 "Wi-Fi" protocol first release
- **1999** – 803.11 VoIP integration

Wireless Concepts

Advantages:

- Installation is fast and easy and eliminates wiring through walls and ceilings.
- Much cheaper due to less amount of physical cabling and hardware.
- It is easier to provide connectivity in areas where it is difficult to lay cable.
- Access to the network can be from anywhere within range of an access point.
- Public places like airports, libraries, schools or even coffee shops offer you constant Internet connections using Wireless LAN.

Wireless Concepts

Disadvantages:

- Security is a big issue and may not meet expectations.
- As the number of computers on the network increases, the bandwidth suffers.
- Wi-Fi enhancements can require new wireless cards and/or access points.
- Some electronic equipment can interfere with the Wi-Fi networks (noise).

2. Wireless Terminologies

Module 17

Wireless Concepts

- **GSM**: Universal system used for mobile transportation for wireless network worldwide.
- **Bandwidth**: Describes the amount of information that may be broadcasted over a connection or a range within a band of frequencies
- **BSSID**: The MAC address of an access point that has set up a Basic Service Set (BSS).
- **ISM band**: A set of frequency for the international Industrial, Scientific, and Medical communities.
- **Access Point**: Used to connect wireless devices to a wireless network.
- **Hotspot**: Places where wireless network is available for public use.

Wireless Concepts

- **Association**: The process of connecting a wireless device to an access point.
- **Orthogonal Frequency-division Multiplexing (OFDM)**: Method of encoding digital data on multiple carrier frequencies.
- **Direct-sequence Spread Spectrum (DSSS)**: Original data signal is multiplied with a pseudo random noise spreading code.
- **Frequency-hopping Spread Spectrum (FHSS)**: Method of transmitting radio signals by rapidly switching a carrier among many frequency channels.

3. Wi-Fi Networks at Home and Public Places

Module 17

Wireless Concepts

- **Wi-Fi at Home**: Wi-Fi networks at home allow you to be wherever you want with your laptop, iPad, or handheld device, and not have to make holes for or hide Ethernet cables.
- **Wi-Fi at Public Places**: You can find free/paid Wi-Fi access available in coffee shops, shopping malls, bookstores, offices, airport terminals, schools, hotels, and other public places.

4. Wireless Technology Statistics

Module 17

Wireless Concepts

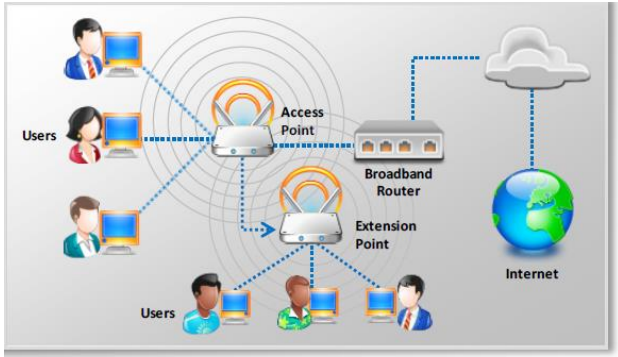
Why Wireless Technology Matters?

- More than half of all open Wi-Fi networks are susceptible to abuse.
- There will be more than 7 billion new Wi-Fi enabled devices in the next 3 years.
- 71% of all mobile communications flows over Wi-Fi.
- By 2017, 60% of carrier network traffic will be offloaded to Wi-Fi.
- A Wi-Fi attack on an open network can take less than 2 seconds.
- 90% of all smartphones are equipped with Wi-Fi capabilities.

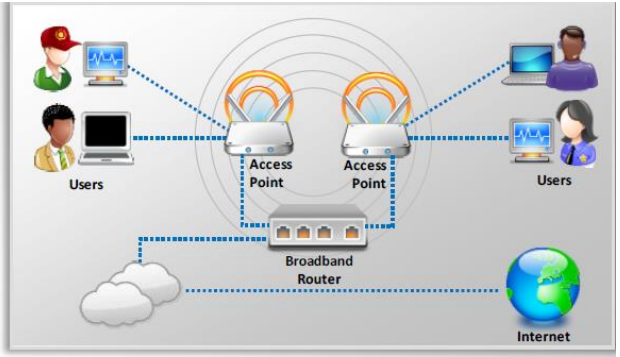
5. Types of Wireless Networks

Module 17

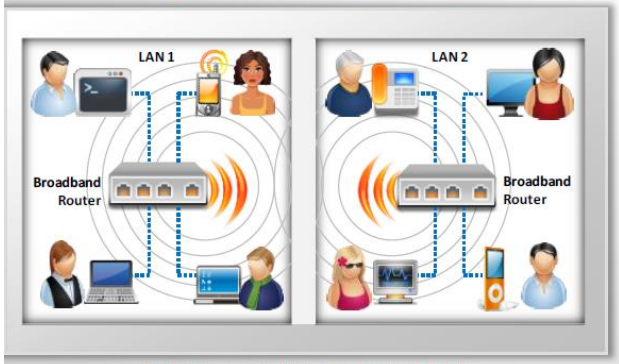
Wireless Concepts



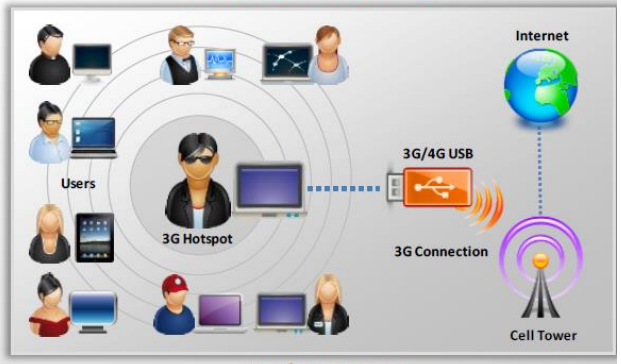
Extension to a Wired Network



Multiple Access Points



LAN-to-LAN Wireless Network

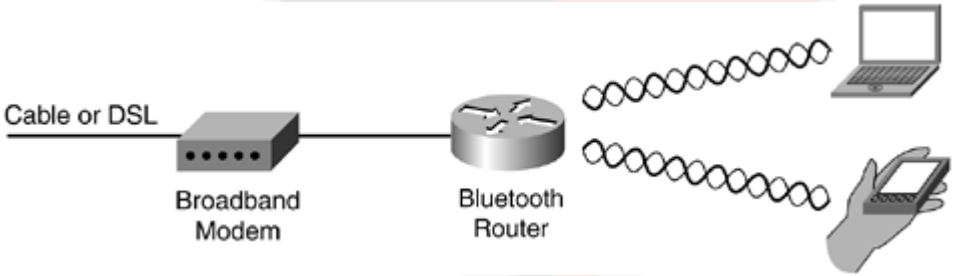


3G/4G Hotspot

Wireless Concepts

Wireless PAN

- Wireless personal area networks (WPANs) connect devices within a relatively small area, typically within a **range** of 10 meters.
- For example, both Bluetooth radio and invisible infrared light provides a WPAN for interconnecting a headset to a laptop.



Wireless Concepts

Wireless LAN

- A wireless local area network (WLAN) links two or more devices over a short distance using a wireless distribution method, 150 feet indoors and 300 feet outdoors, usually providing a connection through an access point for internet access.
- The use of spread-spectrum or OFDM technologies may allow users to move around within a local coverage area, and still remain connected to the network.
- Products using the IEEE 802.11 WLAN standards are marketed under the Wi-Fi brand name

Wireless Concepts

Wireless LAN

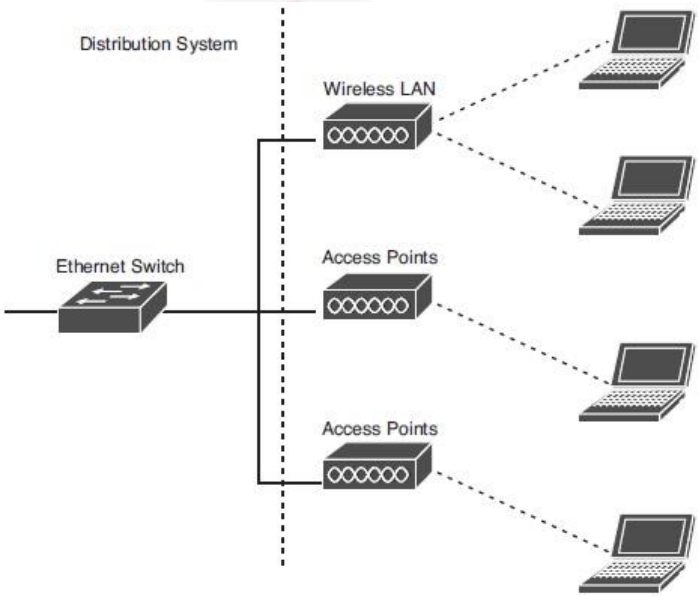


Figure 3-2 *An Infrastructure Wireless LAN Interfaces Client Devices to a Wired Distribution System and Extends Coverage Through Use of Access Points*

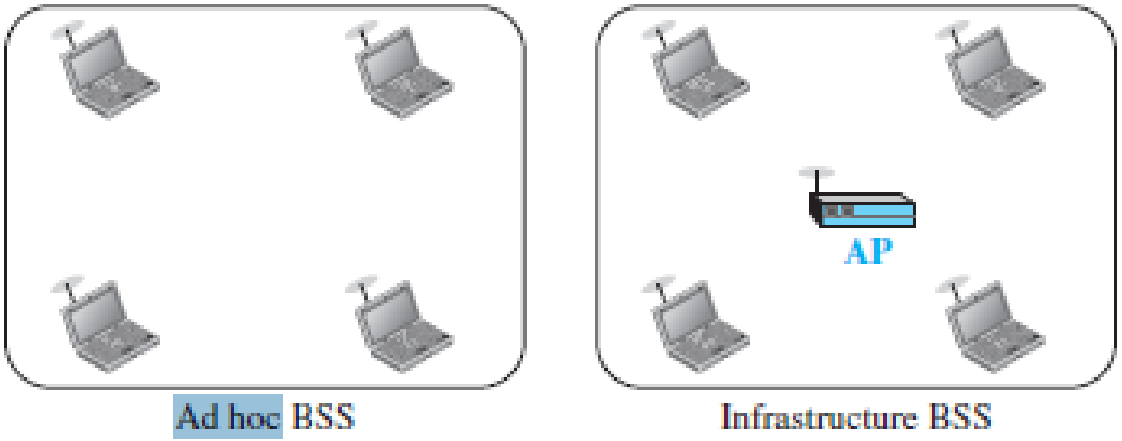
Wireless Concepts

Wireless ad hoc network

- A wireless ad hoc network, also known as a wireless mesh network or mobile ad hoc network (MANET), is a wireless network made up of radio nodes organized in a mesh topology.
- Each node forwards messages on behalf of the other nodes and each node performs routing. Ad hoc networks can "self-heal", automatically re-routing around a node that has lost power.
- Various network layer protocols are needed to realize ad hoc mobile networks, such as Distance Sequenced Distance Vector routing, Associativity-Based Routing, Ad hoc on-demand Distance Vector routing, and Dynamic source routing.

Wireless Concepts

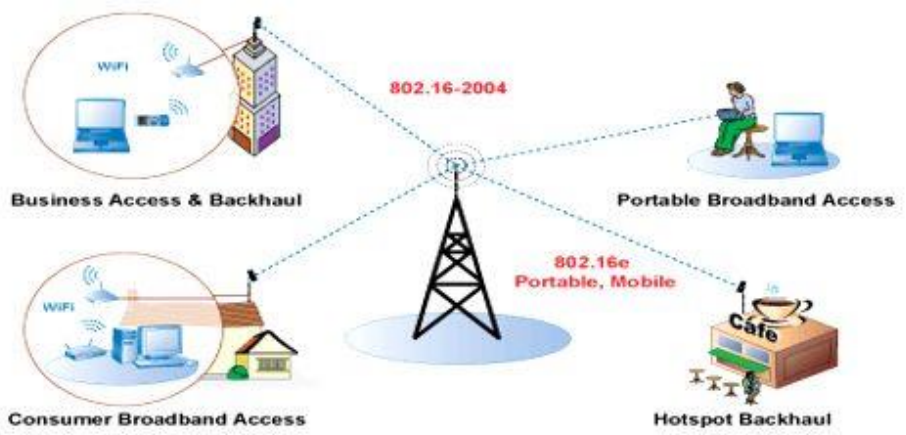
Wireless ad hoc network



Wireless Concepts

Wireless MAN

- Wireless metropolitan area networks are a type of wireless network that connects several wireless LANs.
- WiMAX is a type of Wireless MAN and is described by the IEEE 802.16 standard.



Wireless Concepts

Wireless WAN

- Wireless wide area networks are wireless networks that typically cover large areas, such as between neighboring towns and cities, or city and suburb. These networks can be used to connect branch offices of business or as a public Internet access system.
- The wireless connections between access points are usually point to point microwave links using parabolic dishes on the 2.4 GHz and 5.8Ghz band, rather than omnidirectional antennas used with smaller networks.

6. Wireless Standards

Module 17

Wireless Concepts

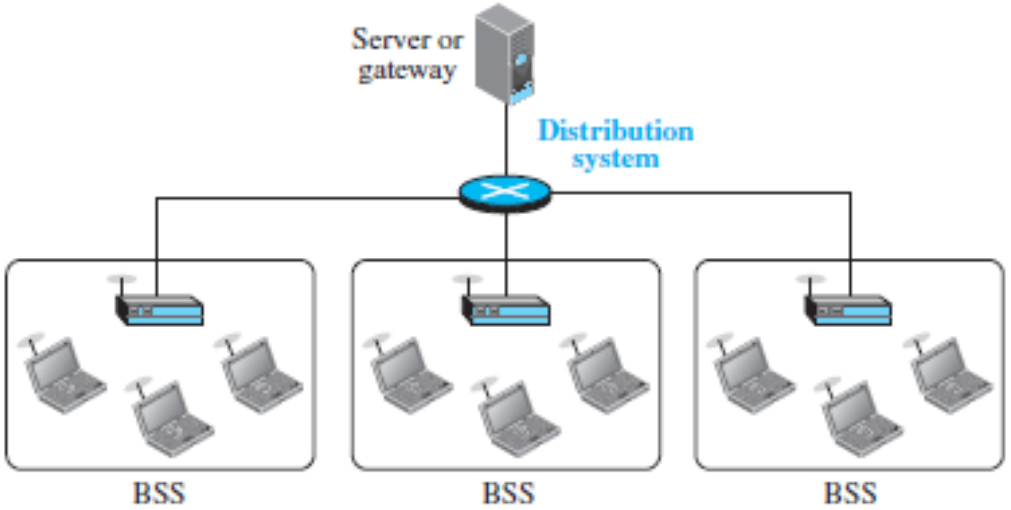
IEEE Standard	Frequency/Medium	Speed	Topology	Transmission Range	Access Method
802.11	2.4GHz RF	1 to 2Mbps	Ad hoc/infrastructure	20 feet indoors.	CSMA/CA
802.11a	5GHz	Up to 54Mbps	Ad hoc/infrastructure	25 to 75 feet indoors; range can be affected by building materials.	CSMA/CA
802.11b	2.4GHz	Up to 11Mbps	Ad hoc/infrastructure	Up to 150 feet indoors; range can be affected by building materials.	CSMA/CA
802.11g	2.4GHz	Up to 54Mbps	Ad hoc/infrastructure	Up to 150 feet indoors; range can be affected by building materials.	CSMA/CA
802.11n	2.4GHz/5GHz	Up to 600Mbps	Ad hoc/infrastructure	175+ feet indoors; range can be affected by building materials.	CSMA/CA

Wireless Concepts

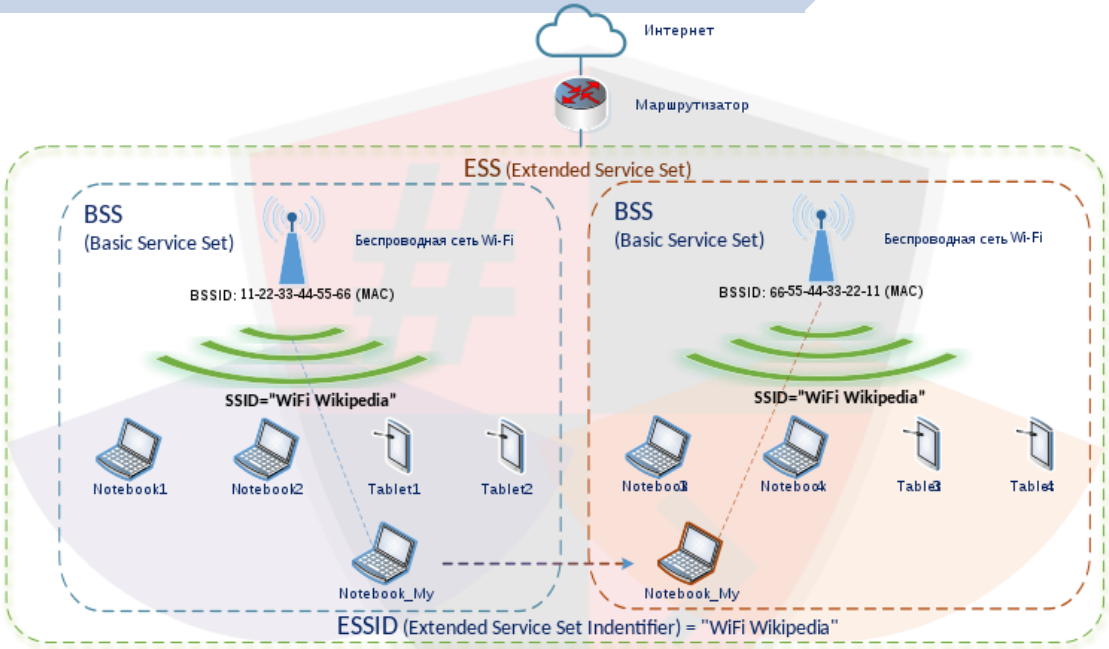
IEEE Standard	RF Used	Spread Spectrum	Data Rate (in Mbps)
802.11	2.4GHz	DSSS	1 or 2
802.11	2.4GHz	FHSS	1 or 2
802.11a	5GHz	OFDM	54
802.11b	2.4GHz	DSSS	11
802.11g	2.4Ghz	DSSS	54
802.11n	2.4/5GHz	OFDM	600 (theoretical)

7. Service Set Identifier (SSID)

Wireless Concepts



Wireless Concepts



Wireless Concepts

- SSID is a token to identify a 802.11 (Wi-Fi) network; by default it is the part of the frame header sent over a wireless local area network (WLAN).
- A service set is also known as extended service set or ESS. The identifier is known as ESSID (for e.g., “Tech Hacker”)
- It acts as a single shared identifier between the access points and clients.
- Access points continuously broadcasts SSID, if enabled, for the client machines to identify the presence of wireless network.
- SSID is a human-readable text string with a maximum length of 32 bytes.

Wireless Concepts

- If SSID of the network is changed, reconfiguration of the SSID on every host is required, as every user of the network configures the SSID into their system.
- A non-secure access mode allows clients to connect to the access point using the configured SSID, a blank SSID, or an SSID configured as "any".
- Security concerns arise when the default values are not changed, as these units can be compromised.
- The SSID remains secret only on the closed networks with no activity, that is inconvenient to the legitimate users.

Wireless Concepts

- **Basic service sets** (**BSS**) are a subgroup of devices within a service set which are additionally also operating with the same physical layer medium access characteristics (i.e. radio frequency, modulation scheme, security settings etc.) such that they are wirelessly networked.
- Devices within basic service sets are identified by BSSIDs (basic service set identifiers), which are 48-bit labels that conform to MAC-48 conventions.
- While devices may have multiple BSSIDs, usually each BSSID is associated with at most one basic service set at a time.[1] There are two classes of basic service sets: access points or infrastructure, and independent stations in a peer-to-peer ad hoc topology (an Independent Basic Service Set- or IBSS.)

8. Wi-Fi Encryption

Module 17

8.1. Types of Wireless Encryption

Module 17

Wi-Fi Encryption

- **WEP**:
  - WEP is an encryption algorithm for IEEE 802.11 wireless networks.
  - It is an old and original wireless security standard which can be cracked easily.
- **WPA**:
  - It is an advanced wireless encryption protocol using TKIP, MIC, and AES encryption.
  - Uses a 48 bit IV, 32 bit CRC and TKIP encryption for wireless security.
- **WPA2**:
  - WPA2 uses AES (128 bit) and CCMP for encryption.

Wi-Fi Encryption

- **EAP**:
  - Supports multiple authentication methods, such as token cards, Kerberos, certificates etc.
- **WPA2 Enterprise**:
  - It integrates EAP standards with WPA2 encryption.
- **TKIP**:
  - A security protocol used in WPA as a replacement for WEP.
- **CCMP**: CCMP utilizes 128-bit keys, with a 48-bit initialization vector (IV) for replay detection.

Wi-Fi Encryption

- **AES:**
  - It is a symmetric-key encryption, used in WPA2 as a replacement of TKIP.
- **802.11i:**
  - It is an IEEE amendment that specifies security mechanisms for 802.11 wireless networks.
- **RADIUS:**
  - It is a centralized authentication and authorization management system.
- **LEAP:**
  - It is a proprietary WLAN authentication protocol by Cisco.

8.2. WEP Encryption

Module 17

Wi-Fi Encryption

WEP Encryption

- **What is WEP**:
  - Wired Equivalent Privacy (WEP) is an IEEE 802.11 wireless protocol which provides security algorithms for data confidentiality during wireless transmissions.
  - WEP uses a 24-bit initialization vector (IV) to form stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity of wireless transmission.

Wi-Fi Encryption

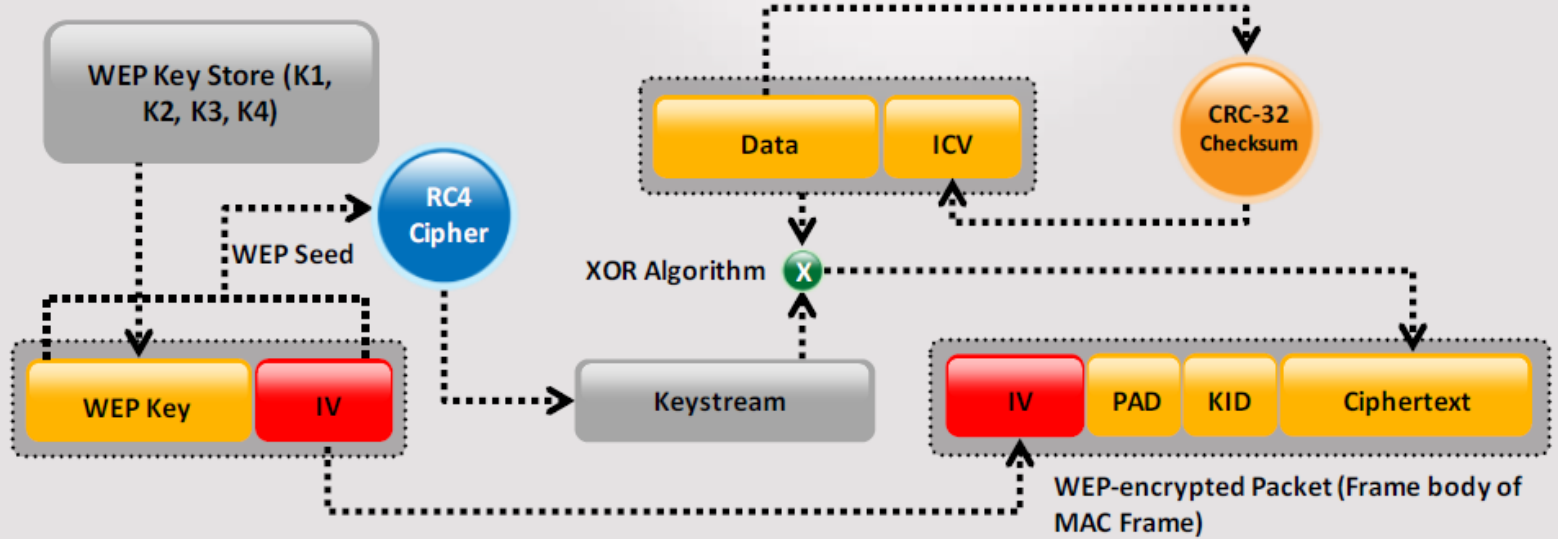
- **WEP encryption can be easily cracked**:
  - 64-bit WEP uses a 40-bit key
  - 128-bit WEP uses a 104-bit key
  - 256-bit WEP uses a 232-bit key
- **It was developed without**:
  - Academic or public review
  - Review from cryptologists
- **WEP Flaws**:
  - It has significant vulnerabilities and design flaws.

Wi-Fi Encryption

How WEP Works

- CRC-32 checksum is used to calculate a 32-bit Integrity Check Value (ICV) for the data, which, in turn, is added to the data frame.
- A 24-bit arbitrary number known as Initialization Vector (IV) is added to WEP key; WEP key and IV are together called as WEP seed.
- The WEP seed is used as the input to RC4 algorithm to generate a key stream (key stream is bit-wise XORed with the combination of data and ICV to produce the encrypted data).
- The IV field (IV+PAD+KID) is added to the ciphertext to generate a MAC frame.

Wi-Fi Encryption



Wi-Fi Encryption

- WEP Weaknesses
  - Weak keys
  - IV length is too short
  - IV values can be reused
  - Key Management and updating is poorly provided for
  - Message integrity checking is ineffective

8.3. What is WPA?

Wi-Fi Encryption

- Wi-Fi Protected Access (WPA) is a data encryption method for WLANs based on 802.11 standards.
- It is a snapshot of 802.11i (under development) providing stronger encryption, and enabling PSK or EAP authentication.
- **TKIP (Temporal Key Integrity Protocol)**:
  - TKIP utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit MIC integrity check.
  - TKIP mitigated vulnerability by increasing the size of the IV and using mixing functions.

Wi-Fi Encryption

- **128-bit Temporal Key**:
  - Under TKIP, the client starts with a 128-bit "temporal key" (TK) that is then combined with the client's MAC address and with an IV to create a keystream that is used to encrypt data via the RC4.
  - It implements a sequence counter to protect against replay attacks.
- **WPA Enhances WEP**:
  - TKIP enhances WEP by adding a rekeying mechanism to provide fresh encryption and integrity keys.
  - Temporal keys are changed for every 10,000 packets. This makes TKIP more resistant to cryptanalytic attacks involving key reuse.

8.4. What is WPA2?

Wi-Fi Encryption

- **WPA2** replaced WPA. WPA2, implements the mandatory elements of IEEE 802.11i. In particular, it includes mandatory support for CCMP, an AES-based encryption mode. WPA2 certification is mandatory for all new devices to bear the Wi-Fi trademark.
- In order to enhance the security, **WPA2** was invented with strong encryption model (AES) and a very strong authentication model based on 802.1x (or PSK).
- **WPA** was introduced just as a staging mechanism for smooth transition to WPA2. A lot of wireless cards did not support the new AES (at that time), but all of them were using RC4 + TKIP. Therefore WPA was also based on that mechanism, just with a few advancements.

8.5. WEP vs WPA vs WPA2

Module 17

Wi-Fi Encryption

The most common encryption algorithms are collected in the following table –

Encryption Algorithm	Type of encryption algorithm	Size of data block
RC4	Stream cipher	---
RC5	Block cypher	32/64/128 bits
DES	Block cypher	56 bits
3DES	Block cypher	56 bits
AES	Block cypher	128 bits

The ones that you will most likely meet (in some form) on the wireless networks are **RC4 and AES**.

Wi-Fi Encryption

Wireless security cheat sheet

Encryption standard	Fast facts	How it works	Should you use it?
WIRED EQUIVALENT PRIVACY (WEP)	First 802.11 security standard; easily hacked due to its 24-bit initialization vector (IV) and weak authentication.	Uses RC4 stream cipher and 64-or 128-bit keys. Static master key must be manually entered into each device.	No
WI-FI PROTECTED ACCESS (WPA)	An interim standard to address major WEP flaws. Backwards compatible with WEP devices. It has two modes: personal and enterprise.	Retains use of RC4, but adds longer IVs and 256-bit keys. Each client gets new keys with TKIP. Enterprise mode: Stronger authentication via 802.1x and EAP.	Only if WPA2 is not available
WPA2	Current standard. Newer hardware ensures advanced encryption doesn't affect performance. Also has personal and enterprise modes.	Replaces RC4 and TKIP with CCMP and AES algorithm for stronger authentication and encryption.	Yes

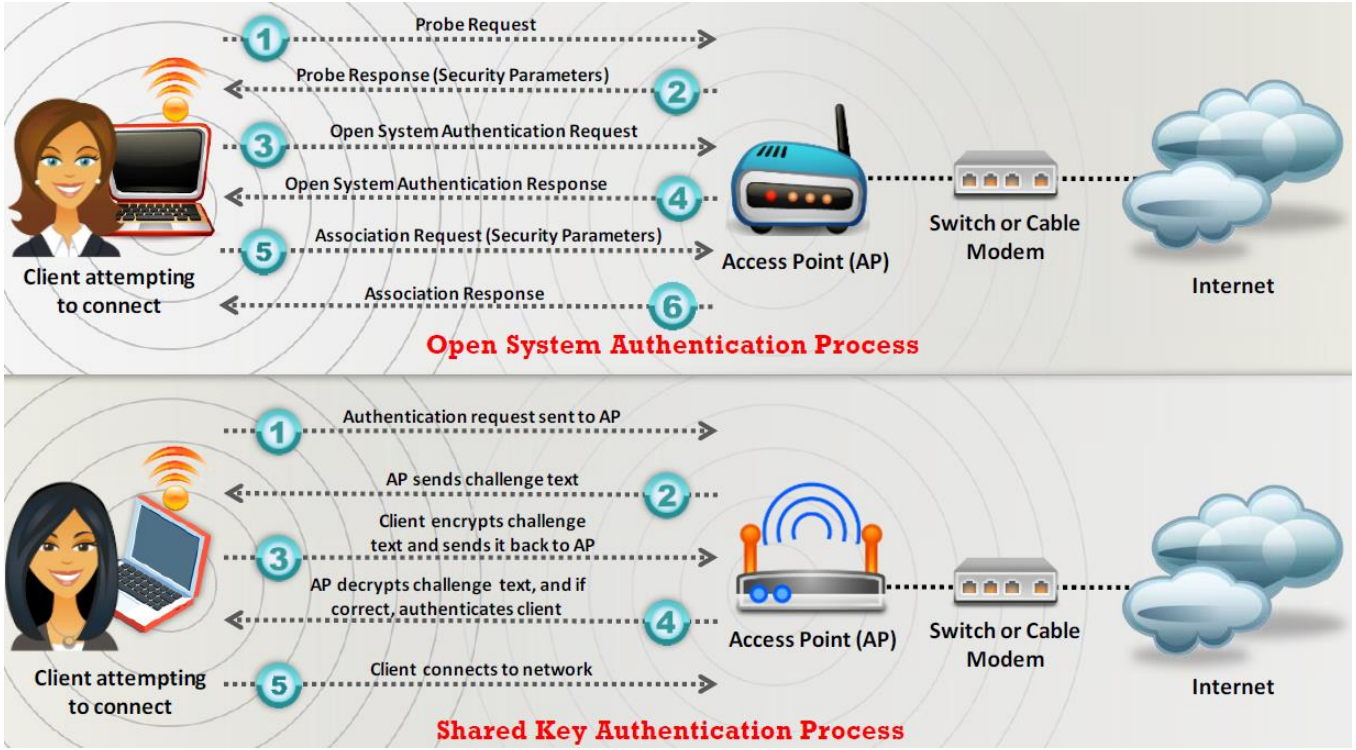
9. Wi-Fi Authentication

Module 17

9.1. Wi-Fi Authentication

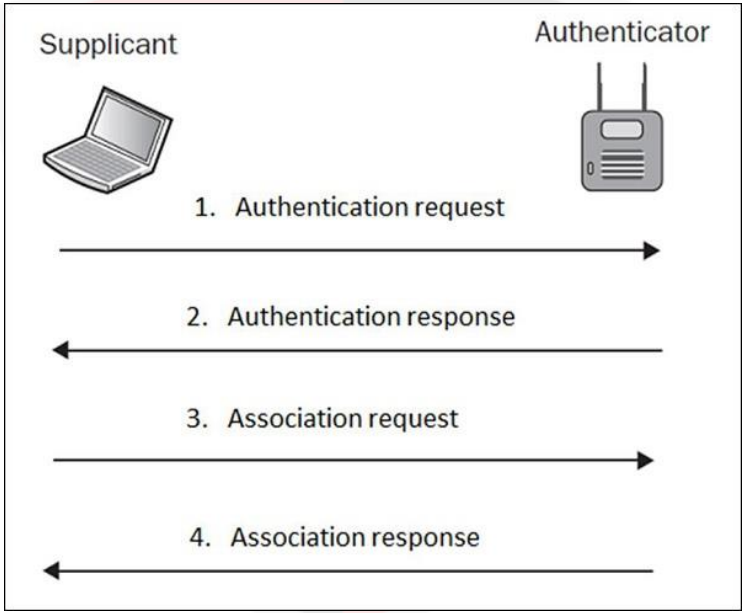
Module 17

Wireless Concepts



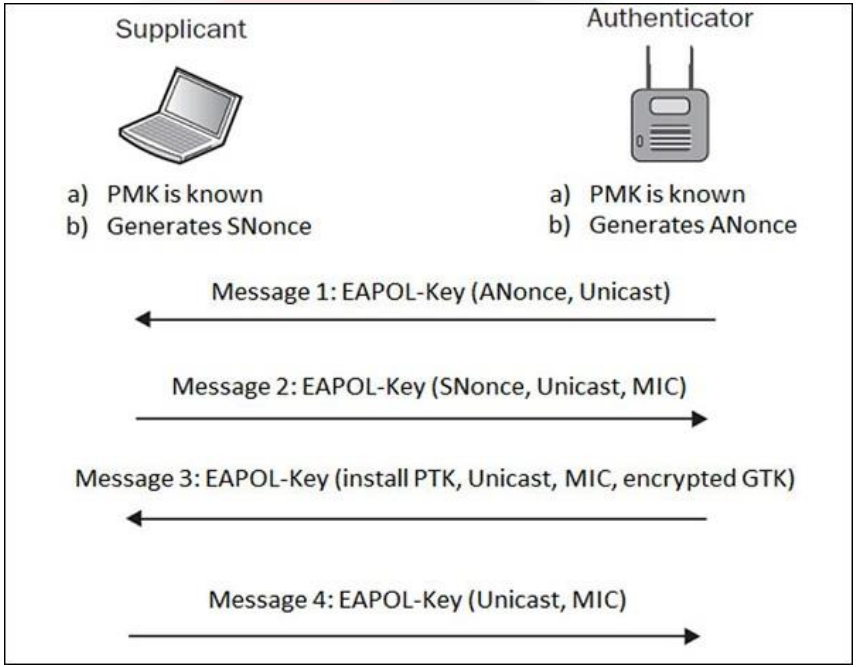
Wireless Concepts

Open Authentication



Wireless Concepts

EAP-based 4-way handshake (with WPA/WPA2)



Wireless Concepts

EAP-based 4-way handshake (with WPA/WPA2)

- The Pairwise Master Key (PMK) is something a hacker would like to collect, in order to break the network encryption scheme. PMK is only known to the Supplicant and Authenticator, but is not shared anywhere in transit.
- HOWEVER, the session keys are the combination of ANonce, SNonce, PMK, MAC addresses of Supplicant and Authenticator. We may write that relation, as the mathematical formula –
  - **Sessions_keys = f(ANonce, SNonce, PMK, A_MAC, S_MAC).**
- In order to derive a PMK from that equation, one would have to break AES/RC4.
- It is definitely a recommended authentication approach to use, and definitely safer than using Open Authentication.

EAP-based 4-way handshake (with WPA/WPA2)

- **PMK- Pairwise Master Key:**
  - PSK (Pre-Shared Key) and passphrase, they are the same but different. The passphrase is the password that we are giving to our network- to our AP.
  - The PSK is the passphrase but he (the PSK) took it and translate it to 256 bits of string. In WPA/WPA2-personal the PMK is the PSK.
  - Both the machines have the PMK in assumed that the client knows the password for the WI-FI.
  - PTK is generated with the help of PMK. As we discussed above in order to generate PTK, we need the following input.
  - *PTK = PRF (PMK + Anonce + SNonce + Mac (AA)+ Mac (SA))*

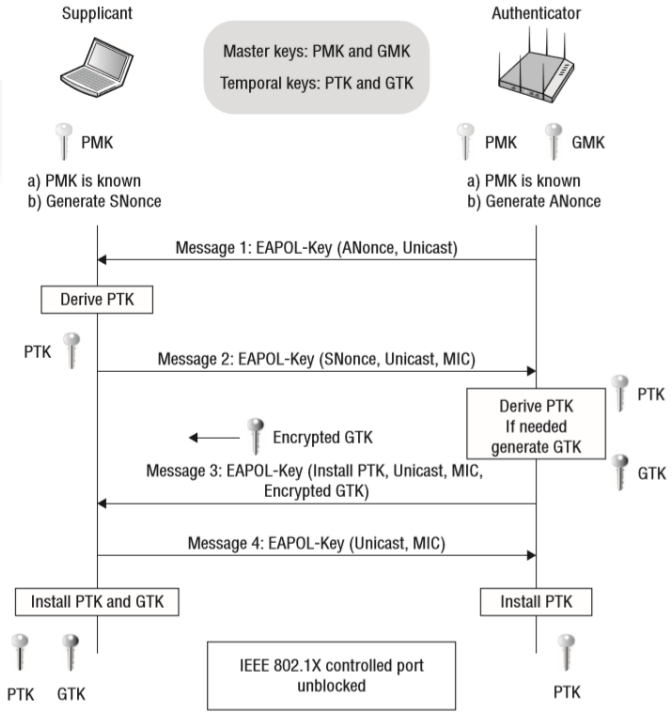
EAP-based 4-way handshake (with WPA/WPA2)

- **GMK- Group Master Key:**
  - Group master key is used in a 4-way handshake to create GTK. GTK is generated on every access point and shared with the devices connected to this AP.
- **GTK (Group Temporal Key):**
  - Group temporal key is used to encrypt all broadcast and multicast traffic between an access point and multiple client devices.
  - GTK is the key which is shared between all client devices associated with 1 access point. For every access point, there will be a different GTK which will be shared between its associated devices.

EAP-based 4-way handshake (with WPA/WPA2)

- **PTK (Pairwise Transit Key):**
  - Pairwise transit key is used to encrypt all unicast traffic between a client station and the access point. PTK is unique between a client station and access point. To generate PTK, client device and access point need the following information.
  - *PTK = PRF (PMK + Anonce + SNonce + Mac (AA)+ Mac (SA))*
  - **Anonce** is a random number generated by an access point (authenticator), **Snonce** a random number generated by the client device (supplicant). MAC addresses of **supplicant** (client device) and MAC address of **authenticator** (access point). **PRF** is a pseudo-random function which is applied to all the input.

Wireless Concepts



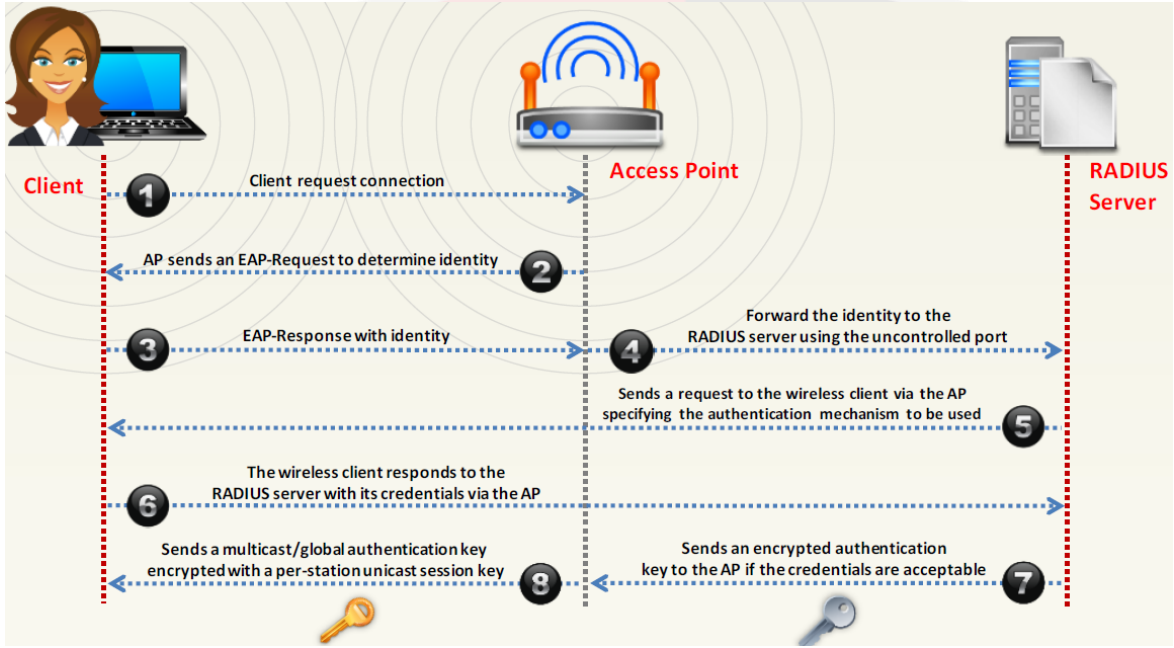
EAP-based 4-way handshake (with WPA/WPA2)

- **Message 1:** AP sends to the client his ***ANONCE***. Now the client has everything he needs to create the ***PTK*** because he got the ANONCE, it was the only thing that was missing for him.
- **Message 2:** The client sends to the AP his ***SNONCE*** with a ***MIC***, the MIC is mainly for the AP to recognize that this message is really from this client, its like a signature (a high level algorithm signature).
  Now, after the AP got the message he has everything he needs to create the PTK and that is what he does.

- **EAP-based 4-way handshake (with WPA/WPA2)**
  - **Message 3:** The AP sends to the client the GTK because he is going to be his new client.
    The client get the GTK and install it.
  - **Message 4:** The client sends to the AP that everything is OK and installed.

Wireless Concepts

Wi-Fi Authentication Process Using a Centralized Authentication Server



9.2. Wi-Fi Protected Setup (WPS)

Module 17

Wireless Concepts

- The **Wifi protected setup (WPS)** is a wireless network security standard that tries to make connection between a router and wireless devices in a faster and secure way.
- WPS works only for wireless networks that use a password that is protected with the ***Wifi Protected Access Personal (WPA)*** or ***Wifi Protected Access2 (WPA2)*** Personal security protocols.
- It comprises of a 8-digit PIN which acts as an optional certification which allows a user to easily protect the network at home or small business.

Wireless Concepts

Modes of WPS

- **PIN method**: PIN is either read from sticker or displayed on the new wireless device. It is provided by the access point, to be entered from the new device.
- **Push button method**: At just one click/push of a button, a user can connect multiple devices to the network, without entering the password. It requires physical access to the access point.
- **Near-field communication method**: Clients are brought nearer to the access point. This provides strong protection against unintended devices.

Wireless Concepts

Advantages of WPS:

- No need to know SSID, passphrases or security keys
- Auto-configuration of SSID and WPA security
- Supported by various OS
- Security keys are random, so cannot be guessed
- Information can be exchanged online using Extensible Authentication Protocol (EAP)

Wireless Concepts

Vulnerabilities in WPS:

- **Online brute-force attack**: On PIN-based WPS. There are 7 unknown digits in each PIN, which can make 10,000,000 combinations.
- **Offline brute-force attack**: Also called ***Pixie-dust***. After obtaining initial value (*E-S1 and ES-2*), attack is performed offline.
- **Physical Security**: Access points have PIN printed on them. If its not kept in a secure area, it is likely to be misused.
- **Reaver tool**: Implements a brute force attack against WPS PINs to recover WPA/WPA2 passphrases. I can recover target APs plaintext WPA/WPA2 passphrase in 4-10 hours.

10. How to break Encryptions?

Module 17

Wi-Fi Encryption

WEP vs WPA vs WPA2

There are three widely known security standards in the world of wireless networking. The biggest difference between those three, are the security model they can provide.

Security Standard	Encryption algorithm user	Authentication methods	Possibility of breaking the encryption
WEP	WEP (based on RC4)	Pre-Shared Key (PSK)	▫ Initialization Vector (IV) collision attack ▫ Weak Key Attack ▫ Reinjection Attack ▫ Bit flipping attack
WPA	TKIP (based on RC4)	Pre-Shared Key (PSK) or 802.1x	- cracking the password during initial 4-way handshake (assuming that it's relatively short password <10 characters)
WPA2	CCMP (based on AES)	Pre-Shared Key (PSK) or 802.1x	

Wireless Threats

Module 17

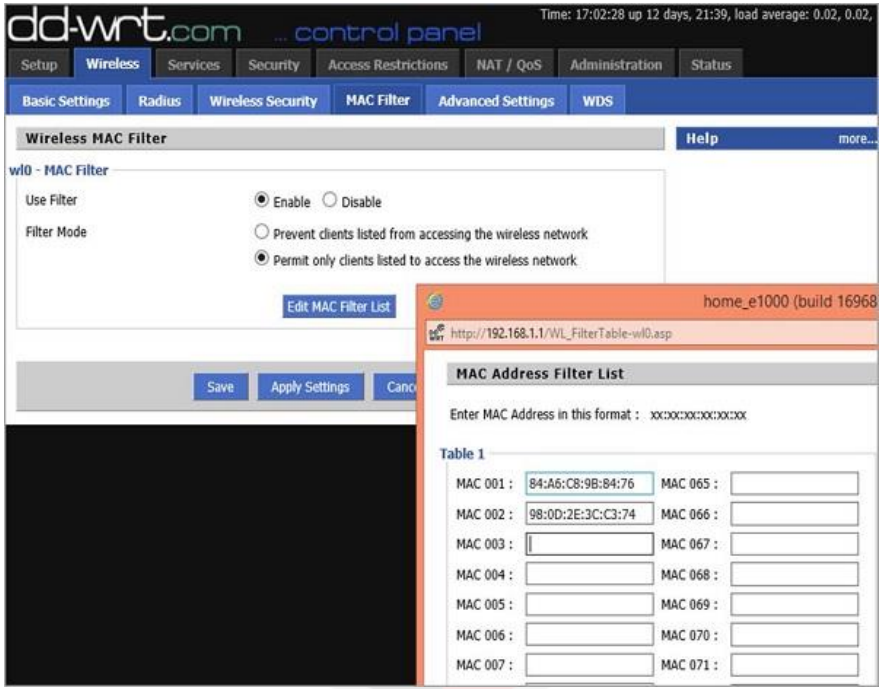
1. Access Control Attacks

Module 17

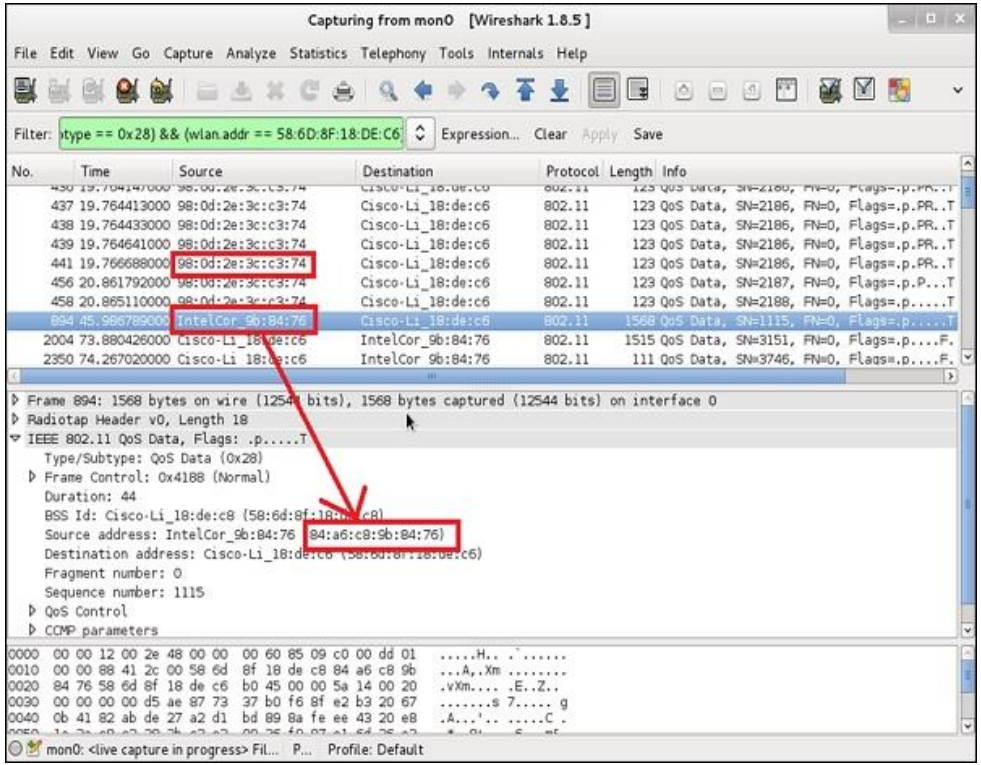
Wireless Threats

- Very well-known access control mechanism used in wireless networks is based on MAC address whitelisting. The AP stores a list of authorized MAC addresses that are eligible to access the wireless network. With tools available nowadays, this security mechanism is not a very strong one, since MAC address may be spoofed very simply.
- The only challenge is to find out what MAC addresses are allowed by AP to authenticate to the network. But since wireless medium is a shared one, anyone can sniff the traffic flowing through the air and see the MAC addresses in the frames with valid data traffic (they are visible in the header that is not encrypted).

Wireless Threats



Wireless Threats



Wireless Threats

```
root@kali:~# ifconfig wlan0 down
[3]   Done                    wireshark
root@kali:~# macchanger --mac=84:A6:C8:9B:84:76 wlan0
Permanent MAC: ac:a2:13:64:53:92 (unknown)
Current   MAC: ac:a2:13:64:53:92 (unknown)
New       MAC: 84:a6:c8:9b:84:76 (unknown)
root@kali:~#
root@kali:~# ifconfig wlan0 up
root@kali:~#
root@kali:~# ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr 84:a6:c8:9b:84:76
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@kali:~#
```

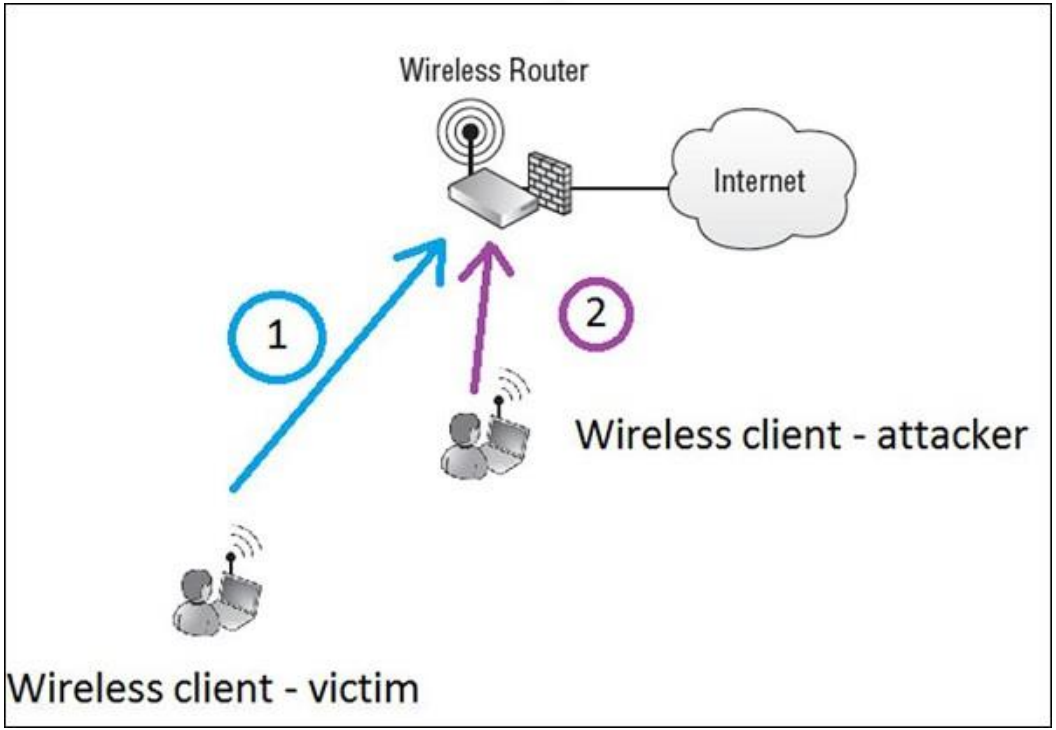
2. Integrity Attacks

Module 17

Wireless Threats

- Suppose that legitimate client called victim (Step 1) is writing an e-mail to the friend asking for money of 1000$ and putting bank account number in the e-mail.
- Assuming the information is not well encrypted (or attacker broke the encryption and have the chance of reading everything in clear text), wireless attacker (Step 2) reads the whole packet flowing in the air to the AP. The attacker modifies a message by swapping the bank account number to its own and re-inject a message back to the air, to go to the internet via the AP.
- In that situation, if there are no integrity checks that would detect a change in the content of the message - the recipient would get a message with a modified bank account number.

Wireless Threats



3. Confidentiality Attacks

Module 17

Wireless Threats

- **No Encryption/ WEP Encryption** – These are not very secure approaches and should not be used under any circumstances.
- **TKIP Encryption** – This encryption model is used in WPA deployments. It has not yet been cracked, but TKIP is not considered as strong mean of encryption, due to the use of weaker RC4 algorithm.
- **CCMP Encryption** – This is used with WPA2. So far, it is considered the safest encryption model that is based on not-breakable (at least for today) AES algorithm.

4. Availability Attacks

Module 17

Wireless Threats

Layer 1 DOS:

- A radio card is configured to send out a constant RF signal (much like a narrow-band signal generator). While, other valid wireless clients never get a chance of accessing the medium, because whenever they perform a clear channel assessment (short process of checking the "air" before sending any traffic over the wireless), the wireless medium is occupied by this constant transmitter.
- Similar to the de-authentication attacks with aireplay-ng.

Wireless Threats

Layer 2 DOS:

- The most common types of Layer 2 DoS attacks involve spoofing of disassociation or de-authentication management frames. The reason, why it is so efficient is that, those frames are NOT the request frames but notifications!
- Because authentication process is a pre-requisite for association a de-authentication frame will automatically disassociate the client as well.
- Mitigation is to use an 802.11w-2009 Standard Management Frame Protection (MFP). Requires that management frames are also signed by a trusted AP, and else, they should be neglected.

Wireless Threats

Layer 3 DOS:

- **Fraggle Attack:** Attacker sends a large amount of UDP echo requests to IP broadcast address.
- **Ping Flood Attack:** Attacker sends a large number of ICMP packet to the target computer using ping.
- **Smurf Attack:** Exactly the same step by step operation, as in case of Fraggle Attack. The only difference is that, Smurf attack uses ICMP echo request packets.

5. Authentication Attacks

Module 17

Wireless Threats

- By sniffing the 4-way handshake between the client and the authenticator (AP), one may perform a brute-force to break the encryption and derive the PSK value.
- **LEAP** (Lightweight Extensible Authentication Protocol) generates dynamic WEP keys. In this setup, the password hashes were flowing over-the-air hashed with MS-CHAP or MS-CHAPv2 algorithms. Attack that may be applied to LEAP would consist of the following steps –
  - The username is sent in a clear text.
  - There is a challenge text in clear text.
  - The response text is hashed.
  - Office dictionary attack, inside "**function(password,challenge) = response**" mathematical formula

6. Rogue Access Point Attacks

Module 17

Wireless Threats

- If the network resources are exposed by a rogue access point, the following risks may be identified –
  - **Data Theft** – Corporate data may be compromised.
  - **Data Destruction** – Databases may be erased.
  - **Loss of Services** – Network services can be disabled.
  - **Malicious Data Insertion** – An attacker may use a portal to upload viruses, key loggers or pornography.
  - **3rd Party Attacks** – A company's wired network may be used as a launching pad for 3rd party attacks against other networks across the internet.

7. Client Misassociation

Module 17

Wireless Threats

- Your laptop remembers the list of WLANs that you were connected to in the past, and stores this list in the so-called **Preferred Network List**.
- A malicious hacker may bring its own wireless AP to the physical area, where you are normally using your Wi-Fi. If the signal from that AP, would be better than the one from original AP, the laptop software will mis-associate to the fake (rogue) access point provided by the hacker (thinking it is the legitimate AP, you have used in the past).
- These kind of attacks are sometimes referred to as **Honeypot AP Attacks**.

Wireless Threats

8. Misconfigured Access Point Attack

Module 17

Wireless Threats

- Most common areas of misconfiguration, that leads to wireless cracking's are –
  - Some AP configurations are left to **factory defaults**, like usernames and passwords or default WLAN's broadcasted (SSID's) and default settings may be found in manuals of the specific vendor on the internet.
  - **Human Error** - advanced security policies are configured on a set of AP's across the organization, and other ones are forgotten and left with default weak security settings.

Wireless Threats

Model	Username	Password
BEFSR series	(none) or admin	admin
E series	admin or (none)	admin or (none)
EA series	admin	admin or (none)
WAG series	admin or (none)	admin or (none)
WRT series	(none)	admin

Wireless Hacking Methodology

Module 17

1. Wi-Fi Discovery

Module 17

Wireless Threats

- Wi-Fi discovery is a process used to learn about WLAN's presence in the environment.
- WiFi discovery process is not against any law, you are simply, passively listening to the Wi-Fi frequency bands, using your wireless client.
- Information you may look for: **SSID** name, received **signal strength**, **802.11 standard** used, **encryption** and **authentication** set on **WLAN, BSSID** (MAC address of the AP, in case you would like create a fake AP with the same MAC address) and what **channel** it operates on.
- You need to use specific tools that uses wireless hardware and listens on either a 2.4GHz or a 5GHz band.

Wireless Threats

Wardriving

- Wardriving is the process of finding a Wireless Network (wireless network discovery) by a person in a car using their personal laptop, smartphone or other wireless client tools.
- Basically, the intention is to find some free-access wireless network, that malicious user can use without any legal obligations. Examples might be some market, that offer free Wi-Fi, without registration or some hotel that you can just register with fake data.
- The method of finding those WLAN's are exactly the same as described above in this wireless discovery section.

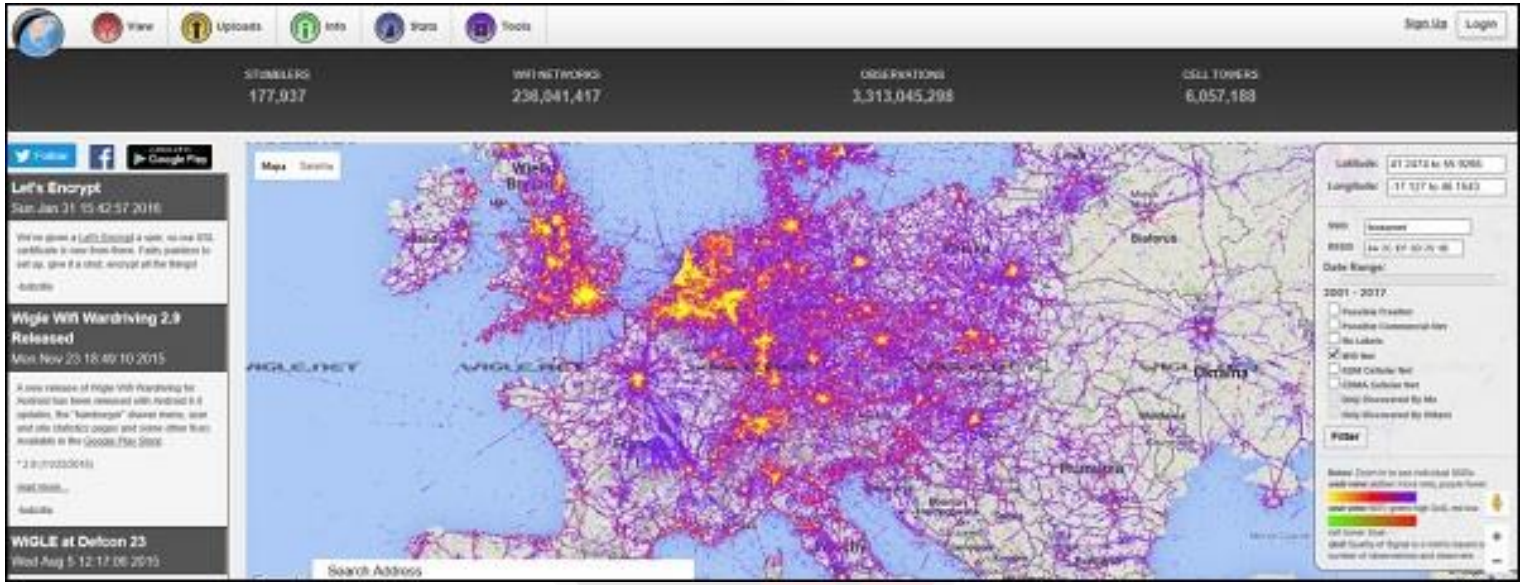
2. GPS Mapping

Module 17

Wireless Threats

- There is a number of satellites that send a low-power radio signal towards the piece of earth it covers. The GPS device that you use, for example a smartphone with google maps, receives that signal from multiple satellites at the same time. The device itself combines those signals together and calculate current geographical location on earth.
- The idea of GPS mapping is to map a wireless network that the user encounters on the global map of wireless network in reference to its geographical location. One may use the already mentioned **Kismet** tool to map its wireless network to the geographical location, and then put its coordinates on the google earth map.
- There is website on the internet **http://wigle.net** that you can use to see how many WLAN's are GPS mapped. You can use this website to map GSM cellular network as well.

Wireless Threats



3. Wireless Traffic Analysis

Module 17

Wireless Threats

- The type of data, that is valuable to collect are BSSID, WEP IV, TKIP IV, CCMP IV, EAP 4-way handshake exchange, wireless beacon frames, MAC addresses of communicating parties, etc.
- Usage of **Wireshark** in both Windows and Linux are very intuitive - both environments provide a GUI that looks the same for both systems.
- When the program starts, you only need to indicate the physical interface, that would be used for traffic sniffing (you can select any interface, either wired one or wireless one), and then proceed with traffic sniffing.

Wireless Threats

- **Filter Field** – Wireshark is equipped with a very good filtering tool that allows limiting the real-time traffic output. It is extremely useful, when you need to extract particular flows out of hundreds of packs coming every second from all the wireless clients.
- **Traffic Output** – In this section, you can see all the packets showing up, that were sniffed on the wireless interface, one by one.
- **Decoded Parameters of the Data** – This section lists all the fields existing in a frame (all the headers + data). We can see, that some set of information is in the form of unreadable data (encrypted), and in 802.11 header you can find CCMP information (AES encrypted), so it must be WPA2 Wi-Fi network.

.

Wireless Threats

- **Hex Dump** – The Hex Dump is exactly the same information you have above in "decoded parameters of the data" but in a hexadecimal format. The reason for that is that, hexadecimal representation is the original way the packet looks like, but Wireshark has thousands of "traffic templates", which are used to map specific HEX values to a known protocol field. For example, in a 802.11 header the bytes from 5 to 11 are always the source of a MAC address of the wireless frame, using the same pattern mapping, Wireshark (and other sniffers) can re-construct and decode static (and well known) protocol fields.

4. Launch Wireless Attacks

Wireless Threats

Passive Attacks

- **Breaking WEP Encryption:** Behind the scenes to break a WEP encryption, one has to sniff a large volume of data packets. The next step is to get the same IV vector inside the wireless frames, and the last step is to break the WEP encryption model offline.
- **Breaking WPA/WPA2 Encryption:** One needs to sniff EAP 4-way handshake between a wireless client and the AP. Afterwards, an offline dictionary (or offline brute-force attack) is conducted on the collected encrypted packets. Sometimes, you need to inject wireless de-authentication frames, forcing the wireless victim to de-authenticate and then re-authenticate again, thus sniffing the new authentication 4-way handshake.

Wireless Threats

Sniffing the traffic between communicating parties

- Assuming that you somehow know the encryption key, you may sniff the communication between parties (for example with Wireshark), and then decode the conversation (since you know the keys). Assuming that parties were not using any protocols that is natively using encryption (for example cleat text HTTP), you are free to see what the user was doing and track his moves on the internet.

Wireless Threats

Active Attacks

- **Injection of Wireless Traffic** – A classic example of Layer 2 DoS, used by flooding of de-authentication frames.
- **Jamming Attacks** – As you remember, this is a type of Layer 1 DoS attack. Jamming devices are used to create interferences with a valid RF of Wi-Fi network, thus leading to WLAN service degradation.
- **Man-in-the-Middle Attack** – The attacker is equipped with two wireless network cards and may use one of them to connect to the original AP as the client; and use the second wireless card to broadcast some fake SSID using software emulating AP. Client associates to "fake AP" and all the client traffic going to the internet is directly forwarded through attacker.

Wireless Threats

Active Attacks

- **Injection of Wireless Traffic** – A classic example of Layer 2 DoS, used by flooding of de-authentication frames.
- **Jamming Attacks** – As you remember, this is a type of Layer 1 DoS attack. Jamming devices are used to create interferences with a valid RF of Wi-Fi network, thus leading to WLAN service degradation.
- **Man-in-the-Middle Attack** – The attacker is equipped with two wireless network cards and may use one of them to connect to the original AP as the client; and use the second wireless card to broadcast some fake SSID using software emulating AP. Client associates to "fake AP" and all the client traffic going to the internet is directly forwarded through attacker.

Setting up your Lab

Module 17

Wireless Threats

Antennas

- Antennas are used to "translate" information flowing as an electrical signal inside the cable and into the electromagnetic field, which is used to transmit the frame over a wireless medium.
- Every wireless device (either AP or any type of wireless client device) has an antenna that includes a transmitter and the receiver module.
- One of the biggest advantages of external antennas (comparing to most of the internal antennas you might meet built-in to the equipment), is that they can be configured in a so-called "***monitor mode***"
- These antennas on the client side are usually embedded in ***wireless adapters***, both internal or external ones.

Wireless Threats

Wireless Threats

Wireless Cards Operation Modes

- Master (acting as an access **point**),
- Managed (client, also known as station),
- **Ad hoc**,
- **Repeater**,
- Mesh,
- Wi-Fi Direct,
- TDLS and
- **Monitor mode**.

Wireless Threats

Monitor Mode

- **Monitor mode**, or RFMON (Radio Frequency MONitor) mode, allows a computer with a wireless network interface controller (WNIC) to monitor all traffic received on a wireless channel.
- Unlike ***promiscuous*** mode, which is also used for packet sniffing, monitor mode allows packets to be captured without having to associate with an access point or ad hoc network first.
- Monitor mode only applies to wireless networks, while promiscuous mode can be used on both wired and wireless networks.
- Not all wireless cards support RFMON mode.

Wireless Threats

Limitations of Monitor Mode

- Usually the wireless adapter is unable to transmit in monitor mode and is restricted to a single wireless channel, though this is dependent on the wireless adapter's driver, its firmware, and features of its chipset.
- Also, in monitor mode the adapter does not check to see if the cyclic redundancy check (*CRC*) values are correct for packets captured, so some captured packets may be corrupted.

Wireless Threats

Packet Injection

- Packet injection means sending data while in Monitor mode because it's a passive-only mode.
- Sending and receiving management and control frames is necessary for impersonating base stations and clients, and for listening to frames that are meant for specific adapters.
- The dreadful ***deauthentication frame***, is used to capture the WPA 4-way handshake or to force a user into a malicious AP, or to recover a hidden SSID, etc.
- Most of the adapters lack support of RFMON and Packet Injection for security and cost efficiency.

Wireless Threats

Soft AP

- **SoftAP** is an abbreviated term for "***software enabled access point***".
- This is software enabling a computer which hasn't been specifically made to be a router into a wireless access point. It is often used interchangeably with the term "***virtual router***".
- ***Microsoft*** added a feature called "***Virtual Wi-Fi***" to Windows 7 and later operating systems, which enabled a Wi-Fi card to act as both a Wi-Fi client and a wireless access point simultaneously.
- The "virtual" Wi-Fi feature allows desktop computers to create a ***wireless hotspot*** that other wireless devices in the vicinity can use.

Wireless Threats

Wireless Adapters Supporting RFMON

- Alfa AWUS036H
- Alfa AWUS036NEH
- Alfa AWUS036NH
- Alfa AWUS036NHA
- Alfa AWUS051NH
- TP-Link TL-WN722N

Wireless Threats

Wireless Adapters Supporting RFMON

- Melon RTL8187L
- RTL 8187L Mini PCI
- TP-Link WN722H
- Panda PAU05

Wireless Threats

Wireless Standards

- IEEE 802.11bgn = 2.4GHz only
- IEEE 802.11gn = 2.4GHz only
- IEEE 802.11agn = 2.4GHz + 5GHz
- IEEE 802.11ac = 2.4GHz + 5GHz
- IEEE 802.11abgn = 2.4GHz + 5GHz

Wireless Threats

5 GHz Supporting Chipsets

- AWUS052NHS - RT3572
- AWUS052NH - RT3572
- AWUS051NH -
- awus052nh - RT3572
- awus052nhs - RT3572 1 antenna only
- AWUS051NH V2
- AWUS051NH (500mW) 5GHz capable.

Wireless Threats

Single Band (2.4 GHz) Wireless Adapters

- Alfa AWUS036NHA
- Alfa AWUS036NH
- TP-LINK TL-WN822N
- D-Link DWA-140
- ASUS USB-N14
- Panda PAU06 USB
- Panda PAU05 USB
- Tenda W311M

Wireless Threats

Dual Band Wireless Adapters

- Alfa AWUS1900
- Alfa AWUS036ACH
- Alfa AWUS036AC
- TRENDnet TEW-809UB
- Panda Wireless PAU09 N600
- ASUS USB-AC68
- ASUS USB-AC56TP-LINK Archer T9UH

Countermeasures

Module 17

1. How to detect and block Rogue AP?

Wireless Threats

- To prevent the installation of rogue access points, organizations can install wireless intrusion prevention systems to monitor the radio spectrum for unauthorized access points.
- In order to detect rogue access points, two conditions need to be tested:
  - whether or not the access point is in the managed access point list: compare wireless MAC address against the managed access point BSSID list.
  - whether or not it is connected to the secure network: cover different types of access point devices, bridging, NAT (router), unencrypted wireless links, encrypted wireless links

Wireless Threats

- If the unauthorized access point is found not connected to the secure network, it is an external access point.
- Most computers will automatically join any network with the same name of a network they've joined before. You should go into your computer's Wi-Fi settings and delete any networks you no longer wish to connect to.
- If you don't want your computer's connection to be taken over by a random network you forgot you connected to weeks ago, make sure to delete these and test to make sure your computer doesn't connect to networks with the same name.
- Make sure to use a VPN whenever possible to ensure that even if your connection is intercepted, it won't be as easy as injecting content into webpages to steal your credentials.

2. How to Defend Against Wireless Attacks?

Wireless Threats

Always Be Suspicious

- If someone presents a story where the solution is to hand over your Wi-Fi credentials, try to present an alternative solution, like "I can look that up for you," and see if they pivot to stay focused on the password.

Better Passwords

- Using password managers like LastPass and KeePassX can make it easier to use unique passwords, but you should avoid passwords like phone numbers, addresses, and not at all related to any other information you've made public.

Wireless Threats

Static IP addressing

- Typical wireless access points provide IP addresses to clients via DHCP. Requiring clients to set their own addresses provides little protection against a sophisticated attacker.

SSID hiding

- A simple but ineffective method to attempt to secure a wireless network is to hide the SSID. This provides very little protection against anything but the most casual intrusion efforts.

MAC ID filtering

- One of the simplest techniques is to only allow access from known, pre-approved MAC addresses.

Wireless Threats

Least Privilege

- Only give out your password on a need-to-know basis.
- If someone has a burning desire to get the Wi-Fi password, ask yourself why, and treat it as seriously as giving out a PIN for a bank account. If you don't have the time to secure your network above and beyond what the average person does, don't risk letting anyone in that you don't trust.

Wireless Threats

Disable WPS & Verify with Testing

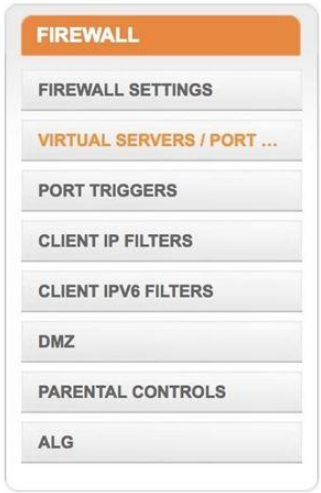
- While many routers offer the convenience of WPS setup PINs, most can be disabled to prevent Reaver or Pixie-Dust attacks from succeeding. Once this is done, restart the router and check to see if the setting is still disabled.
- While this may be enough for some routers, some older models may say they've disabled the WPS setup PIN when in reality they still respond to WPS and Pixie-Dust attacks. If you suspect this may be the case, it would be wise to run a tool like Wash, which will locate every network nearby which has the WPS PIN enabled. If your router appears on this list even after you changed the setting, it's probably time to buy a new router.

Wireless Threats

Disable Remote Access & Port Forwarding

- The first step you can take to ensure your devices aren't exposing ports directly to the internet is to log into the administrative portal and look for a tab that mentions "Port Forwarding" rules or settings.
- This is the section of the router where you can add port forwarding rules, and it may be located under the "Advanced" tab on some devices. When you find the page, you should expect to see no port forwarding rules there, as seen in the image below.

Wireless Threats



Virtual Servers / Port Forwarding

This function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network.

Virtual Servers / Port Forwarding

Description	Inbound Port	Type	Private IP Address	Local Port
☐ BIG HAXX	22-22	TCP	192.168.0.8	22-22

Add Delete

HACKING

Is an art, practised through a creative mind.