COMP47860: Ethical Computer Hacking

Lecture 9: Wireless Hacking

Assoc. Prof. Mark Scanlon

Agenda

- Ethics
- What is Wi-Fi
- Types of Wi-Fi Security
  - Open Networks
  - Wired Equivalent Privacy (WEP)
  - Wi-Fi Protected Access (WPA)
  - Wi-Fi Protected Setup (WPS)
  - WPA Enterprise (RADIUS)
- Attack Types
  - User
- Protect Yourself

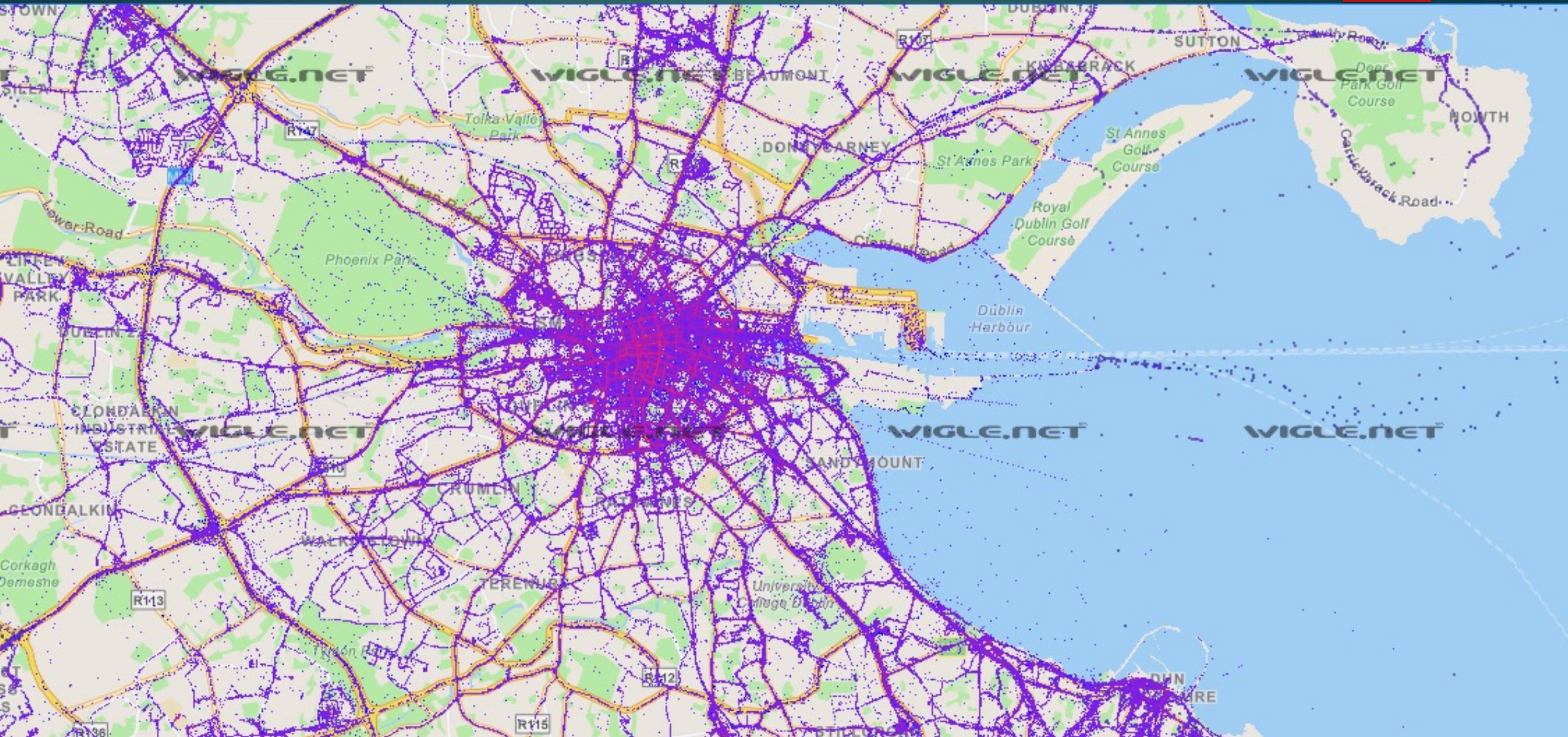
Disclaimer

- Everything you will be shown is for educational purposes only.
- DO NOT USE THESE SKILLS WITHOUT EXPLICIT WRITTEN PERMISSION
  This is what separates Ethical Hackers from the Black Hats
- There are plenty of "safe playgrounds" to hone your skills
  - Security Shepherd
  - Damn Vulnerable Web App (DVWA)
  - Mutillidae
  - Web Goat

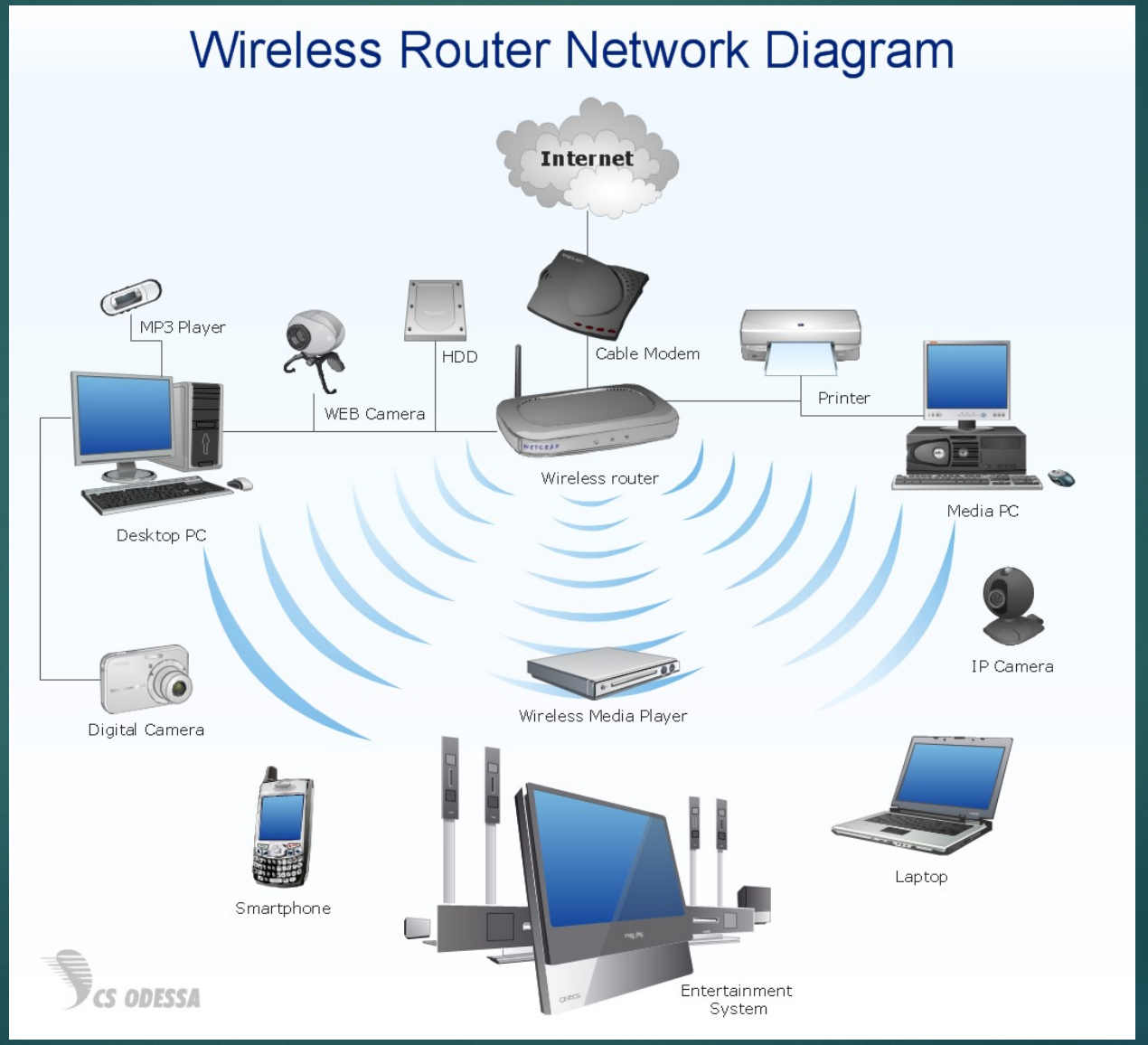
What is Wi-Fi?

- Wi-Fi or WLAN
- Industry used in early 1990's
- Consumer routers arrived in 2000
- Network
- Data is sent over the air
- Noisy
- Doesn’t like solid objects
- Cheap! Convenient!
- a/b/g/n/ac/az
- Easily mapped - https://wigle.net

Easily Mapped



What is Wi-Fi


Wireless Router Network Diagram
Internet
MP3 Player
HDD
Cable Modem
Printer
WEB Camera
Wireless router
Media PC
Desktop PC
IP Camera
Digital Camera
Wireless Media Player
Smartphone
Laptop
Entertainment System
CS ODESSA

What is Wi-Fi

- Wardriving
  - Mapping of wireless networks by a vehicle
  - Kismet and Netstumbler were the tools of choice
  - USB GPS device support
- 2012 – Google got in trouble for recording Wi-Fi hotspots with the Google Street View vehicles
  - https://arstechnica.com/gadgets/2012/05/googles-street-view-engineer-knew-data-collection-was-questionable/

Wi-Fi Security Types: Open

- Open
  - No password required to access the network
  - Common in the hospitality industry
  - Business resources not always segmented
    - Point of sale (POS)
    - Printer
  - No restriction on who can join the network

Wi-Fi Security Types: Open

- Captive Portal
  - “Please agree to the terms... etc”
  - “Free Wi-Fi is slow, but sign up for super fast connection"
- Any one in range can see your traffic
- Attacker does not need to be connected to the network to see:
  - Who is connected
  - What is being sent over the network
  - Kick devices off the network

Wi-Fi Security Types: Open

- Open source analysis tools available
- Airodump-ng
  - Part of the Aircrack-ng suite of tools to assess Wi-Fi network security.

```
root@kali:~# airodump-ng wlan0


 CH 11 ][ Elapsed: 0 s ][ 2018-11-26 16:29

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 90:CD:B6:83:43:B2  -34        3        0    0   5   65  WPA2 CCMP   PSK  Oppo
 D8:C8:E9:C2:CB:18  -82        2        0    0  10  130  WPA2 CCMP   PSK  perfe
 E4:6F:13:B6:DB:03  -67        3        0    0  10  270  WPA2 CCMP   PSK  Fligh
 F0:D7:AA:E0:4F:E4  -61        6        0    0   3   65  OPN              Ashu
 7A:11:DC:6E:C0:78  -66        7        8    3   3  130  WPA2 CCMP   PSK  LIFCA
 78:11:DC:5E:C0:78  -63        7        0    0   3  130  WPA2 CCMP   PSK  Xiaom
 B8:C1:A2:3B:16:0C  -59        2        4    0  11  130  WPA2 CCMP   PSK  (JTP-
 10:DA:43:72:41:C2  -84        1        1    0  13  54   WPA2 CCMP   PSK  Nextr
 58:D7:59:EC:1F:68  -80        3        0    0   7  130  WPA2 CCMP   PSK  tie d
 0A:28:19:E1:9F:5B  -46        3        0    0   7  130  WPA2 CCMP   PSK  LAPTO
 C0:FF:D4:91:49:DF  -48        1       31   15   7  130  WPA2 CCMP   PSK  NETGE
 0C:D2:B5:49:D5:C4  -66        4        5    2   7   65  WPA  CCMP   PSK  Airte
```

Wi-Fi Security Types: Open

- Does not work with all wireless cards
  - Issue is driver support.
    - Proprietary drivers from some manufacturers
- Favoured Wi-Fi cards for Linux are one with Ralink and Atheros chipsets due to support
- Supported chipsets required for injection

- External USB adapters can be mounted in a Kali VM

Wi-Fi Security Types: WEP

- Wired Equivalent Protection (WEP)
- Released in 1997
- Original encryption standard for wireless
- Not the default any more (broken)
- 64bit
  - 10 hexadecimal characters
  - 5 ASCII characters
- 128 bit
  - 26 hexadecimal characters
  - 13 ASCII characters

Wi-Fi Security Types: WEP

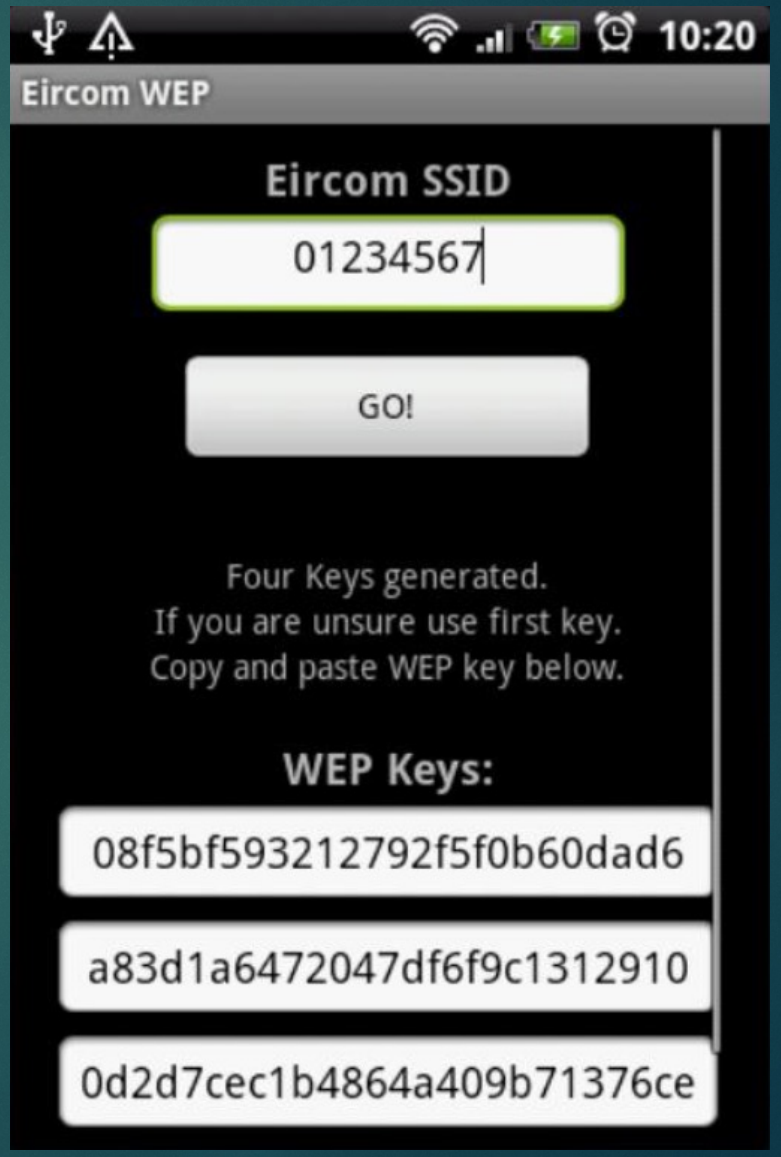
- WEP can be broken with a bruteforce attack on the password
- 2001 – Cryptanalysis of RC4 used in WEP reveals weakness.
- Attack requires gathering of wireless packets
- Passive attack – just listen (stealth)
- Aggressive attack – stimulate packets (injection required)
  - Deauth – kick someone off the network
  - ARP replay – reinject ARP requests
- Same shared key to all users
- 2001 - 200k packets required
- 2007 – optimized attack – 40k-80k packets

Wi-Fi Security Types: WEP

- Optimization of the attack brought cracking time from +1 hour attack taking a few minutes
- Opensource tools became available
- Aircrack-ng - suite of tools to assess Wi-Fi network security.
  - Airmon-ng – Sets wireless card in Monitor Mode
  - Airodump-ng – collect wireless traffic
  - Aircrack-ng – Recover password for network
  - Airdecap-ng – Remove wireless wrapper, and can be resulting pcap can be loaded in packet analyzer, e.g., Wireshark, or searched for plain text content, e.g., Commandline: strings, grep

Wi-Fi Security Types: WEP

- Eircom WEP routers (2010)
  - Setup tool shipped with every router on CD
  - Input required Serial number from router
  - Letterkenny hacker reverse engineered the application
  - Produced a script that took the SSID and returned the WEP key
  - Windows, Android and iOS applications were quick to follow



Wi-Fi Security Types: WPA

- Wi-Fi Protected Access (WPA)
- Available from 1999
- Consumer routers didn't really support until 2003 due to expensive hardware required.
- WPA-Personal
  - Also known as WPA-PSK (pre-shared key)
  - Passphrase of 8 to 63 ASCII characters
  - WPA passphrase and SSID - 256-bit pre-shared key (more on this later)

Wi-Fi Security Types: WPA

- Attacks against WPA-PSK are a bruteforce attack against a captured handshake
  - 4-way handshake
  - Initial conversation between client and router
  - 4-way handshake doesn't contain the passphrase itself but has values that can be used to verify the hash
  - More on the WPA algorithm here
- Attack is offline and handshake can be captured as long as your in range of both AP and client.
- Passwords can be generated on the fly using an open source tool like John the Ripper or downloaded from the internet

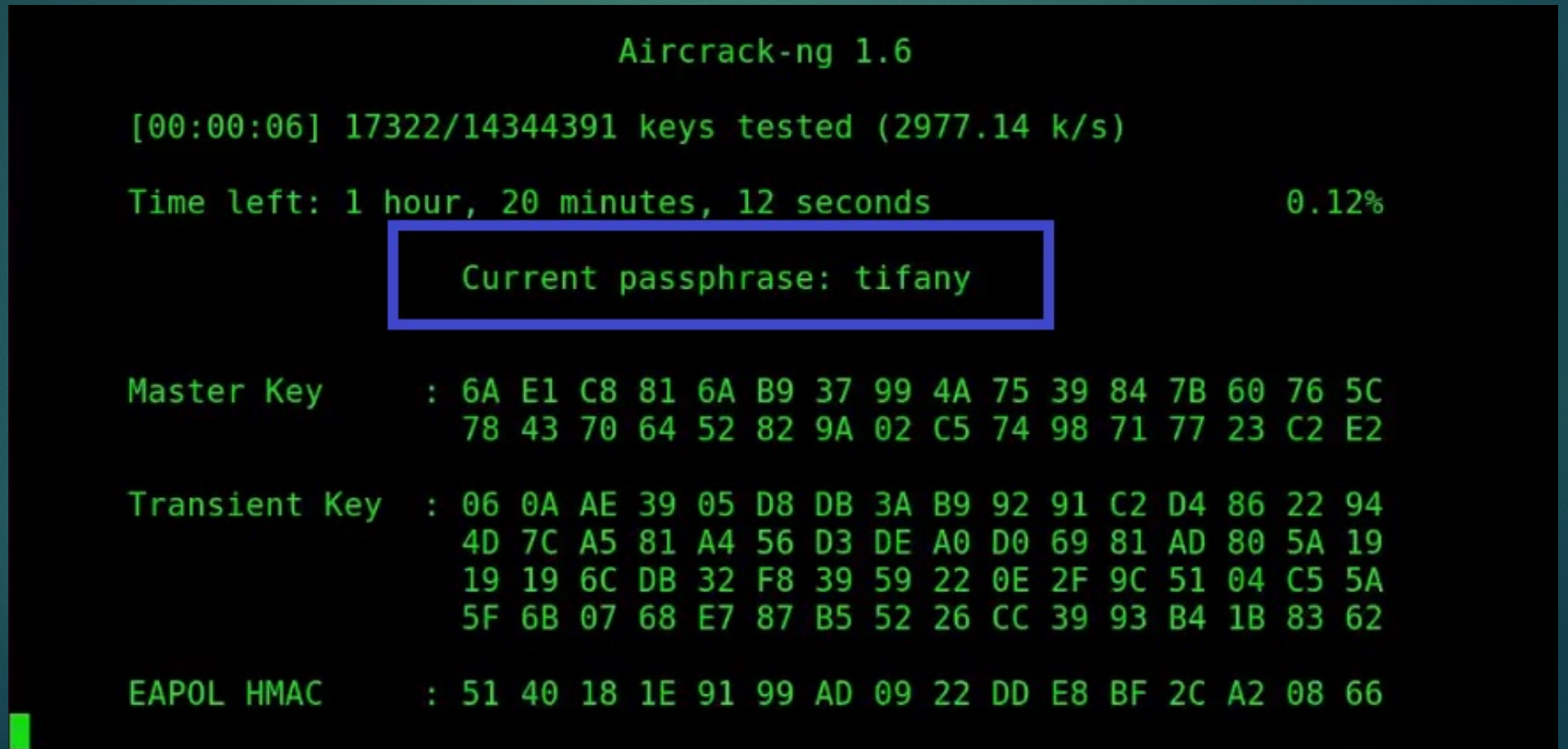
Wi-Fi Security Types: WPA

- Airodump-ng

```
root@kali:~# airodump-ng wlan0


 CH 11 ][ Elapsed: 0 s ][ 2018-11-26 16:29

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 90:CD:B6:83:43:B2  -34        3        0    0   5   65  WPA2 CCMP   PSK  Oppo
 D8:C8:E9:C2:CB:18  -82        2        0    0  10  130  WPA2 CCMP   PSK  perfe
 E4:6F:13:B6:DB:03  -67        3        0    0  10  270  WPA2 CCMP   PSK  Fligh
 F0:D7:AA:E0:4F:E4  -61        6        0    0   3   65  OPN              Ashu
 7A:11:DC:6E:C0:78  -66        7        8    3   3  130  WPA2 CCMP   PSK  LIFCA
 78:11:DC:5E:C0:78  -63        7        0    0   3  130  WPA2 CCMP   PSK  Xiaom
 B8:C1:A2:3B:16:0C  -59        2        4    0  11  130  WPA2 CCMP   PSK  (JTP-
 10:DA:43:72:41:C2  -84        1        1    0  13  54   WPA2 CCMP   PSK  Nextr
 58:D7:59:EC:1F:68  -80        3        0    0   7  130  WPA2 CCMP   PSK  tie d
 0A:28:19:E1:9F:5B  -46        3        0    0   7  130  WPA2 CCMP   PSK  LAPTO
 C0:FF:D4:91:49:DF  -48        1       31   15   7  130  WPA2 CCMP   PSK  NETGE
 0C:D2:B5:49:D5:C4  -66        4        5    2   7   65  WPA  CCMP   PSK  Airte
 50:C8:E5:AF:F6:33  -25        5        0    0   6   65  WPA2 CCMP   PSK  BS1A-
 50:64:2B:CE:B4:F4  -79        0        3    1   1  -1   WPA              <leng
 A8:F5:AC:65:82:7C  -71        1        2    0   1  130  WPA2 CCMP   PSK  Vashi

root@kali:~#
```

Wi-Fi Security Types: WPA

- Airocrack-ng



Wi-Fi Security Types: WPA

- Verifying thousands of passwords against your handshake can be computationally expensive
- Each passphrase is hashed 4096 times with SHA-1 and 256 bits of the output is the resulting hash
- SSID and the SSID length is seeded into the passphrase hash
- It is possible to pre generate hash tables ahead of time
- One issue is the SSID of the WPA network must match that of the target AP
- This might be fine for "Linksys" or "default" or "Netgear"
- Not so for "CorpNet12" or "CompanyNamePrv"

Wi-Fi Security Types: WPA

- A weak password or a known value will help with this
  - A Cafe, Bar or Hotel will usually have it written somewhere for guests
- Some manufactures of routers have default passwords of 8 digits, or the password contains the company name, e.g., ISPNAME-12345
- Generating a password list with known information is trivial
- 8 digit password file containing 00000000 – 99999999 (14MB) can be checked in less than 30 minutes on modern machine
- TP-Link was known to have the WPA password as the last 8 characters of the MAC address

Wi-Fi Security Types: WPA

- WPA uses a Pairwise Master Key (PMK) individual to each client
- Renegotiation at a certain interval (usually 1 hour)
- If you want to decrypt the traffic you must catch the complete 4-way-handshake otherwise packets sniffed after this interval cannot be decrypted
- For example, If you have 6 hours of traffic recorded, and miss the renegotiation after an hour, and can only decrypt the first hour of traffic.

Wi-Fi Security Types: WPS

- Wireless Protected Setup(WPS)
- Allows the user to enter an 8 digit code to receive the password from the router
- Allows AP owner to set a nice, secure password on the router
- Most routers require you to press a button on the AP then WPS is available for a short period of time.
- Flaw was found in 2001 to reduce guessing the pin from 99999999 guesses to about 11,000.
  - A different error was returned if the first half of the 8 digit code was correct.
- Article about the WPS attack: https://arstechnica.com/information-technology/2011/12/researchers-publish-open-source-tool-for-hacking-Wi-Fi-protected-setup/

Wi-Fi Security Types: WPS

- Some routers responded to WPS requests even when the button or feature was not active
- Most routers today will lock up for a few hours after 3 failed attempts
- Some brands don't lock up if you have a delay between attempts.
- Some brands have a default WPS code
- Wash – displays AP that supports WPS and locked status

```
Wash v1.4 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

BSSID                 Channel       RSSI       WPS Version       WPS Locked        ESSID
-------------------------------------------------------------------------------------------
20:AA:4B:[redacted]   6             00         1.0               No                6C956
00:23:69:48:33:95     6             00         1.0               No                linksys
```

Wi-Fi Security Types: WPS

- Reaver

```
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 00005678
```

Wi-Fi Security Types: WPA-Enterprise

- WPA-Enterprise
  - Designed for enterprise networks
  - A lot more complicated to set up and manage
  - Typically a username and password is required.
  - Credentials individual to each user and/or device
  - Digital certificates and RSA tokens can also be utilized to verify authentication
  - Requires a RADIUS server to verify credentials and certificates

Wi-Fi Security Types: WPA-Enterprise

- Attacks against WPA-Enterprise involve setting up a rogue access point, and waiting for a connection.
- Once we have the hashed credentials, it becomes an offline bruteforce attack
- Pinned certificates on the client can protect against this attack
- Cloud instances can be used to aid in password recovery – GPU cracking
- Article on hacking WPA-Enterprise with Kali: https://www.offensive-security.com/penetration-testing/hacking-wpa-enterprise-with-kali-linux/

Other Attack Types: User

- Rogue access point
  - Open – Dublin Bus, Starbucks, Dublin Airport
  - WPA – Known passphrase - Café, Hotel
- Clients remember network name
  - Auto connect
  - Probe for networks in its saved list
- Wi-Fi Pineapple
- Mana – rogue access point toolkit (kali)

https://www.flickr.com/photos/doctorow/35460674813

Other Attack Types: User

- Deauth Attacks
  - Deauth the real AP to the rouge network is available to the client
- Man in the Middle attacks
  - SSL Strip – downgrade attack
  - SSL Split – rogue SSL
  - Some phone apps use HTTP
  - Modify the users packets
- When a client connects:
  - Installed apps will automatically sync

Protect Yourself

- Use a VPN
- Review your saved Wi-Fi networks on your laptop and mobile phone
- Use Mobile Data
- Avoid using public (untrusted) Wi-Fi

Summary

- Wireless is still a network
  - You are still open to network attacks
  - Is Tomcat listening publicly on your laptop?
- Open wireless should never be trusted
- WEP is dead, and shouldn't be used publicly any more
- WPA is great as long as it is secured properly with a password.
- WPA-Enterprise is safer but still susceptible to attack
- Protecting yourself is always the best option