

# Hackerská hračka Pwnagotchi

2426 K programátor obrábacích a zváracích strojov a zariadení

2022

Poprad

**Riešiteľ:** Jakub Heger

**Ročník štúdia:** Tretí

# Hackerská hračka Pwnagotchi

2426 K programátor obrábacích a zvracích strojov a zariadení

2022

Poprad

**Riešitel:** Jakub Heger

**Ročník štúdia:** Tretí

**Konzultant:** Bc. Peter Jurčík

## **Prehlasenie**

Čestne prehlasujem, že som prácu neprihlásil a neprezentoval v žiadnej inej súťaži schválenej MŠVVaŠ SR. Vyhlasujem, že prácu som vypracoval samostatne s použitím uvedenej literatúry a pomocou vlastných vedomostí.

V Poprade \_\_\_\_\_

\_\_\_\_\_  
Jakub Heger

# Obsah

|         |   |    |
|---------|---|----|
|         | Prehlasenie . . . . .                       | 3  |
|         | Obsah . . . . .                             | 4  |
|         | Úvod . . . . .                              | 5  |
| 1.1     | Tereotické Východiska . . . . .             | 6  |
| 1.1.1   | O projekte pwnagotchi . . . . .             | 6  |
| 1.1.2   | Ako to funguje . . . . .                    | 7  |
| 1.1.3   | Režimy provozu . . . . .                    | 8  |
| 1.1.3.1 | Režim MANU . . . . .                        | 8  |
| 1.1.3.2 | Režim AUTO . . . . .                        | 8  |
| 1.1.3.3 | Režim AI . . . . .                          | 8  |
| 1.1.4   | Potrebný hardver a sofver . . . . .         | 9  |
| 1.1.4.1 | Softvér . . . . .                           | 9  |
| 1.1.4.2 | Hlavna doska . . . . .                      | 9  |
| 1.1.4.3 | Displej . . . . .                           | 9  |
| 1.1.4.4 | Bateria . . . . .                           | 9  |
| 1.2     | Montáž zariadenia . . . . .                 | 10 |
| 1.2.1   | Poskladanie . . . . .                       | 10 |
| 1.2.2   | Príprava SD karty . . . . .                 | 10 |
| 1.2.3   | Počiatočná konfiguracia . . . . .           | 11 |
| 1.2.4   | Pripojenie cez SSH . . . . .                | 12 |
| 1.2.5   | Konfiguracia pripojenia bluetooth . . . . . | 13 |
| 1.2.6   | Webové grafické rozhranie . . . . .         | 14 |
| 1.2.7   | Bettercap . . . . .                         | 15 |
| 1.2.8   | Nastavenie ochrany sd karty . . . . .       | 16 |
| 1.2.9   | Pluginy . . . . .                           | 16 |
| 1.3     | Používanie zariadenia . . . . .             | 17 |
| 1.3.1   | Chytanie handshakov . . . . .               | 17 |
| 1.3.2   | Vyhodenie užívateľa zo siete . . . . .      | 18 |
| 1.3.3   | Rozlusknutie hesla . . . . .                | 18 |
|         | Diskusia . . . . .                          | 19 |
|         | Zhrnutie . . . . .                          | 20 |
|         | Resumé . . . . .                            | 21 |
|         | Zoznam použitej literatúry . . . . .        | 22 |

## Úvod

V dnešnej dobe už väčšina ľudí používa Wi-Fi siete, no málokto vie, či sú bezpečne. Môže vás prekvapiť, keď zistíte, ako je ľahké pre utočníka získať Wi-Fi heslo do vašej siete alebo vás "vykopnúť" zo siete.

Rozhodli sme sa demonštrovať bezpečnosť Wi-Fi sieti tak, že zostrojíme malé hackerske zariadenie a pokúsime sa získať heslo od našej súkromnej Wi-Fi siete a "vykopneme" naše zariadenie zo siete.

## 1.1 Tereotické Východiska

### 1.1.1 O projekte pwnagotchi

Pwnagotchi je open-source<sup>1</sup> Wi-Fi hackerská hračka, ktorá je veľmi podobná digitálnej hračke Tamagotchi z deväťdesiatych rokov minulého storočia. Je to zariadenie, ktoré dokáže chytať Wi-Fi heslá a vyhadzovať užívateľov zo siete. Toto zariadenie používa umelú inteligenciu, ktorá sa neustále učí a zlepšuje svoje schopnosti v chytaní Wi-Fi hesiel a vyhadzovaní užívateľov zo siete.

Je to projekt, ktorý vyvíja a vylepšuje široká komunita open-source dobrovoľníkov, do ktorej sa môžete pridať aj vy. Existuje mnoho rozširujúceho softvéru pre tento projekt tzv. pluginy, ktoré pridávajú zábavné funkcie alebo zlepšujú funkčnosť zariadenia.



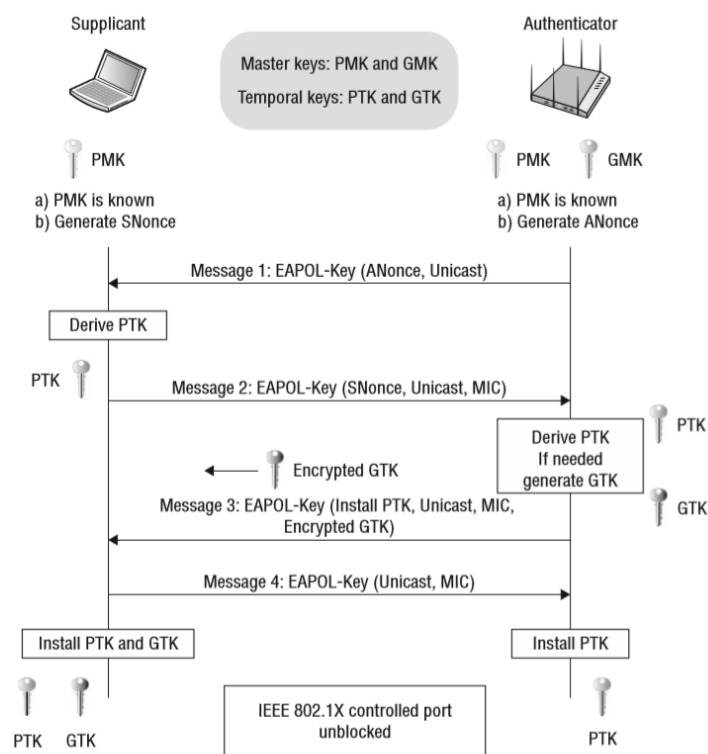
Obr. 1.1: foto Jakub Heger, 2022

---

<sup>1</sup>Softvér s otvoreným zdrojovým kódom

### 1.1.2 Ako to funguje

Wi-Fi Handshaky sú výmeny informácií medzi routrom a užívateľským zariadením. Routre používajú handshaky na overenie užívateľov, ktorí sa chcú pripojiť na sieť. Handshaky obsahujú rôzne kľúče v hashovej forme, ktoré slúžia na overenie Wi-Fi prihlasovacieho hesla zadaneho užívateľom. Každá Wi-Fi sieť uskutočňuje túto funkciu na overenie užívateľov.



Obr. 1.2: foto <https://www.wifi-professionals.com/2019/01/4-way-handshake>, 2022

Pwnagotchi monitoruje Wi-Fi signály a čaká na handshaky. Môže to trvať aj dlhší čas, kým sa niekto bude pripájať na Wi-Fi sieť, tak si Pwnagotchi pomáha vyhadzovaním užívateľov zo sietí. Pwnagotchi sa niekedy náhodne rozhodne "vykopnúť" nejakých užívateľov zo siete, aby sa potom pripojili znovu na sieť a vykonali Wi-Fi handshake. Tento Wi-Fi handshake Pwnagotchi uvidí a uloží si ho do *.pcap* súboru.

Pomocou týchto handshakov vieme rozlusknúť Wi-Fi heslo. Avšak na to budeme potrebovať výkonnejší počítač. Handshake sa musí preniesť do iného počítača na to, aby bol hash hesla rozlusknutý pomocou programu Hashcat alebo Hashkiller. Na rozlusknutie hesla sa používajú metódy ako sú slovníkové útoky, kde sa používajú tzv. heslové slovníky a "bruteforce", kde sa skúša každá možnosť hesla, t. j. písmenko po písmenku.

### 1.1.3 Režimy provozu

Zariadenie Pwnagotchi môže fungovať v troch režimoch.

#### 1.1.3.1 Režim MANU

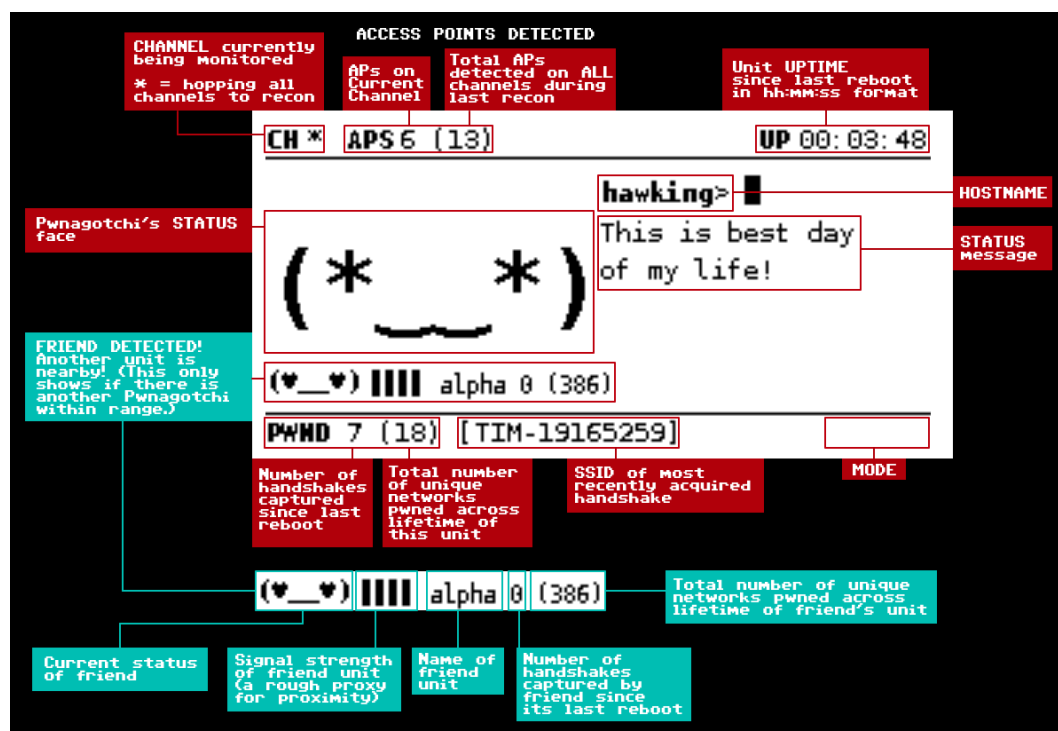
Režim MANU sa zapne pri spustení zariadenia, keď je usb data kábel pripojený do zariadenia. Tento režim je dobrý pre zalohovanie systému, aktualizácie softvéru a používanie webového rozhrania na zmenu nastavenia zariadenia. V tomto režime zariadenie nehľadá Wi-Fi handshaky a nevyhadzuje užívateľov zo siete.

#### 1.1.3.2 Režim AUTO

Režim AUTO je, keď algoritmus zariadenia beží automaticky a AI mod je vypnutý. V tomto režime Pwnagotchi hľadá Wi-Fi handshaky a vyhadzuje ľudí zo siete. Tento režim sa prepne do AI režimu po pätnástich alebo dvadsiatich minútách.

#### 1.1.3.3 Režim AI

Tento režim sa zapne, keď sa všetky moduly umelej inteligencie úspešne načítajú do systému. Tento režim umožňuje zariadeniu trénovať, učiť sa a zlepšovať svoje skúsenosti v chytaní Wi-Fi handshakeov.



Obr. 1.3: foto <https://pwnagotchi.ai/usage/>



#### 1.1.4 Potrebný hardver a softvér

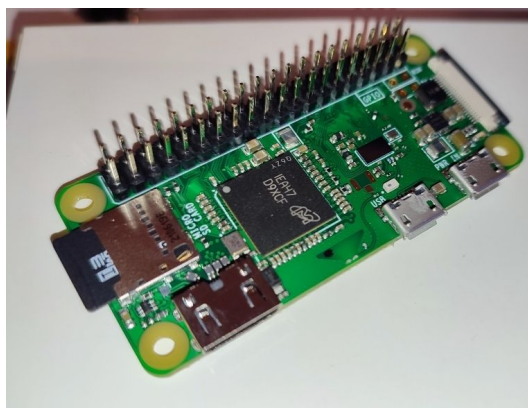
Pre zariadenie Pwnagotchi budeme potrebovať zopár súčiastok a nejaký softvér. Všetky súčiastky okrem jednodoskového počítača Raspberry Pi Zero W sú nepovinné.

##### 1.1.4.1 Softvér

Pre inštaláciu softvérového vybavenia zariadenia sme potrebovali operačný systém v skupine Linux pre náš počítač a .iso obrazec modifikovaného operačného systému Raspbian pre samotné zariadenie.

##### 1.1.4.2 Hlavná doska

Ako hlavnú dosku, ktorá ovláda všetko v zariadení sme použili jednodoskový počítač Raspberry Pi Zero W.



Obr. 1.4: foto Jakub Heger, 2022

##### 1.1.4.3 Displej

Ako displej sme použili e-ink displej Waveshare V2. Je to displej, ktorý by ste mohli nájsť v čítačkách elektronických kníh. Používame tento displej, pretože spotrebuje málo energie.

##### 1.1.4.4 Bateria

Nechceli sme, aby náš Pwnagotchi bol stále pripojený na napájací kábel, tak sme si pripravili Waveshare UPS Lite modul s batériou pre Raspberry Pi Zero W.

## 1.2 Montáž zariadenia

### 1.2.1 Poskladanie

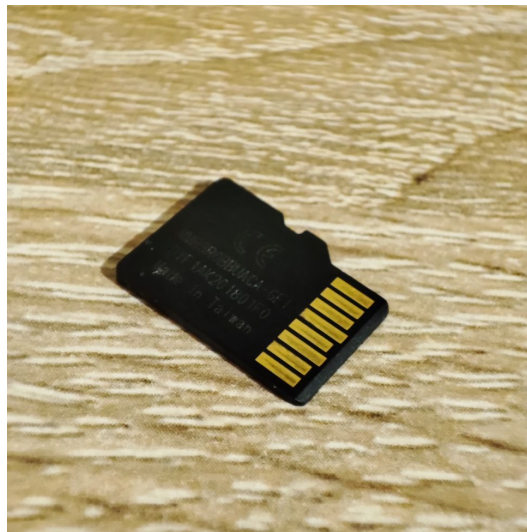
Na poskladanie zariadenia Pwnagotchi je potrebný len jednoduchý krížový skrutkovač a kovové stojančeky. Najprv sme spojili batériu s hlavnou počítačovou doskou Raspberry Pi Zero W pomocou kovových stojančekov a nakoniec sme pripojili e-ink displej jednoduchým potlačením.

### 1.2.2 Príprava SD karty

Na to, aby sme mohli začať konfigurovať zariadenie Pwnagotchi, sme museli pripraviť mikro sd kartu. Museli sme ju kompletne resetovať. Pomocou programu `gdisk` sme vymazali všetky zväzky na sd karte a formatovali sme ju na súborový systém *ext4*.

Na našom počítači sme z Githubu projektu Pwnagotchi stiahli archivový zip súbor, v ktorom sa nachádzal iso obrazec pripraveného softvérového vybavenia. Po extrahovaní súboru sme sa presunuli do terminálu a pomocou príkazu `dd` sme na sd kartu flashli potrebné softverové vybavenie.

```
1 $ dd if=path/to/pwnagotchi-raspbian-lite-1.5.5.img of=/dev/sdc bs=1M
```



Obr. 1.5: foto Jakub Heger, 2022

### 1.2.3 Počiatočná konfigurácia

Pred tým, ako sme spustili zariadenie Pwnagotchi, sme vytvorili konfiguračný súbor *config.toml* a uložili sme ho do *boot* zväzku mikro sd karty. Po uložení súboru sme pripojili mikro sd kartu do Raspberry Pi Zero W a zapli zariadenie.

```
1  main.name = "pwnagotchi"
2  main.lang = "en"
3  main.whitelist = [ "Heger" ]
4
5  main.plugins.grid.enabled = true
6  main.plugins.grid.report = true
7  main.plugins.grid.exclude = [ "Heger" ]
8
9  ui.display.enabled = true
10 ui.display.type = "waveshare_2"
11 ui.display.color = "black"
12
13 ui.web.username = "pwnagotchi"
14 ui.web.password = "ukazkove_heslo"
```

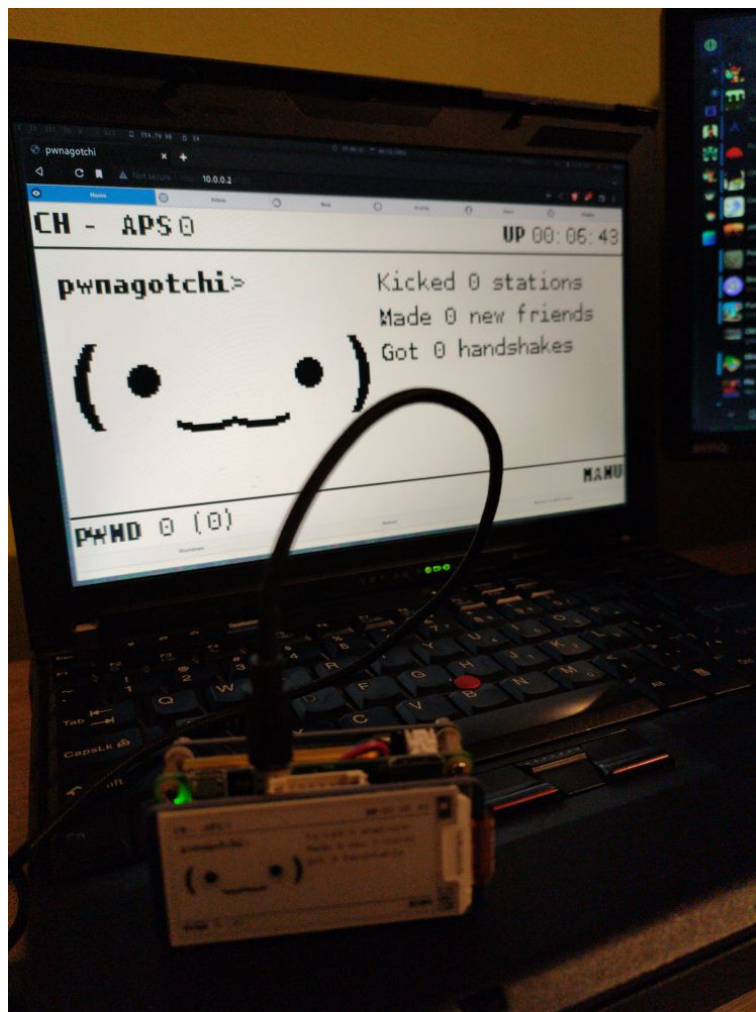
### 1.2.4 Pripojenie cez SSH

Aby sme sa mohli pripojiť na zariadenia Pwnagotchi, museli sme pripojiť usb kábel do data portu. Po zapojení sme počkali, kým sa zariadenie kompletne zapne a s naším počítačom sme našli označenie sieťového adaptéru pomocou príkazu *ip addr*. Po zistení označenia sme zapli pripojenie na zariadenie pomocou príkazu *ifconfig*.

```
1 $ ifconfig enp0s29f7u1 inet 10.0.0.1 netmask 255.255.255.0 up
```

A potom sme sa do zariadenia pripojili pomocou príkazu *ssh*.

```
1 $ ssh pi@10.0.0.2
```



Obr. 1.6: foto Jakub Heger, 2022

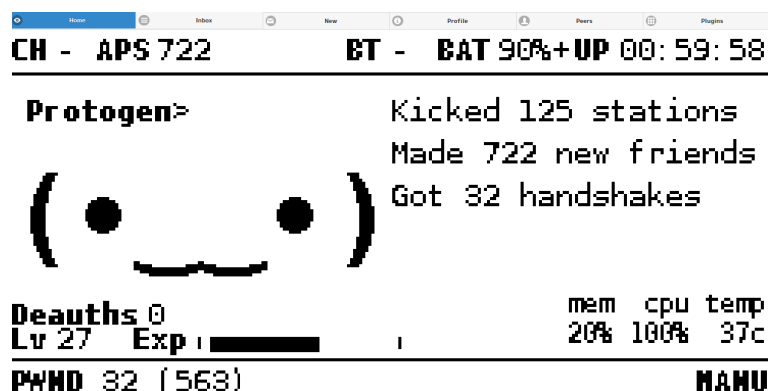
### 1.2.5 Konfiguracia pripojenia bluetooth

Na to, aby sa náš telefón pripájal na zariadenie Pwnagotchi sme museli zariadenie spárovať a zadať *MAC* adresu bluetooth adaptéru nášho telefónu do konfiguračného súboru. Najprv sme spustili terminálový program *bluetoothctl* a spustili sme napájanie bluetooth adaptéru. Potom sme zapli skenovanie okolitých bluetooth zariadení a našli sme medzi nimi náš telefón. Pomocou jeho *MAC* adresy sme telefón a zariadenie spárovali a následne sme sa pripojili na Pwnagotchi cez náš telefón.

Po dokončení predchádzajúcich krokov sme sa mohli pripojiť na webové grafické rozhranie zariadenia na adrese *http://192.168.44.44:8080*.

### 1.2.6 Webové grafické rozhranie

Pre jednoduchšie a rýchlejšie používanie zariadenia počas presúvania sa z miesta na miesto, sme sa pripoji na webové rozhranie na našom notebooku.



Obr. 1.7: foto Jakub Heger, 2022

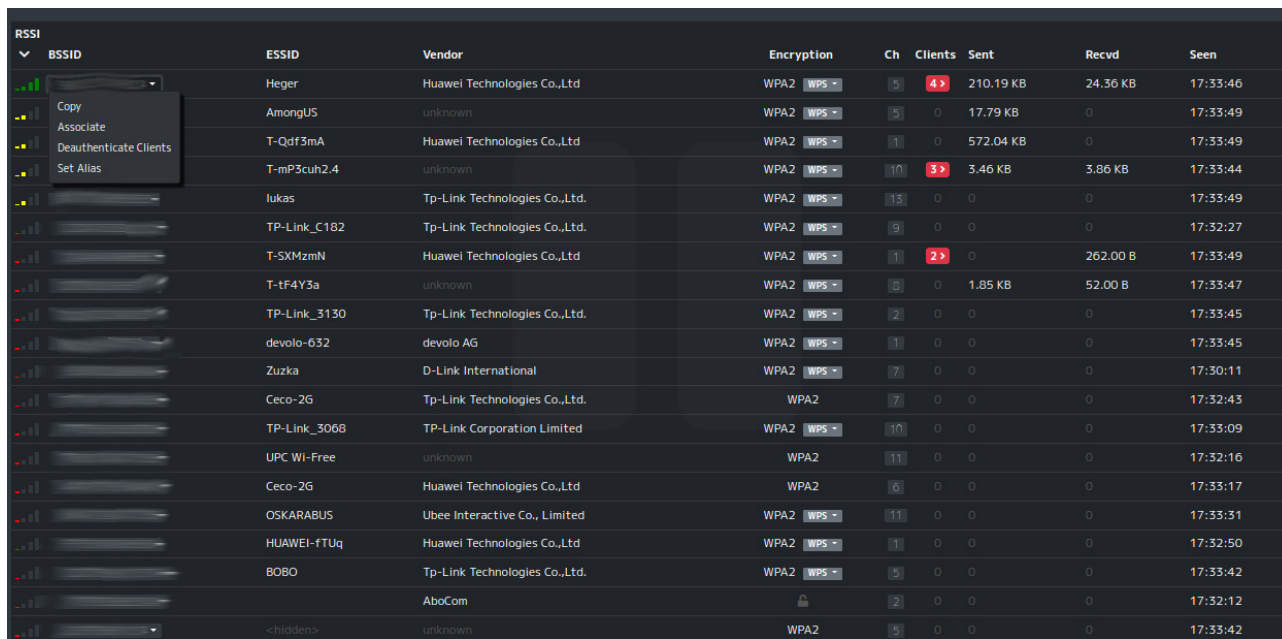
Toto webové grafické rozhranie je super funkcia tohto zariadenia, pretože máte rýchly a jednoduchý prehľad o fungovaní zariadenia. Mohli sme si tam zapnúť a vypnúť pluginy a meniť nastavenia zariadenia



Obr. 1.8: foto Jakub Heger, 2022

## 1.2.7 Bettercap

Pre lepšie ovládanie zariadenia sme sa pripojili do Bettercap webového rozhrania, je to sieťový nástroj na odchyt handshake a vyhadzovanie užívateľov zo sietí. V tomto rozhraní sme mali najlepší prehľad o okolitých Wi-Fi sieťach. Na to, aby sme sa pripojili na toto rozhranie sme museli prepnúť Pwnagotchi do režimu MANU.



| RSSI | BSSID | ESSID        | Vendor                        | Encryption | Ch | Clients | Sent      | Recvd    | Seen     |
|------|-------|--------------|-------------------------------|------------|----|---------|-----------|----------|----------|
| ...  | ...   | Heger        | Huawei Technologies Co.,Ltd   | WPA2 WPS   | 5  | 4       | 210.19 KB | 24.36 KB | 17:33:46 |
| ...  | ...   | AmongUS      | unknown                       | WPA2 WPS   | 5  | 0       | 17.79 KB  | 0        | 17:33:49 |
| ...  | ...   | T-Qdf3mA     | Huawei Technologies Co.,Ltd   | WPA2 WPS   | 1  | 0       | 572.04 KB | 0        | 17:33:49 |
| ...  | ...   | T-mP3cuh2.4  | unknown                       | WPA2 WPS   | 10 | 3       | 3.46 KB   | 3.86 KB  | 17:33:44 |
| ...  | ...   | lukas        | Tp-Link Technologies Co.,Ltd. | WPA2 WPS   | 13 | 0       | 0         | 0        | 17:33:49 |
| ...  | ...   | TP-Link_C182 | Tp-Link Technologies Co.,Ltd. | WPA2 WPS   | 9  | 0       | 0         | 0        | 17:32:27 |
| ...  | ...   | T-SXMzmN     | Huawei Technologies Co.,Ltd   | WPA2 WPS   | 1  | 2       | 0         | 262.00 B | 17:33:49 |
| ...  | ...   | T-tf4Y3a     | unknown                       | WPA2 WPS   | 5  | 0       | 1.85 KB   | 52.00 B  | 17:33:47 |
| ...  | ...   | TP-Link_3130 | Tp-Link Technologies Co.,Ltd. | WPA2 WPS   | 2  | 0       | 0         | 0        | 17:33:45 |
| ...  | ...   | devolo-632   | devolo AG                     | WPA2 WPS   | 1  | 0       | 0         | 0        | 17:33:45 |
| ...  | ...   | Zuzka        | D-Link International          | WPA2 WPS   | 7  | 0       | 0         | 0        | 17:30:11 |
| ...  | ...   | Ceco-2G      | Tp-Link Technologies Co.,Ltd. | WPA2 WPS   | 7  | 0       | 0         | 0        | 17:32:43 |
| ...  | ...   | TP-Link_3068 | TP-Link Corporation Limited   | WPA2 WPS   | 10 | 0       | 0         | 0        | 17:33:09 |
| ...  | ...   | UPC Wi-Free  | unknown                       | WPA2 WPS   | 11 | 0       | 0         | 0        | 17:32:16 |
| ...  | ...   | Ceco-2G      | Huawei Technologies Co.,Ltd   | WPA2 WPS   | 6  | 0       | 0         | 0        | 17:33:17 |
| ...  | ...   | OSKARABUS    | Ubee Interactive Co., Limited | WPA2 WPS   | 11 | 0       | 0         | 0        | 17:33:31 |
| ...  | ...   | HUAWEI-FTUq  | Huawei Technologies Co.,Ltd   | WPA2 WPS   | 1  | 0       | 0         | 0        | 17:32:50 |
| ...  | ...   | BOBO         | Tp-Link Technologies Co.,Ltd. | WPA2 WPS   | 5  | 0       | 0         | 0        | 17:33:42 |
| ...  | ...   | AboCom       | AboCom                        | WPA2 WPS   | 2  | 0       | 0         | 0        | 17:32:12 |
| ...  | ...   | <hidden>     | unknown                       | WPA2 WPS   | 5  | 0       | 0         | 0        | 17:33:42 |

Obr. 1.9: foto Jakub Heger, 2022

### 1.2.8 Nastavenie ochrany sd karty

Na to, aby sme trošku predĺžili životnosť sd karty sme do konfiguračného súboru *config.toml* pridali tento kód:

```
1 fs.memory.enabled = true
2 fs.memory.mounts.log.enabled = true
3 fs.memory.mounts.data.enabled = true
4
5 fs.memory.mounts.log.enabled = true      # switch
6 fs.memory.mounts.log.mount = "/var/log"  # which directory to map into memory
7 fs.memory.mounts.log.size = "50M"       # max size to put into memory
8 fs.memory.mounts.log.sync = 60           # interval in seconds to sync back onto disk
9 fs.memory.mounts.log.zram = true          # use zram for compression (recommended)
10 fs.memory.mounts.log.rsync = true        # use rsync to copy only the difference (
      recommended)
```

### 1.2.9 Pluginy

Projekt Pwnagotchi má mnoho rozširujúcich modulov tzv. pluginov. Niektoré z týchto pluginov nám môžu priniesť mnoho zábavy a ostatné nám prinášajú viac funkcií a pomáhajú nám s lovom Wi-Fi handshakeov. Rozhodli sme sa nainštalovať niektoré z pluginov ako napríklad status skúseností, automatické odstraňovanie nerozluskateľných handshakeov, atď..

Najprv sme museli pridať riadok s odkazom na priečinok, kde sú naše pluginy uložené a samotné pluginy sme presunuli do priečinku, ktorý sme zapísali do konfiguračného súboru. Po dokončení týchto akcií sme ich zapli pomocou terminálového príkazu a reštartovali sme zariadenie.

```
1 + main.custom_plugins = "/usr/local/pwnagotchi/plugins/custom"
```



## 1.3 Používanie zariadenia

Samotne používanie zariadenia je jednoduché, stačí ho zapnúť a čakať. Pwnagotchi spraví všetku prácu za vás. Chceli sme mať lepší prehľad o statuse zariadenia, hoci je uložené niekde v batohu. Pwnagotchi sme pripojili z nášho mobilného telefónu cez bluetooth a pozorovali sme priebeh chytania Wi-Fi handshakov a status zariadenia.

### 1.3.1 Chytanie handshakov

Zariadenie sme si zobrali na takú prechádzku cez poľské mesto Krakow, aby sme si otestovali funkčnosť zariadenia. Zariadenie sme zapli v centre mesta a pozorovali sme priebeh chytania Wi-Fi handshakov, keďže sa tam nachádzalo mnoho Wi-Fi sietí, tak sme asi po pol hodine chytili tridsaťosem handshakov. Po odchode z Krakowa sme všetky chytené handshaky zo zariadenia vymazali.

### 1.3.2 Vyhodenie užívateľa zo siete

Vytvorili sme Wi-Fi hotspot a pripojili sme sa s piatimi mobilnými telefonmi. Zapli sme zariadenie Pwnagotchi a čakali sme. Po pätnástich minútach sa zariadenie preplo do režimu umelej inteligencie. V priebehu pol hodiny Pwnagotchi "vykoplo" zo Wi-Fi siete všetky mobilné telefóny asi tak trinásťkrát. Zariadenie nevyhadzoval užívateľov zo siete veľa krát pretože je to tak nastavené hlboko v kóde, Pwnagotchi má byť len hackerska hračka, nie funkčne a praktické zariadenie na útoky.

### 1.3.3 Rozlusknutie hesla

Po chytení handshaku medzi naším routerom a mobilným telefonom sme presunuli *.pcap* súboru na náš počítač a konvertovali sme *.pcap* súbor na *.hccapx* format. Potom sme si pripravili heslové slovníky, ktoré obsahujú najčastejšie heslá a kombinácie slov a spustili sme crackovanie hesla. Po piatich a pol hodinách sme rozluskli heslo našej Wi-Fi siete.

Každé heslo je iné, niektoré sú silné, ale ostatné sú slábe. Dĺžka času na rozlusknutie Wi-Fi hesla závisí od sily hesla.

A screenshot of a terminal window with a dark background. The window title bar shows the time 6:57, date 15/12/2022, and window controls. The terminal text shows a user at a root prompt on a machine named Protogen, in the directory ~/handshakes. The user enters the command 'ls | grep Heger'. The output lists four files: 'Heger\_9ce374f98cc4.net-pos.json', 'Heger\_9ce374f98cc4.pcap', and 'Heger\_9ce374f98cc4.pcap.cracked'. The prompt returns after the command is executed.

```
root@Protogen:~/handshakes# ls | grep Heger
Heger_9ce374f98cc4.net-pos.json
Heger_9ce374f98cc4.pcap
Heger_9ce374f98cc4.pcap.cracked
root@Protogen:~/handshakes#
```

Obr. 1.10: foto Jakub Heger, 2022

## Diskusia

Počas skúšania zariadenia Pwnagotchi sme sa dozvedeli, aké je jednoduché pre útočníka narušať vaše pripojenie na sieť a získať Wi-Fi heslo od vašej siete. Heslá od siete sú veľmi časté a je vidieť, že prevádzkovatelia sietí nedbajú na silné heslá.

Tento problém by sme vyriešili používaním silnejších hesiel pre Wi-Fi siete a menili by sme ich aspoň raz za šesť mesiacov pre zvýšenú bezpečnosť Wi-Fi siete.

## Zhrnutie

Sučiasťky nášho zariadenia sme zmontovali a pomocou nášho linuxového počítača sme si pripravili softvérové vybavenie na mikro sd kartu, následne sme vytvorili, upravili a presunuli konfiguračný súbor do *boot* zväzku sd karty. Zariadenie sme zapli a čakali sme, kým sa plne zapne. Potom sme zistili adresu sieťového adaptéru zariadenia pomocou príkazu *ip addr*. Vytvorili sme pripojenie a na zariadenie sme pripojili cez USB kábel pomocou protokolu SSH. Pripojili sme na grafické webové rozhranie zariadenia a v konfiguračnom súbore sme zmenili pár nastavení na ochranu sd karty. Následne sme sa pripojili na zariadenie cez bluetooth, aby sme sa mohli potom pripájať na zariadenie cez mobilný telefón. Pridali sme pár pluginov a zapli sme ich. Nakoniec sme zariadenie otestovali, úspešne sme chytili Wi-Fi handshaky, vyhodili užívateľov zo siete a rozluskli heslo od siete.

## Resumé

We have assembled all the parts together and using our linux computer we have prepared the software on our micro sd card, then we have created, edited and moved the configuration file into the boot partition of the sd card. We switched on the device and waited till it booted up into the system and loaded all the components. Later we have connected our computer to the device with an USB cable and found the private ip address of the device's network adapter using command *ip addr*. We created an connection between the device and computer and then we connected directly into the device using the protocol SSH. Then we have connected to the web interface of the device and in changed few things in the configuration file to protect the sd card from too much data writing. Then we have connected the device to our phones using bluetooth so we can connect to the device on the go via and check the device status with ease. We have added and turned on few plugins. And finally, we have successfully tested the device, we have chatched few Wi-Fi handshakes, kicked few users out of the network and cracked a password of our Wi-Fi access point.

## Zoznam použitej literatúry

- <https://www.waffelo.net/blog/the-cutest-hacking-toy.html> (2022-12-6)
- <https://pwnagotchi.ai/>
- <https://www.wifi-professionals.com/2019/01/4-way-handshake> (2019-01-24)