

Proxmox3

PAWEŁ SZEWCZAK

Plan prezentacji

- ▶ Czym jest Proxmark3
- ▶ Konfiguracja Proxmark3 na Windows10
- ▶ Praktyczne zastosowanie Proxmark3
- ▶ Mifare – „łamanie” - dostępne metody
- ▶ Możliwości urządzenia – przegląd sieci



Czym jest
Proxmox3?

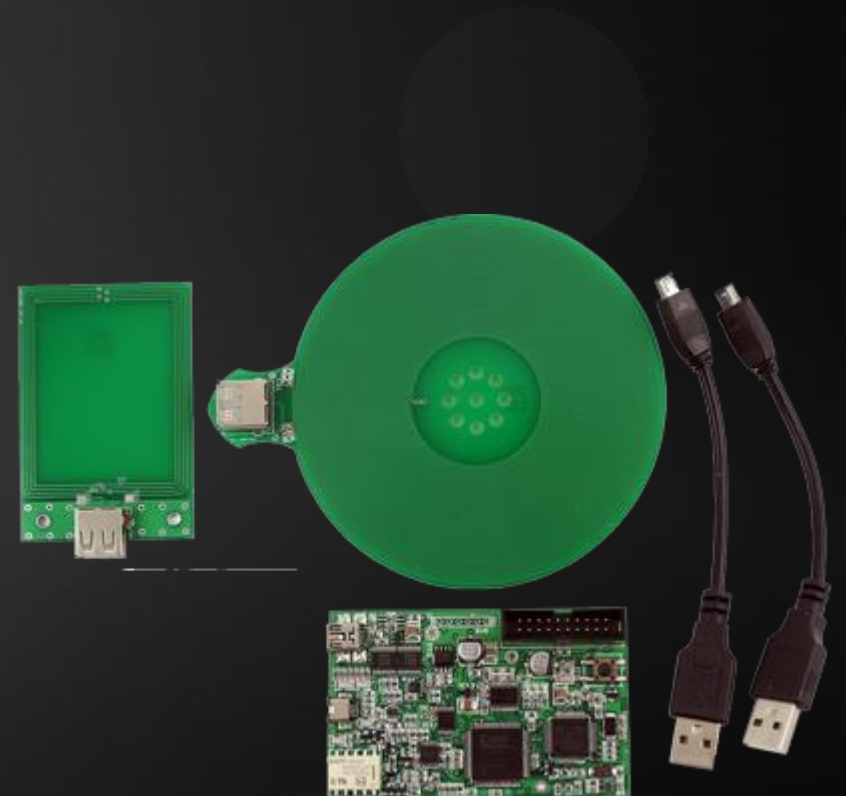
Czym jest Proxmark3?

- ▶ Proxmark3 jest czytnikiem RFID ogólnego przeznaczenia, który potrafi odczytać niemal każdy rodzaj znacznika RFID
- ▶ Oryginalnie stworzony/zbudowany przez Jonathana Westhuesa
- ▶ Możliwości:
 - ✓ Odczytanie tagów niskiej częstotliwości (125 kHz),
 - ✓ Odczytanie tagów wysokiej częstotliwości (13,56 MHz),
 - ✓ Dodatkowo: możliwość analizy sygnałów odbieranych,
 - ✓ Możliwość udawania, że sam jest tagiem.

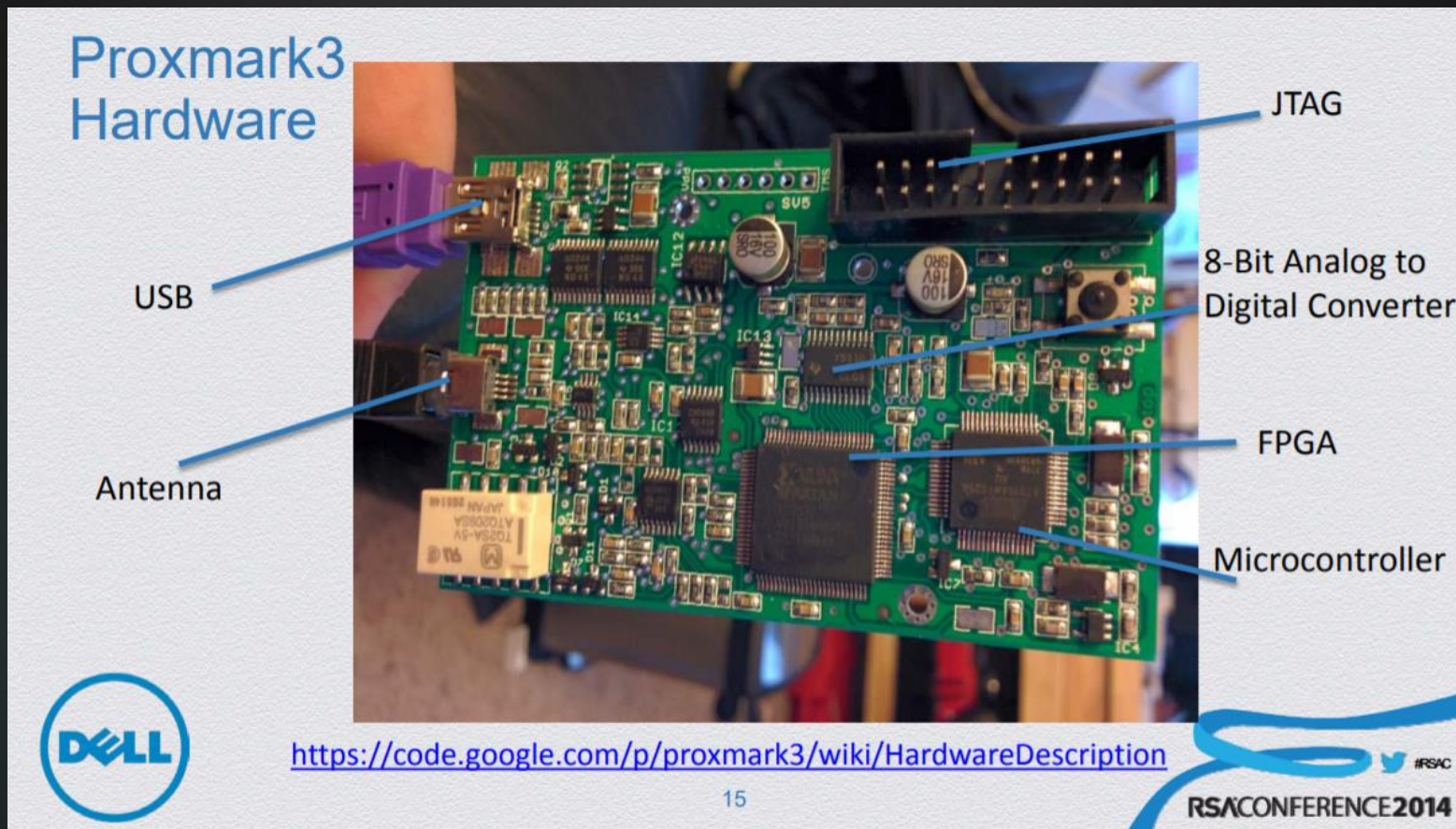
Czym jest Proxmark3?

Technical Specifications

- ▶ **CPU** Variants of AT91SAM7S512
- ▶ **Storage** 512Kb SPI flash
- ▶ **HF tags:** Mifare Ultralight, Mifare 1K, Mifare 4K, Mifare Desfire 4K and HID iClass 2000.
- ▶ **LF Tags:** HID 1326, EM4100, T5577.
- ▶ **Interface** Typically, 1x mode LEDs, 1x button.
- ▶ **Antennas**
 - ▶ **LF** Untuned, external
 - ▶ **HF** Untuned, external



Czym jest Proxmark3?

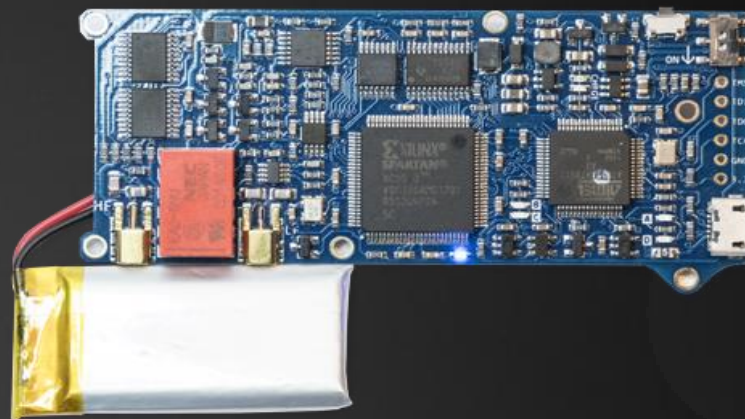


https://www.rsaconference.com/writable/presentations/file_upload/br-r04a-fun-with-proxmark3.pdf

Inne rodzaje Proxmark

► Proxmark 3 RDV 2

- Firma: Elechouse
- Cena: 200\$
- Ulepszony układ FPGA i pamięć flash



► Proxmark 3 Easy

- Firma: Elechouse
- Prostszy nie potrafiący wielu ataków
- Nowe kompaktowe, dostrojone anteny HF i LF



Inne rodzaje Proxmarka

► Proxmark 3 RDV4

- Firma: RRG
- Cena: 90\$
- Kompatybilny z Androidem
- Możliwość rozbudowy (WiFi)



► Proxmark 3 EVO

- Cena: 270\$
- Zminiaturyzowany poprzednik
- Wbudowane anteny



Konfiguracja w Windows 10

- ▶ Konfiguracja jest nieintuicyjna i wymaga wspierania się wiedzą z Internetu
- ▶ Windows10 sam wykrywa nowy sprzęt i sam instaluje odpowiedni sterownik (starsze wersje systemu wymagają ręcznej instalacji)
- ▶ Moja konfiguracja dostępna w osobnym PDF

Pierwsze uruchomienie

- Uruchomienie środowiska - Sprawdzenie wersji proxmark3

Komenda „**hw version**”

```
proxmark3> hw version
[[[ Cached information ]]]

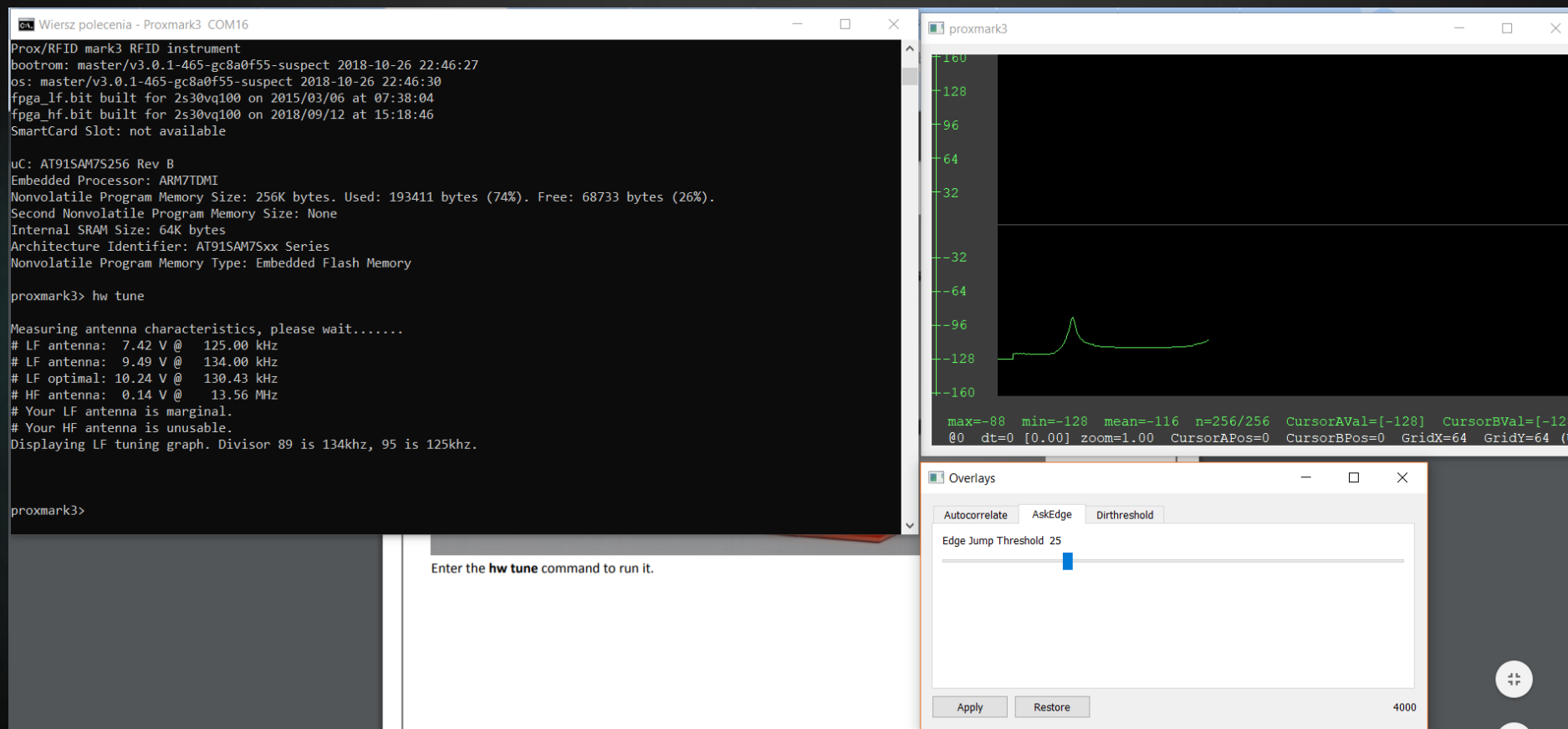
Prox/RFID mark3 RFID instrument
bootrom: master/v3.0.1-465-gc8a0f55-suspect 2018-10-26 22:46:27
os: master/v3.0.1-465-gc8a0f55-suspect 2018-10-26 22:46:30
fpga_lf.bit built for 2s30vq100 on 2015/03/06 at 07:38:04
fpga_hf.bit built for 2s30vq100 on 2018/09/12 at 15:18:46
SmartCard Slot: not available

uC: AT91SAM7S256 Rev B
Embedded Processor: ARM7TDMI
Nonvolatile Program Memory Size: 256K bytes. Used: 193411 bytes (74%). Free: 68733 bytes (26%).
Second Nonvolatile Program Memory Size: None
Internal SRAM Size: 64K bytes
Architecture Identifier: AT91SAM7Sxx Series
Nonvolatile Program Memory Type: Embedded Flash Memory
```

Testowanie anteny

- Testowanie anteny LF - Sprawdzenie wersji proxmark3

Komenda „*hw tune*”



Testowanie anteny HF

- ▶ Testowanie anteny HF - Sprawdzenie wersji proxmark3

Komenda „**hw tune**”

```
proxmark3> hw tune

Measuring antenna characteristics, please wait.....
# LF antenna:  0.00 V @   125.00 kHz
# LF antenna:  0.00 V @   134.00 kHz
# LF optimal:  0.00 V @ 12000.00 kHz
# HF antenna: 17.05 V @   13.56 MHz
# Your LF antenna is unusable.
proxmark3>
```

Komendy podstawowe HF

► Komenda „*hf search*”

```
proxmark3> hf search
```

```
UID : 9b ab fd 5c
ATQA : 00 04
SAK : 08 [2]
TYPE : NXP MIFARE CLASSIC 1k | Plus 2k SL1
proprietary non iso14443-4 card found, RATS not supported
#db# halt error. response len: 1
Answers to chinese magic backdoor commands: YES

Valid ISO14443A Tag Found - Quitting Search
```

```
proxmark3> hf search
```

```
UID : f5 98 71 14
ATQA : 00 04
SAK : 01 [2]
TYPE : NXP TNP3xxx Activision Game Appliance
SAK incorrectly claims that card doesn't support RATS
ATS : 13 78 80 72 02 80 31 80 66 b1 84 0c 01 6e 01 83 00 90 00 11 d8
- TL : length is 19 bytes
- T0 : TA1 is present, TB1 is present, TC1 is present, FSCI is 8 (FSC = 256)
- TA1 : different divisors are NOT supported, DR: [], DS: []
- TB1 : SFGI = 2 (SFGT = 16384/fc), FWI = 7 (FWT = 524288/fc)
- TC1 : NAD is NOT supported, CID is supported
- HB : 80 31 80 66 b1 84 0c 01 6e 01 83 00 90 00
Answers to chinese magic backdoor commands: NO
```

Komendy podstawowe HF

- Zmiana UID na inny
Komenda: „**hf mf csetuid ID**”

```
proxmark3> hf 14a read
UID : 77 77 77 77
ATQA : 00 04
SAK : 08 [2]
TYPE : NXP MIFARE CLASSIC 1k | Plus 2k SL1
proprietary non iso14443-4 card found, RATS not supported
Answers to chinese magic backdoor commands: YES
proxmark3> hf mf csetuid 1eae5ae6
--wipe card:NO uid:1e ae 5a e6
old block 0: 77 77 77 77 00 88 04 00 00 00 00 00 00 00 00
new block 0: 1e ae 5a e6 0c 88 04 00 00 00 00 00 00 00 00
old UID:77 77 77 77
new UID:1e ae 5a e6
proxmark3> hf 14a read
UID : 1e ae 5a e6
ATQA : 00 04
SAK : 08 [2]
TYPE : NXP MIFARE CLASSIC 1k | Plus 2k SL1
proprietary non iso14443-4 card found, RATS not supported
Answers to chinese magic backdoor commands: YES
proxmark3>
```


Komendy podstawowe LF

Symulacja dowolnego taga

- ▶ Wyszukiwanie taga
- ▶ Komenda „**lf search**”

```
proxmark3> lf search
Reading 30000 bytes from device memory

Data fetched
WARNING: Command buffer about to overwrite command! This needs to be fixed!
Samples @ 8 bits/smpl, decimation 1:1
NOTE: some demods output possible binary
      if it finds something that looks like a tag
False Positives ARE possible

Checking for known tags:

HID Prox TAG ID: 2004e2068a (837) - Format Len: 26bit - FC: 113 - Card: 837

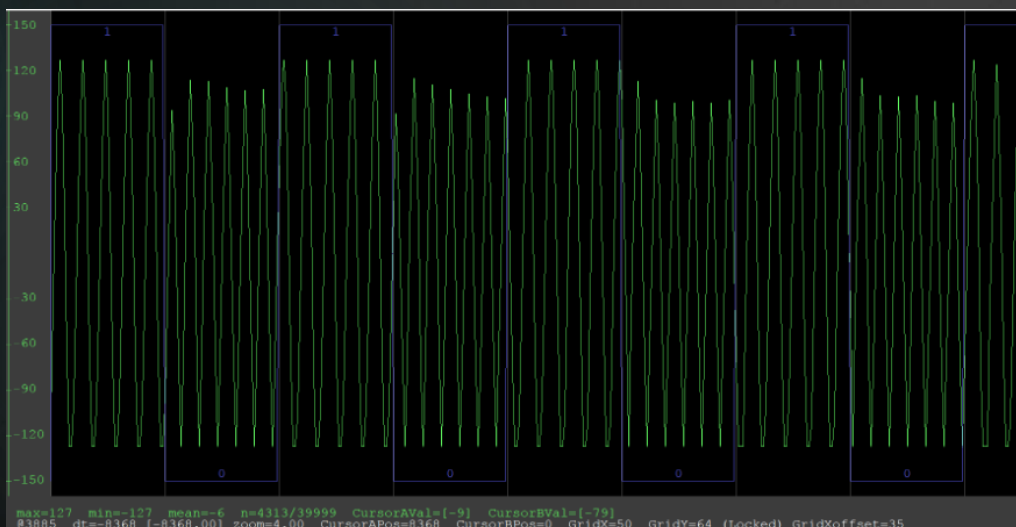
Valid HID Prox ID Found!
```

```
proxmark3> lf hid sim 284ed0ffb
Emulating tag with ID 2      84ed0ffb
Press pm3-button to abort simulation
```

- ▶ Symulacja dowolnego taga
- ▶ Polecenie **lf hid sum ID**

Komendy podstawowe LF

- ▶ Odczytywanie sygnału oraz rysowanie jego przebiegu
- ▶ Komenda „**lf read**” oraz „**data plot**”



```
proxmark3> lf read
#db# LF Sampling config:
#db# [q] divisor:      95
#db# [b] bps:          8
#db# [d] decimation:    1
#db# [a] averaging:     1
#db# [t] trigger threshold: 0
#db# Done, saved 40000 out of 40000 seen samples at 8 bits/sample
#db# buffer samples: 73 73 74 73 73 74 73 73 ...
Reading 39999 bytes from device memory

Data fetched
Samples @ 8 bits/smpl, decimation 1:1
proxmark3> data plot
proxmark3> data samples 20000
Reading 20000 bytes from device memory

Data fetched
Samples @ 8 bits/smpl, decimation 1:1
proxmark3> data plot
```

Mifare

- ▶ **MIFARE** – bezdotykowy standard karty opracowany przez firmę Philips w roku 2006
- ▶ **2 mld** kart MiFare Classic na całym świecie
- ▶ Najważniejszą wadą kart RFID zgodnych ze standardem MiFare Classic jest słabe zabezpieczenie kryptograficzne transakcji

Mifare - łamanie kart

- ▶ W marcu 2008 r. Grupa badawcza Digital Security [27] z Uniwersytetu Radboud w Nijmegen ogłosiła, że przeprowadziła całkowitą inżynierię odwrotną i była w stanie klonować i manipulować zawartością chip-chipu OV, który wykorzystuje chip MIFARE Classic - Do demonstracji wykorzystano **urządzenie Proxmark**
- ▶ Wystarczy czytnik NFC w połączeniu z biblioteką libnfc.
- ▶ Szyfrowanie MIFARE Classic Crypto-1 może zostać przerwane w około 200 sekund na laptopie
- ▶ Proxmark3, powinny być w stanie sklonować dowolną kartę MIFARE Classic w nie więcej niż **10 sekund**.

Mifare - łamanie kart

- ▶ **MIFARE DESFire attacks**

- ▶ Schematy łamania w artykułach oraz na stronie GitHub
- ▶ Rok 2010

- ▶ **MIFARE Ultralight attack**

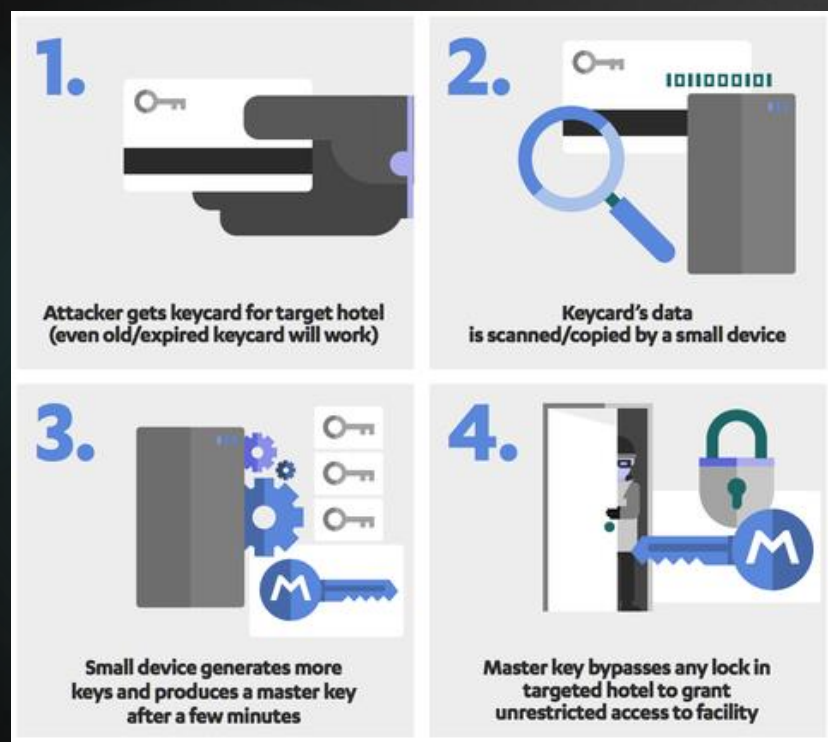
- ▶ Aplikacja na Androida, umożliwiając podróżnym zresetowanie salda karty i podróżowanie za darmo.
- ▶ Atak nie na układ scalony, ładowanie rejestru
- ▶ Wykład: „NFC For Free Rides and Rooms (on your phone)„
- ▶ Rok 2012

- ▶ **Nested attack**

- ▶ **Darkside attack**

Możliwości urządzenia – przegląd sieci

- ▶ Włamanie Szwedzkiej firmy F-Secure do hotelowych pokoi oraz wind



Możliwości urządzenia – przegląd sieci

- ▶ Włamania Mifare (poprzednie slajdy)
- ▶ Klonowanie kart różnego rodzaju
- ▶ Włamania za pomocą kart do budynków
- ▶ Odczytywanie danych z karty kredytowej
- ▶ Płacenie kartami ?

Przyszłość proxmark

- ▶ Bezprzewodowe urządzenie mające wszystkie możliwości proxmarka
 - ▶ *Bezprzewodowa*
 - ▶ *Bateria*
 - ▶ *Możliwości proxmark3*
 - ▶ *Czerwiec 2019*
 - ▶ *Menu ze wszystkimi opcjami*

**Cloning a Tag with
ProxmarkPro**

Dziękuję za uwagę