

Smartkarty a NFC

Workshop

Ondrej Mikle • ondrej.mikle@nic.cz • 30.11.2013

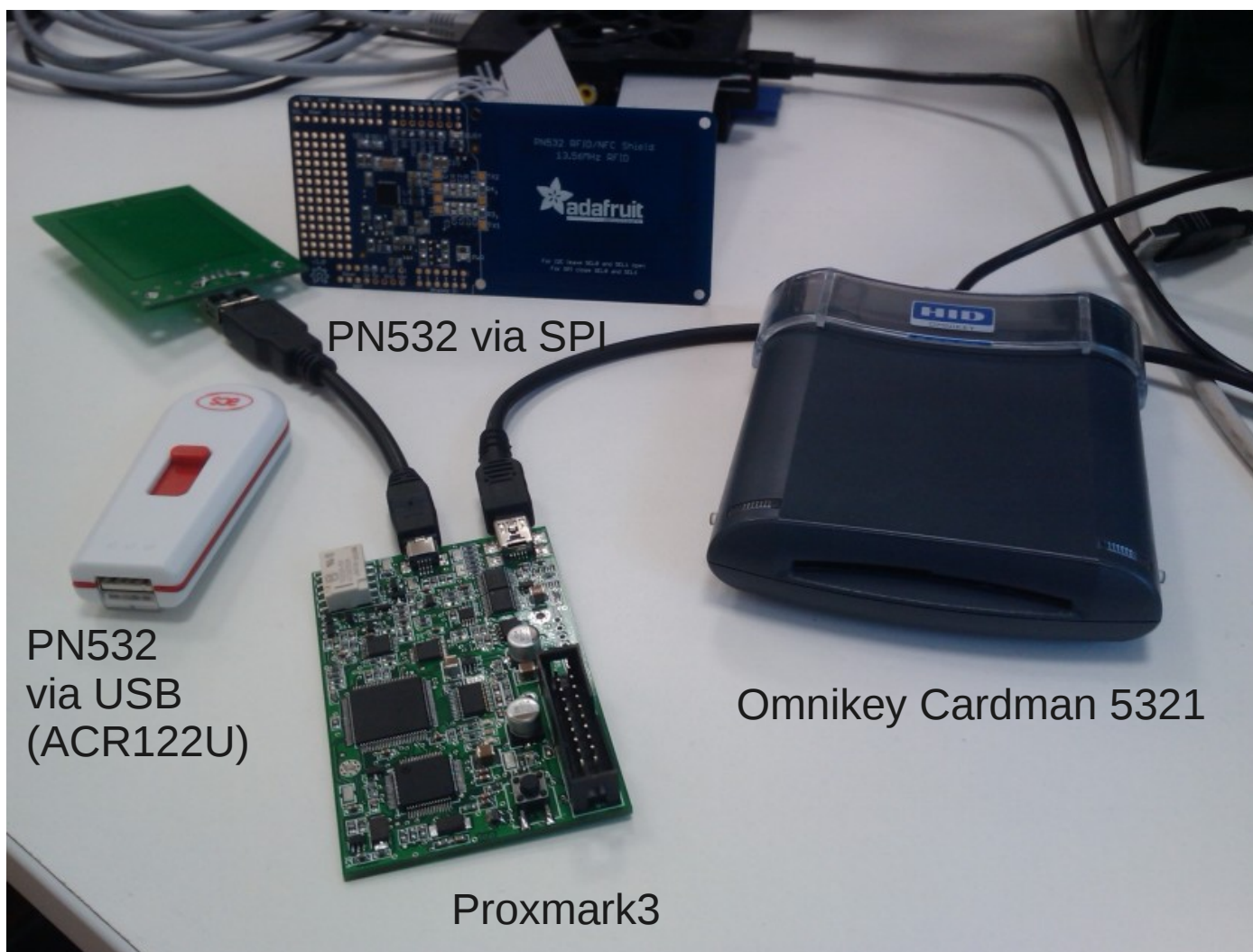


Přehled

- hardware
- kontaktní ISO 7816 smartkarty
 - PC/SC komunikace
- nízkofrekvenční karty
 - demodulace, simulace
- vysokofrekvenční karty
 - ISO14443 protokol



Hardware



HID Omnikey Cardman 5x2x

- kontaktní i bezkontaktní varianty
- dobrá podpora v různých OS
- bezkontaktní část funguje jen na x86/x86_64
 - vyžaduje binární blob výrobce
- podpora z mnoha PS/SC knihoven různých jazyků



PN532 čtečky

- pro vysokofrekvenční karty
- libnfc - přímá komunikace s čipem PN532
 - lowlevel přístup, ale nelze jednoduše emulovat UID
- ACR122U
 - USB verze
 - funguje i přes PC/SC interface
- Adafruit PN532 shield
 - připojení SPI, I2C nebo UART
 - mnohem stabilnější než USB verze



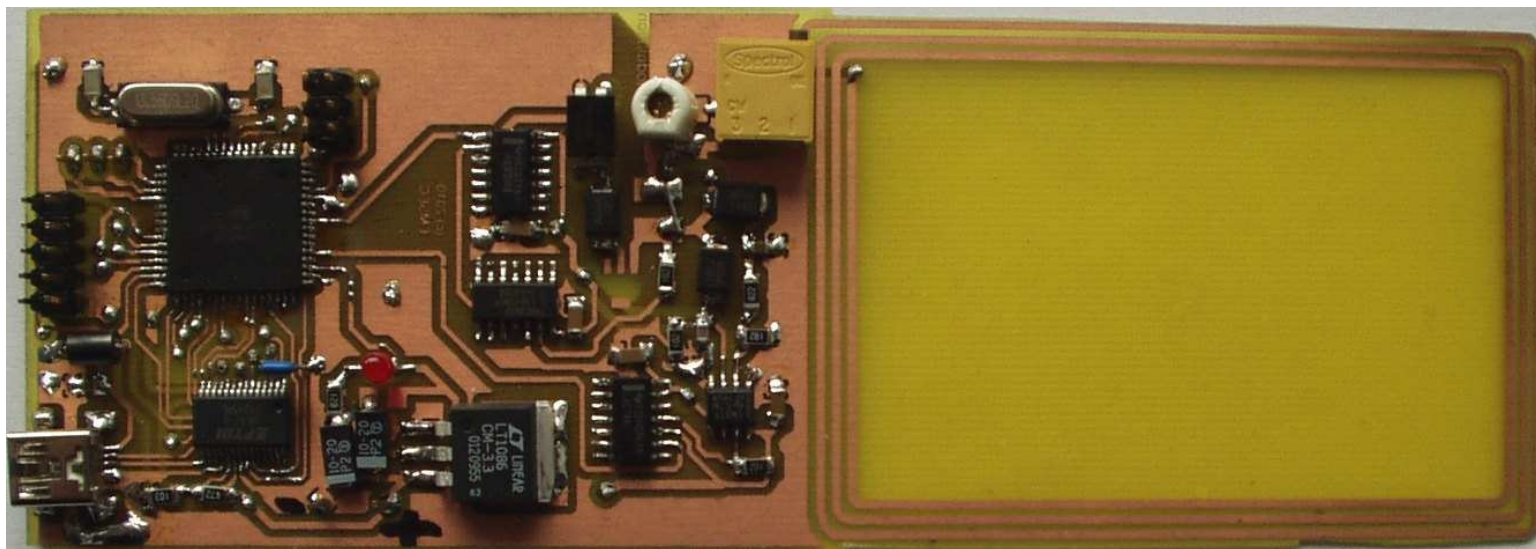
Proxmark3

- „švýcarský nožík pro RFID“
- FPGA demoduluje signál
- ARM procesor řídí vyšší logiku – dekodování a protokoly
- lze používat samostatně (napájení z baterie)
- command-line klient, skriptovatelný v Lua



Chameleon 14443

- specializovaná deska pro low-level komunikaci
- jednodušší než Proxmark – ATxmega192A3
- nutno postavit ručně



APDU ISO-7816

- APDU = „assembler“ smartkaret
- forma: **CLA INS P1 P2 [Lc] [Data] [Le]**
- CLA = class, 1 byte
- INS = opkód instrukce
- P1, P2 – parametry závislé na CLA/INS
- Lc, Data, Le – datové položky
- mnoho bichlí s referencí (EMV, SIM...)



Příklady APDU

- SELECT – INS 0xA4 (výběr aplikace/souboru)
 - 00 A4 00 00 02 3F 00 – select main file (MF)
 - A0 A4 00 00 02 7F 10 – select DF TELECOM
- VERIFY – INS 0x20 (autentizace PINem)
 - 00 20 00 01 08 31 32 33 34 FF FF FF FF
- READ BINARY – INS 0xB0
 - 00 B0 00 02 30 – čti max 0x30 bytů z offsetu 0x02
- READ RECORD – INS 0xB2
 - A0 B2 03 04 28 – čti max 0x28 bytů ze záznamu 0x03



EMV karty

- předdefinované AID (application ID) pro karetní společnosti a typ karty, př.:
 - Visa credit or debit – A0000000031010
 - Visa electron – A0000000032010
 - MasterCard credit or debit - A0000000041010
- číslo karty, jméno, expirace, historie transakcí atd. volně čitelné
 - i přes NFC interface, pokud ho karta má
- existují dedikované nástroje pro čtení EMV



Implementace programů smartkaret

- nejčastěji je to javacard (JCOP)
 - „osekaná Java“ bez new, String, atd.
 - očekávatelně se to blbě debuguje
- exploity na embedded JVM
 - Karsten Nohl fixnul problém s autentizací binárních SMS exploitem, který patchnul firmware
 - umožňuje plný R/W přístup k EEPROM
 - zatím není zveřejněno jak, ale šlo o řetěz dereferencí



ISO-7816 „firewall“



- pinpad reader Gemalto CT710
 - trochu kuriozita z Estónska
- odfiltruje APDU pokoušející se autentizovat pocházející z počítače
 - např. INS 0x20, 0x82, 0x88
 - malware se nemůže autentizovat kradeným PIN-em



Bezkontaktní karty

- 125kHz / 134.2kHz:
 - EM4x0x, Casi Rusco, HITAG 1, HITAG 2, HITAG S, MIRO, TIRIS/HDX, UNIQUE, AWID, Cardax, FDX-B, G-Prox II, Honeywell Nexwatch, IDTECK, Pyramid, Q5, TITAN, T55x7, ZOODIAC, Legic, Indala, HID Prox
- ISO14443 A+B (kompatibilní s částí 4 - transmission protocol):
 - Mifare DESFire | Plus | Classic | Ultralight | ..., my-d move, PayPass
- ISO15693:
 - Tag-It, my-d vicinity, ICODE SLI, M24LR16/64, PicoPass, HID iCLASS
- ISO18092 / NFC:
 - NFCIP-1: Passive communication mode, NFC Forum Tag Type 2-4, Sony FeliCa



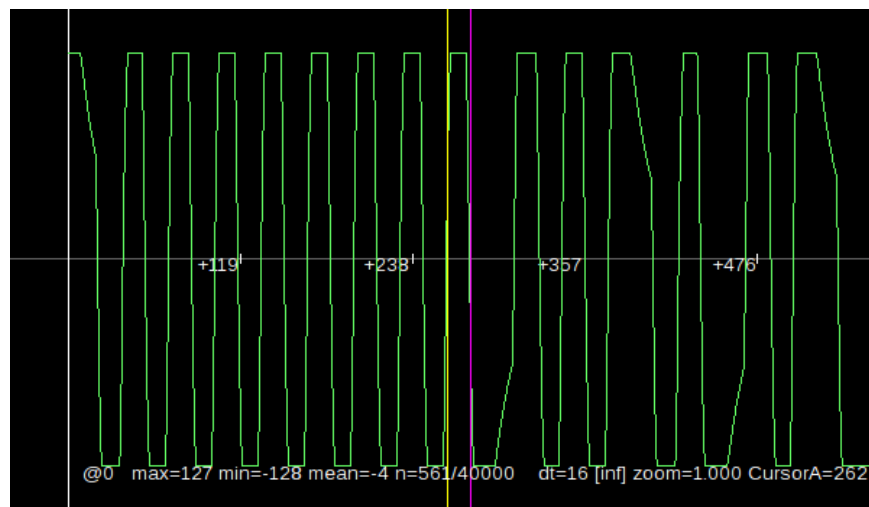
Nízkofrekvenční karty (125-134 kHz)

- většinou velmi jednoduché
- čip vysílá v cyklu svůj obsah, ~64 bitů
- EM410x
 - amplitudové klíčování (ASK)
 - kódování Manchester
- HID Prox
 - frekvenční klíčování (FSK)

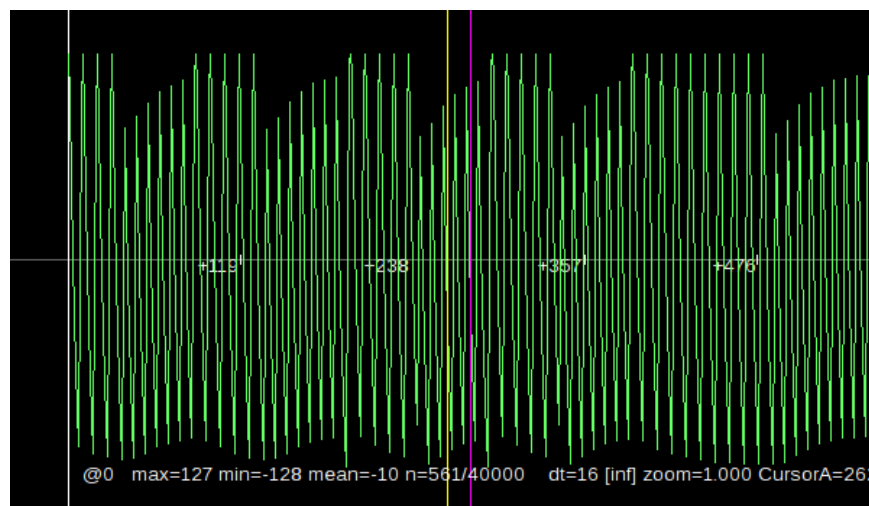


LF demo

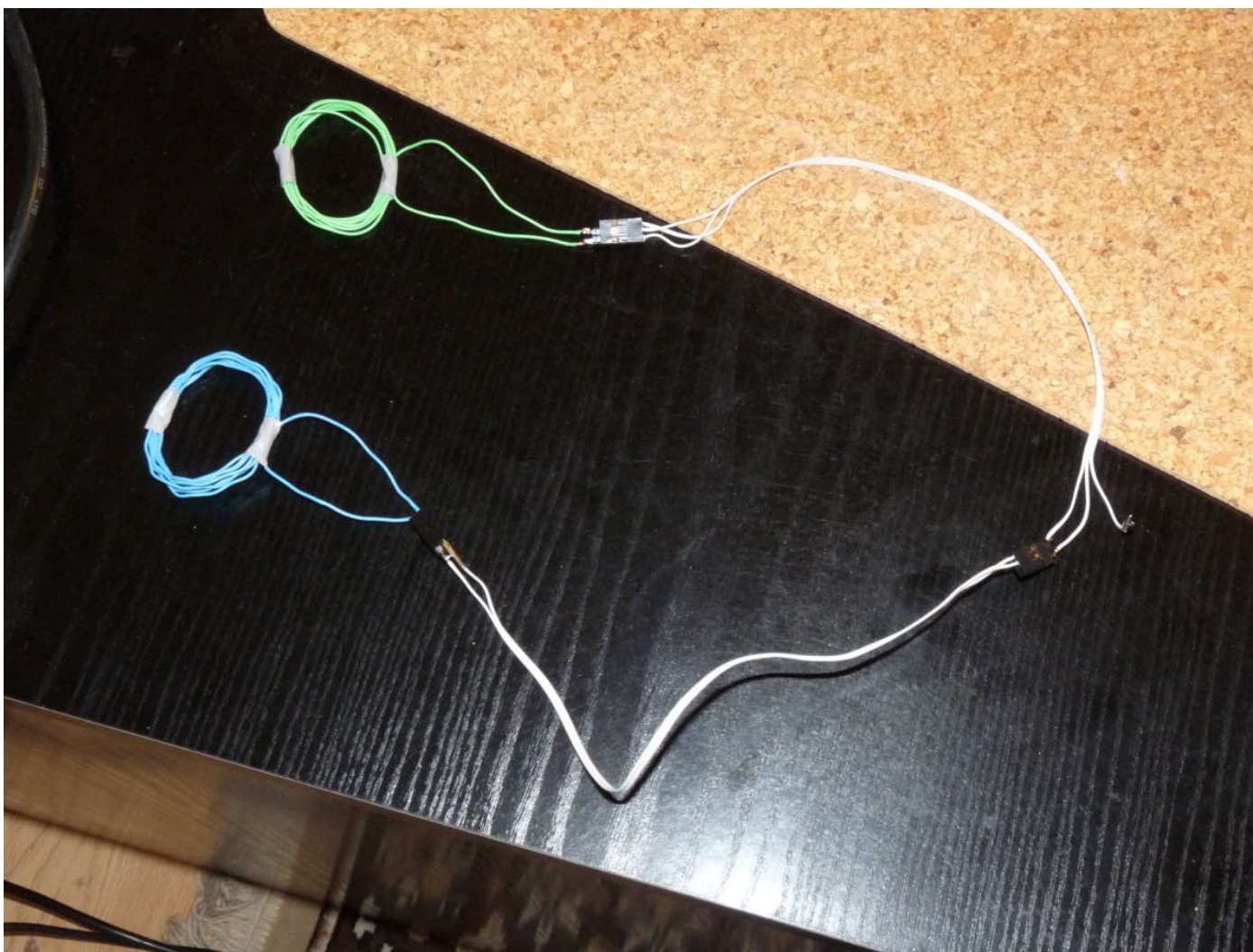
EM410x



HID Prox



„Wormhole“ útok

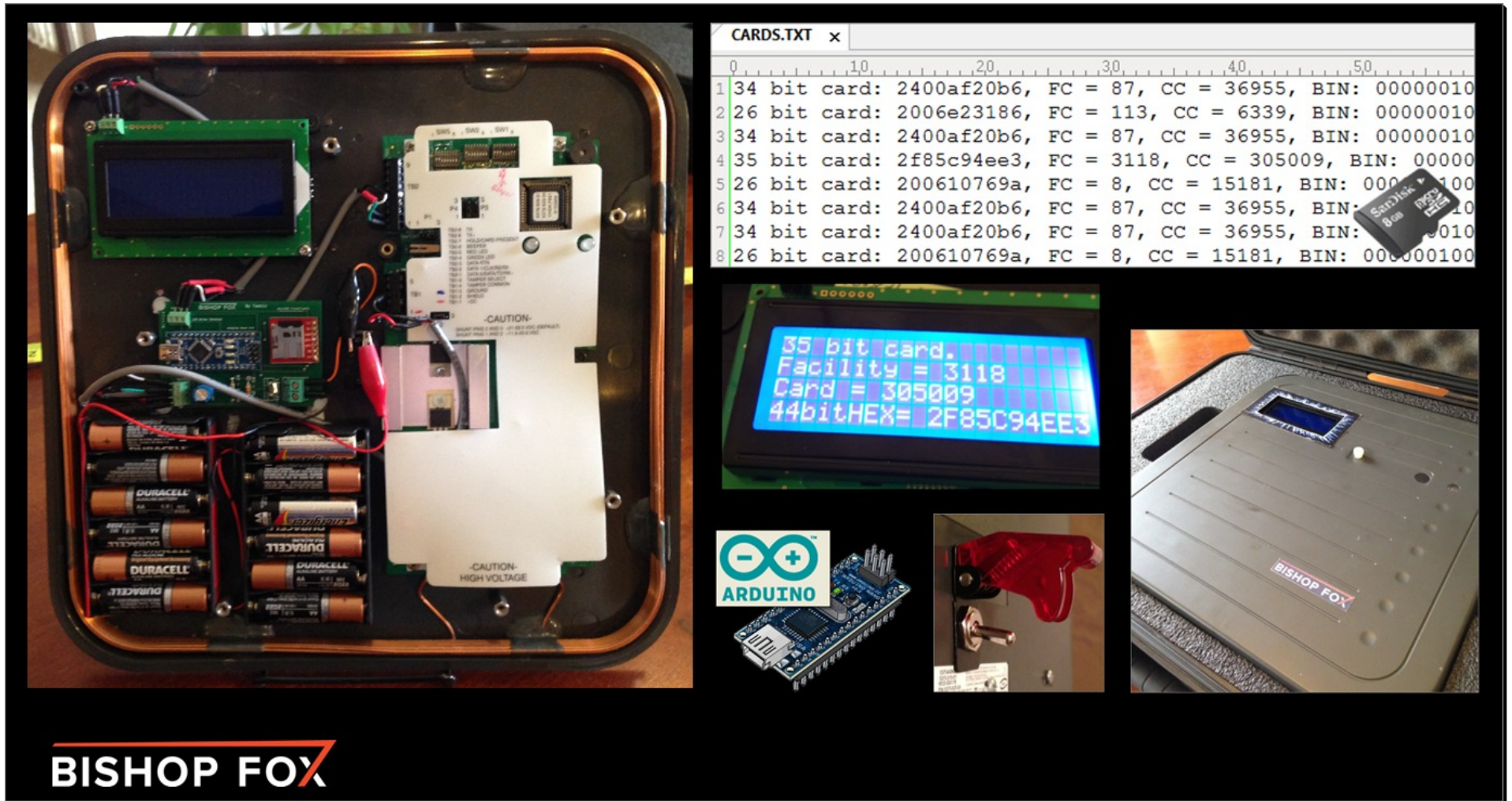


Sniffing LF karet na dálku

- spolehlivě proti pasivnímu tagu na 1 m
- jednoduchá simulace a klonování do prázdných tagů (Q5, T55x7)



Tastic RFID pro HID Prox (1m dosah)



The collage displays the internal hardware of the Tastic RFID device, including a green PCB with an LCD screen, an Arduino board, and several Duracell batteries. A screenshot of a text file named 'CARDS.TXT' lists the following data:

```
CARDS.TXT x
0 10 20 30 40 50
1 34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: 00000010
2 26 bit card: 2006e23186, FC = 113, CC = 6339, BIN: 00000010
3 34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: 00000010
4 35 bit card: 2f85c94ee3, FC = 3118, CC = 305009, BIN: 00000
5 26 bit card: 200610769a, FC = 8, CC = 15181, BIN: 00000100
6 34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: 0000010
7 34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: 0000010
8 26 bit card: 200610769a, FC = 8, CC = 15181, BIN: 00000100
```

A close-up of the LCD screen shows the following text:

```
35 bit card.
Facility = 3118
Card = 305009
44bitHEX= 2F85C94EE3
```

The external device casing is labeled 'BISHOP FOX' and features a red HID Prox lock.



Vysokofrekvenční karty (13.56 MHz)

- sdruženy pod standardy ISO 14443A/B, 18092, 15693
- každý z nich úplně jiný, standard „vyjmenováním speciálních případů“
- nejběžnější – NXP Mifare (ISO 14443 A)
 - Mifare Classic starší, s proprietárním šifrováním
 - Mifare DESfire novější, 3DES nebo AES
 - další varianty (Ultralight, Plus)

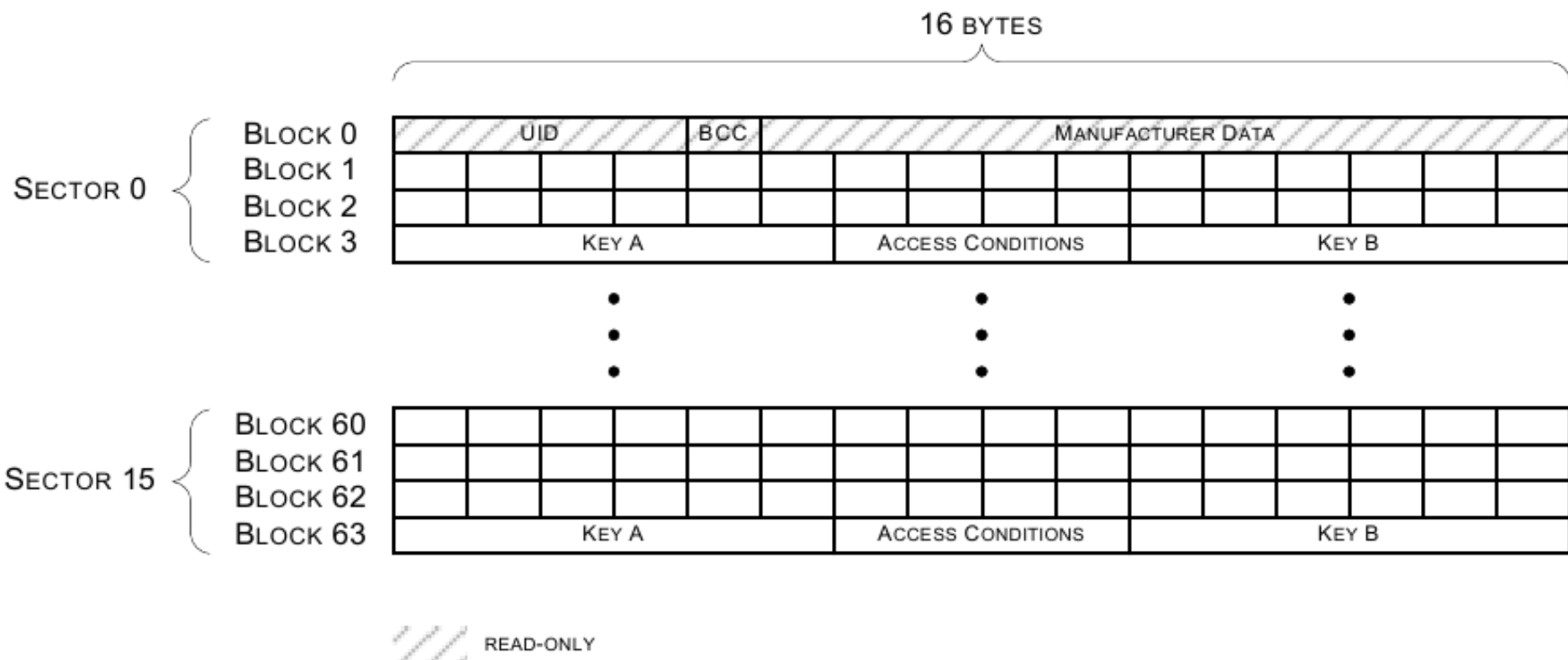


Mifare Classic

- velikost 1K-4K
 - „EEPROM s RF interface“
- 64 bytové sektory složené ze 4 bloků po 16 B
- nultý blok je speciální – obsahuje UID
 - u normálních Mifare nepřepsatelný
- UID často používané v starších přístupových systémech
 - emulace UID => získání přístupu



Mifare Classic 1K sector



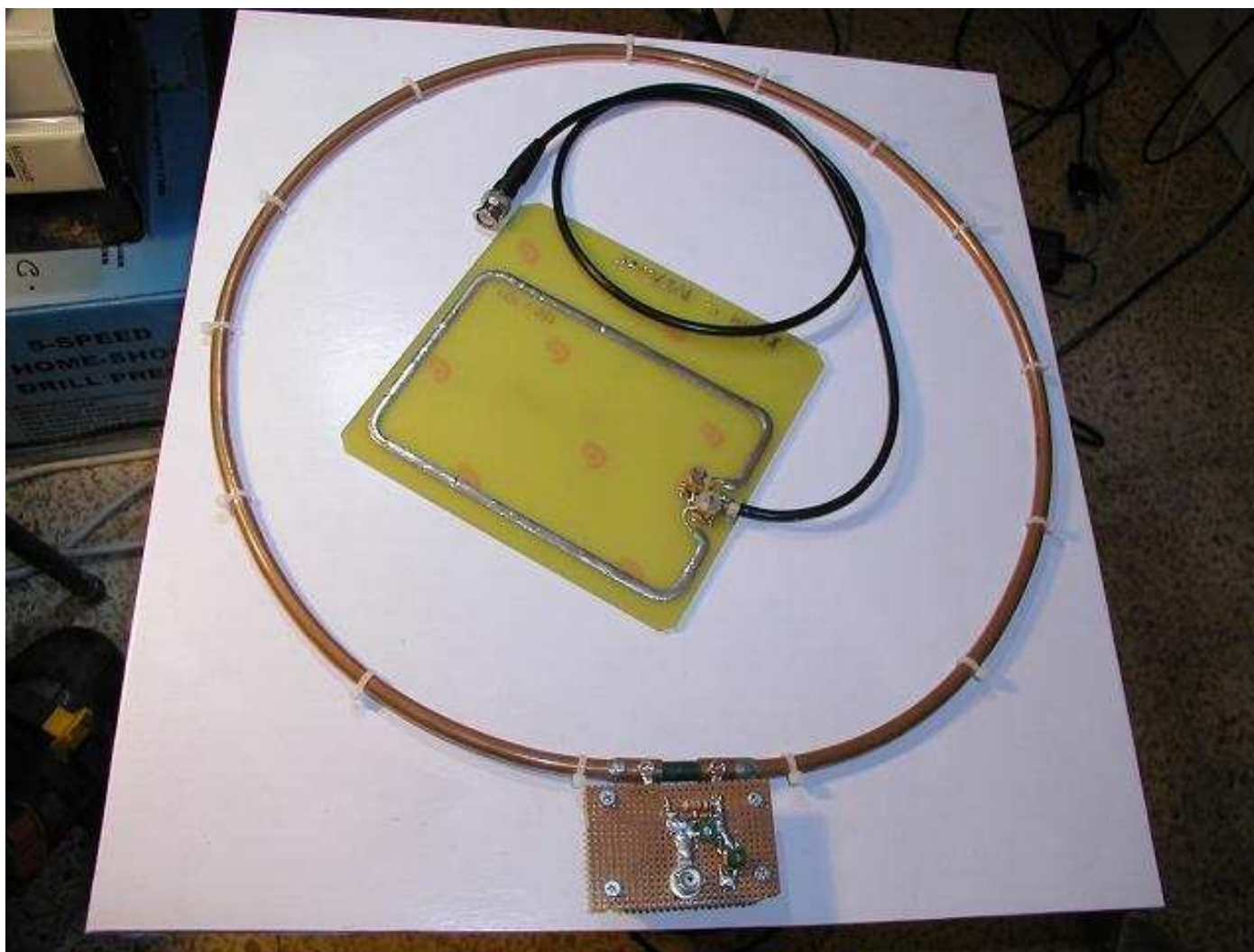
Sniffing ISO14443 provozu

Zdroj	Data	Význam
čtečka	26 (7 bitů)	REQA
karta	44 00	ATQA
čtečka	93 20	SELECT – antikolize, kaskáda 1
karta	88 <u>04 c2 4c</u> 02	UID karty 4 byte + BCC 1 byte
čtečka	93 70 88 04 c2 4c 02 f3 08	SELECT 8804C24C + BCC + CRC
karta	04 da 17	SAK 1 byte + CRC 2 byte
čtečka	95 20	SELECT – antikolize, kaskáda 2
karta	<u>e9 ad 27 80</u> e3	druhá část UID + BCC
čtečka	95 70 e9 ad 27 80 e3 06 04	SELECT E9AD32780 + BCC + CRC
karta	00 fe 51	SAK 1 byte + CRC 2 byte

UID je podtrženo, byte 0x88 před UID je „cascade tag“ používaný u UID delších 4 byty
Poslední SAK kóduje typ karty (zde 0x00 = Mifare Ultralight C).
ATQA kóduje zda karta podporuje antikolizi a jak dlouhé je UID.



Zvětšení dosahu ISO14443



ISO14443 sniffing „na dálku“

- nefunguje na moc velké vzdálenosti
- čtení anténou z předchozího slajdu dokáže komunikovat s pasivní kartou do 25 cm
- na větší vzdálenosti lze odposlouchávat jen probíhající komunikaci
 - dosah 2.2 - 3 m obousměrně
 - směr od čtečky k tagu i na 10 m
 - 18 m z vyšších harmonických (laboratorní podmínky)



Crypto1

- Crypto1 – proprietární šifra pro Mifare Classic
- „darkside“ útok
 - vhodný na zjištění jednoho klíče k jednomu sektoru, pokud žádný neznáme
 - na některých kartách je fixnutý PRNG (nefunguje)
- „nested“ útok
 - je nutné znát klíč alespoň k 1 sektoru
 - často alespoň 1 klíč je z defaultních
 - utilita MFOC – „mifare offline cracker“



Emulace Mifare classic

- kopírovat na prázdnou
 - klíče A i B víme případně lousknout
 - čínské „magic Mifare“ dovolí zapsat blok 0 s UID
 - jen 4 byte UID, karta nepodporuje kaskádový SELECT potřebný pro 7 a 10-byte UID
 - má i „magický mód“ zápisu a čtení bez klíčů
- Proxmark3
 - umí emulovat kompletně komunikaci
 - může být pomalý při čtení obsahu sektorů



Emulace NFC Forum Tagu

- libnfc s PN532 umí emulovat vyšší vrstvy
 - emulace smartkarty přes NFC/RFID
- „NFC vizitky“ jsou některý z NFC Forum Tagů
- Forum Tag Type 4 je „aktivní“, tj. smartkarta
 - soubor 0xE103 – Capability Container
 - určuje, kde je obsah zprávy, typicky soubor 0xE104
 - data jsou formátována v NDEF záznamech
 - typ (SMS, URI, text, ...) + obsah



Mifare DESFire

- něco mezi smartkartou a „EEPROM s rádiem“
- až tři typy příkazů
 - nativní formát
 - wrapped – nativní formát zabalen „jako APDU“
 - APDU pro NFC Forum Tag 4
- paměť rozdělena na „aplikace“ (3 byte ID)
 - aplikace rozděleny na soubory (1 byte ID)
 - každá aplikace může mít přiřazeno vícero klíčů s různými právy



Mifare DESFire komunikace

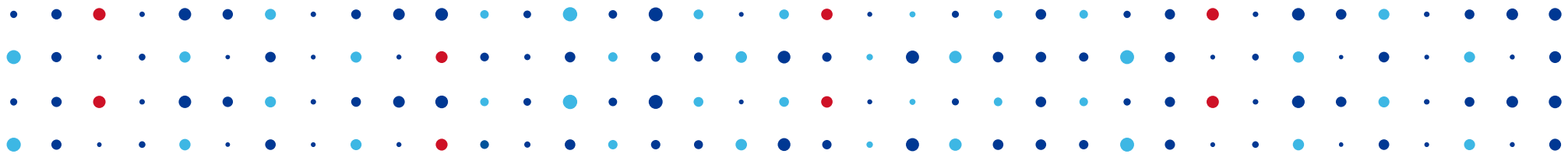
- některé nativní příkazy:
 - 0x60 – get version
 - 0xAF – request more data
 - 0x6A – list application IDs
 - 0x5A 0x01 0x00 0x00 – select AID 01 00 00
- libfreefare
 - musí se dost hackovat, aby to fungovalo
 - formátování, čtení a zápis NDEF tagů



Mifare DESFire útoky

- autentizace s DES/3DES nebo AES
 - nenalezena analytická zranitelnost
- starší MF3ICD40 umožňuje extrakci klíčů
 - postranní kanály
 - již se nevyrábí





Děkuji za pozornost

Ondrej Mikle • ondrej.mikle@nic.cz

