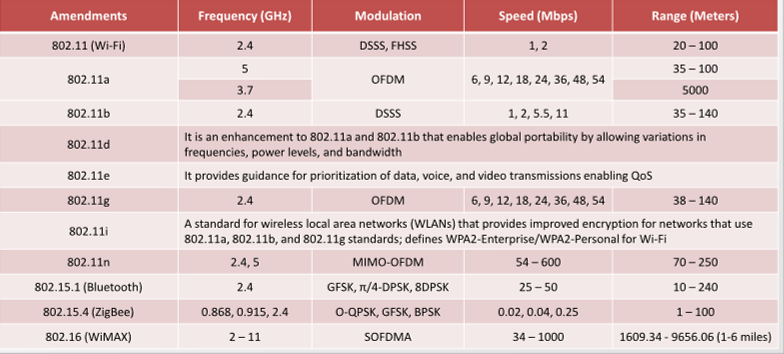
**Module 16: Hacking Wireless Networks**

**Concept**

* GSM
* Bandwidth
* AP
* **BSSID:** Mac address of an AP
* ISM band
* Hotspot
* Association
* **SSID:** Name of a WLAN
* OFDM
* MIMO-OFDM
* DSSS (Direct-sequence Spread Spectrum)
* FHSS

**Wireless Network**

* Types
  + Extension to a wired network
    - SAPs (Software APs)
    - HAPs (Hardware APs)
  + Multiple Access Points
  + LAN-to-LAN wireless network
* Wireless Standards

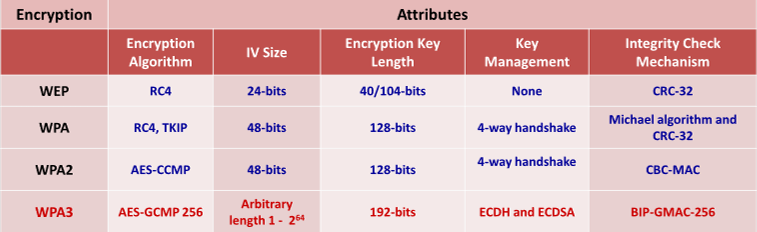


* SSID: Maximum length of 32 bytes, a human-readable text string
  + WIFI authentication modes
    - Open system authentication process
    - Client->AP: Probe request
    - AP->Client: Proble response
    - Client->AP: Open system authentication request
    - AP->Client: Open system authentication response
    - Client->AP: Association request
    - AP->Client: Association response
  + Shared key authentication process
    - Client->AP: Authentication request
    - AP->Client: Challenge text
    - Client->AP: Encrypted challenge text
    - AP->Client: Decrypt challenge text, if corrent, authenticate
    - Client->AP: Connect
* WIFI authentication process using a centralized authentication server
  + A centralized authentication server known as the **RADIUS (Remote authentication dial in user service)** sends authentication keys to both the **AP** and the client.
* Types of wireless antennas
  + Directional antenna
  + omnidirectional antenna: **360 degree** jprozpmta; radoatopm pattern
  + parabolic grid antenna
  + yagi antenna
  + dipole antenna
  + reflector antenna

**Wireless Encryption**

* 802.11i
* WEP
  + Use **24bit IV** to form stream cipher RC4 and CRC-32 checksum
* EAP
* LEAP: Proprietary version of EAP developed by cisco
* WPA: use **TKIP** and **MIC** to provide strong…
  + Use **TKIP (Temporal Key Intergrity Protocol)** that utilizes the RC4 with **128bit** keys and 64bits MIC
  + TKIP elimimateds the weakness of WEP by including **per-packet mixing functions, MIC, extended IV, re-keying mechanisms**
* TKIP: Used in **WPA** to replace WEP
* WPA2: Use **AES** and **CCMP**
  + **WPA2-Person:** Use **PSK (pre-shared key)**
  + **WPA2-Enterprise:** Include **EAP** or **RADIUS**
* AES: Used in **WPA2** to replace TKIP
* CCMP (chaining message authentication code protocol): Used in **WPA2**
* WPA2 Enterprise: Integrate **EAP**
* RADIUS: a centralized authentication and authorization management system
* PEAP
* WPA3: use **AES-GCMP-256** and **HMAC-SHA-384**
  + **WPA3-person:** Mainly used to deliver password-based authentication usging the **SAE** protocol, also known as **Dragonfly Key Exchange.** Resistant to offline dictionary attacks and key recovery attacks
  + **WPA3-enterprise:** Using **GCMP-256** for encryption, **HMAC-SHA-384** for generating keys, **ECDSA-384** for exchanging keys

**Comparison of WEP, WPA, WPA2, and WPA3**

* 

**Issues in WEP, WPA, WPA2**

* **WEP**
  + **CRC32 is insufficient to ensure the complete cryptographic integrity of a packet:** By capturing two packets, an attacker can reliably flip a bit in the encrypted stream and modify the checksum so that the packet is accepted.
  + **IVs are of 24 bits:** The IV is a 24-bit field, which is too small to be secure, and is sent in the cleartext portion of a message. An AP broadcasting 1500-byte packets at 11 Mbps would exhaust the entire IV space in five hours.
  + **WEP is vulnerable to known plaintext attacks:** When an IV collision occurs, it becomes possible to reconstruct the RC4 keystream based on the IV and the decrypted payload of the packet.
  + **WEP is vulnerable to dictionary attacks**: Because WEP is based on a password, it is prone to password-cracking attacks. The small IV space allows the attacker to create a decryption table, which is a dictionary attack.
  + **WEP is vulnerable to DoS attacks:** This is because associate and disassociate messages are not authenticated.
  + **An attacker can eventually construct a decryption table of reconstructed keystreams**: With approximately 24 GB of space, an attacker can use this table to decrypt WEP packets in real time.
  + **A lack of centralized key management makes it difficult to change WEP keys regularly. All Rights Reserved. Reproduction is Strictly Prohibited.**
  + **IV is a value used to randomize the keystream value, and each packet has an IV value:** The standard IV allows only a 24-bit field, which is too small to be secure, and is sent in the cleartext portion of a message.
  + **The standard does not require each packet to have a unique IV:** Vendors use only a small part of the available 24-bit possibilities. Consequently, a mechanism that depends on randomness is not random at all, and attackers can easily determine the keystream and decrypt other messages.
  + **The use of RC4 was designed to be a one-time cipher and not intended for use with multiple messages**
* **WPA**
  + **Weak passwords:** If users depend on weak passwords, the WPA PSK is vulnerable to various password-cracking attacks.
  + **Lack of forward secrecy:** If an attacker captures a PSK, they can decrypt all the packets encrypted with that key (i.e., all the packets transmitted or being transmitted can be decrypted).
  + **Vulnerability to packet spoofing and decryption:** Clients using WPA-TKIP are vulnerable to packet-injection attacks and decryption attacks, which further allows attackers to hijack Transmission Control Protocol (TCP) connections.
  + **Predictability of the group temporal key (GTK):** An insecure random number generator (RNG) in WPA allows attackers to discover the GTK generated by the AP. This further allows attackers to inject malicious traffic in the network and decrypt all the transmissions in progress over the Internet.
  + **Guessing of IP addresses:** TKIP vulnerabilities allow attackers to guess the IP address of the subnet and inject small packets into the network to downgrade the network performance.
* **WPA2**
  + **Weak passwords:** If users depend on weak passwords, the WPA2 PSK is vulnerable to various attacks such as eavesdropping, dictionary, and password-cracking attacks.
  + **Lack of forward secrecy:** If an attacker captures a PSK, they can decrypt all the packets encrypted with that key (i.e., all the packets transmitted or being transmitted can be decrypted).
  + **Vulnerability to man-in-the-middle (MITM) and denial-of-service (DoS) attacks:** The Hole96 vulnerability in WPA2 allows attackers to exploit a shared group temporal key (GTK) to perform MITM and DoS attacks.
  + **Predictability of GTK:** An insecure random number generator (RNG) in WPA2 allows attackers to discover the GTK generated by the AP. This further allows attackers to inject malicious traffic in the network and decrypt all the transmissions in progress over the Internet.
  + **KRACK vulnerabilities:** WPA2 has a significant vulnerability to an exploit known as key reinstallation attack (KRACK). This exploit may allow attackers to sniff packets, hijack connections, inject malware, and decrypt packets.
  + **Vulnerability to wireless DoS attacks:** Attackers can exploit the WPA2 replay attack detection feature to send forged group-addressed data frames with a large PN to perform a DoS attack.
  + **Insecure WPS PIN recovery:** In some cases, disabling WPA2 and WPS can be a time-consuming process, in which the attacker needs to control the WPA2 PSK used by the clients. When WPA2 and WPS are enabled, the attacker can disclose the WPA2 key by determining the WPS personal identification number (PIN) through simple steps.

**Wireless Threats**

* **Access control attacks**
  + **WarDriving:** WLANs are detected by sending probe requests over a connection or by listening to web beacons
  + **Rogue AP:** An AP is installed on a trusted network without authorization
  + MAC spoofing
  + AP Misconfiguration
  + **Ad hoc association:** Using any USB adapter or wireless card, connect the host to an unsecured client to attack a specific client or to avoid AP security
  + Promiscuous client
  + Client mis-association
  + Unauthorized association
* **Integrity attacks**
  + Data frame injection
  + WEP injection
  + Bit-flipping attacks
  + Extensible AP replay
  + Data replay
  + IV replay attacks
  + RADIUS replay
  + Wireless network virus
* **Confidentiality attacks**
  + Eavesdropping
  + Traffic analysis
  + Cracking wep key
  + Evil twin ap
  + Honeypot ap
  + Session hijacking
  + **Masquerading:** Pretend to be an authorized user to gain…
  + MITM attack
  + **Wormhole attack:** Exploit dynamic routing protocols. Attackers locate himself strategically in the target network to sniff and record the ….
* **Availablility Attacks**
  + AP theft
  + Disassociation attacks
  + EAP-failure
  + Beacon flood
  + DoS
  + De-authenticate flood
  + Routing attacks
  + Authenticate flood
  + ARP cache poisoning attack
  + Power saving attacks
  + TKIP MIC exploiot
  + Jamming signal attack
* **Authentication attacks**
  + PSK cracking
  + LEAP cracking
  + VPN login cracking
  + Domain login cracking
  + Key reinstallation attacks
  + ID theft
  + Shared key guessing
  + Password speculation
  + Application login theft
  + **aLTEr attack:** Usually perrformed on LTE devices. Install a virtual comunication tower between authentic endpoints intending too mislead the victim
  + **Sinkhole attack:** Use a malicious node and advertise this node as the shortest possible route to reatch the base station.

**Wireless Hacking Methodology**

* Wifi discovery
  + Passive footprinting: Sniff the packets from the airwave
  + Active footprinting: Send out a probe
  + Wifi chalking techniques
    - **Warwalking:** Walk around with WIFI enabled laptops to detect open wireless network
    - **Warchalking:** Draw symbols in public places to advertise open WIFI networks
    - **Warflying:** Use drones to detect open wireless network
    - **WarDriving:** Drive arount with WIFI enabled laptops to detect…
  + Find wps-enabled aps: **sudo wash -I wlan0**
  + Tools: **inSSIDer Plus, NetSurveyor**
* GPS mapping: Track the location of…
  + Tools: Maptitude Mapping Software, Skyhook
* Wireless traffic analysis
  + Sniff
  + Spectrum analysis: measure the power of the specture
* Launch of wireless attacks
  + Tool: Aircrack-ng Suite
    - **Airbase-ng:** It captures the WPA/WPA2 handshake and can act as an ad-hoc AP.
    - **Aircrack-ng**: This program is the de facto WEP and WPA/WPA2 PSK cracking tool.
    - **Airdecap-ng:** It decrypts WEP/WPA/ WPA2 and can be used to strip wireless headers from Wi-Fi packets.
    - **Airdecloak-ng**: It removes WEP cloaking from a pcap file.
    - **Airdrop-ng:** This program is used for the targeted, rule-based de-authentication of users.
    - **Aireplay-ng:** It is used for traffic generation, fake authentication, packet replay, and ARP request injection.
    - **Airgraph-ng:** This program creates a client–AP relationship and common probe graph from an airodump file.
    - **Airmon-ng:** It is used to switch from the managed mode to the monitor mode on wireless interfaces and vice versa.
    - **Airodump-ng**: This program is used to capture packets of raw 802.11 frames and collect WEP IVs.
    - **Airolib-ng:** This program stores and manages ESSID and password lists used in WPA/ WPA2 cracking.
    - **Airserv-ng:** It allows multiple programs to independently use a Wi-Fi card via a client–server TCP connection.
    - **Airtun-ng:** It creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into a network.
    - **Easside-ng:** This program allows the user to communicate via a WEP-encrypted AP without knowing the WEP key.
    - **Packetforge-ng:** Attackers can use this program to create encrypted packets that can subsequently be used for injection.
    - **Tkiptun-ng:** It injects frames into a WPA TKIP network with QoS and can recover MIC keys and keystreams from Wi-Fi traffic.
    - **Wesside-ng:** This program incorporates various techniques to seamlessly obtain a WEP key in minutes.
    - **WZCook:** It is used to recover WEP keys from the Wireless Zero Configuration utility of Windows XP.
  + Detection of hidden ssids
    - run **airmon-ng** in monitor mode
    - start **airodump-ng** to discover SSIDs
    - use **aireplay-ng** to **de-authenticate** the client to reveal hidden SSID
    - switch to airodump to view the revealed SSID
  + Fragmentation attack
    - When successful, can obtain **1500 bytes of PRGA (pseudo random generation algorithm)**
    - **Do not recover the WEP key** itself
    - PRGA can be used to generate packets with **packetforge-ng**, used for injection attacks
    - At least one packet to be received from the AP
  + MAC Spoofing attack
    - Tools: Technitium MAC Address Changer
  + DoS: Disassociation and De-authentication attacks
  + MITM
    - run **airmon-ng** in monitor mode
    - start **airdump** to discover ssid
    - de-authenticate the client using **aireplay-ng**
    - associate your wireless card with the AP you are accessing with airplay-ng
  + Wireless ARP poisoning
    - Tools: **Ettercap**
  + Rouge AP
    - Tools: MANA Toolkit
  + Evil Twin
  + aLTEr attack
  + Wi-jacking attack
* Wifi encryption cracking
  + WEP encryption cracking
    - airmon-ng
    - airodump
    - associate your wireless card with the target AP
    - inject packets using **aireplay-ng**
    - wait for more than **50000** IVs, crack WEP key using **aircrack-ng**
  + WPA PSK
    - airmon-ng
    - airodump-ng
    - deauthenticate the client: **aireplay-ng**
    - run the capture file through **aircrack-ng**
* Cracking WPA/WPA2 using Wifiphisher
* Cracking WPS using reaver
  + **airmon-ng**
  + Use **wash utility** to detect wps-enabled devices
  + Or **airodump-ng**
  + use reaver
* WPA3
  + dragonblood is a set of vulnerabilities in the WPA3 security standard
  + Tools: **dragonslayer, dragonforce, dragondrain, dragontime**
* WEP cracking and WPA brute forcing
  + WEP cracking tool: **wesside-ng**
  + WPA/WPA2 brute forcing tool: **Fern wifi cracker**
* Compromise the wifi network

**Wireless Hacking Tools**

* WEP/WPA/WPA2 Cracking Tools: **Elcomsoft wireless security auditor**
* Packet snifffer: **SteelCentral Packet Analyzer**, **Omnipeek Network Protocol Analyzer, Kismet, CommView for WIFI**
* Traffic analyzer tools: **AirMagnet Wifi Analyzer PRO**

**Bluetooth Stack**

* A short range wireless communication technology
* Share data over short distances
* Bluetooth hacking
  + **Bluesmacking:** DoS attack, **overflowing bluetooth-enabled devices** with random packets
  + **Bluejacking: send unsolicited messages** via **OBEX** protocol
  + **Bluesnarfing:** the **theft of info** from a wireless device through a bluetooth connection
  + **BlueSniff:** proof of concept code for a bluetooth **wardriving** utility
  + **Bluebugging:** remotely accessing a device and using its features
  + **BluePrinting:** collect info about devices, such as manufacturer, model…
  + **Btlejacking:** bypass security mechanism and listen to info being shared
  + **KNOB attack:** exploit a vulnerability in bluetooth to **eavesdrop all the data** being shared, such as keystrokes, chats, and documents.
  + **MAC Spoofing attack**
  + **MITM / Impersonation attack**
* Bluetooth reconnaissance using **BlueZ**
* Btlejacking using **BtleJack**
* Tools: **Bluetooth View, BlueScan**

**Countermeasure**

* Use WPA2 with AES/CCMP
* Use VPN
* Implement a NAC (Network Access control) or NAP

**Wireless Security Tools**

* Wireless IPS
* Wifi security auditing tools: **Cisco adaptive wireless IPS**
* **WatchGuard WIPS**
* Wifi predictive planning tools: **AirMagnet Planner**
* Wifi vulnerability scanning tools: Zenmap