16.1 WIRELESS CONCEPTS

- Overview
- SSID
- Authentication Modes

WIRELESS LAN (WLAN)

- LAN based on wireless (radio) technologies
- Wi-Fi is the most common implementation
- Adds security risks because the network is “unbounded”

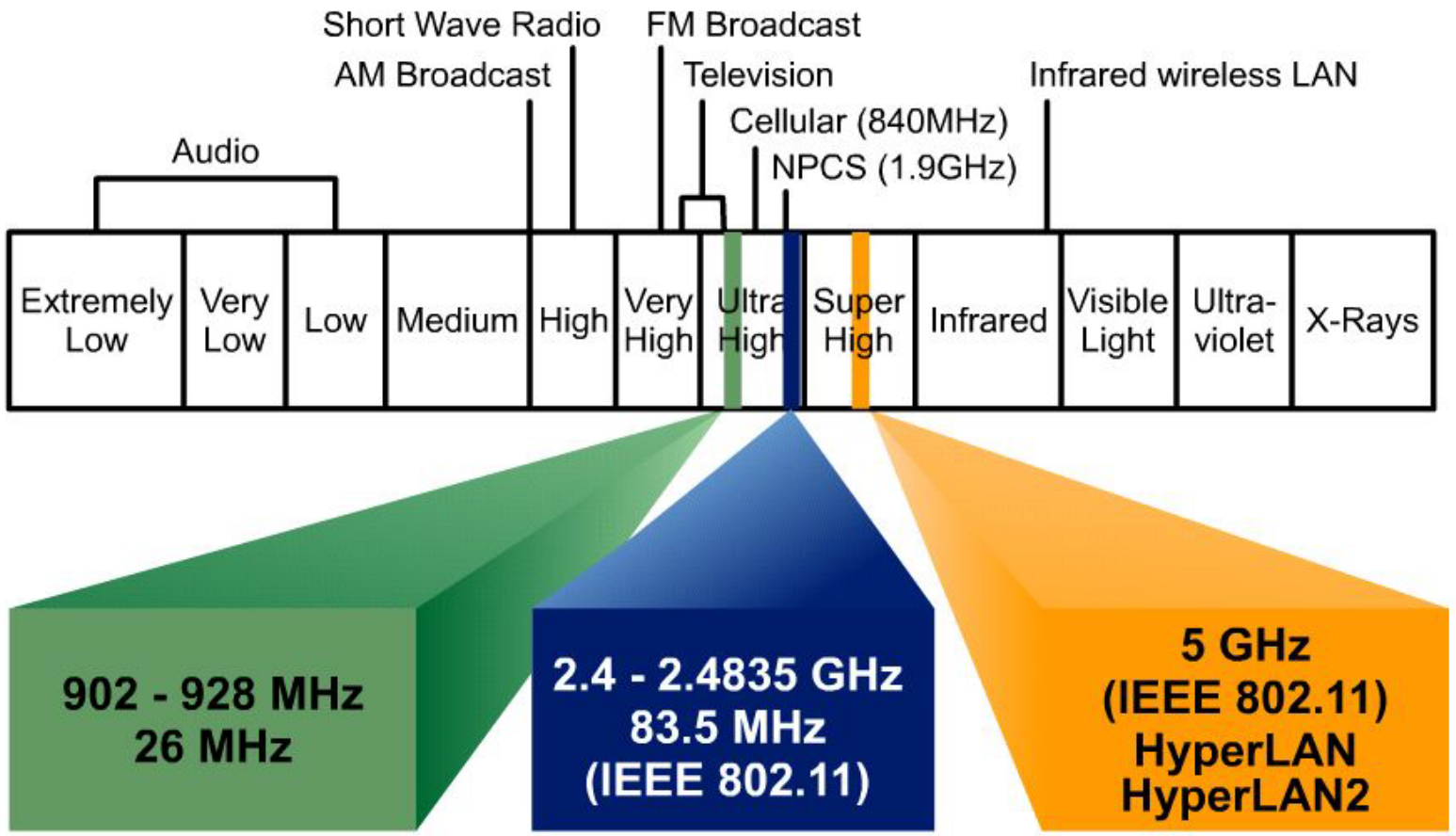
WIRELESS ADVANTAGES AND DISADVANTAGES

- Advantages
  - Fast, easy installation
  - Easy connectivity where cables can't easily be used
  - Connectivity from anywhere, so long as you are in range of an access point
  - Seamlessly extends a wired LAN
  - Makes it easy to offer free Internet for workers and guests
- Disadvantages
  - The unbounded nature of radio makes security a greater concern than in a wired network
  - A single access point can become overwhelmed by too many client requests
  - Enhancements may need new wireless access points and/or wireless cards
  - Wi-Fi networks can be disrupted by electromagnetic and radio frequency interference

ISM BAND

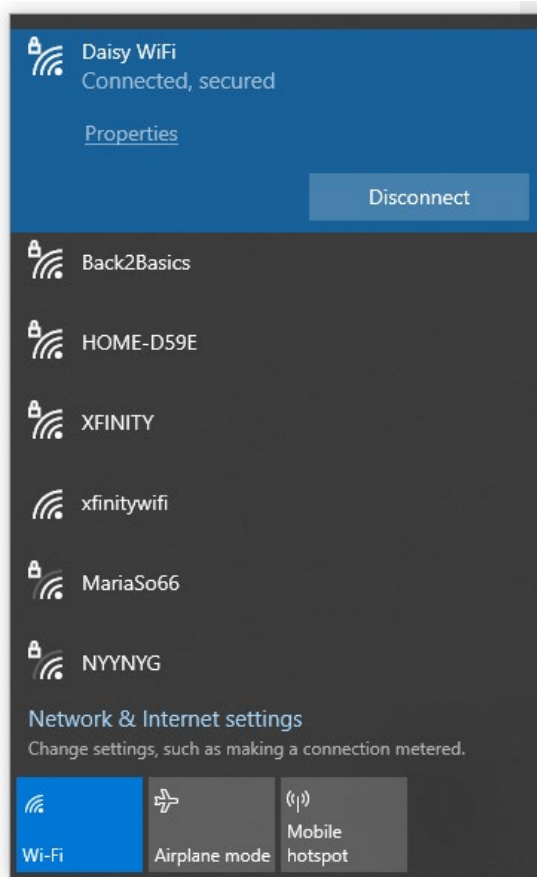
- Industrial, Scientific, Medical Band
- Collection of frequency ranges for various uses
- Devices need not be licensed
- Transmission power must not exceed 1 watt
- Wi-Fi uses the 2.4 GHz, 5 GHz, and 6 GHz bands

ISM ON THE ELECTROMAGNETIC FREQUENCY SCALE



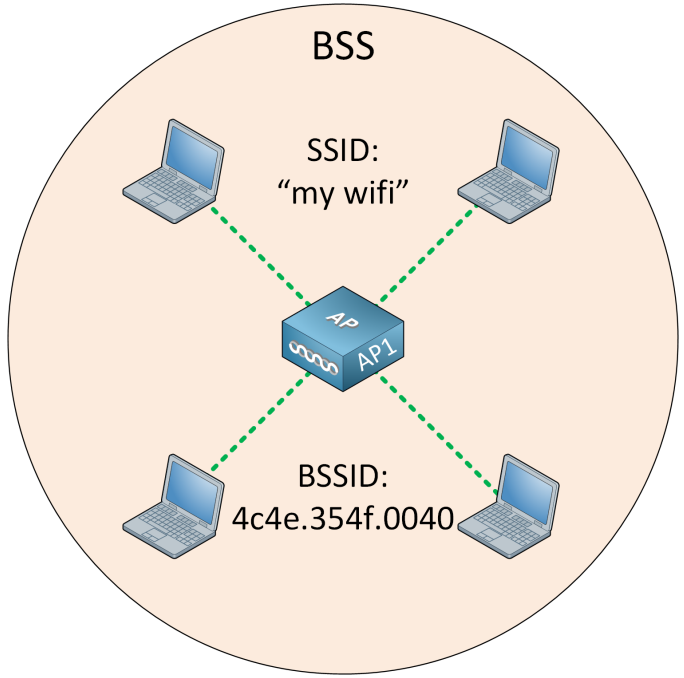
SERVICE SET IDENTIFIER (SSID)

- The friendly name given to a wireless network
- Need not be unique
- Can be hidden (not advertised)
  - You can still connect to the WLAN if you know the SSID
  - You'll have to manually enter the SSID



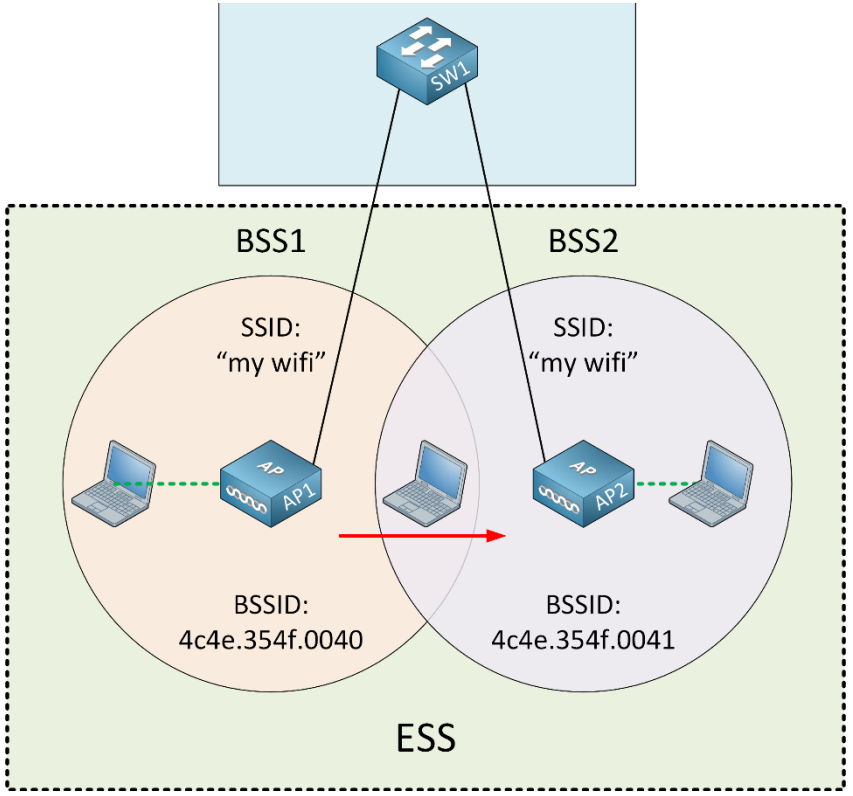
BASIC SERVICE SET (BSS)

- Simple WLAN with ONE:
  - Wireless access point
  - SSID (AP advertises itself)
  - Channel
  - BSSID (MAC address of AP)
- Typically can accommodate up to 10 clients
- Usually an extension of the LAN
- Traffic might also be routed straight to the Internet



EXTENDED SERVICE SET (ESS)

- Several interconnected BSSs acting as one
- APs that are physically close to each other will use different channels
  - Avoid interfering with each other
- All participating BSSs use the same SSID
  - To the client, the ESS appears as a single BSS



AUTHENTICATION MODES FOR WI-FI

- Open-System Authentication Process
  - No authentication
  - Clients must have their own protection (such as firewall, anti-virus)
  - Often used for guest Wi-Fi
- Pre-Shared Key (PSK) Authentication Process
  - Password is set on WAP and clients
- Centralized Authentication
  - Authentication forwarded to a centralized server
    - Typically a RADIUS server
- 802.1x
  - WAP or switch forwards authentication to a centralized server
  - Uses the Extensible Authentication Protocol (EAP) to allow many authentication types

802.1X

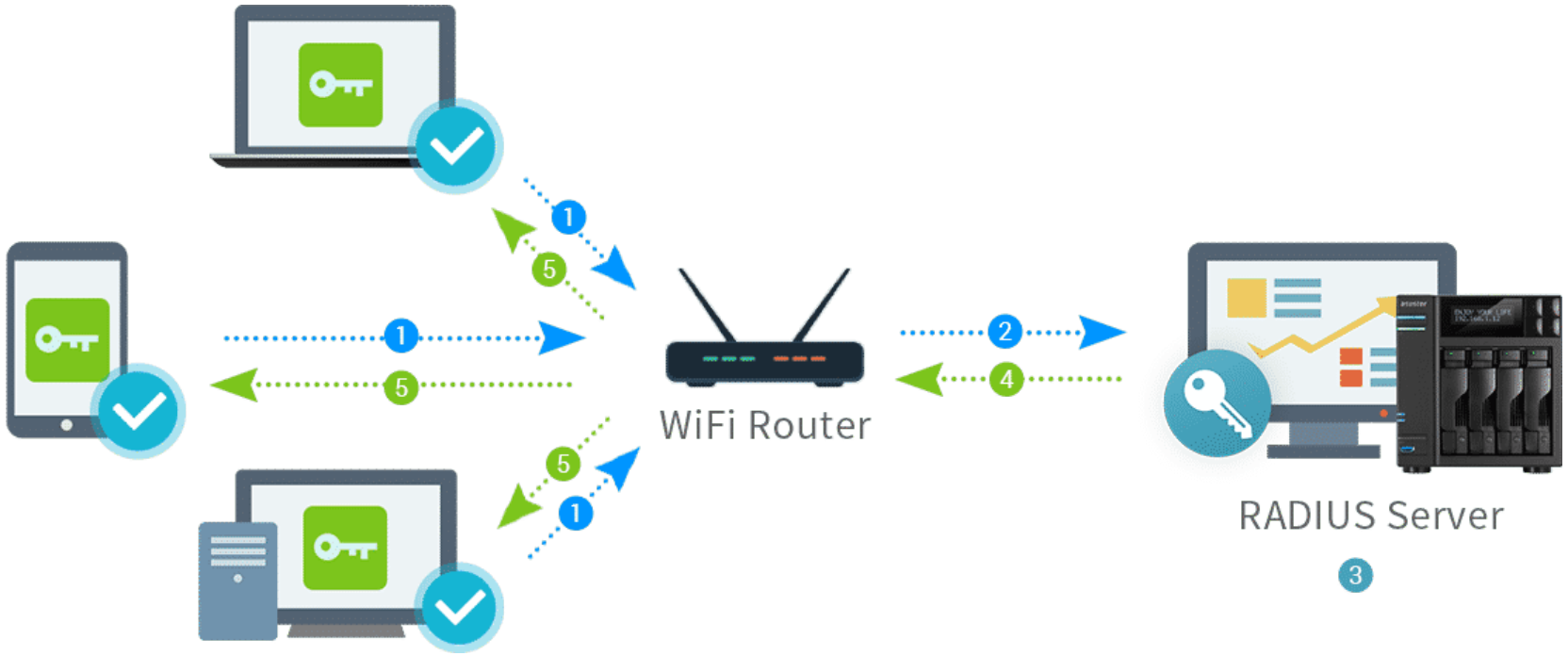
- An IEEE Standard for port-based Network Access Control
- It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN
- It uses EAP to provide a wide range of authentication types
- The 802.1x process is as follows:
  1. The wireless client connects to the 802.1x-enabled access point
  2. The access point places the client connection on hold
  3. A browser opens to a captive portal
  4. Either the client or the user authenticates
  5. The AP forwards the authentication attempt to a RADIUS server
  6. If the authentication is successful, the AP allows the client on the network
  7. The client caches a short-term session token

EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

- Used by 802.1x to allow for a wide range of user and client authentication mechanisms including:
  - Plain text passwords
  - Challenge-Handshake (CHAP)/MS-CHAP/MS-CHAPv2 passwords
  - certificates, tokens, smartcards, authenticator apps
  - biometrics

RADIUS

- RADIUS is a protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) authentication
- A RADIUS server usually serves as the back-end server in 802.1x authentication



16.2 WI-FI SECURITY STANDARDS

- WEP
- WPA
- WPA2
- WPA3

WIRED EQUIVALENT PRIVACY (WEP)

- 64/128 bit
- Rivest Cipher 4 (RC4) Stream Cipher Algorithm
- Pre-Shared Key (PSK) 40 or 104 bits long
- Used a 24 bit Initialization Vector (IV) to extend the key to 64 or 128 bits
- No digital signatures
- No sequence numbers
- Susceptible to replay attacks
- Short key = quick to crack

- ⚠ Very old and insecure

WI-FI PROTECTED ACCESS (WPA)

- Created to address the security problems of WEP
- Still uses RC4
- Included TKIP (Temporal Key Integrity Protocol) to change the key for every packet
- Initialization Vector (IV) is larger and an encrypted hash
- Every packet gets a unique 128-bit encryption key
- Personal | WPA-PSK
  - TKIP + PSK
  - 64/128 bit RC4 MIC
- Enterprise | WPA-802.1X
  - TKIP + RADIUS
  - 64/128 bit RC4 MIC
  - Authenticates users individually with an authentication server (e.g., RADIUS)

TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)

- Changes the encryption key for every packet
  - Combines the secret root key with the IV
- Prevents replay attacks
  - Adds sequence counter
- Protects against tampering
  - Implements a 64-bit Message Integrity Check
- TKIP has its own set of vulnerabilities
- Deprecated in the 802.11-2012 standard

WPA2

- IEEE 802.11i
- CCMP replaced TKIP
  - Large key with message authentication
- AES (Advanced Encryption Standard) replaced RC4
- Also comes in PSK or Enterprise (802.1x) modes

For the longest time, WPA2 with AES encryption was the strongest Wi-Fi security type.

WPA3

- The Wi-Fi Alliance now requires all devices that wish to be certified to support WPA3
- Mandates the adoption of Protected Management Frames that protect against eavesdropping and forging
- Standardized 128-bit cryptographic suite and disallows obsolete security protocols
- Uses zero-knowledge proof
- No elements of the password are transmitted over the network
- Session key derived from the process
- QR codes can be used to gain network connection details
- Enterprise version has optional 192-bit security encryption and a 48-bit IV for better protection
- GCMP - Galois/Counter Mode Protocol WPA3-Personal uses CCMP-128 and AES-128

16.3 WI-FI DISCOVERY TOOLS

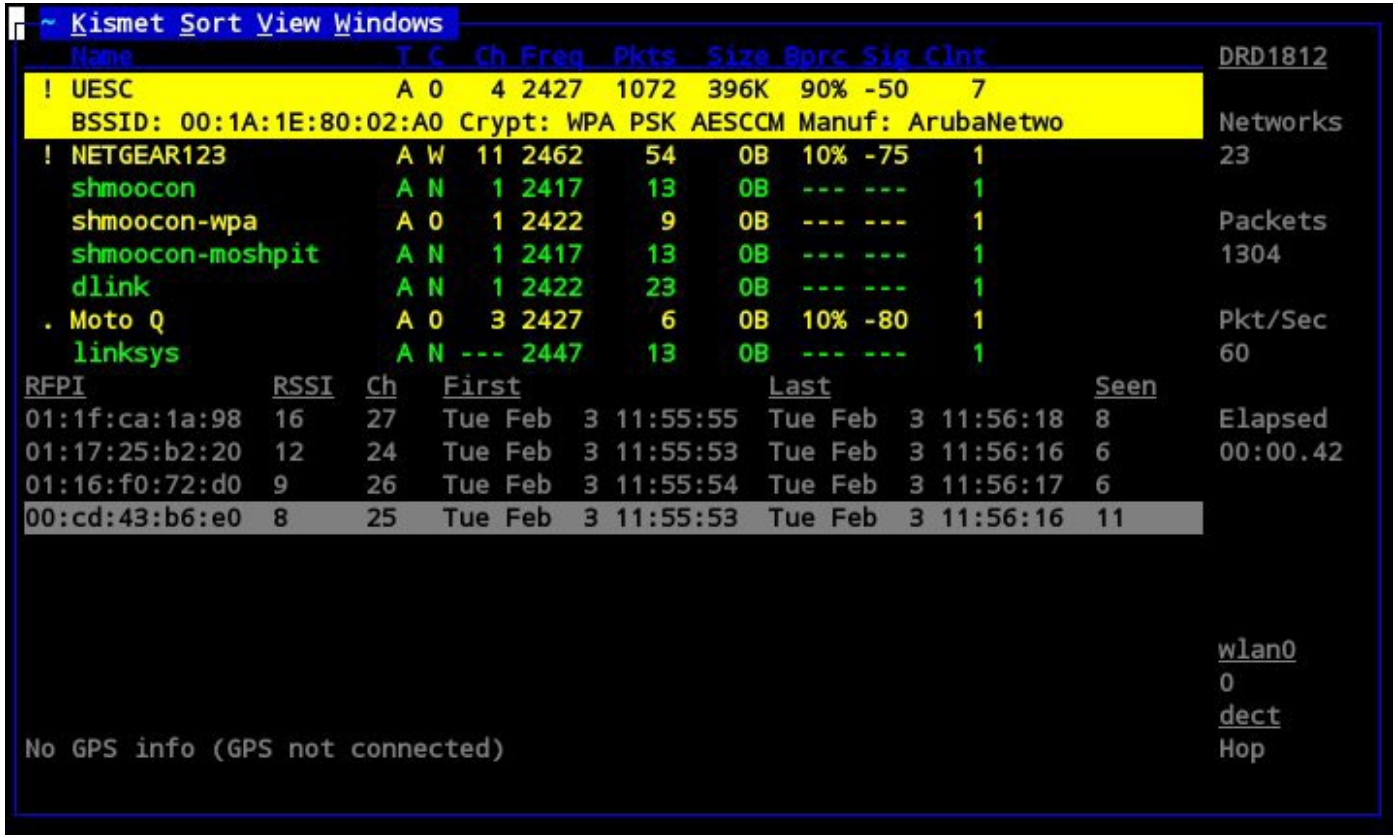
- Wi-Fi Sniffing
- Discovery Tools

WI-FI ADAPTER REQUIREMENTS

- To be able to sniff and perform various Wi-Fi attacks, you will need a wireless adapter with a good antenna and the correct drivers:
- Windows
  - AirPcap (legacy)
  - pcap
- Linux
  - libpcap
- If your laptop's Wi-Fi adapter doesn't support what you need
  - Get an external one such as:
  - Alfa AWUS036NHA
  - Alfa Long-Range Dual-Band AC1200

WIRELESS SNIFFERS

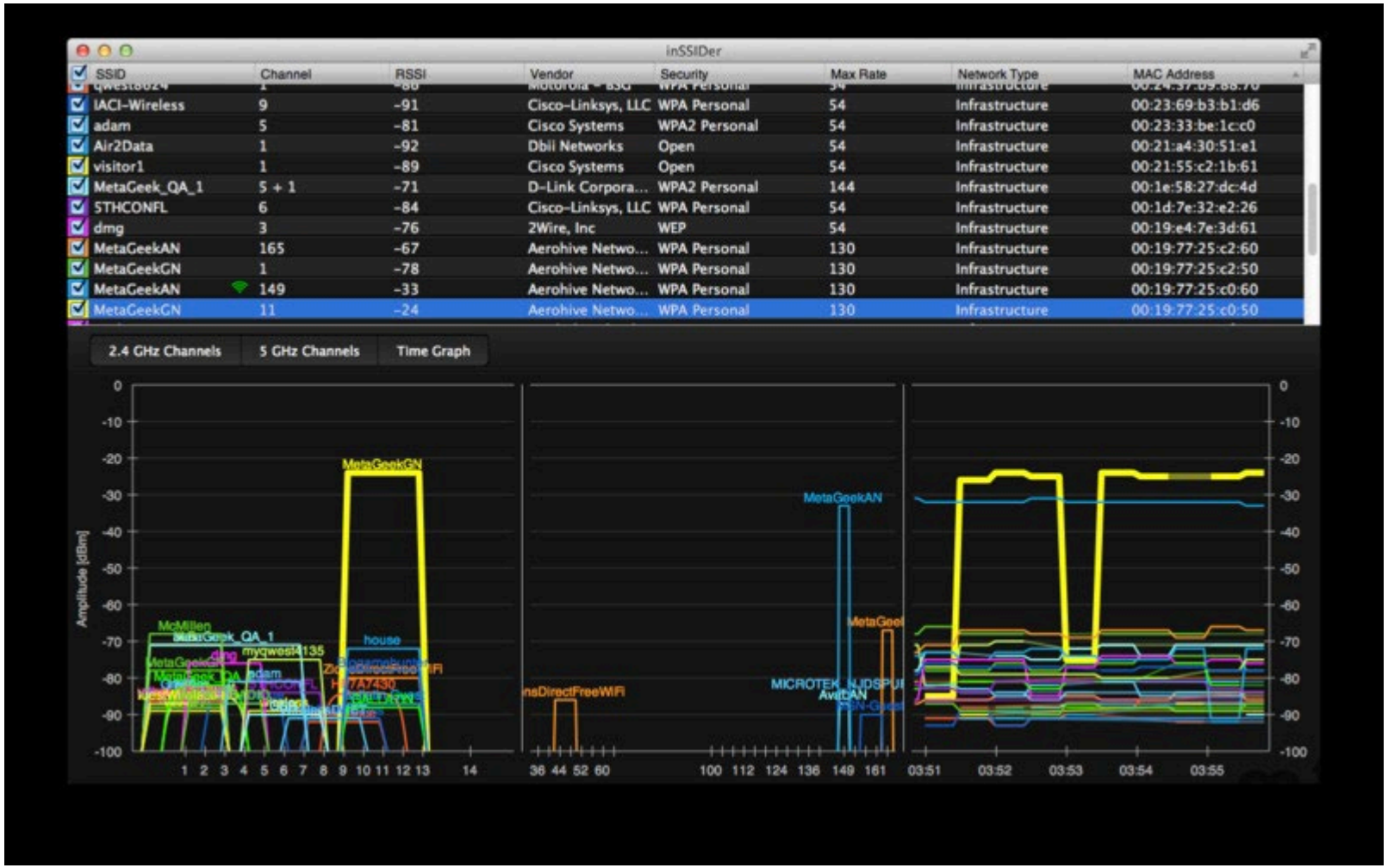
- Kismet
- Wireshark
- TCPdump
- Airodump-ng
- OmniPeek
- Vericode
- Monitis



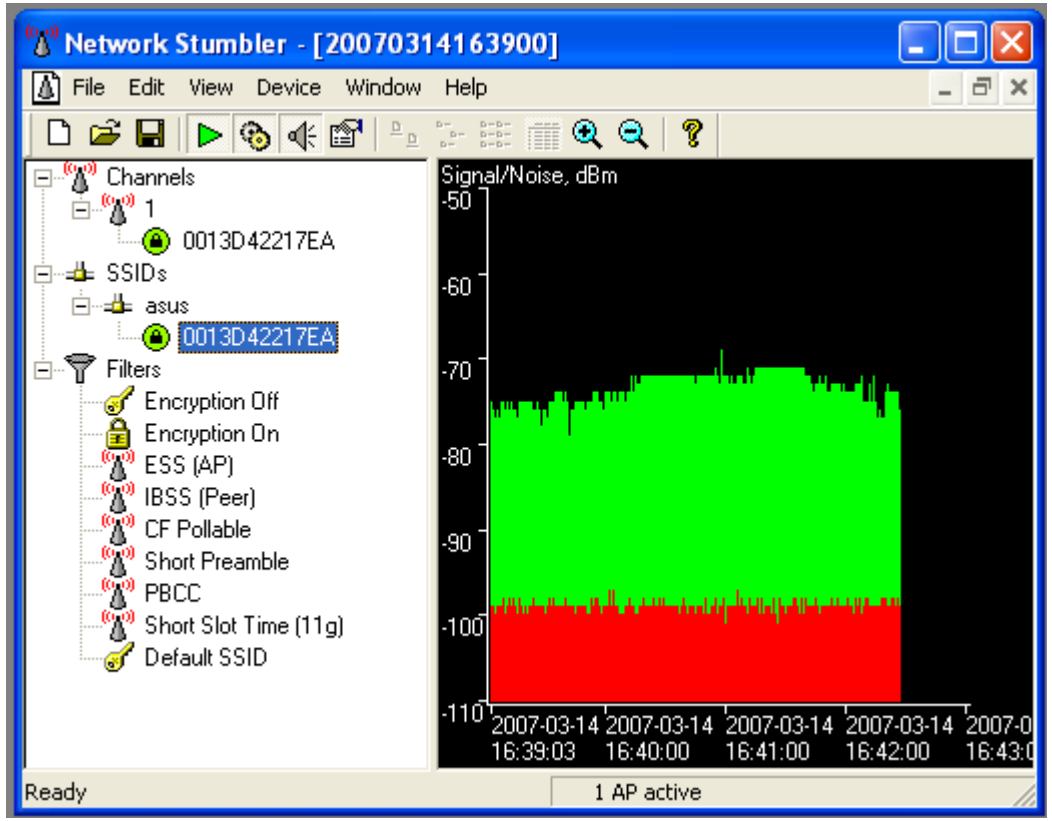
WIRELESS ACCESS POINT DISCOVERY TOOLS

- inSSIDer
- NetSurveyor
- Vistumbler
- NetStumbler
- WirelessMon
- Kismet
- KisMac
- CommonView for Wi-Fi
- WiFi Hopper
- Wavestumbler
- iStumbler
- WiFinder
- Wellenreiter
- AirCheck Wi-Fi Tester
- AirRaider 2
- Xirrus Wi-Fi Inspector
- WiFi Finder
- WeFi

INSSIDER EXAMPLE



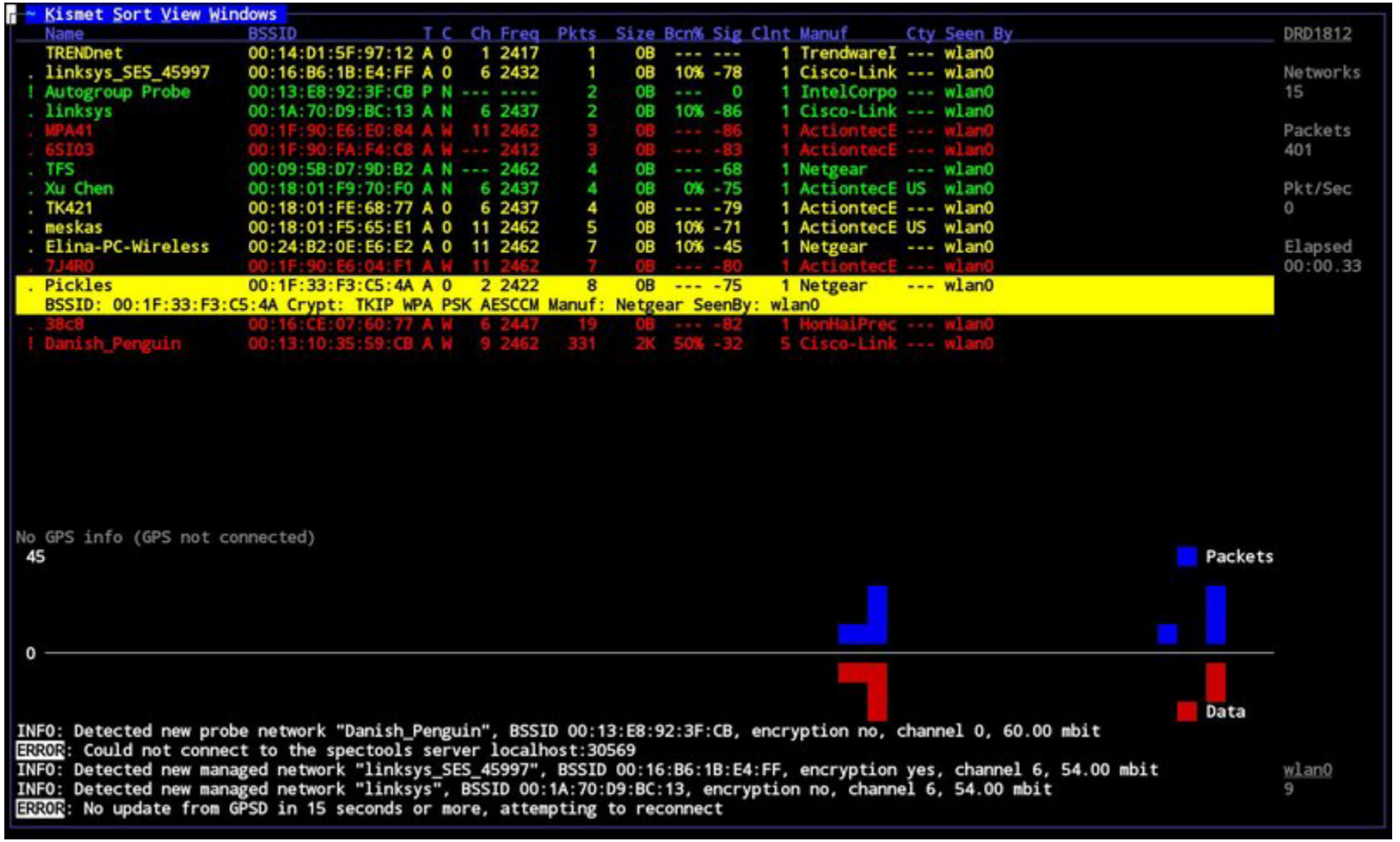
NETSTUMBLER EXAMPLE



KISMET

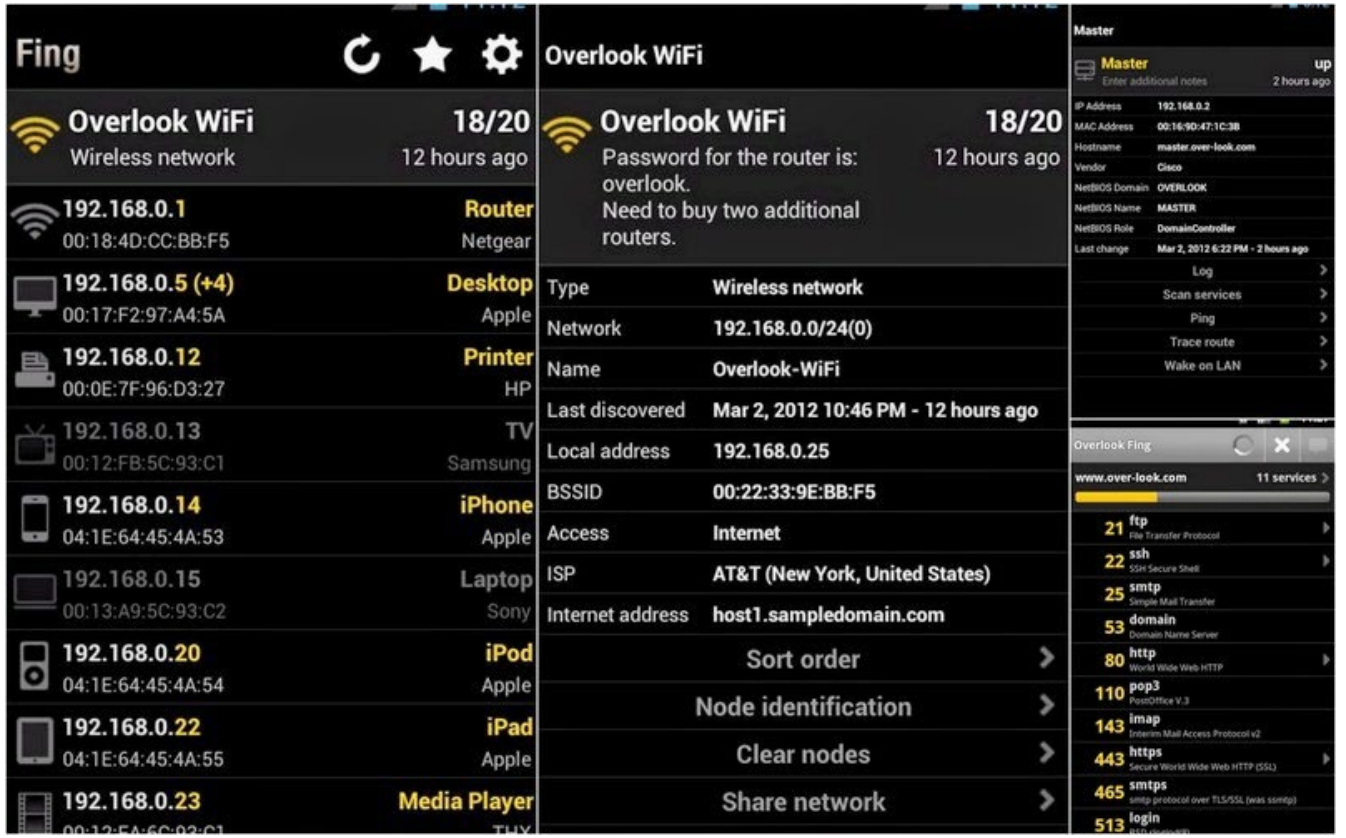
- A wireless network detector, packet sniffer, and intrusion detection system (IDS)
- Works with any wireless card supporting raw monitoring (rfmon) mode
- Can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic
- Works on Linux, Mac OSX, and Windows 10 under the WSL framework.
- Commonly found on Linux computers

KISMET EXAMPLE



MOBILE WIRELESS DISCOVERY TOOLS

- WiFiFoFum-WiFi Scanner
- WiFi Manager
- Network Signal Info
- OpenSignal Maps
- Fing
- Overlook WiFi



WARDRIVING TOOLS

- Airbase-ng
- ApSniff
- WiFiFoFum
- MiniStumbler
- WarLinux
- MacStumbler
- WiFi-Where
- AirFart
- AirTraf
- 802.11 Network Discover Tools

16.4 COMMON WI-FI ATTACKS

- Common Attacks
- Rogue Access Points
- DoS

WIRELESS VS WIRED EXPLOITS

- Most wired exploits will also work against Wi-Fi wireless:
  - Sniffing
  - Spoofing
  - MITM/Hijacking
  - Deauthentication
  - DoS
- In addition, wireless devices have technology-specific vulnerabilities

WIRELESS IS INHERENTLY VULNERABLE

LONG RANGE WI-FI ANTENNA

- Highly directional YAGI
- Can snoop/attack up to several miles away

COMMON WIRELESS ATTACKS

- Sniffing
  - Use Wireshark or other tools to passively sniff wireless traffic
- Spoofing
  - Change the MAC (or other) address of the attacker device to that of a victim
- Rogue Access Point
  - Unauthorized access point plugged into a wired one (can be accidental)
  - Tools for Rogue AP: Wi-Fi Pumpkin, Wi-Fi Pineapple
- Evil Twin
  - Intentional rogue AP that is broadcasting the same (or very similar) SSID
  - Also known as a mis-association attack
  - Honeyspot - faking a well-known hotspot with a rogue AP
  - KARMA Attack - Responding to, and impersonating, any SSID the client beacons for
- Wi-Fi Phishing
  - AKA Wi-Fishing
  - Combination KARMA/Evil Twin and login page spoofer for password capturing

COMMON WIRELESS ATTACKS (CONT'D)

- Ad Hoc Connection Attack
  - Connecting directly to another phone via ad-hoc network
  - Requires social engineering - the other user has to accept connection
- Deauthentication Attack
  - The wireless client is "knocked" off the network by the attacker
  - Usually done to force the client to reauthenticate to the WAP
    - The attacker then captures packets from the client to perform other attacks
  - Can also be used for simple denial-of-service
- Replay Attack
  - The high-speed repeated retransmission of a captured packet
  - Usually for the purpose of collecting key material from the access point
- DoS Attack
  - Uses deauth, signal jamming, or ARP spoofing to perform denial-of-service
  - With a de-auth, you can have the users connect to your AP instead if it has the same name
  - Jammers are very dangerous as they are illegal
- Password Cracking
  - WEP/WPA/WPA2/WPS cracking

DEAUTHENTICATION ATTACK

- In WEP networks, use deauthentication to force a client to reconnect (and hopefully ARP) to the access point
  - Capture the encrypted ARP for a replay attack
- In WPA/WPA2 networks, use deauthentication to capture the four-way handshake:
  - Client must perform handshake when reconnecting
  - Capture PSK exchanged in handshake
  - Try cracking the PSK using:
    - Hashcat, John-the-Ripper, aircrack-ng
  - Or send the captured handshake to an online cracking service

REPLAY ATTACK

- Capturing and re-transmitting a packet to force a response from the access point
  - Used to speed up the time an attack takes
- WEP cracking:
  - You capture an encrypted ARP packet
  - You replay it at high speed to the AP
  - The AP will respond with increased initialization vectors (IVs) that each provide some key material
  - Once you have collected enough IVs, you can crack the password
- WPA/WPA KRACK Attack:
  - When a client joins a network, it executes a 4-way handshake to negotiate a fresh encryption key
  - It will install this key after receiving message 3 of the 4-way handshake
  - Because messages may be lost or dropped, the Access Point (AP) will retransmit message 3 if it did not receive an appropriate response as acknowledgment
  - An attacker can collect and replay retransmissions of message 3 of the 4-way handshake
  - Each time the client accepts the connection it reveals a small amount of key material
  - When enough of the key material has been captured, the key can be cracked

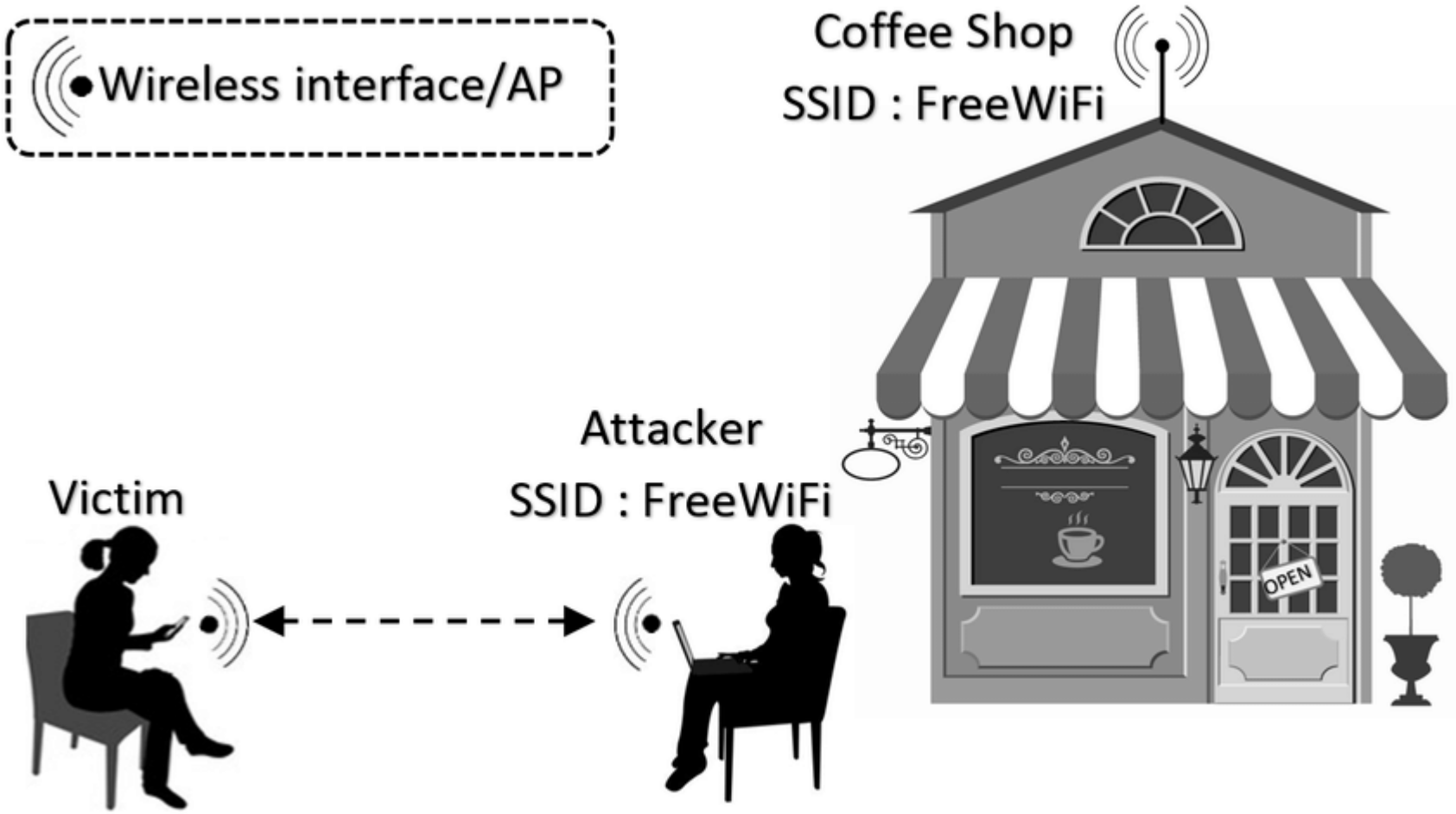
ROGUE ACCESS POINTS

- Evil Twin
- MITM
- KARMA
- Wi-Fi Phishing

EVIL TWIN ATTACK

- A type of attack where a rogue access point attempts to deceive users into believing that it is a legitimate access point
- A form of social engineering
- Often facilitated through deauthentication
  - Attacker knocks client off real network
  - Evil Twin should have a stronger signal/be placed closer to the victim
    - It will appear above the legitimate AP in the victim's list of available networks
  - Client reconnects to rogue AP
- Can launch all manner of attacks against connected victim
  - SSL downgrade/SSL strip
  - Sniffing traffic and capturing credentials

EVIL TWIN ATTACK EXAMPLE

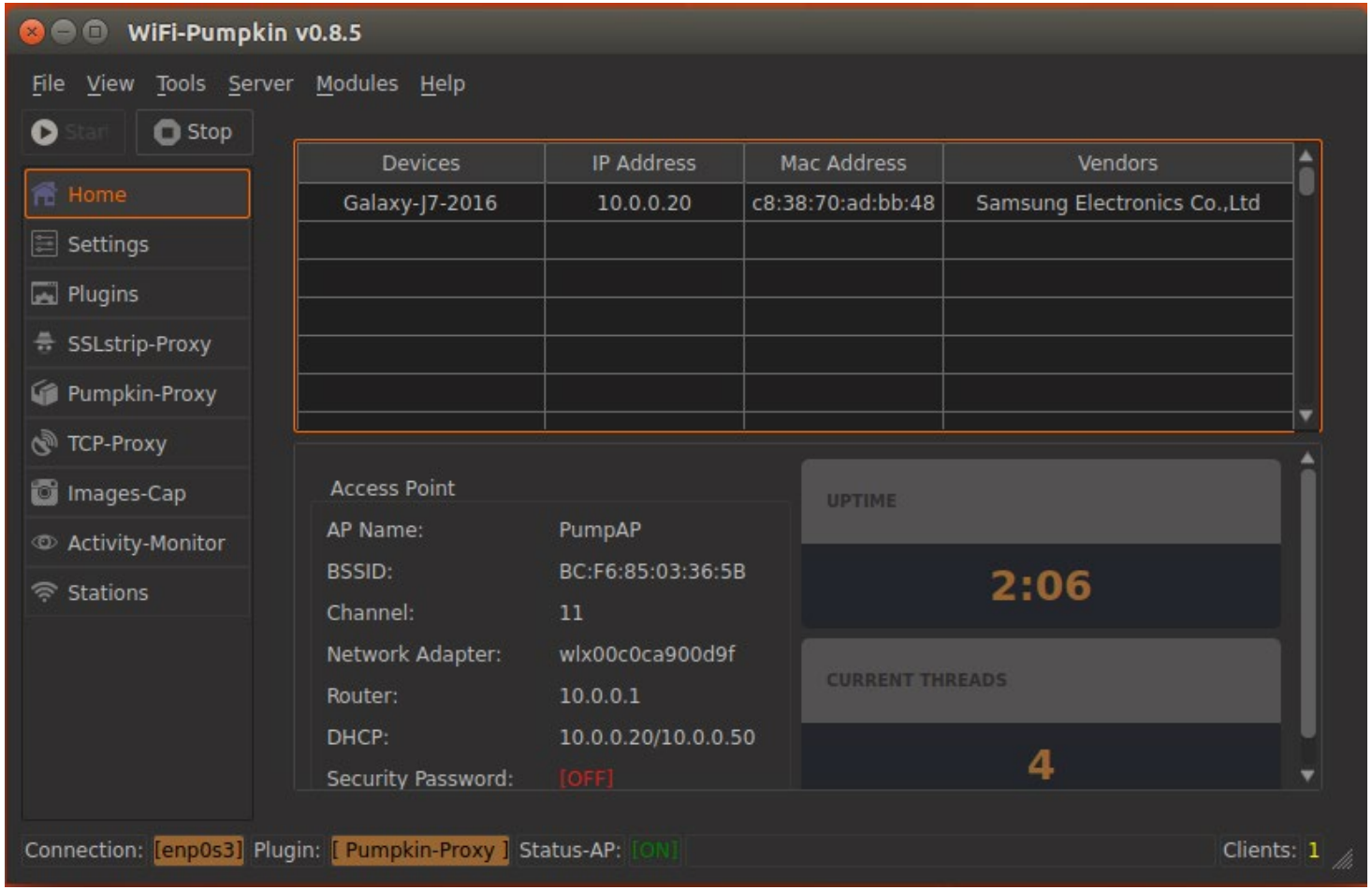


ALT EVIL TWIN EXAMPLE

MITM / EVIL TWIN / WI-FI PHISHING TOOLS

- Wi-Fi Pineapple
- Wi-Fi Pumpkin
- SKA Simple Karma Attack

WI-FI PUMPKIN EVIL TWIN EXAMPLE



KARMA ATTACK

- A variant of the evil twin attack
- Exploits the behavior of a wireless client trying to connect to its preferred network
  1. The client has a list of SSIDs it has connected to in the past
  2. The client beacons to determine if any of these SSIDs are within range
  3. The attacker answers the request
     - Pretends to be any SSID it hears in the client beacon
  4. The user connects to the evil twin
- KARMA Attack Tools:
  - Wifiphisher
    - Rogue AP framework
  - hostapd-mana
    - Rogue AP with many features
  - WIFI PINEAPPLE
    - Hardware Rogue AP
  - FruityWIFI
    - Multi-featured wireless audit tool for Raspberry PI or any Debian-based system

WIFIPHISHER

- Available in Kali Linux
- Performs Wi-fishing attacks:
  - Jammer
  - MITM
  - Spoofed Captive Portal

```
root@kali:~# wifiphisher -nJ -e "Free Wi-Fi" -T firmware-upgrade
[*] Starting Wifiphisher 1.1GIT at 2017-02-22 13:52
[+] Selecting wlan0 interface for creating the rogue Access Point
[*] Cleared leases, started DHCP, set up iptables
[+] Selecting Firmware Upgrade Page template
[*] Starting the fake access point...

Jamming devices:



DHCP Leases:
1487839973 c0:cc:f8:06:53:93 10.0.0.93 Victims-iPhone 11:c0:cc:38:66:a3:b3


HTTP requests:
[*] GET 10.0.0.93
[*] GET 10.0.0.93
[*] GET 10.0.0.93
[*] POST 10.0.0.93 wfphshr-wpa-password=s3cr3tp4s5
[*] GET 10.0.0.93
[*] GET 10.0.0.93
[*] GET 10.0.0.93
```

WI-FI SCENARIO

- You are conducting a wireless penetration test against an organization
- During your reconnaissance, you discover that their network is known as "BigCorpWireless" has its SSID broadcast is enabled
- You configure your laptop to respond to requests for connection to "BigCorpWireless" and park at the far end of the parking lot
- At the end of the workday, as people get in their cars in the parking lot, you see numerous smartphones connecting to your laptop over WiFi
- What kind of attack are you implementing?
- KARMA Attack
- You have configured your laptop rogue AP to automatically respond to the clients

WI-FI SCENARIO #2

- You are conducting a wireless penetration test against an organization
- You have been monitoring the WPA2 encrypted network for almost an hour but have been unable to successfully capture a handshake
- What kind of attack can you perform to more quickly capture a handshake?
- A deauthentication attack
- It would force the client to reauthenticate with a new handshake to the AP

DENIAL-OF-SERVICE

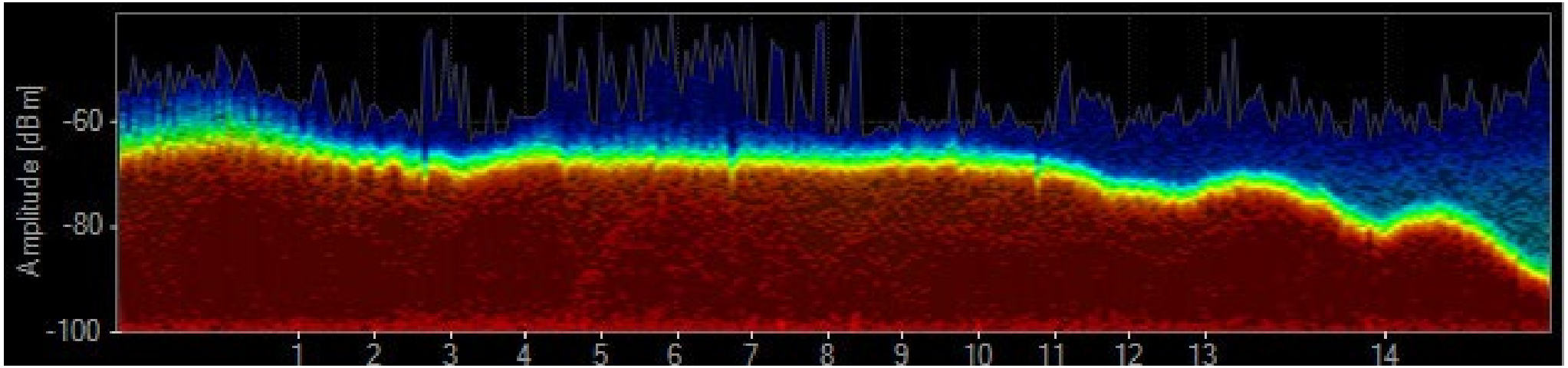
- Jamming
- ARP Spoofing

DENIAL-OF-SERVICE TOOLS

- AirJack
  - DoS and Packet Injector
- Arcai Netcut

FREQUENCY JAMMING

- The simplest and crudest form of wireless attack
- Denial-of-Service at the radio frequency level
- The wireless system and all of its clients are overwhelmed by a more powerful signal
- Authorized signals get buried in noise

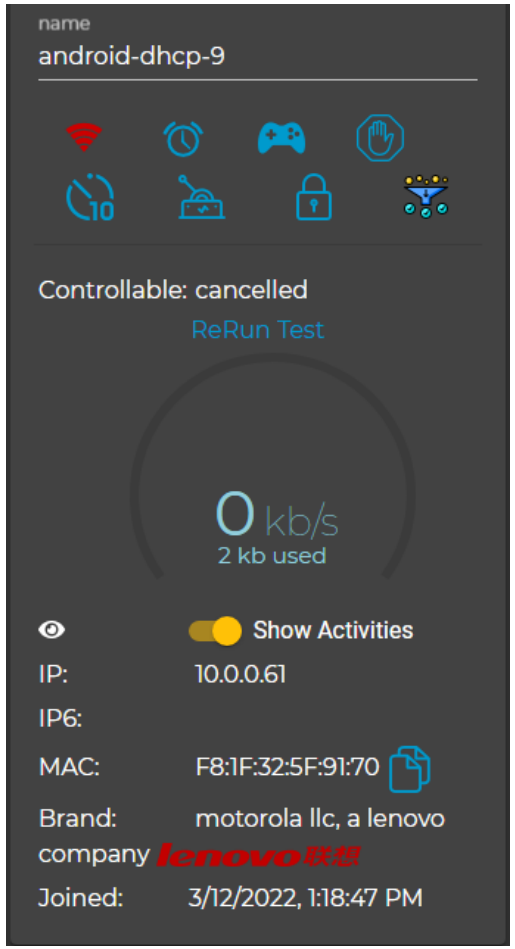


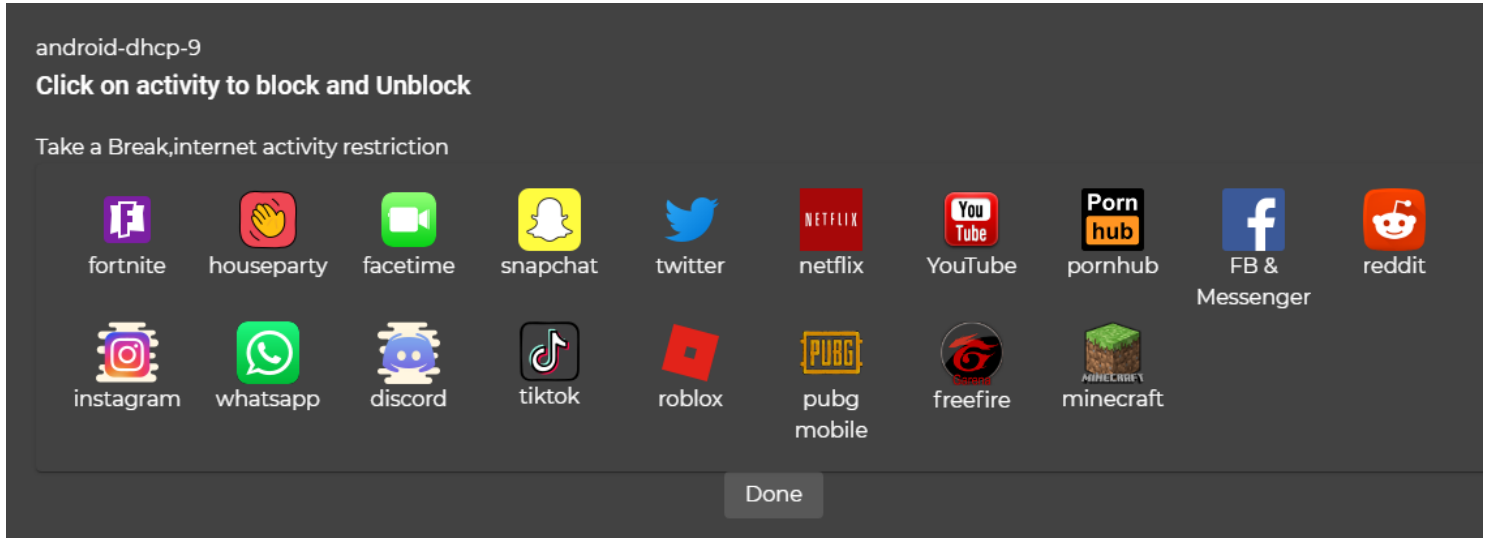
2.4/5 GHZ RADIO FREQUENCY JAMMER EXAMPLES

ARP SPOOFING TOOL - ARCAI NETCUT

- A very convenient and easy-to-use tool to manage wireless devices on your network
- Uses carefully controlled ARP spoofing to execute selective denial-of-service attacks
- An administrator can use it to control activity for a specific device including:
  - Bandwidth throttling
  - Kick device off network
  - Control popular app traffic
  - Inject latency on wireless game controllers
- An attacker can use it to completely cut a device off of the wireless network
- Available for PC, macOS, and Android
  - Limited free trial
  - Inexpensive paid subscription

NETCUT EXAMPLE





16.5 WI-FI PASSWORD CRACKING

- Tools
- Online Sites
- Mobile Apps

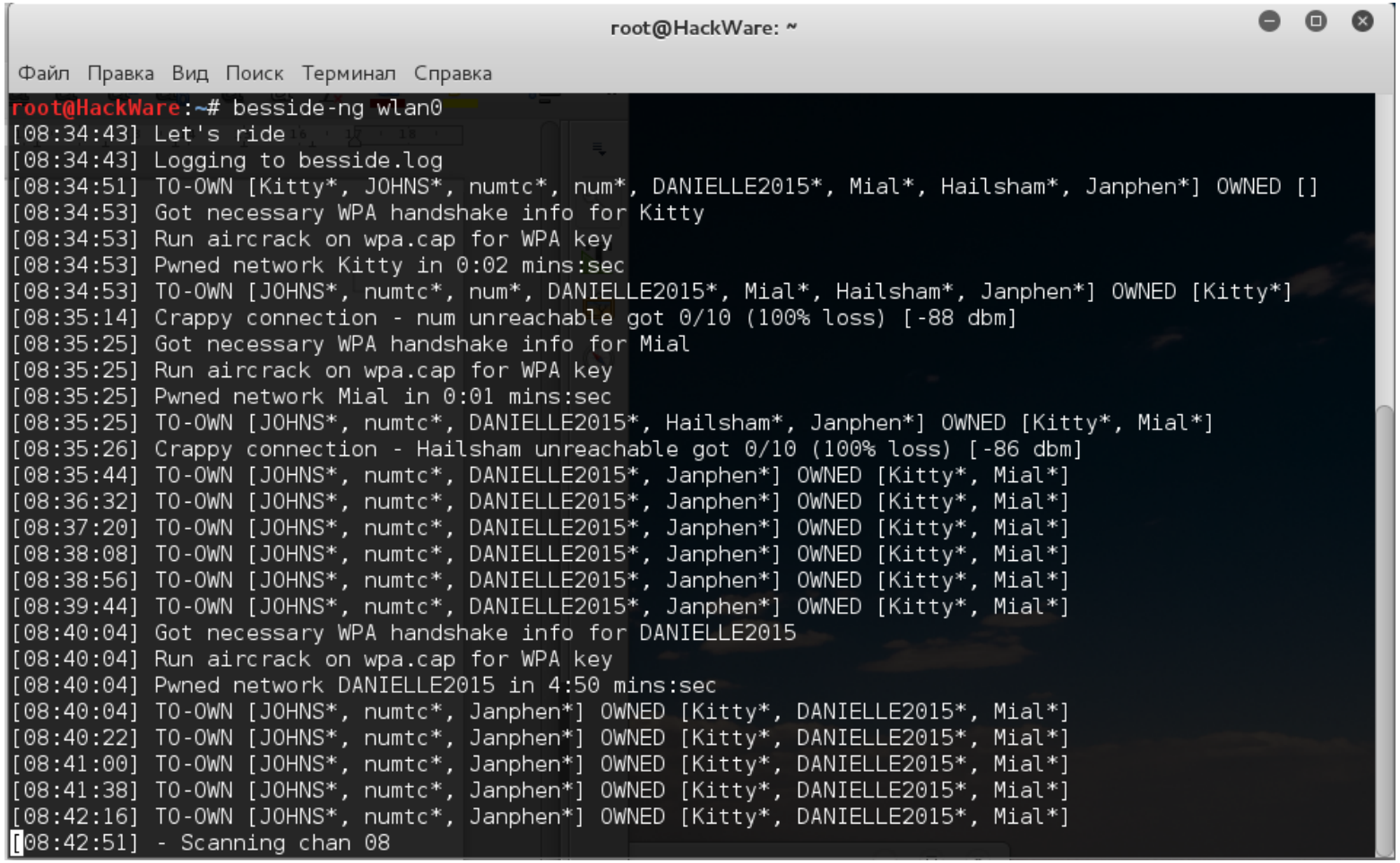
WI-FI PASSWORD CRACKING

- Wi-Fi password cracking has similarities and differences from other types of password cracking
- Cannot be done offline - you can't just steal the account database
- You could perform a dictionary attack or capture the PSK through MITM
- The attacker captures packets that each contain a small amount of encryption key material
- When enough key material is captured, the packets can be sent to a password cracker

WI-FI PASSWORD CRACKING TOOLS

- Aircrack-ng
  - Suite of tools for monitoring, testing, attacking and cracking WEP and WPA PSK passwords
  - Tools include: airmon-ng, airodump-ng, aireplay-ng, besside-ng, airbase-ng and many more
- besside-ng
  - Automatically discovers and cracks WEP networks
  - Automatically captures WPA handshakes
- Wifite
  - Automated WEP, WPA, and WPS cracking tool
- WEPAttack
  - WEP dictionary cracker

BESSIDE-NG EXAMPLE



WI-FI PASSWORD CRACKING TOOLS (CONT'D)

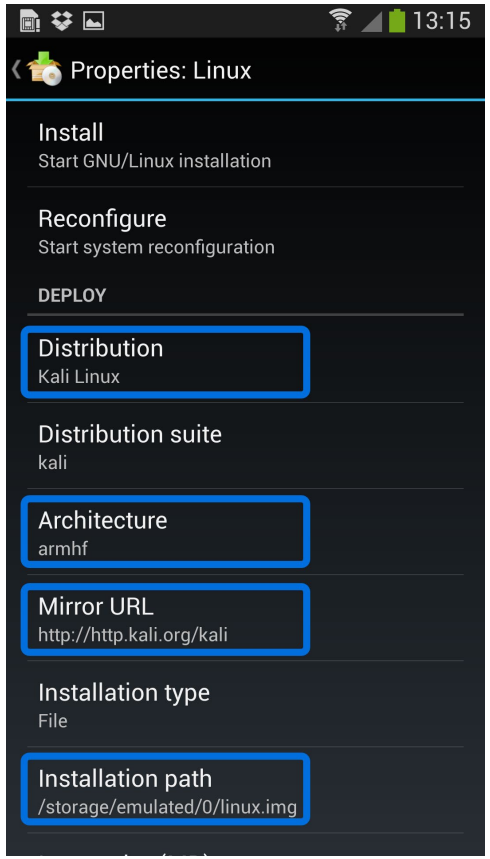
- Pyrit
  - WPA/2 PSK brute force cracker
- Airgeddon
  - A script that simplifies Wi-Fi cracking
  - Requires Aircrack-ng
- Cain and Abel
  - Sniffer and password cracker
- CoWPAtty
  - WPA dictionary cracker
- AirSnort
  - Sniffer and password cracker

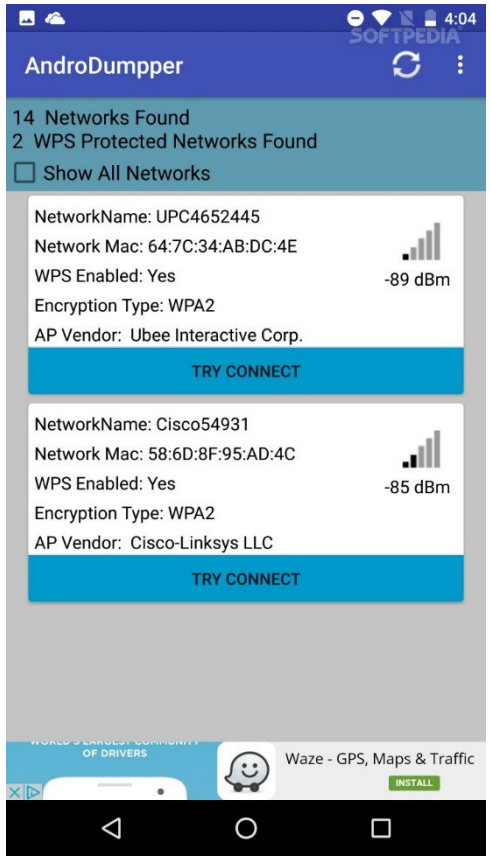
WI-FI PASSWORD CRACKING TOOLS (CONT'D)

- Fern WiFi Cracker
  - Automated WEP, WPA, WPS cracking
  - Has a nice GUI
  - Written in Python bully
  - WPS brute forcer. Includes improvements over reaver
- bully
  - WPS brute forcer with improvements over reaver and pixiewps
- reaver
  - WPS brute forcer
- pixiewps
  - Offline WPS brute forcer

MOBILE APPS FOR WI-FI CRACKING

- Linux Deploy
  - Kali Linux on Android
- WiFi WPS WPA Tester
- AndroDumper
  - WPS cracker
- Penetrate Pro
  - WEP/WPA cracker
- RfA Reaver for Android
  - WPS cracker

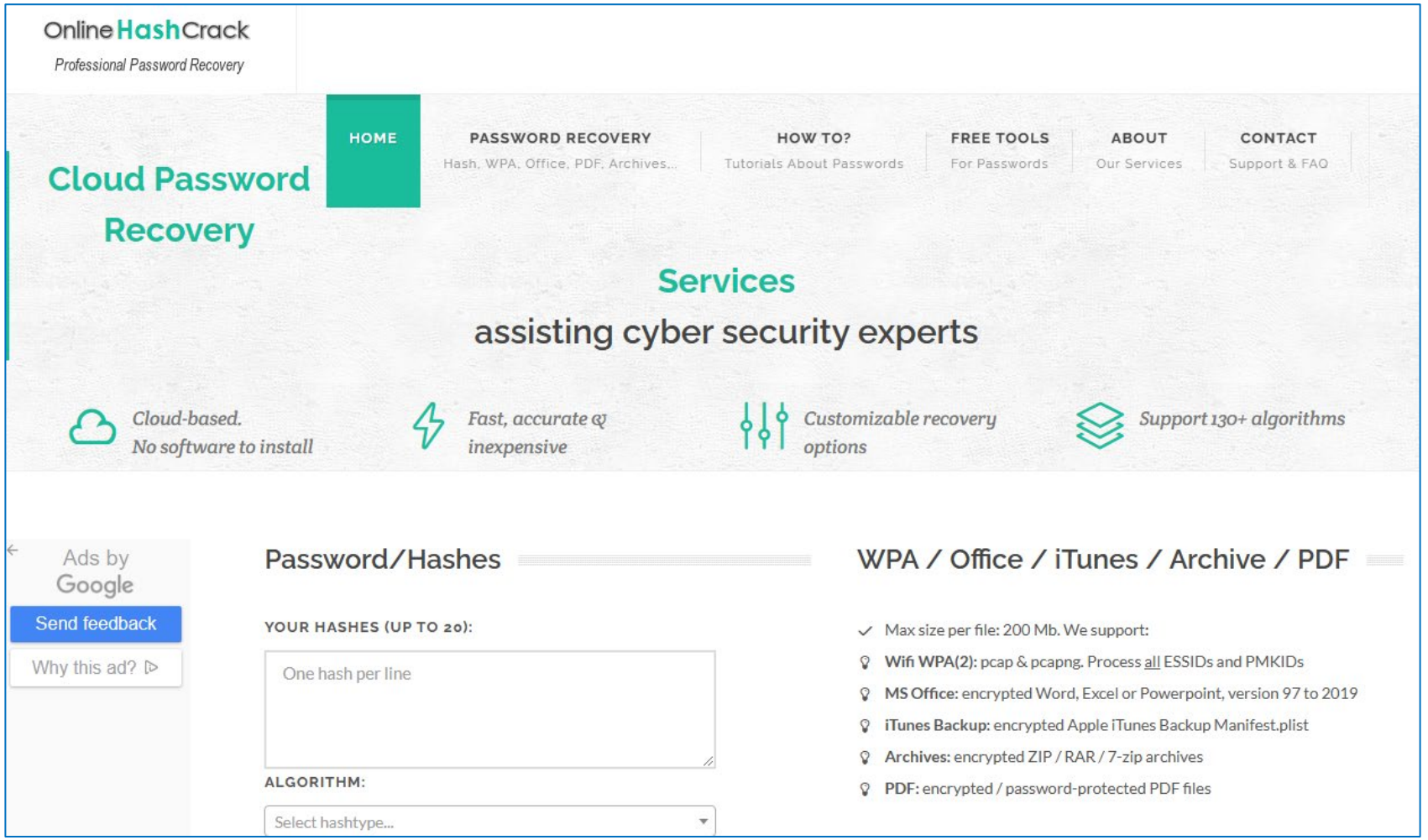




ONLINE CRACKING SITES

- Onlinehashcrack.com
  - WPA/2, MS Office, iTunes backups, ZIP/RAR/7-zip, PDFs
- Cloud Cracker
  - Online cracking tool for WPA/WPA2, NTLM, SHA-512, MD5, MS-CHAPv2
  - Offers an API for your app

ONLINEHASHCRACK.COM EXAMPLE



16.6 WEP CRACKING

- WEP Attack Types

WEP CRACKING

- WEP uses a weak implementation of the RC4 algorithm
  - Uses Initialization Vectors IVs to stretch the pre-shared key
  - New IVs are created periodically by the AP and sent in clear text to the client
  - IV pseudo-random generation has a bias
  - Can run a statistical analysis password crack if you capture enough IVs
  - 20,000 IVs for 40-bit key (64-bit encryption)
  - 40,000 IVs for 104-bit key (128-bit encryption)
- No digital signatures
- No sequencing
- Can capture a client ARP request and replay to accelerate IV generation
  - Chosen ciphertext attack
  - Replay attack

WEP ATTACK TYPES

- **You can use the Aircrack-ng suite to perform various attacks:**
- **ARP Request Replay Attack**
  - Classic ARP replay attack
  - Most effective way to induce the AP to generate new initialization vectors (IVs)
  - The attacker captures an encrypted ARP packet transmitted by another client
    - Replays it to the AP at high speed
  - The AP will respond in kind with new IVs
  - When enough IVs have been captured, the key can be cracked
- **KoreK chopchop**
  - When successful, can decrypt a WEP data packet without knowing the key
  - The attack does not recover the WEP key itself, but merely reveals the plaintext
  - You cut off the last byte of the ciphertext
  - Then figure out the missing character to make the CRC check valid again
  - Some APs are not vulnerable to this type of attack

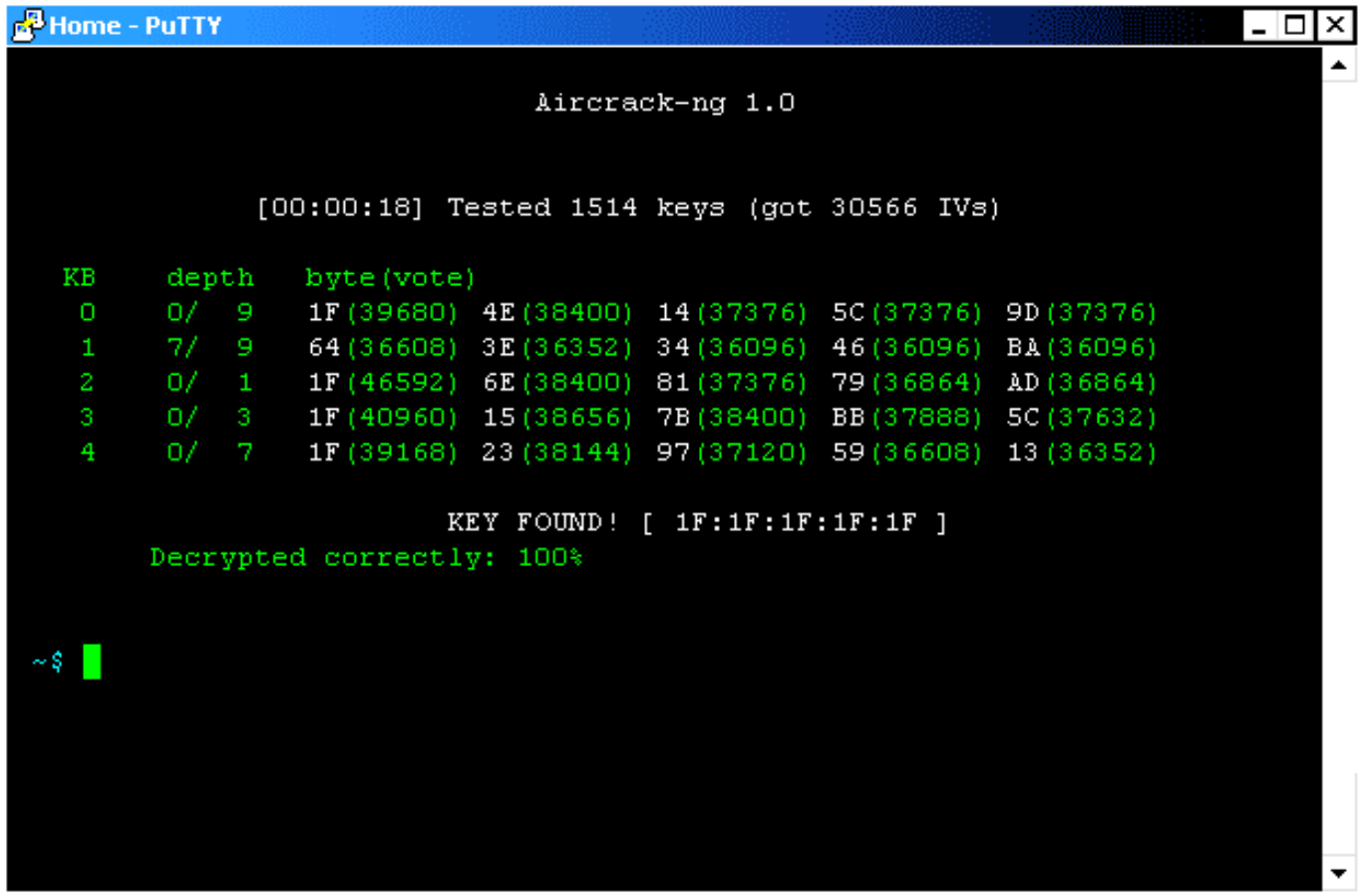
WEP ATTACK TYPES (CONT'D)

- **Fragmentation Attack**
  1. There are very few clients connected to the AP
     - The attacker has been waiting, but so far has not been able to capture an ARP from a client
  2. The attacker captures a packet
  3. Since all WEP headers are similar, the attacker can take the first 8 bytes of ciphertext and figure out what the plaintext should be
  4. The attacker can XOR the 8 bytes of cipher and plain text to know 8 bytes of keystream
  5. The attacker can create 16 8-byte fragments using this little bit of keystream and transmit it to the AP
     - You need 16 fragments to create the minimum packet size
     - Half of the bytes are for "data", half for integrity check

WEP ATTACK TYPES (CONT'D)

- **Fragmentation Attack (cont'd)**
  6. The AP will take the received fragments and assemble them into a single 64 byte packet with 64 bytes of keystream
  7. The AP echoes the assembled packet with keystream data back to the attacker
  8. The attacker has now leveraged 8 bytes of keystream into 64 bytes
  9. By repeating this process, the attacker can collect up to 1500 bytes of keystream (pseudo-random generating algorithm - PRGA)
  10. The attacker can now create full 1500 byte broadcast packets and send them to the AP
  11. Since they are broadcasts, the AP will relay them but with a new Initialization Vector (IV)
  12. If done enough times, enough IVs can be collected to crack the actual WEP key

WEP CRACKING EXAMPLE



BESSIDE-NG WEP CRACKING EXAMPLE

```
┌──(kali㉿kali)-[~]
└─$ sudo besside-ng wlan0mon -c 1 -b 64:66:B3:56:EF:7C
[21:51:12] Let's ride
[21:51:12] Appending to wpa.cap
[21:51:12] Appending to wep.cap
[21:51:12] Logging to besside.log
[21:51:12] | Scanning chan 01
Bad beacon
[21:51:12] / Scanning chan 01
Bad beacon
[21:51:12] - Scanning chan 01
Bad beacon
[21:51:12] | Scanning chan 01
Bad beacon
[21:51:12] / Scanning chan 01
Bad beacon
[21:51:13] - Scanning chan 01
Bad beacon
[21:51:13] \ Scanning chan 01
Bad beacon
[21:51:13] | Scanning chan 01
Bad beacon
```

```
[21:53:01] / Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 15012 IVs rat
[21:53:01] - Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 15012 IVs rat
[21:53:01] | Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 15012 IVs rat
[21:53:01] / Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 15012 IVs rat
[21:53:01] - Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 15013 IVs rat
[21:53:01] \ Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 15013 IVs rat
[21:53:01] | Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 15013 IVs rat
[21:53:01] / Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 15014 IVs rat
[21:53:01] - Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 15014 IVs rat
[21:53:01] | Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 15014 IVs rat
[21:53:01] / Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 15015 IVs rat
[21:53:01] - Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 15015 IVs rat
[21:53:01] \ Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 15015 IVs rat
[21:53:01] | Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 15015 IVs rat
[21:53:01] Got key for Hack_Me_If_You_Can [31:32:33:34:35] 15015 IVs
[21:53:01] Pwned network Hack_Me_If_You_Can in 0:52 mins:sec
[21:53:01] TO-OWN [] OWNED []
[21:53:01] All neighbors owned

Dying...
[21:53:01] TO-OWN [] OWNED []

┌──(kali㉿kali)-[~]
└─$
```

WEP SCENARIO

- You are conducting a wireless penetration test against an organization
- You have identified that they are using WEP encryption on their wireless access points
- You are impatient and do not want to wait to collect enough packets to find a repeated initialization vector
- You decide to extract part of the key material from one of the packets and use it to send an ARP request to the AP.
- What kind of attack are you conducting?
- A fragmentation attack

16.7 WPA/WPA2/ WPA3 CRACKING

- WPA Attack Types
- KRACK and KROOK
- Enterprise Attacks
- WPA3 Attacks

WPA/WPA2 CRACKING

- WPA introduced TKIP (key rotation)
  - Each packet is encrypted with a unique key
- WPA2 uses much stronger encryption (AES/CCMP)
- Both use sequence numbers so replay can't be used
- Both are still susceptible to a dictionary attack
- There are several cracking exploits you can use:
  - 4-way handshake dictionary attack
  - KRACK / KR00K

WPA/WPA2 HANDSHAKE CRACKING

- In WPA/WPA2 networks, use deauthentication to capture four-way handshake
- Client must perform handshake when connecting/reconnecting
- The handshake is protected by the PSK
- Use besside-ng to automatically capture and save handshakes:

```
sudo airmon-ng start wlan0
iwconfig
besside-ng wlan
```

- Alternatively, use airodump-ng to sniff for handshake:

```
airodump-ng -c <channel> --bssid <MAC address> -w capture wlan0
```

- Use aircrack-ng to crack the PSK or upload to an online cracking site

WPA/WPA2 HANDSHAKE CRACKING EXAMPLE

```
airmon-ng start ath0
airodump-ng -c 6 --bssid 00:14:6C:7E:40:80 -w out ath0
(switch to another console)
aireplay-ng -0 5 -a 00:14:6C:7E:40:80 -c 00:0F:B5:AB:CB:9D ath0
(wait for a few seconds)
aircrack-ng -w /path/to/dictionary out.cap
```

Explanation:

- Channel 6
- -bssid 00:14:6C:7E:40:80 is the AP you are attacking
- -w out is the file prefix of the file name to be written
- ath0 is the interface name
- -0 means deauthentication attack
- 5 is number of groups of deauthentication packets to send out

KEY REINSTALLATION ATTACK (KRACK)

1. The attacker inserts themselves between a client and a legitimate access point
2. The rogue acts as a relay between the client and the AP
   - The rogue does not attempt to create a WPA2 session with the client
   - The rogue also does not know the original PSK that the client used to connect to the AP
3. The client and the AP perform an initial 4-way handshake, already protected by the PSK
4. At step 3 of the handshake, the AP gives the client a session key
5. The client is supposed to use this session key to encrypt its data
6. The rogue, however, replays the AP's step 3 messages repeatedly
7. The client ends up reinstalling the same key, reusing it to encrypt various packets
   - The key is supposed to be different with each packet
8. If the client sends a packet with known content (such as an ARP), the rogue now has the plaintext version of the ciphertext, and can easily derive the used keystream
9. As the client continues to use the same keystream, the rogue can decrypt the packets

KROOK

- A KRACK variant
- The client is deauthenticated by the attacker
- It destroys its session key and for security overwrites the key as a series of zeroes on any outbound packets still left in its transmit queue
- The client is NOT supposed to transmit anything left it its queue, but it does anyway, with a session key of all zeroes
- The attacker can sniff the packets and decrypt them with an all-zeroes session key
- The client will attempt to reauthenticate with a new handshake
- The attacker repeats the deauth cycle, thus collecting and decrypting packets that the client never has a chance to properly send

KR00K

- KrØØk (CVE-2019–15126)
  - Updated the WPA2 KRACK Attack

Changing the password won't help!

KRACK	Kr00k
KRACK, as the expanded acronym suggests, is a series of attacks – exploits	Kr00k, on the other hand, is a vulnerability – bug
The basic idea behind KRACK is that the Nonce is reused to acquire the keystream	The main idea behind Kr00k is that data is encrypted with an all-zero session key (TK)
Triggered during the 4-way handshake	Triggered after a disassociation
Affects most Wi-Fi capable devices, as it exploits implementation flaws in the WPA2 protocol itself	Affects the most widespread Wi-Fi chips (by Broadcom & Cypress)

KRACK/KROOK TOOLS

- krackattack-all-zero-tk-key (GitHub)
- r00kie-kr00kie.py (GitHub)

KRACK or its variants work against nearly any unpatched WPA2 device, regardless if authentication is PSK or 802.1x

R00KIE-KR00KIE EXAMPLE

```
python3 r00kie-kr00kie.py -i wlan0 -b D4:38:9C:82:23:7A -c 88:C9:D0:FB:88:D1 -l 11
```

1. The victim connects to a Wi-Fi hotspot
2. The attacker sends disassociation requests to the client and, by doing so, disconnects the victim from the hotspot
3. Wireless Network Interface Controllers (WNIC) Wi-Fi chip of the client clears out a session key (Temporal Key) used for traffic decryption
4. However, data packets, which can still remain in the buffer of the WiFi chip after the disassociation, will be encrypted with an all-zero encryption key and sent.
5. The adversary intercepts all the packets sent by the victim after the disassociation and attempts to decrypt them using a known key value (which, as we remember, is set to zero)
6. PROFIT!

BESSIDE-NG WPA/WPA2 CRACKING EXAMPLE

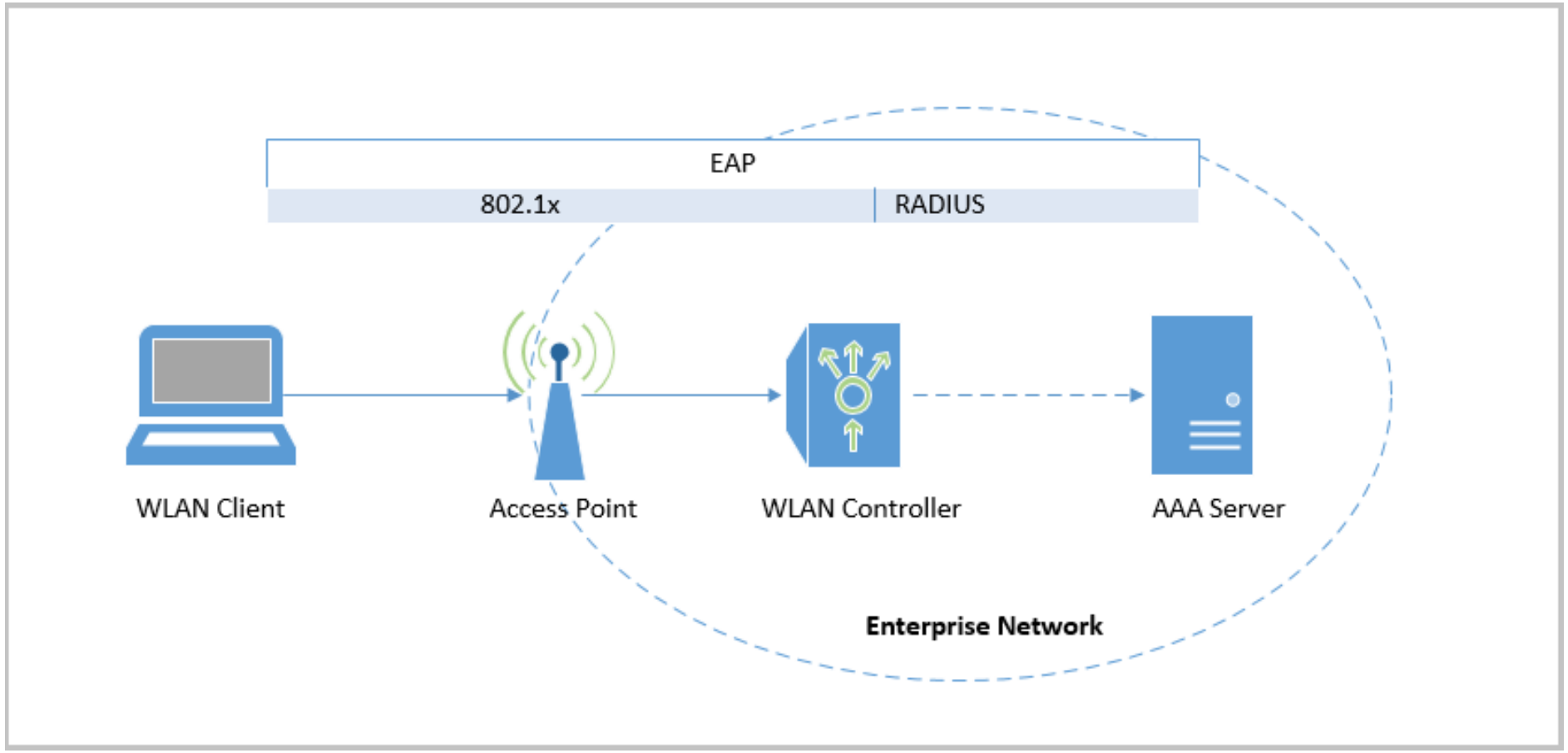
```
[06:57:50] / Attacking [Hack_Me_If_You_Can] WPA - DEAUTH (know 1 clients)
Bad beacon
[06:57:50] - Attacking [Hack_Me_If_You_Can] WPA - DEAUTH (know 1 clients)
Bad beacon
[06:57:50] \ Attacking [Hack_Me_If_You_Can] WPA - DEAUTH (know 1 clients)
Bad beacon
[06:57:50] | Attacking [Hack_Me_If_You_Can] WPA - DEAUTH (know 1 clients)
Bad beacon
[06:57:50] / Attacking [Hack_Me_If_You_Can] WPA - DEAUTH (know 1 clients)
Bad beacon
[06:57:50] - Attacking [Hack_Me_If_You_Can] WPA - DEAUTH (know 1 clients)
Bad beacon
[06:57:51] \ Attacking [Hack_Me_If_You_Can] WPA - DEAUTH (know 1 clients)
Bad beacon
[06:57:51] | Attacking [Hack_Me_If_You_Can] WPA - DEAUTH (know 1 clients)
Bad beacon
[06:57:51] Got necessary WPA handshake info for Hack_Me_If_You_Can
[06:57:51] Run aircrack on wpa.cap for WPA key
[06:57:51] Pwned network Hack_Me_If_You_Can in 0:06 mins:sec
[06:57:51] TO-OWN [] OWNED []
[06:57:51] All neighbors owned

Dying...
[06:57:51] TO-OWN [] OWNED []
```

WPA2 ENTERPRISE

- WPA2 without a pre-shared key
- Instead, authentication requests are forwarded to a RADIUS server
- 802.1x-compliant WAPs put the client session on hold until the user (or client) successfully authenticates
- There is no pre-shared key

WPA2 ENTERPRISE RADIUS EXAMPLE



WPA2 ENTERPRISE ATTACK

- If the client devices (supplicants) authenticate themselves to a RADIUS server with their own password, you can use a MITM attack to capture the user password
- Hostapd is a Linux-based attack tool that sets up:
  - a rogue AP
  - a rogue RADIUS server
- You must present a stronger signal to the clients than the legitimate AP
  - You need them to connect to your rogue, rather than the legitimate AP
- The steps are:
  1. Use airodump-ng to enumerate clients
  2. Use aireplay-ng to deauthenticate a client so they reconnect to you
  3. Your rogue becomes a MITM relay between the client and the AP
  4. As the user logs on, you capture their hashed password
  5. Use dictionary crackers such as asleap or John the Ripper to crack the user's password

WPA2 ENTERPRISE ATTACK EXAMPLE

```
root@alpha:~# hostapd ./hostapd.conf
Configuration file: ./hostapd.conf
Using interface wlan1 with hwaddr 60:e3:27:12:b2:de and ssid "EnterpriseWireless"
wlan1: RADIUS Authentication server 127.0.0.1:1812
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
```

Set up a rogue

```
root@alpha:~# cat /usr/local/var/log/radius/freeradius-server-wpe.log
mschap: Sun Nov 22 11:49:25 2015

        username: ICT\mattiareggiani
        challenge: 8f:49:cf:90:e7:aa:58:17
        response: 17:3c:45:ec:8f:19:2f:ec:68:c3:80:68:90:48:92:3c:45:ec:8f:19:2f:ec:68:a9
        john NETNTLM: ICT\mattiareggiani:$NETNTLM$73c45f90e7aa5867$173c45438f19245438f192fec8434790df0e5c34790d1
aa9
```

Capture a hashed password

```
root@alpha:~# asleap -C 8f:49:cf:90:e7:aa:58:17 -R 17:3c:45:ec:8f:19:2f:ec:68:c3:80:68:90:48:92:3c:45:ec:8f:19:2
f:ec:68:a9 -W myWordList.lst
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com
Using wordlist mode with "myWordList.lst".
        hash bytes:         051d
        NT hash:            07d2940c9d4ca2940c9d4es20448201a
        password:           passwordtest:)
```

Crack the password

WPA3 ATTACKS

- WPA3 Vulnerabilities

WPA3

- The best Wi-Fi security standard currently available
- Uses Elliptic Curve Diffie-Hellman key exchange
  - A smaller key provides the same strength encryption as RSA
  - Uses considerably less power
  - Great for small devices
- Uses a "dragonfly" handshake
  - AKA Simultaneous Authentication of Equals (SAE) handshake
  - Password Authenticated Key Exchange (PAKE)
  - Turns a password into a high-entropy key (has a high level of randomness)
  - Prevents offline dictionary attacks and provides forward secrecy

WPA3 VULNERABILITIES

- CERT ID #VU871675: Downgrade attack against WPA3-Transtition mode leading to dictionary attacks
  - Force clients that support WPA3 into connecting to the rogue WPA2-only network
  - The captured partial WPA2 handshake can be used to crack the password (using brute-force or dictionary attacks)
  - No man-in-the-middle position is required to perform this attack
- CERT ID #VU871675: Security group downgrade attack against WPA3's Dragonfly handshake
  - Reduced key strength
- CVE-2019-9494: Timing-based side-channel attack against WPA3's Dragonfly handshake
  - The amount of times it takes for an AP to respond to client commit frames may leak information about the password
- CVE-2019-9494: Cache-based side-channel attack against WPA3's Dragonfly handshake.
  - Memory access patterns reveal information about the password being used
  - Leaked patterns can be used to perform a dictionary attack
  - Performed by simulating the memory access patterns associated to a password
- CERT ID #VU871675: Resource consumption attack (DoS) against WPA3's Dragonfly handshake.
  - Causes high CPU usage on the AP, drains its battery, prevents or delays other devices from connecting to the AP using WPA3
  - May also halt or slow down other functionality of the AP as well
- Dictionary brute force attack
  - It is possible to brute force the password of a WPA3 access point
  - Use a tool such as WACKER or other Python scripts

WPA3 ONLINE BRUTE FORCE ATTACK EXAMPLE

```
ddos@DESKTOP-UVQDIBV:~/wacker$ python3 wacker.py -h
usage: wacker.py [-h] --wordlist WORDLIST --interface INTERFACE --bssid BSSID
                 --ssid SSID --freq FREQ [--start START_WORD]

A WPA3 dictionary cracker. Must run as root!

optional arguments:
  -h, --help            show this help message and exit
  --wordlist WORDLIST   wordlist to use
  --interface INTERFACE
                        interface to use
  --bssid BSSID         bssid of the target
  --ssid SSID           the ssid of the WPA3 AP
  --freq FREQ           frequency of the ap
  --start START_WORD    word to start with in the wordlist
```

16.8 WPS CRACKING

- Wi-Fi Protected Setup

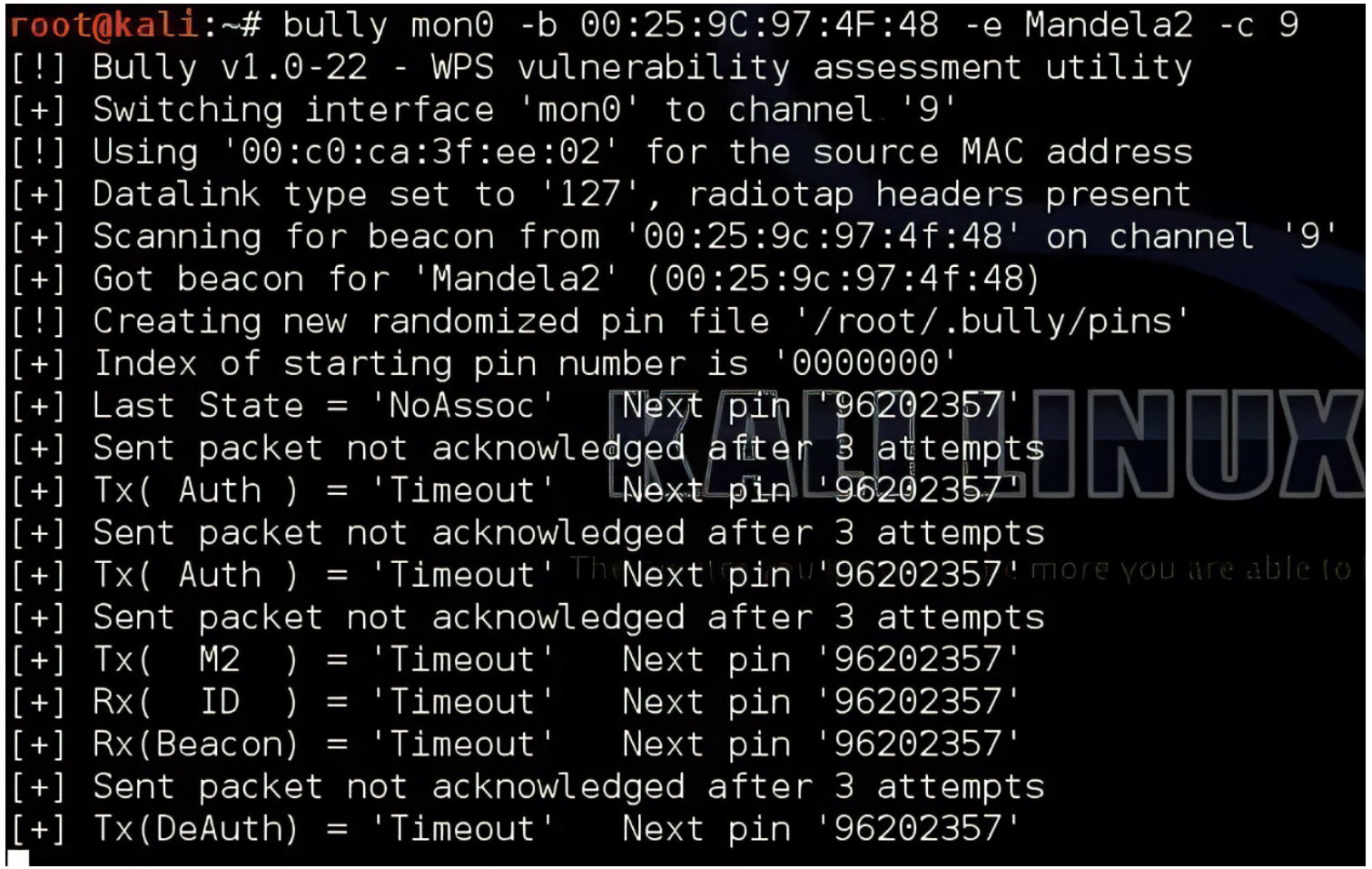
WI-FI PROTECTED SETUP (WPS)

- A method for setting up a secure Wi-Fi network at home with minimum effort
- Eliminates the need for the user to enter a WPA/WPA2 pre-shared key on the wireless client device
- Can be implemented in several ways:
  - The user presses a button the Wi-Fi access point
    - The PSK is transmitted to the client device long enough for a connection to be made
  - The user enters a PIN (on a sticker pasted to the WAP)
    - Key exchange is protected by the PIN
  - Devices use Near Field Communications (NFC)
    - Key exchange is performed "out of band" using NFC
  - A USB flash drive or cable is used to exchange the key between the device and the WAP

WPS ATTACK

- If a PIN is used:
  - Each PIN half is calculated separately
  - There are only 11,000 possible values
  - Easy to crack within hours
- Lockout policies on the WAP/router can hamper PIN cracking online
  - Might take a couple weeks, but still feasible
  - Lockout may look for MAC address, so spoofing could be used to bypass
  - Brute forcing may trigger DoS on certain WAPs
- Automated brute-forcing tools can be used to ultimately crack WPS

BULLY WPS ATTACK EXAMPLE

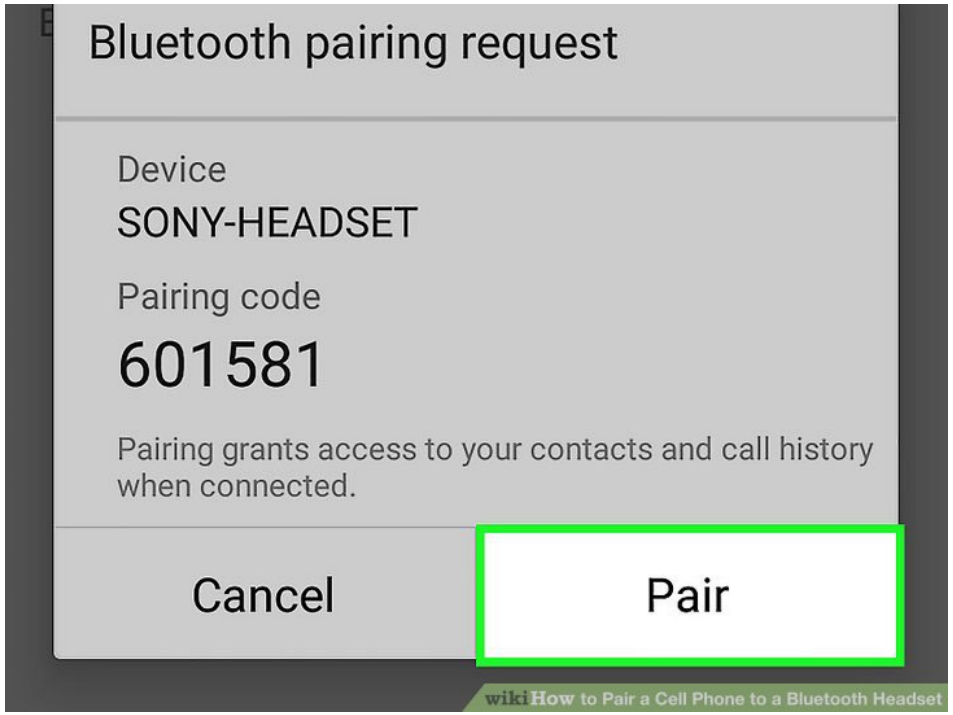


16.9 BLUETOOTH HACKING

- Threats
- Attack Types
- Tools

BLUETOOTH MODES

- Discoverable Modes:
  - Discoverable
    - The device broadcasts its presence and is able to be "seen" (detected) by other Bluetooth devices in range
  - Limited Discoverable
    - The device is discoverable for only a short period of time
  - Non-discoverable
    - Prevents the device from being listed when another device searches for Bluetooth-enabled devices
    - Does not actually turn Bluetooth off
    - A non-discoverable device can still be attacked if its MAC address is known or determined by brute force
- Pairing Modes
  - Non-pairable
  - Pairable



BLUETOOTH THREATS

- Personal information disclosure
- Remote code execution
- Social engineering / false SMS messages
- Unauthorized calls / using the victim's airtime

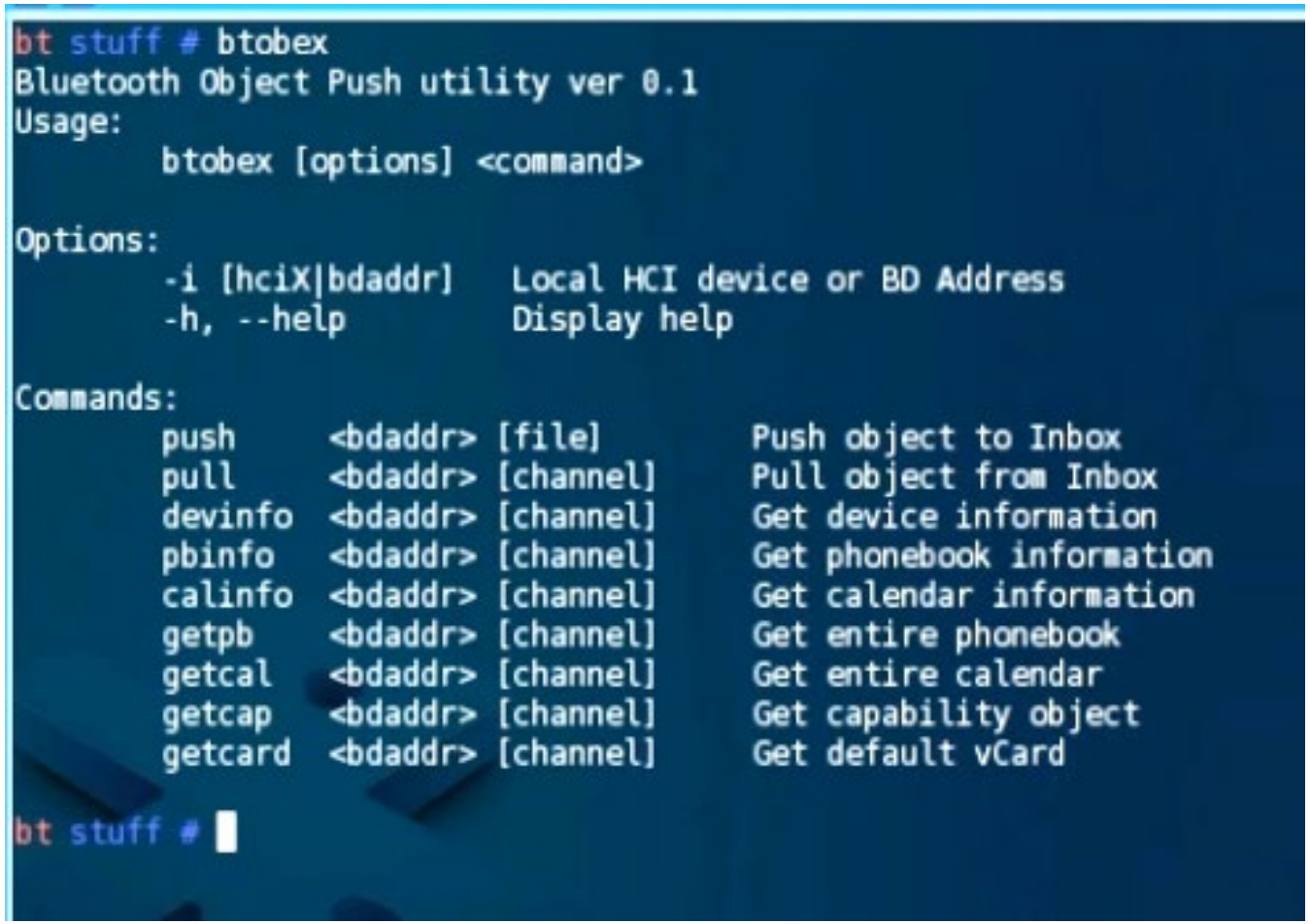
BLUETOOTH ATTACK TYPES

- Blueborne Attack
  - Collection of overflow attacks that could result in arbitrary code execution
  - An attack virus that spreads through air
  - Gets into a device via bluetooth
  - Takes full control of the device
  - Does not require pairing
  - The device need not be in discoverable mode
- Bluejacking
  - Sending unsolicited messages to Bluetooth-enabled devices
  - Can include a malicious payload such as a trojan horse
- Bluesnarfing
  - Unauthorized access to emails, messages, contacts, etc. on the target
- Bluebugging
  - Remote access to phone features such as the microphone or camera

BLUETOOTH ATTACK TYPES (CONT'D)

- Bluesmacking
  - Denial-of-Service attack
- Bluesniffing
  - Locate Bluetooth devices
- BluePrinting
  - Enumerate details about Bluetooth-enabled devices
- MAC Spoofing Attack
  - Used to clone or MITM Bluetooth devices
- Man-in-the-Middle Attack
  - Manipulate communications between Bluetooth devices
  - Often uses MAC spoofing
  - Commonly used against Bluetooth Low Energy IoT devices and their smartphone app

BLUESNARFING EXAMPLE



BLUETOOTH HACKING TOOLS

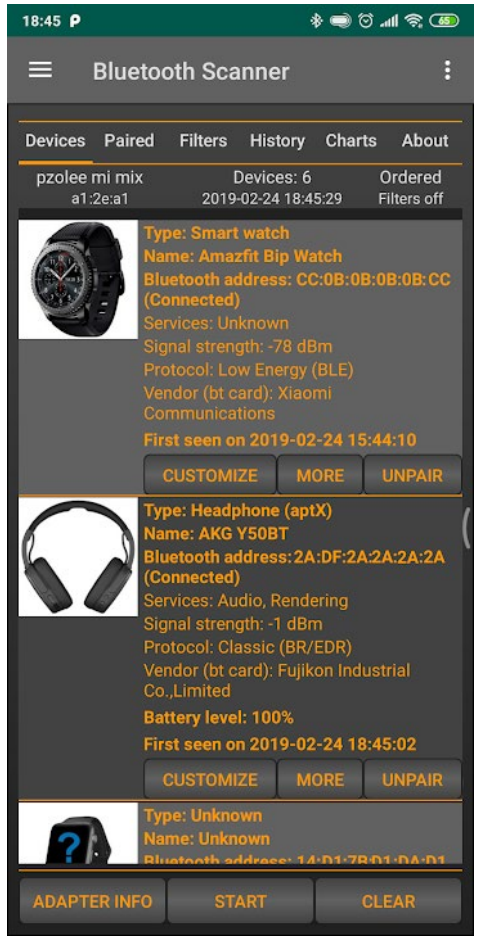
- BlueBorne
  - Blueborne exploit framework available on GitHub
- spooftooph
  - Automates spoofing or cloning of a Bluetooth device
- BlueScanner, btscanner
  - Bluetooth device scanners
  - Designed to extract as much information as possible from Bluetooth devices without pairing
- btCrawler
  - Scans for visible Bluetooth devices
- Bluedriving
  - Bluetooth wardriving utility
- PhoneSnoop
  - Allows you to turn a Blackberry into a room bugging device

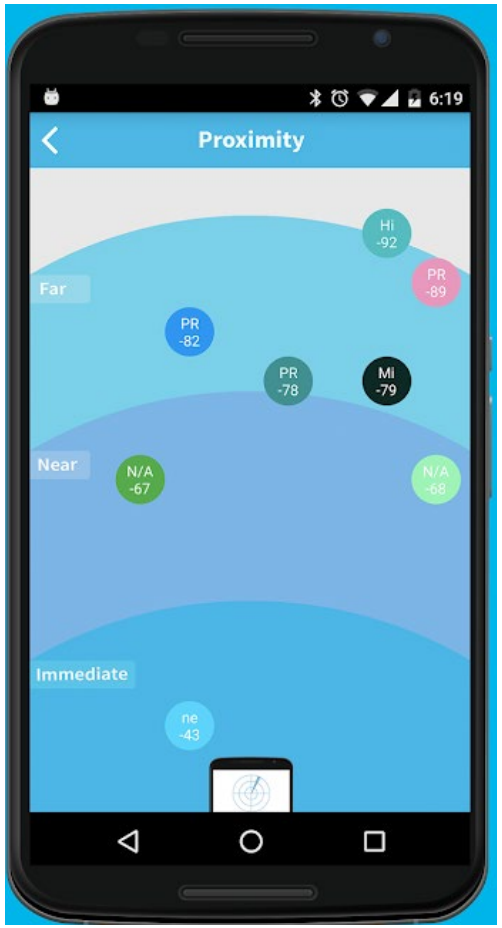
BLUETOOTH HACKING TOOLS

- BH BlueJack
  - Open-source Bluejacking software
- Bluesnarfer, btobex
  - Bluetooth bluesnarfing utility
- Blooover II
  - Bluebug/bluejack/bluesnarfer
- Bluediving
  - Tool suite that can spoof, Bluebug, BlueSnarf, and BlueSmack
- GATTacker, BtleJuice
  - Bluetooth Low Energy eavesdropping and MITM tools
  - Conduct attacks against BLE peripherals (such as IoT wearables) and a phone

BLUETOOTH MOBILE APP TOOLS

- Blue Sniff
  - Bluetooth scanner that runs on iPhone
- BLE Scanner
  - Bluetooth scanner that runs on Android
- Super Bluetooth Hack
  - Bluesnarfer that runs on Android
- CIHwBT
  - Bluetooth exploit suite (BlueSnarf, BlueJack, DoS) that runs on Windows Mobile





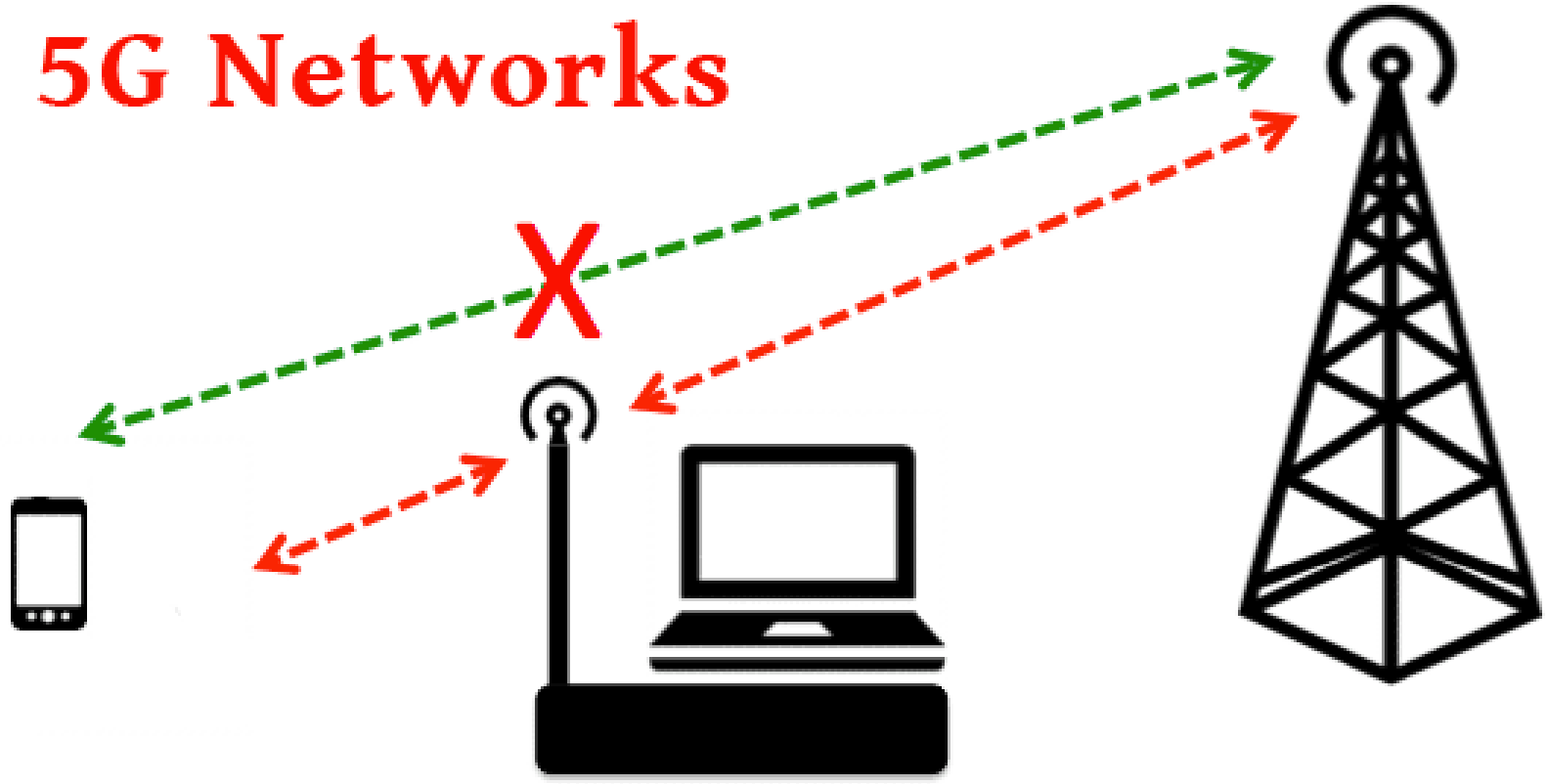
16.10 OTHER WIRELESS HACKING

- Cellular
- RFID
- NFC

CELLULAR

New Attacks Against

4G, 5G Networks



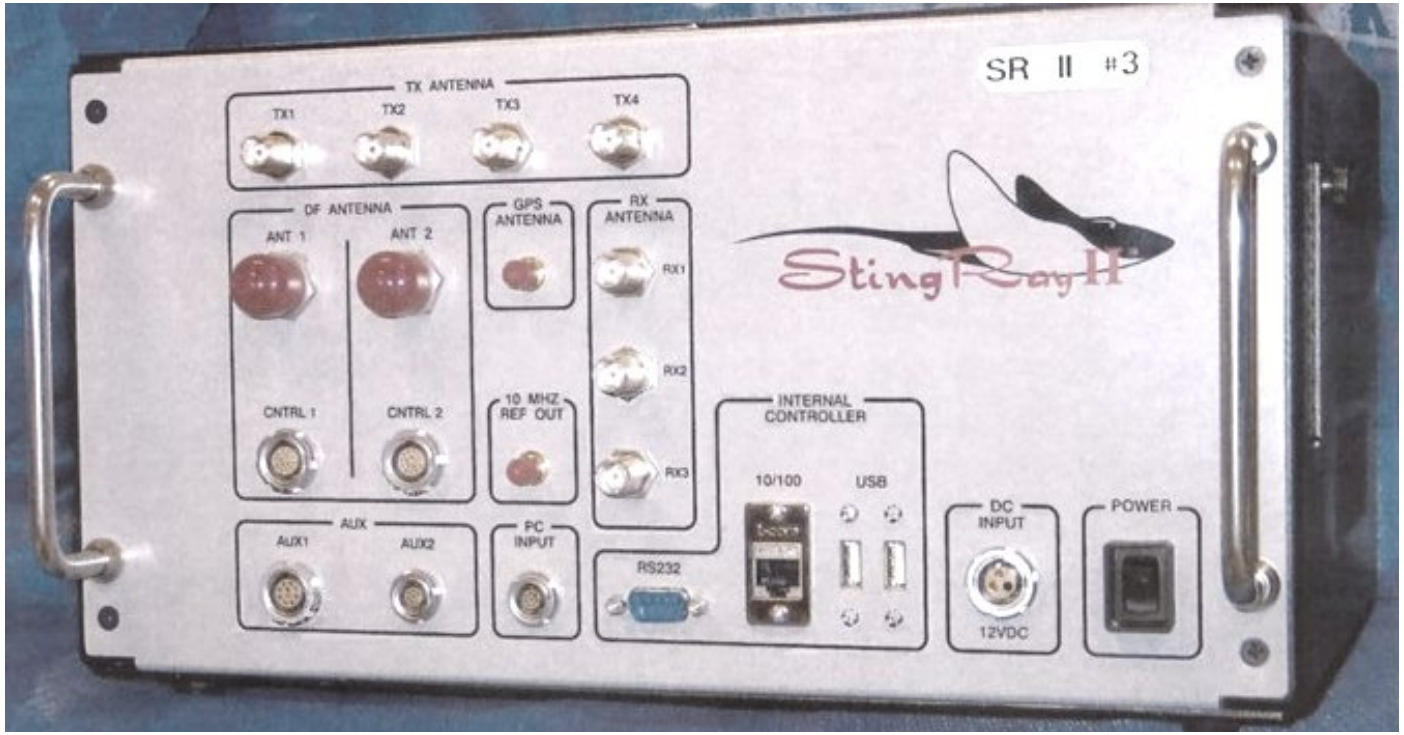
NEW CELLULAR ATTACKS AGAINST 4G, 5G

- Torpedo Attack
  - Exploits a weakness in the cell tower paging system
  - Allows an attacker to track a phone's location
  - Spoof, inject, or block emergency alerts such as severe weather warnings and Amber alerts
- Piercer Attack
  - An attacker can determine an international mobile subscriber identity (IMSI) number
- IMSI-Cracking Attack
  - An attacker can crack the encrypted IMSI number in order to clone it
- StingRay Cell Tower Simulator
  - Cell phone surveillance and eavesdropping

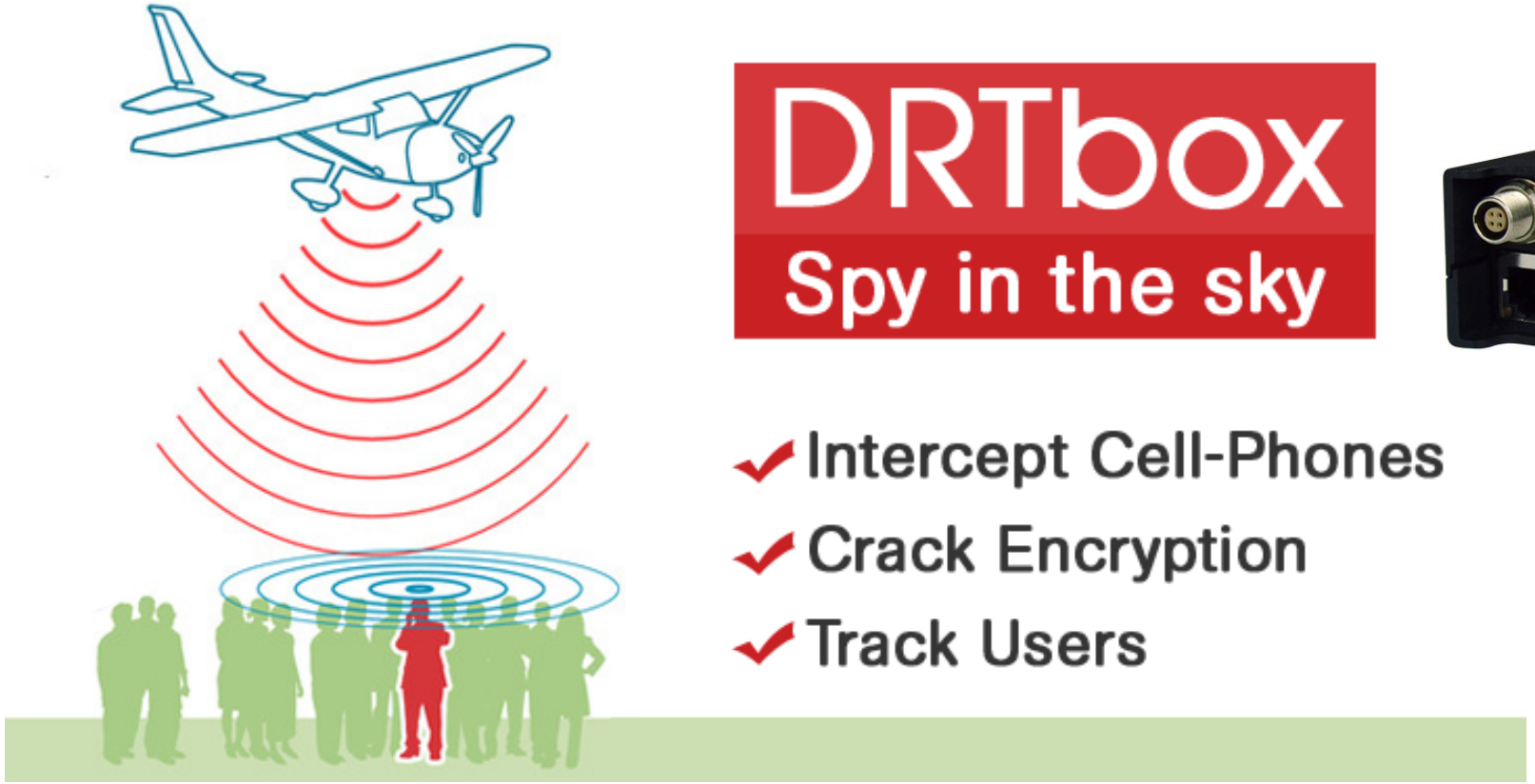
CELL TOWER SIMULATORS

- AKA IMSI catcher
- Device masquerades as a legitimate cell phone tower
- Tricks phones within a certain radius (up to 500 meters) into connecting to it rather than a legitimate tower
- Can be used to intercept call information:
  - Cell phone's International Mobile Subscriber Identity (IMSI) number
  - Metadata about calls (number dialed, duration of call)
  - Content of SMS and voice calls
  - Data usage and websites visited
- Can also spoof text messages and Caller ID
- Currently only works on 3G and 4G networks
  - However many 5G carriers also provide 4G parallel capability
  - A victim could be forced to downgrade to 4G for a particular call
- Popular products include Stingray, DRTBox

STINGRAY EXAMPLE



DRTBOX EXAMPLE



DRTbox

Spy in the sky

- ✔ Intercept Cell-Phones
- ✔ Crack Encryption
- ✔ Track Users

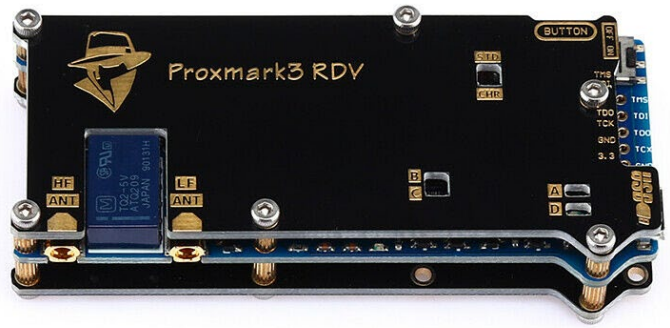
RFID BADGE CLONING

- Badge cloning is the act of copying authentication data from an RFID badge's microchip to another badge
- The attacker can obtain authorization credentials without actually stealing a physical badge from the organization
- The older RFID badge technology uses the unencrypted 125 kHz EM4100 protocol
  - Device will begin transmitting data to any receivers that are nearby

RFID BADGE CLONING (CONT'D)

- Proxmark 3
  - The "swiss army knife" of badge cloners
  - NFC and RFID badge cloner
  - You can attach hi and low frequency, as well as long-range antennas
- iCopy-X
  - Hand-held rapid cloner
  - Built on Proxmark 3
- You can hide everything in a backpack
  - Just get within a foot or two from the victim
  - Crowded elevator, food counter, checkout line, go up and talk to them!

ICOPY-X AND PROXMARK 3 EXAMPLES



NFC BADGE/TAG CLONING

- NFC badges/tags use MIFARE encrypted 13.56 MHz
- You can buy an NFC RFID reader/writer tool
  - There are several models available online
  - You will also need to set up a laptop with software *

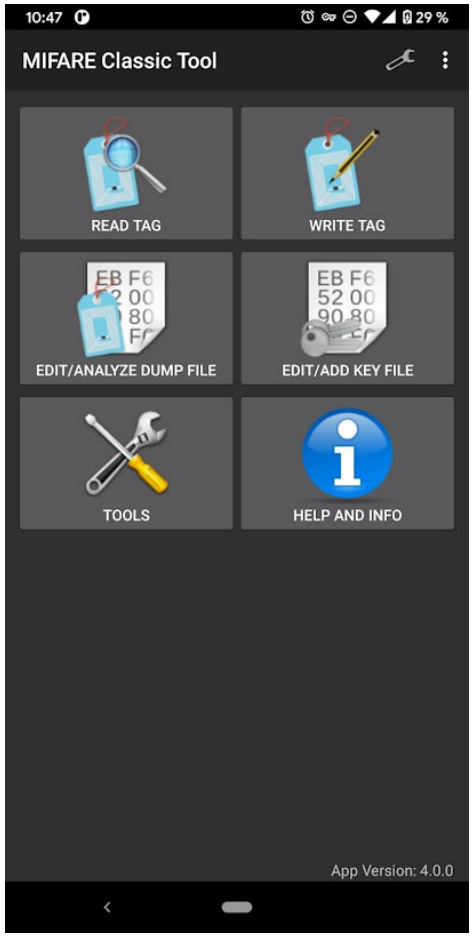
* For exact steps, see:
https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf

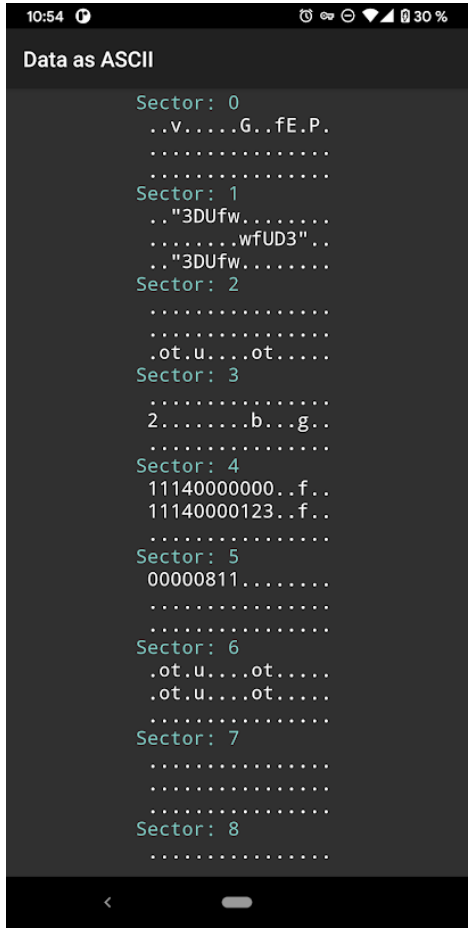
NFC BADGE/TAG CLONING

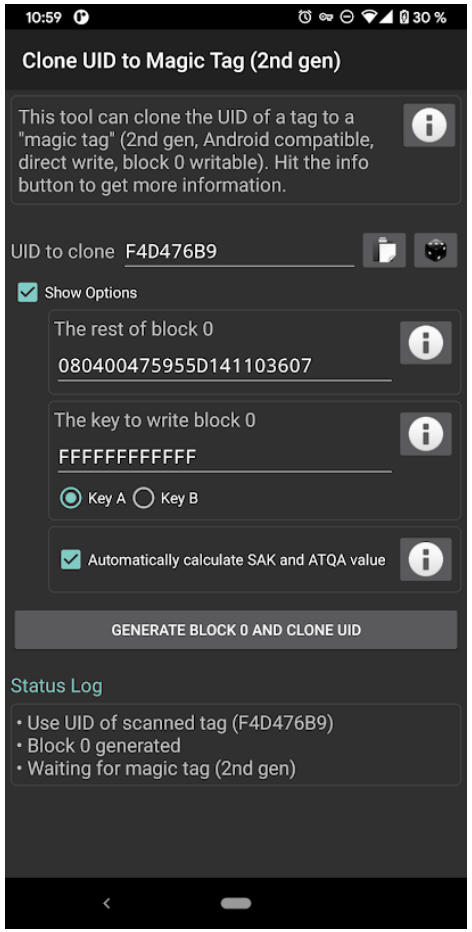
- An Android phone provides an easier way to clone NFC
  - Android has built-in NFC capabilities
  - Download the MiFARE Classic Tool app
    - Key brute force cracker
    - Also comes with NFC card manufacturer default keys
    - Many organizations do not bother to change the default key, allowing you to easily clone the badge
- MTools MKeys is another mobile app NFC key cracker
  - Performs dictionary attacks

For more information on MTools see:
https://why.yuyeye.cc/post/mtools-guide/

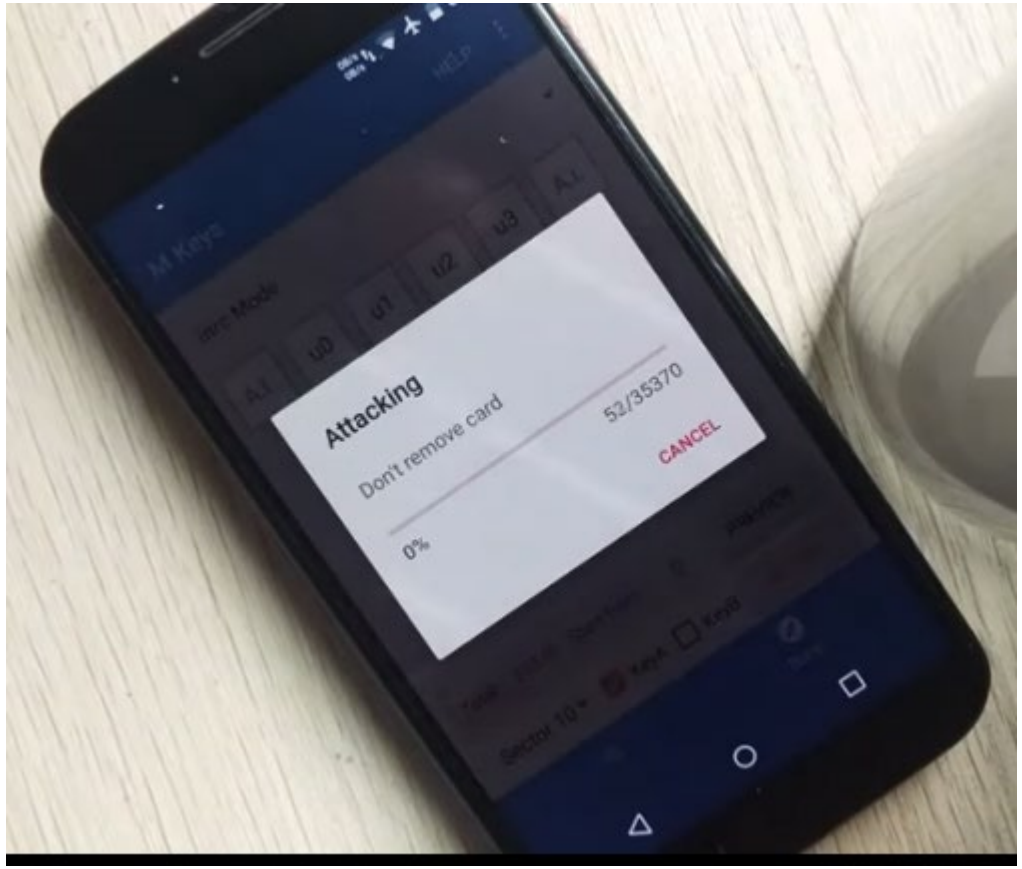
MIFARE CLASSIC TOOL APP EXAMPLE







MTOOLS MKEYS EXAMPLE



16.11 WIRELESS SECURITY TOOLS

- Vulnerability Scanners
- WIPS
- Mobile

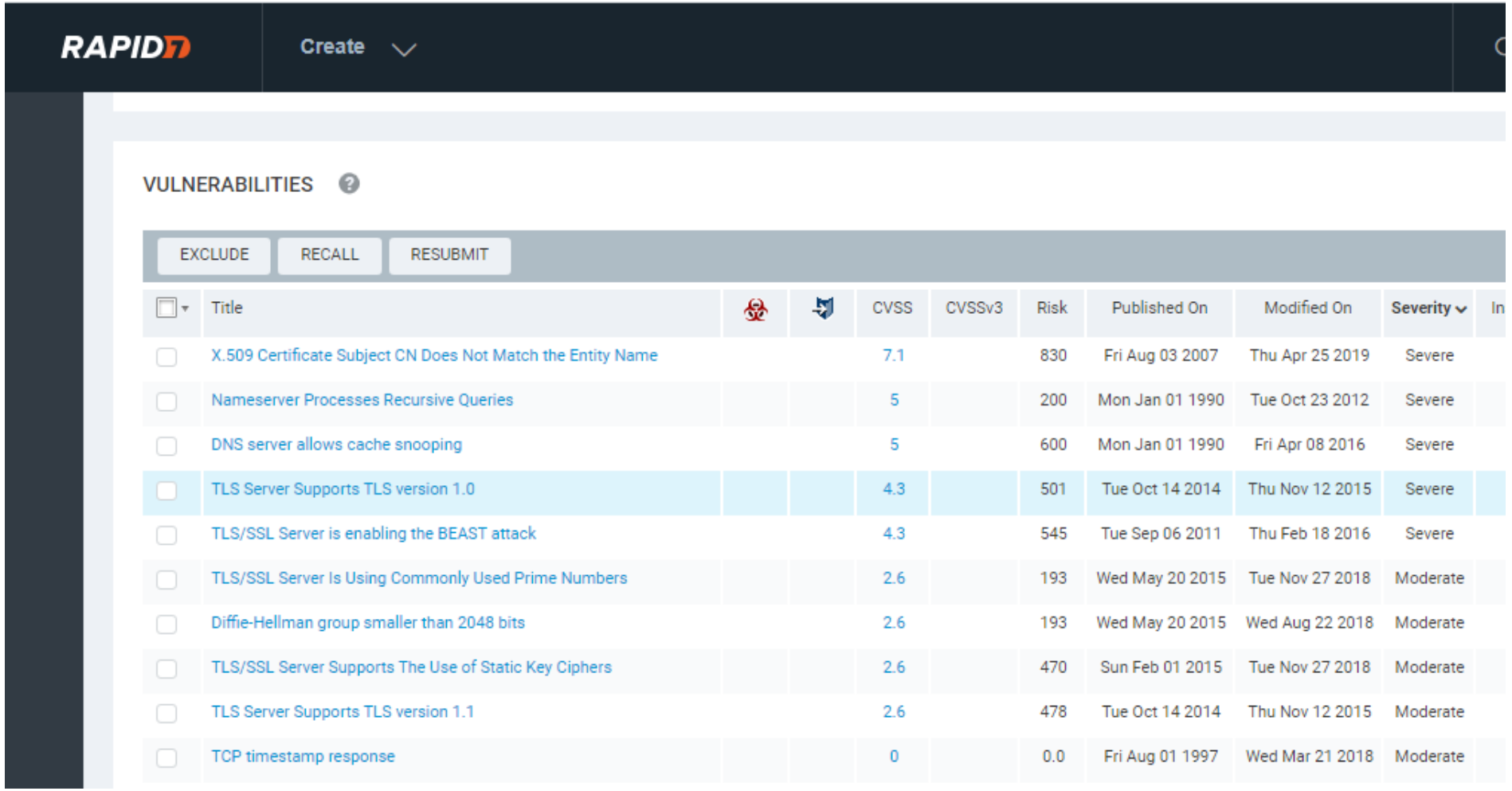
WIRELESS SECURITY TOOLS

- Kismet
  - Wi-Fi device detector, sniffer, WIDS framework
  - Detects 802.11a/b/g/n Aps
  - Runs on Linux
- Solar Winds Network Performance Monitor / Rogue AP Detection
  - All-in-one network monitor.
- OSWA-Assistant
  - Free standalone wireless auditing toolkit
- Moocherhunter
  - Geolocate unauthorized wireless clients (moochers and hackers!)
- Rapid 7 Nexpose
  - Network vulnerability scanner
  - Can scan wireless networks and devices as easily as wired
- WiFish Finder (SourceForge)
  - Open source testing tool to see if active wireless devices are vulnerable to 'Wi-Fishing' attacks

WIRELESS SECURITY TOOLS (CONT'D)

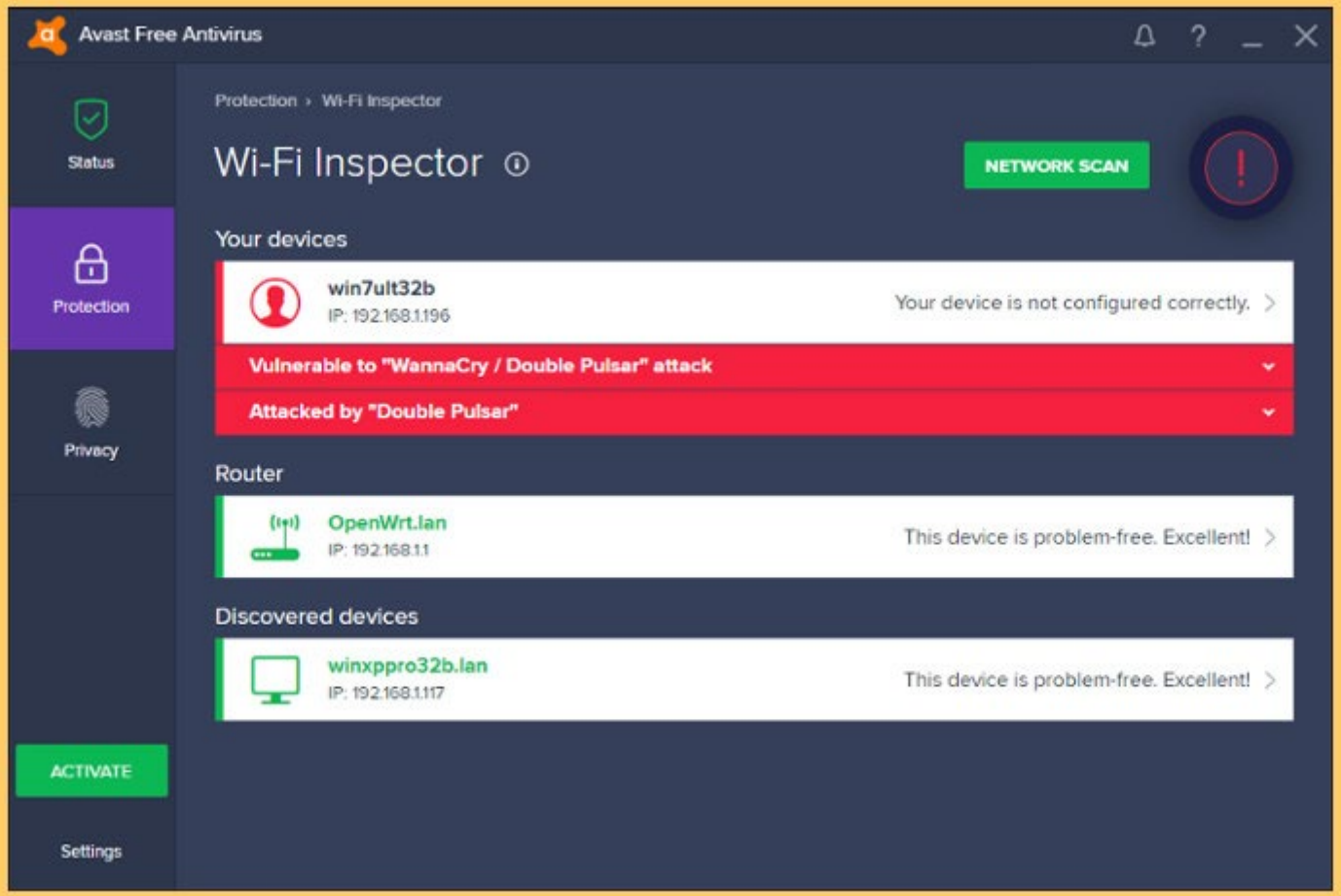
- F-Secure Router Checker
  - Test for router - DNS hijacking
- Avast Wi-Fi Inspector
  - Test for weak/default router passwords, router firmware vulnerabilities, unencrypted wireless networks, DNS hijacking, open network ports on the router
- Panda Wi-Fi Protection
  - Vulnerability scanner
- Bitdefender Home Scanner
  - Vulnerability scanner

RAPID 7 NEXPOSE EXAMPLE

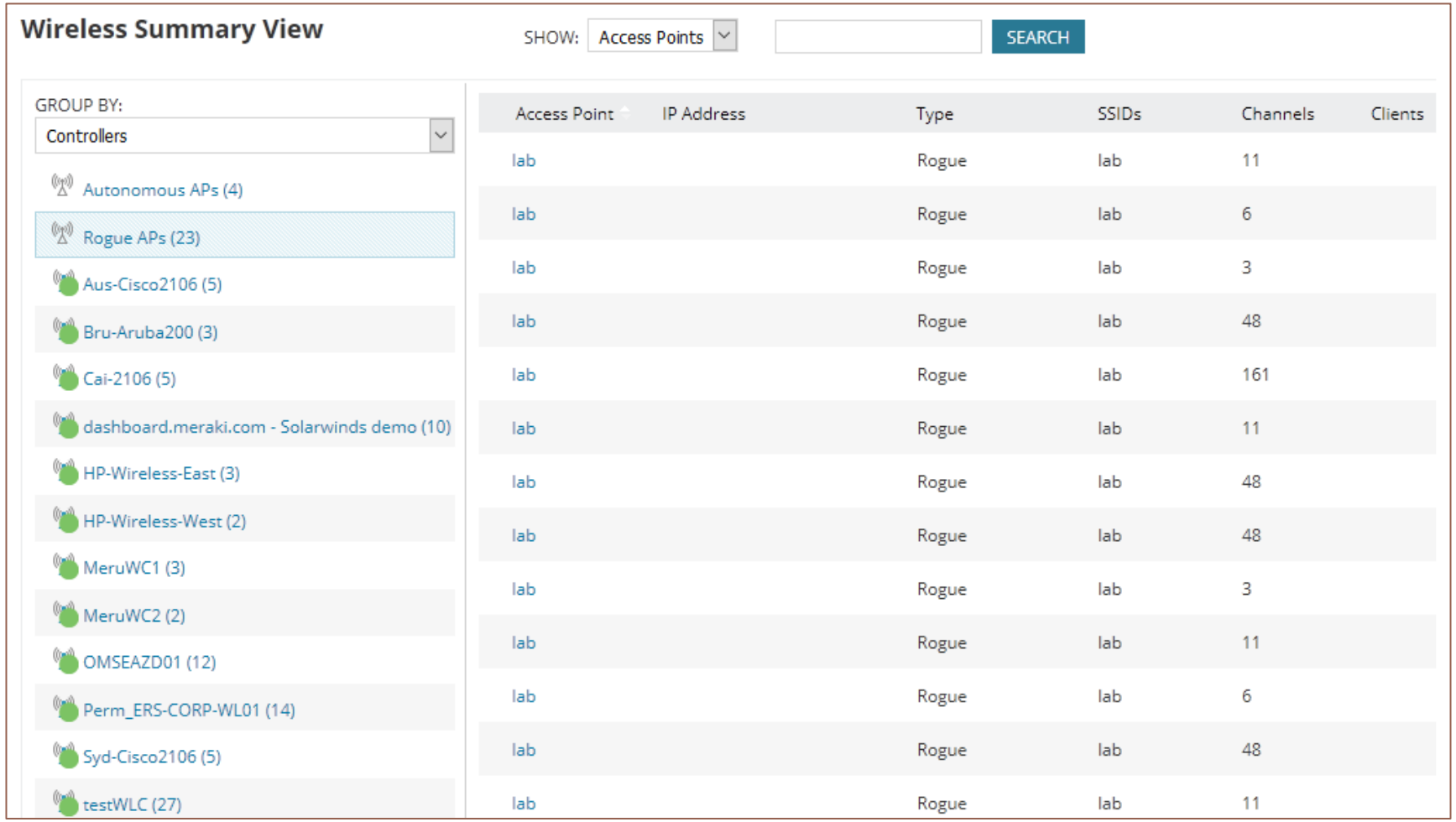


Title	CVSS	CVSSv3	Risk	Published On	Modified On	Severity	In
X.509 Certificate Subject CN Does Not Match the Entity Name	7.1		830	Fri Aug 03 2007	Thu Apr 25 2019	Severe	
Nameserver Processes Recursive Queries	5		200	Mon Jan 01 1990	Tue Oct 23 2012	Severe	
DNS server allows cache snooping	5		600	Mon Jan 01 1990	Fri Apr 08 2016	Severe	
TLS Server Supports TLS version 1.0	4.3		501	Tue Oct 14 2014	Thu Nov 12 2015	Severe	
TLS/SSL Server is enabling the BEAST attack	4.3		545	Tue Sep 06 2011	Thu Feb 18 2016	Severe	
TLS/SSL Server Is Using Commonly Used Prime Numbers	2.6		193	Wed May 20 2015	Tue Nov 27 2018	Moderate	
Diffie-Hellman group smaller than 2048 bits	2.6		193	Wed May 20 2015	Wed Aug 22 2018	Moderate	
TLS/SSL Server Supports The Use of Static Key Ciphers	2.6		470	Sun Feb 01 2015	Tue Nov 27 2018	Moderate	
TLS Server Supports TLS version 1.1	2.6		478	Tue Oct 14 2014	Thu Nov 12 2015	Moderate	
TCP timestamp response	0		0.0	Fri Aug 01 1997	Wed Mar 21 2018	Moderate	

AVAST WI-FI INSPECTOR EXAMPLE

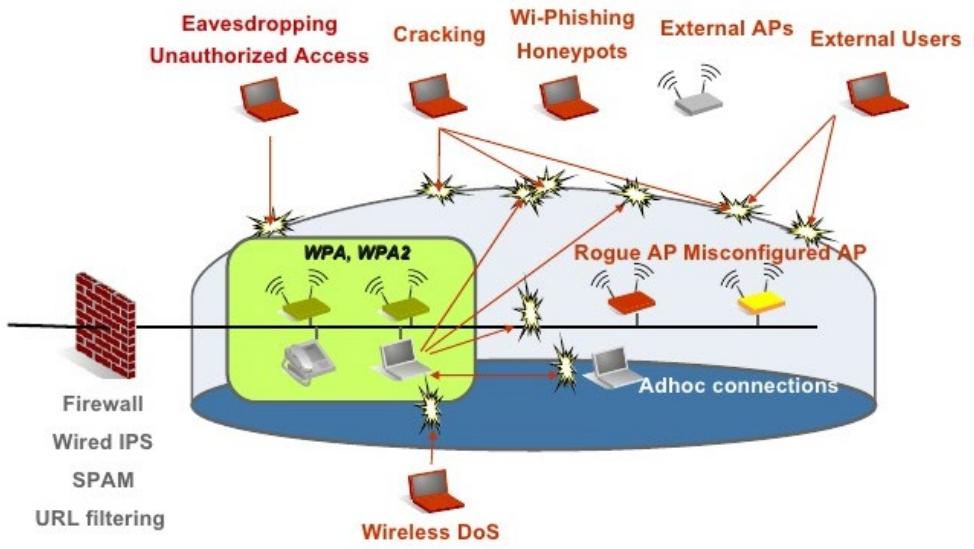


SOLAR WINDOWS ROGUE AP DETECTION EXAMPLE



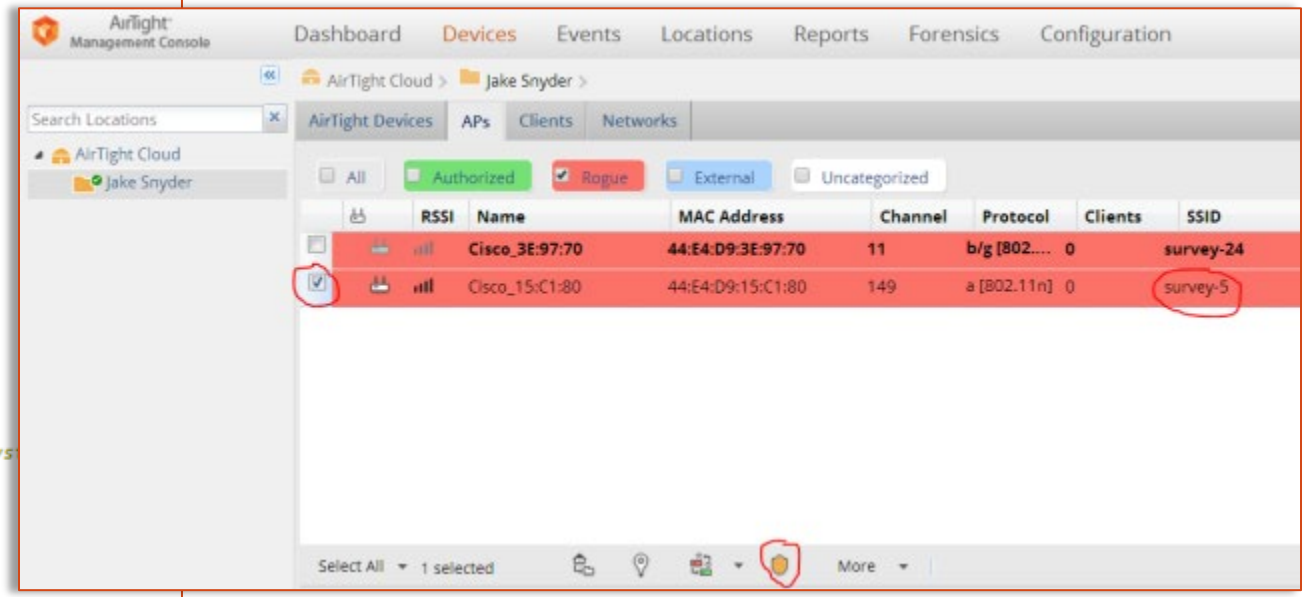
WIRELESS IPS TOOLS

- Extreme Networks Intrusion Prevention System
- AirMagnet Enterprise
- Dell SonicWALL Clean Wireless
- HP TippingPoint NX Platform NGIPS
- Mojo AirTight WIPS
- Network Box IDP
- AirMobile Server
- Wireless Policy Manager (WPM)
- ZENworks Endpoint Security Management
- FortiWiFi



MOJO AIRTIGHT WIPS EXAMPLE

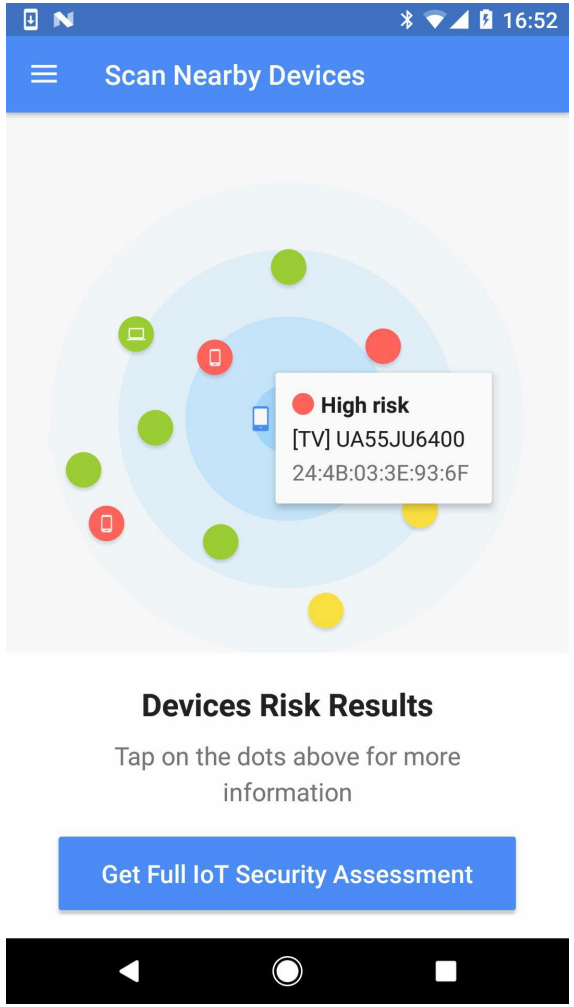
```
Packet Info
    Packet Number:          148
    Flags:                  0x00000000
    Status:                 0x00000000
    Packet Length:          30
    Timestamp:              21:40:20.492739400 02/26/2014
    Data Rate:              12  6.0 Mbps
    Channel:                149  5745MHz  802.11a
    Signal Level:           44%
    Signal dBm:             -72
    Noise Level:            0%
    Noise dBm:              25
802.11 MAC Header
    Version:                0 [0 Mask 0x03]
    Type:                   %00  Management [0 Mask 0x0C]
    Subtype:                %1100  Deauthentication [0 Mask 0xF0]
    Frame Control Flags:    %00000000 [1]
                              0... .... Non-strict order
                              .0.. .... Non-Protected Frame
                              ..0. .... No More Data
                              ...0 .... Power Management - active mode
                              .... 0... This is not a Re-Transmission
                              .... .0.. Last or Unfragmented Frame
                              .... ..0. Not an Exit from the Distribution Sys
                              .... ...0 Not to the Distribution System
    Duration:               321  Microseconds [2-3]
    Destination:            FF:FF:FF:FF:FF:FF  Ethernet Broadcast [4-9]
    Source:                 44:E4:D9:15:C1:80  Cisco:15:C1:80 [10-15]
    BSSID:                  44:E4:D9:15:C1:80  Cisco:15:C1:80 [16-21]
    Seq Number:             1860 [22-23 Mask 0xFFF0]
    Frag Number:            0 [22 Mask 0x0F]
802.11 Management - Deauthentication
    Deauthentication Reason Code: 2  Previous authentication no longer valid [24-25]
FCS - Frame Check Sequence
    FCS:                    0x23E1B2F5  Calculated
```



MOBILE WI-FI SECURITY TOOLS

- Armis BlueBorne Vulnerability Scanner
  - Check if your device, or the devices around you, are at risk
- Acrylic Bluetooth Low Energy Analyzer
  - Can identify Bluetooth devices including new IOT devices around you
- WiFi Protector
  - Wireless VPN
- SoftPerfect WiFiGuard
  - Network scanner that runs at set intervals and reports any unrecognized connected devices
- Xirrus Wifi Inspector
  - Realtime monitor of traffic performance and clients; rogue detector

Armis BlueBorne Vulnerability Scanner



BLUETOOTH SECURITY TOOLS

- BlueAuditor
- Frontline Bluetooth Protocol Analyzer
- Ellisys Bluetooth Tracker
- Acrylic LE Analyzer
- BLE Scanner for PC
- BlueMaho

16.12 WIRELESS HACKING COUNTER-MEASURES

- Router Configuration
- SSID Settings
- Authentication
- Additional Security
- Bluetooth
- Other Wireless

WI-FI ROUTER CONFIGURATION BEST PRACTICES

- Strategically place antennas to always point inward into the building/complex
- If possible, maintain low power levels on WAPs
  - Add more WAPs to make up for coverage gaps
- Ensure remote router login is disabled
- Ensure router access password is set and firewall protection is enabled
- Ensure MAC Address filtering is enabled on routers/access points
  - WAP won't respond to connection requests from clients that are not on the approved list
- Ensure SSID broadcasts are disabled at access points and passphrase is changed frequently

SSID SETTINGS BEST PRACTICES

- Change the default SSID
- Hide the SSID when practical
- Keep passphrases free of SSID, network/company name, or anything that is easy to figure out
- Ensure there is a firewall/packet filter between AP and Intranet
- Keep wireless network strength low enough avoid detection outside organization
- Regularly ensure there are no issues with setup/configuration
- Use extra traffic encryption

AUTHENTICATION BEST PRACTICES

- When practical, implement MAC filtering on the Access Point
- Use captive portals for legal protection and to enforce user/device registration
- Use the highest security standard possible
  - WPA3 for SOHO use
  - 802.1x for enterprise use
- Ensure access points are in secure locations
- Ensure all wireless drivers are up-to-date
- Ensure network is disabled when it isn't needed

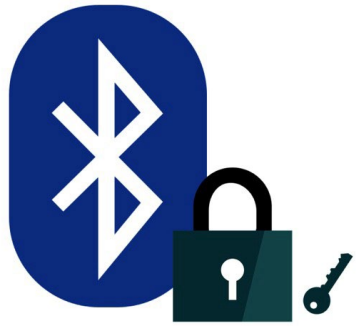
ADDITIONAL WIRELESS SECURITY BEST PRACTICES

- Use different SSIDs and VLANs to isolate users / devices by security level:
  - Guests
  - Wireless clients
- Enroll devices (including BYOD) into Mobile Device Management to:
  - Implement Geofencing
  - Enforce end point protection
  - Enforce separation of business and personal data
  - Disallow jailbroken or rooted devices on the network
- Educate users on the risks of using public / free Wi-Fi

Realize that MDM and endpoint security software is *not* used to protect the mobile device, but instead used to protect the network *from* mobile devices

BLUETOOTH HACKING COUNTERMEASURES

- Ensure PIN keys use non-regular patterns
- Ensure device is always in hidden mode
- Keep track of all past paired devices and delete suspicious devices
- Ensure BT is kept disabled unless required
- Never accept pairing requests from unknown devices



BLUETOOTH HACKING COUNTERMEASURES (CONT'D)

- Ensure encryption is enabled when connecting to a PC
- Keep device network range at its lowest
- Only pair with other devices in a secure area
- Ensure antivirus is installed
- Ensure default security settings are changed to the best possible standard
- Ensure all BT connections use Link Encryption
- Ensure encryption is empowered for multiple wireless communications

OTHER WIRELESS ATTACK COUNTERMEASURES

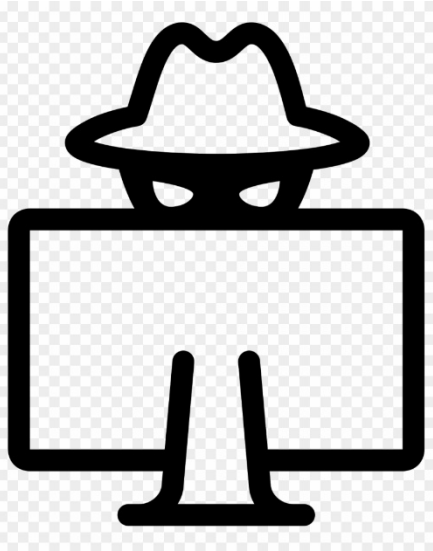
- Cellular
  - Upgrade to 5G
  - Use encryption when making Wi-Fi calls
  - Prefer encrypted messaging platforms over unencrypted SMS
- RFID / NFC
  - Upgrade older 125 KHz RFID systems to newer 13.56 MHz NFC systems
  - Change default keys on NFC systems
  - Use RFID blocking sleeves or cards to protect the card from RFID pickpocketing

16.13 HACKING WIRELESS NETWORKS REVIEW

- Review

WIRELESS NETWORK HACKING REVIEW

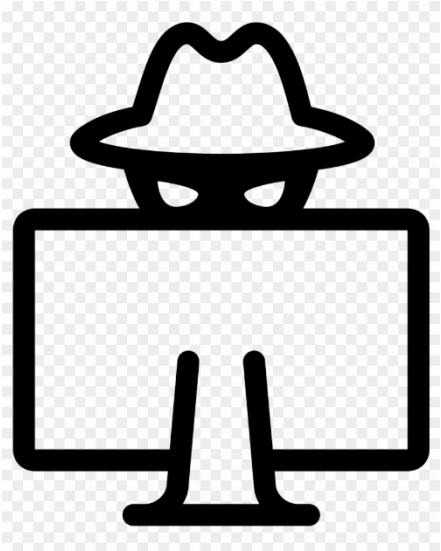
- Wi-Fi infrastructure is made of software and hardware
- The SSID is a friendly name for a Wi-Fi network
- The BSSID is the MAC address of a wireless access point
- A BSS is a Wi-Fi network with one AP
- An ESS is a Wi-Fi network with multiple APs
  - The APs typically use the same SSID



- WEP uses a 24-bit IV, stream cipher RC4, and a CRC-32 checksum
- Because WEP has no digital signature or anti-replay capability, you can use aireplay-ng to perform a replay attack against the AP
  - This speeds up collecting IVs for cracking the password
- You can also use a fragmentation attack against WEP to collect keying information from the header of a captured packet
  - You can use that to quickly obtain more keying material from the AP until you have the PRGA
  - You can use the PRGA with packetforge-ng to create a custom packet to quickly obtain IVs for password cracking

WIRELESS NETWORK HACKING REVIEW (CONT'D)

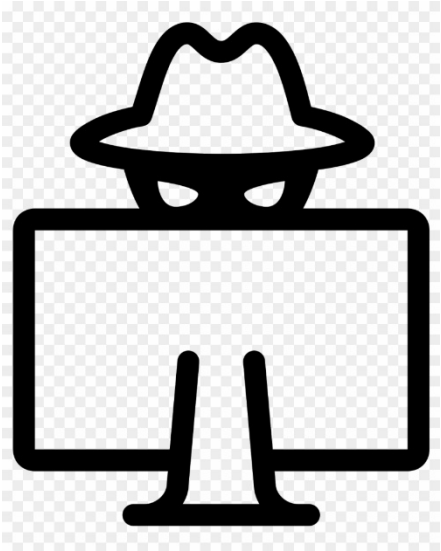
- WPA introduced TKIP to change the encryption key for every packet
- It also uses sequence numbers to guard against replay attacks
- The IV is 48-bit, and the key is 128-bit
- WPA2 introduced CCMP-AES for encryption
- Both WPA and WPA2 have an imperfect 4-way handshake that can be captured and cracked



- Both WPA and WPA2 offer an enterprise version that uses 802.1x and RADIUS to centralize authentication
- 802.1x access points put the client connection on hold, typically offering the user a captive portal
- The user or client's authentication is forwarded to the RADIUS server
- If authentication is successful, the client can enter the network
- 802.1x uses the Extensible Authentication Protocol (EAP) to allow a wide range of authentication factors including MS-CHAPv2 passwords, certificates and tokens, and biometrics

WIRELESS NETWORK HACKING REVIEW (CONT'D)

- WPA3 has been recently introduced
  - It is possible to brute force a WPA3 key
- Bluetooth has a variety of vulnerabilities and exploits that allow you to:
  - Send spam messages to the victim, read the victim's messages and contact list, and remotely execute code on the device
- Cellular devices are susceptible to StingRay and DRTBox MITM attacks



- RFID and NFC badges and tokens can be cloned from a short distance
- There are several NFC hacking apps you can use to crack the NFC key
- There are a number of vulnerability scanners you can use to test Wi-Fi networks
- There are also a number of Wi-Fi security tools and IPSes available to protect the wireless network