chapter-16

Hacking Wireless Concepts

Concepts

OFDM

- Orthogonal Frequency division Multiplexing
- encode digital data on multiple carrier frequencies.

MIMO-OFDM

- Multiple Input Multiple Output OFDM
- 4G, 5G broadband wireless communication

DSSS

- Direct Sequence Spread Spectrum
- Original signal multiplied with Pseudo random noise spreading the code

FHSS

- Frequency Hopping Spread Spectrum

- transmits radio signals by switching carrier → many frequency channels.

Amendments	Frequency (GHz)	Modulation	Speed (Mbps)	Range (Meters)
802.11 (Wi-Fi)	2.4	DSSS, FHSS	1, 2	20 – 100
802.11a	5	OFDM	6, 9, 12, 18, 24, 36, 48, 54	35 – 100
	3.7			5000
802.11b	2.4	DSSS	1, 2, 5.5, 11	35 – 140
802.11d	It is an enhancement to 802.11a and 802.11b that enables global portability by allowing variations in frequencies, power levels, and bandwidth			
802.11e	It provides guidance for prioritization of data, voice, and video transmissions enabling QoS			
802.11g	2.4	OFDM	6, 9, 12, 18, 24, 36, 48, 54	38 – 140
802.11i	A standard for wireless local area networks (WLANs) that provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards; defines WPA2-Enterprise/WPA2-Personal for Wi-Fi			
802.11n	2.4, 5	MIMO-OFDM	54 – 600	70 – 250
802.15.1 (Bluetooth)	2.4	GFSK, π/4-DPSK, 8DPSK	25 – 50	10 – 240
802.15.4 (ZigBee)	0.868, 0.915, 2.4	O-QPSK, GFSK, BPSK	0.02, 0.04, 0.25	1 – 100
802.16 (WiMAX)	2 – 11	SOFDMA	34 – 1000	1609.34 - 9656.06 (1-6 miles)

WiFi Authentication Mode

1. Probe Request & Response
2. Open Authentication (Req & Response)
3. Association Req. and Response

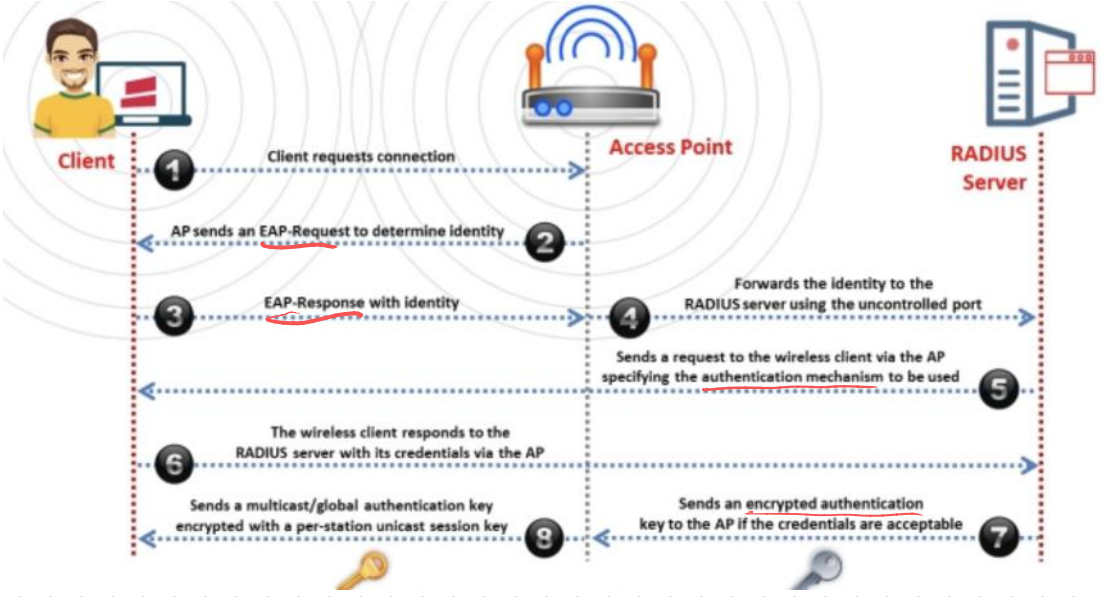
Open Authentication

Shared key Authentication

1. Auth request ; challenge text
2. client encrypt challenge; authentication
3. client connects network.

Radius

1. client Request ; EAP - Request (AP)
2. EAP response : (AP)
3. forwards to RADIUS Server (RS)
4. (RS) request ; client respond.
5. RS → AP (encrypted auth)
6. AP → client (auth key - Session key)



Antenna Types

- Directional (single)
- Omnidirectional (360°)
- Parabolic Grid (satletite dish)
- Yagi (unidirection)
- Dipole (bidirection)
- Reflector (electromagentic energy)

Encryption Types

- WEP
- WPA (TKIP)
- WPA 2 (AES) (CCMP)
- EAP (multiple auth, token, Kerberos, Certs)
- LEAP (cisco - EAP)
- WPA 3 (GCMP)
- PEAP (EAP-TLS)

WEP

- Wired Equivalent Privacy
- 24 bit initialization Vector
- RC4 Cipher → CRC 32 checksum

Problem: Password Cracking, analytical attack.

WPA (Temporal Key Integrity Protocol)

- WiFi Protected Access.
- TKIP - RC4 cipher encryption
- 64 bit MIC Integrity check (MIC)
- rekeying mechanism, message integrity check, per packet mixing function.
- Problem: evaesdrop, spoof packet, GTK discover

WPA2

- Upgrade of WPA.
- CCMP - Counter mode
- AES encryption mode.
- both Personal & Enterprise.
  - Personal → PSK
  - Enterprise → EAP / RADIUS
- Problem: KRACK, GTK discover, MITM, DoS, dictionary attacks.

WPA3

- AES - GCMP 256 encryption
- Personal: SAE Protocol
- Enterprise: GCMP-256.

Encryption	Attributes				
	Encryption Algorithm	IV Size	Encryption Key Length	Key Management	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bits	None	CRC-32
WPA	RC4, TKIP	48-bits	128-bits	4-way handshake	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bits	128-bits	4-way handshake	CBC-MAC
WPA3	AES-GCMP 256	Arbitrary length 1 - 2^{64}	192-bits	ECDH and ECDSA	BIP-GMAC-256

Attacks & Threats

Access Control Attacks

- Wireless access control attacks aim to penetrate a network by **evading WLAN access control measures**, such as AP MAC filters and Wi-Fi port access controls
  - WarDriving
  - Rogue Access Points
  - MAC Spoofing
  - AP Misconfiguration
  - Ad Hoc Associations
  - Promiscuous Client
  - Client Mis-association
  - Unauthorized Association

Integrity Attacks

- In integrity attacks, attackers **send forged control, management**, or **data frames over a wireless network** to misdirect the wireless devices to perform another type of attacks (e.g., DoS)
  - Data Frame Injection
  - WEP Injection
  - Bit-Flipping Attacks
  - Extensible AP Replay
  - Data Replay
  - Initialization Vector Replay Attacks
  - RADIUS Replay
  - Wireless Network Viruses

Confidentiality Attacks

- These attacks attempt to **intercept confidential information sent over wireless associations**, regardless of whether they were sent in clear text or encrypted by Wi-Fi protocols
  - Eavesdropping
  - Traffic Analysis
  - Cracking WEP Key
  - Evil Twin AP
  - Honeypot AP
  - Session Hijacking
  - Masquerading
  - Man-in-the-Middle Attack

Availability Attacks

- Availability attacks aim at **obstructing the delivery of wireless services to legitimate users**, either by crippling those resources or by denying them access to WLAN resources

Access Point Theft	Denial-of-Service	Authenticate Flood
Disassociation Attacks	De-authenticate Flood	ARP Cache Poisoning Attack
EAP-Failure	Routing Attacks	Power Saving Attacks
Beacon Flood		TKIP MIC Exploit

Authentication Attacks

- The objective of authentication attacks is to **steal the identity of Wi-Fi clients**, their personal information, login credentials, etc. to gain unauthorized access to network resources

PSK Cracking	Key Reinstallation Attack	Identity Theft
LEAP Cracking		Shared Key Guessing
VPN Login Cracking		Password Speculation
Domain Login Cracking		Application Login Theft

Rogue AP attack (rogue wireless AP)

Client Mis association

- Setup AP outside corporate perimeter.
- bypass enterprise security policy.

Misconfigured AP:

- SSID Broadcast.
- Weak password.

Unauthorised Association

Soft AP → client card / WLAN to launch virus program.

Attacker → User Machine → Soft AP

↓

Enterprise ← Connection ← Virus

Ad-Hoc Connection

- connects via Ad Hoc Mode (Users)
- Ad-Hoc → Insecure, No auth, encryption
- easily compromise enterprise client.

HoneyPot Attack (Same Name, high power)

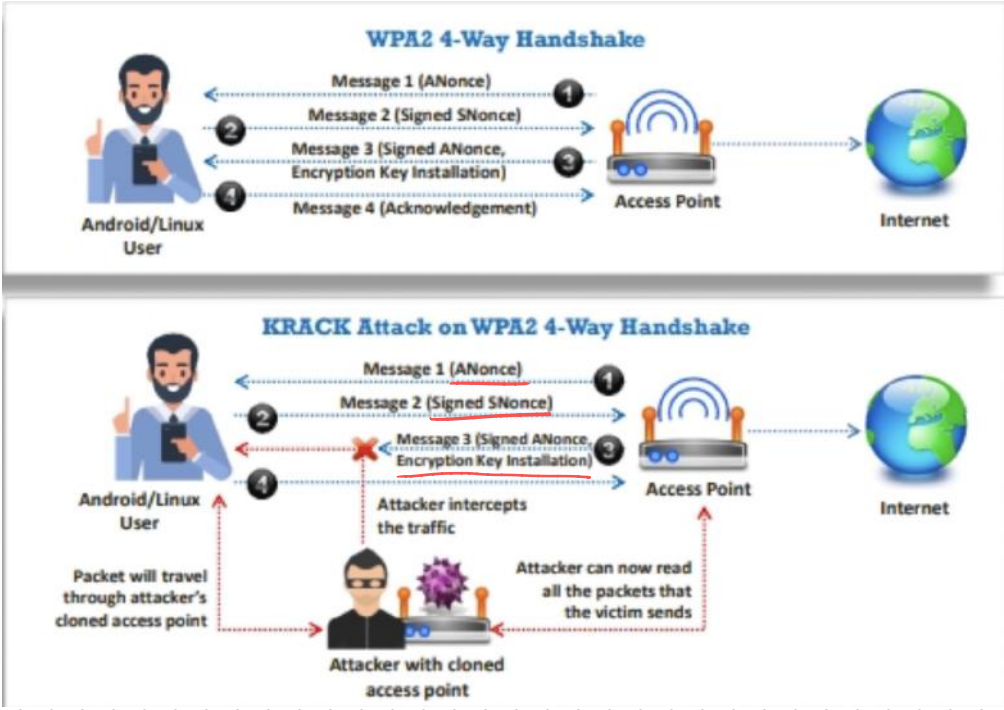
AP MAC Spoofing (spoof Wireless Access Point MAC)

Denial of Service (deauthenticate connection)

KRACK

Sniff

- Key Reinstallation Attack.
- WiFi → 4 way handshake → encryptkey
- exploits 4-way handshake to steal info.



Jamming Signals (CSMA/CA → silence)

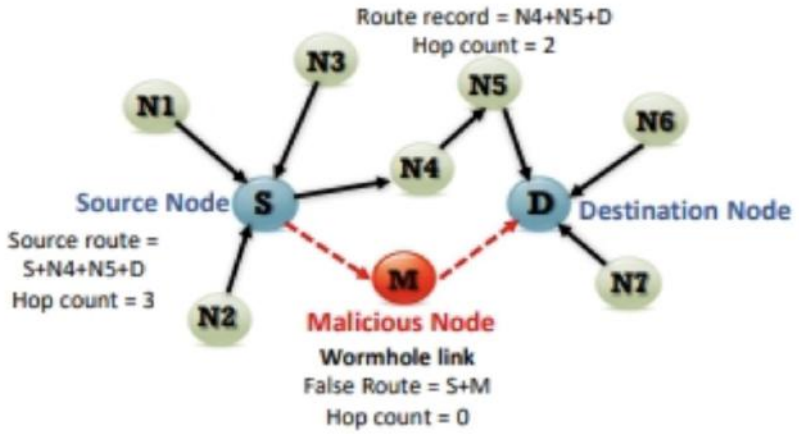
- high gain amplifier → drown AP

aLTEr attack

- performed on LTE device.
- installs virtual / fake tower
- Intercept data transmission.

Wormhole Attack

- exploits dynamic routing protocols (DSR, AODV)
- locates into network (sniff, record)
- creates tunnel to forward (data b/w source & dest)

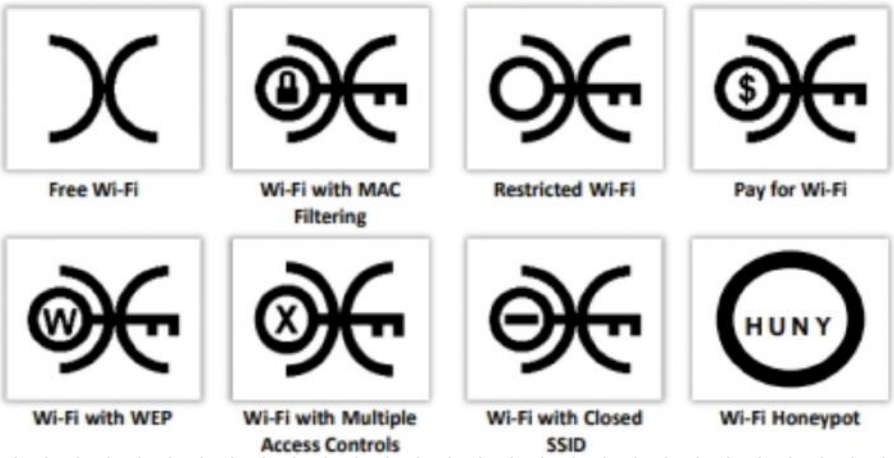


Sinkhole Attack (fake routing – neighbour node)

- Selective forwarding attack
- uses malicious node, advertise node as shortest route to base station.
- attracts all neighbour nodes with fake routing.
- Performs data forging attack.

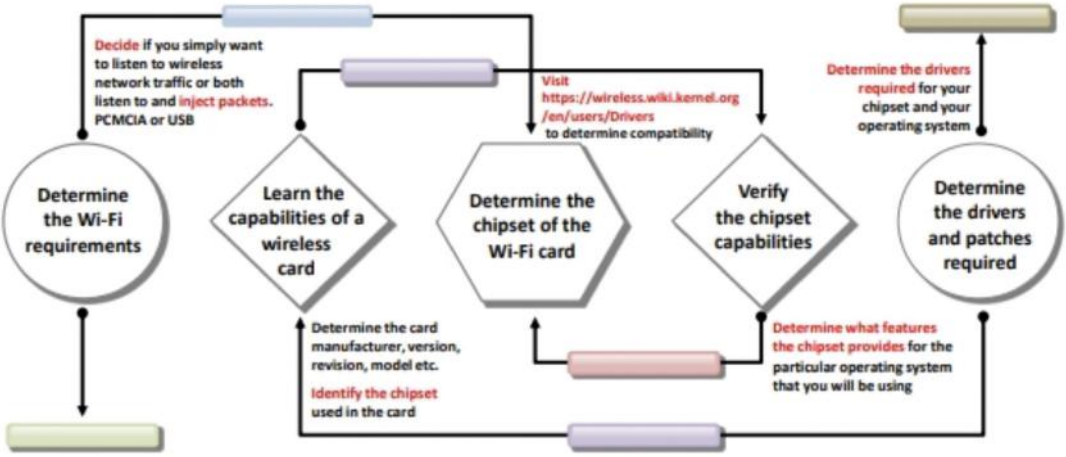
Hacking Methodology

- WiFi Discovery & footprinting
  - Foot printing - active, passive
  - War Walking (walk around)
  - War chalking (draw symbols)



  - War Flying (drone to detect)
  - War driving (drive - laptops)
  - Finding WPS - AP (wash utility) 5GHz
  - Tools: inSSIDer Plus, NetSurveyor

- GPS Mapping
  - Map all discovered networks in database
  - track location (WiGLE) → website
  - Tools: Maptitude Mapping, WiFi Finder (hotspot)
- Wireless Traffic Analysis
  - determine appropriate strategy
  - identify vulnerability
  - determine Broadcast SSID, multiple AP, recovering SSID, authentication, WLAN
  - Tools: AirMagnet, Wireshark, SteelCentral, OmniPeek, CommView
  - choose optimal wifi card.



- Sniffing traffic (Monitor mode)
- Perform Spectrum Analysis
  (RF explorer) → radio Frequency.
- Launch of Wireless Attacks.
  - Aircrack-ng Suite (detector, Sniffer)
  - detection of hidden SSIDs
    (airmon, aireplay)
  - Fragmentation attack. (PRGA)
  - MAC Spoofing (Technitium) (user)
  - Disassociation, Deauthentication.

- MITM attack (forged AP).
  - Aircrack-ng
- Wireless ARP poisoning. (Ettercap)
- Rogue APs (Pocket sized, device, software, USB)
  Tool: MANA Toolkit.
- Evil Twin. (AP, Fake hotspot)
- aLTEr attack. (gather, Attack)
- Wi-Jacking (dnsmasq → karma attack)
- WEP encryption Cracking (airodump)
- WPA/WPA2 cracking (offline/brute)
  ↓ handshake. ↓ PSK.
  Tool: WiFi phisher
- Cracking WPS (Reaver)
- WPA3 (dragonblood exploit)
  tool: Dragonslayer, Dragonforce.

- WEP / WPA Cracking / Brute Force.

  Tool: Wesside ng, Fern Cracker.

  (PRGA, XOR)

Tools:

- Elcomsoft Security Auditor.
- WIBR + (WiFi BRuteforce) [Mobile]
  - discovers weak Password
- Steel Central, OmniPeek, CommView, kismet } (sniffers)
- AirMagnet [WiFi Analyser]

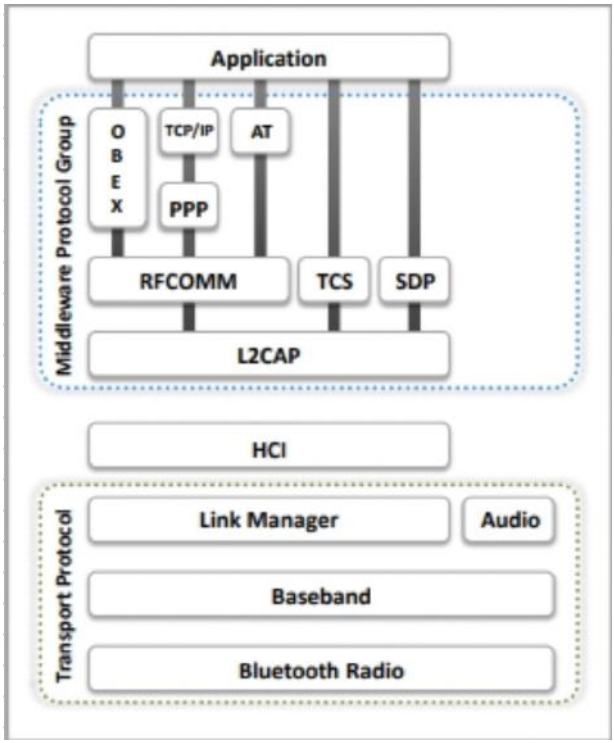
Bluetooth Hacking

Modes:

- Discoverable mode

  (discoverable, limited, non-discover)

- Pairing Mode (Non Pairable, Pairable)



Bluesmacking (overflow, crash)

Bluejacking (unsolicited messages) [obex Protocol]

Bluesnarfing (data exfiltration)

Blesniff (PoC – wardriving)

Bluebugging (remote access)

BluePrinting (reconnaissance)

BtleJacking (bypass security, evaesdrop)

KNOB (evaesdrop data)

Mac Spoofing

MITM

Bluetooth Recon — BlueZ

Btle Jacking — BtleJack.

Tools:

Bluetooth View (Monitors Activity)

Security Tools

- Wireless IPS
- WIPS deployment (several components)
  - AP, (Monitor mode)
  - Mobility Service Engines (alarm)
  - Local Mode (AP)
  - WLAN controllers
  - Wireless Control System
- Cisco Adaptive wireless IPS (threat detection)
- WatchGuard WIPS
- AirMagnet Planner (Predictive Planning)
- ZenMap (Vulnerability Scanning)
- Bluetooth Firewall