Smartkarty a NFC

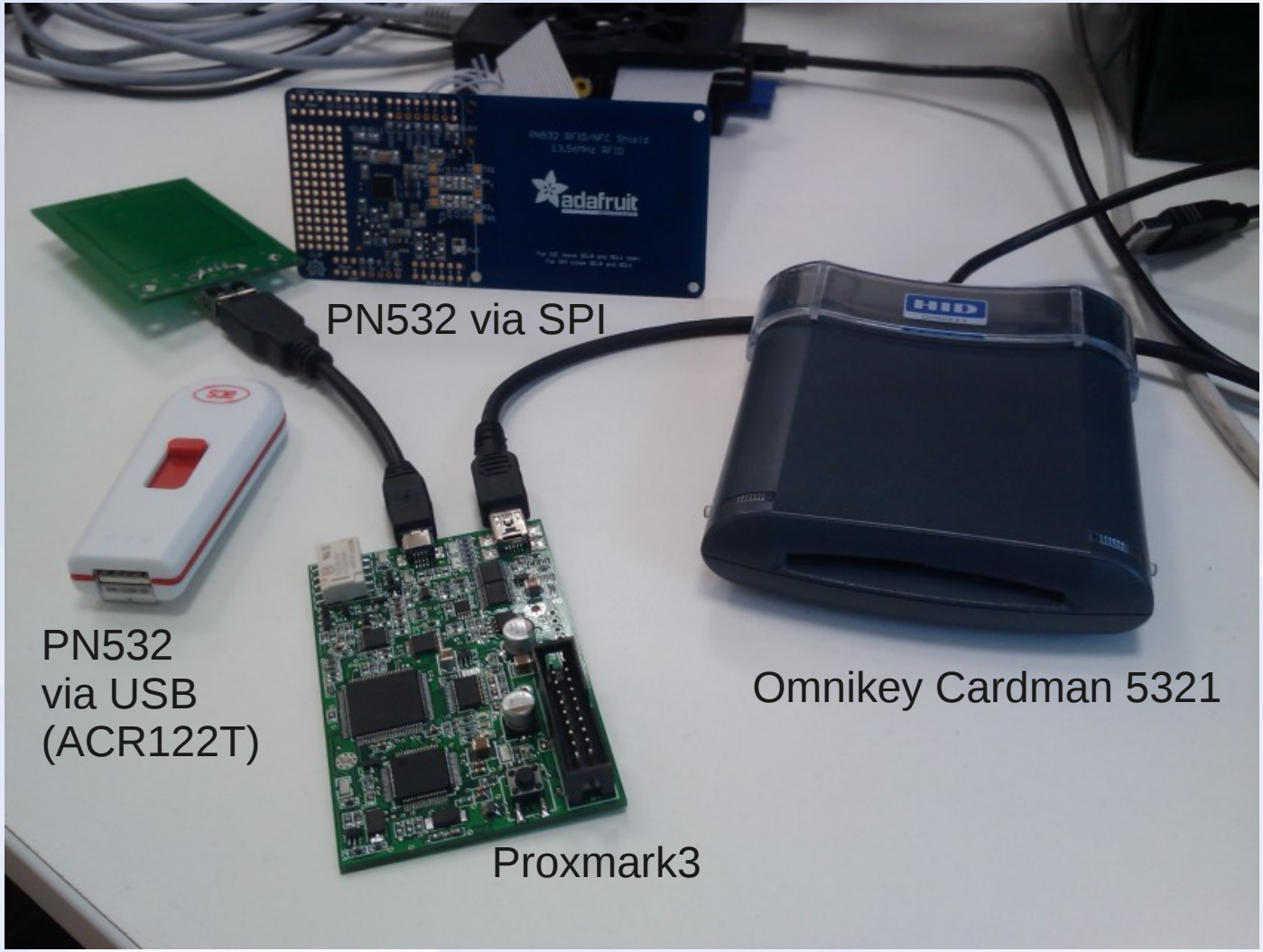
a příbuzné protokoly (EMV, SIM/GSM)

Ondrej Mikle • ondrej.mikle@gmail.com • 10.2.2014

Přehled

- hardware
- kontaktní ISO 7816 smartkarty
  - PC/SC komunikace
- nízkofrekvenční karty
  - demodulace, simulace
- vysokofrekvenční karty
  - ISO14443, ISO15693, ISO18092 protokoly

Hardware


PN532 via SPI
PN532
via USB
(ACR122T)
Omnikey Cardman 5321
Proxmark3

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

PN5xx čtečky

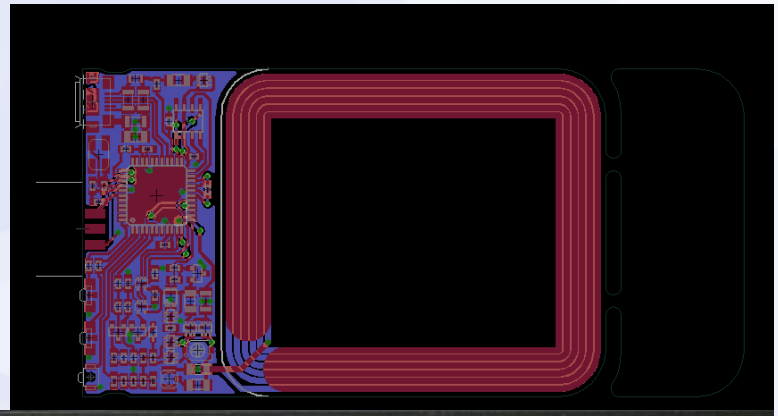
- pro vysokofrekvenční karty
- libnfc - přímá komunikace s čipem PN532
  - lowlevel přístup, ale nelze emulovat UID
  - PN532, PN533, PN544, (PN65?)
- ACR122T (PN532)
  - USB verze, funguje i přes PC/SC interface
- Adafruit PN532 shield
  - připojení SPI, I2C nebo UART
  - mnohem stabilnější než USB verze

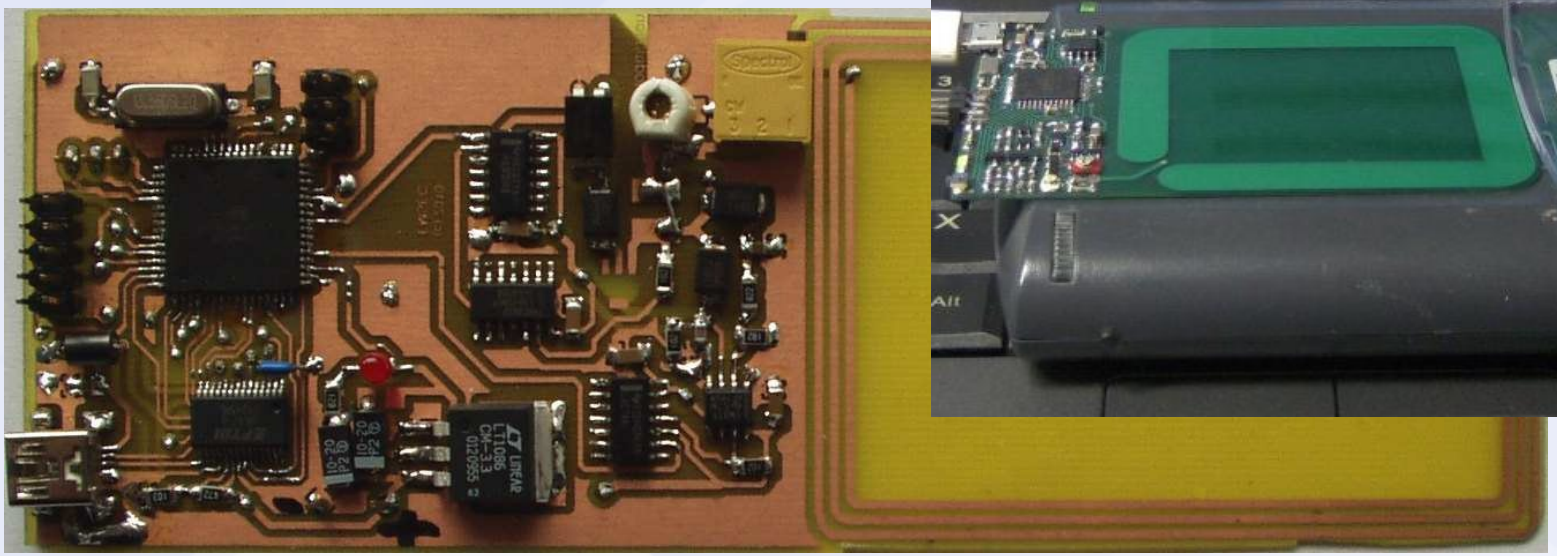
Proxmark3

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

Chameleon 14443 + mini verze

- 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 DFTELECOM
- 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, offset 2
- READ RECORD – INS 0xB2
  - A0 B2 03 04 28 – čti max 0x28 bytů ze záznamu 0x03

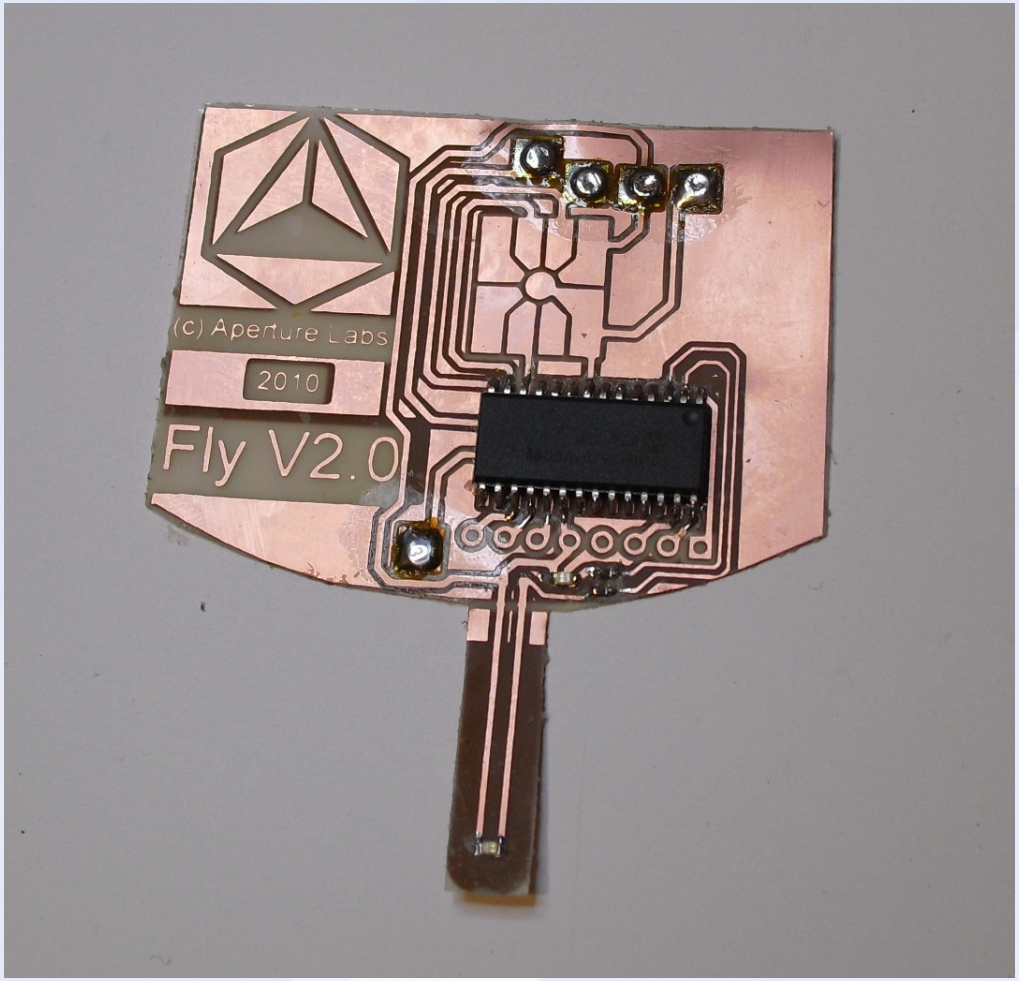
SIM karty

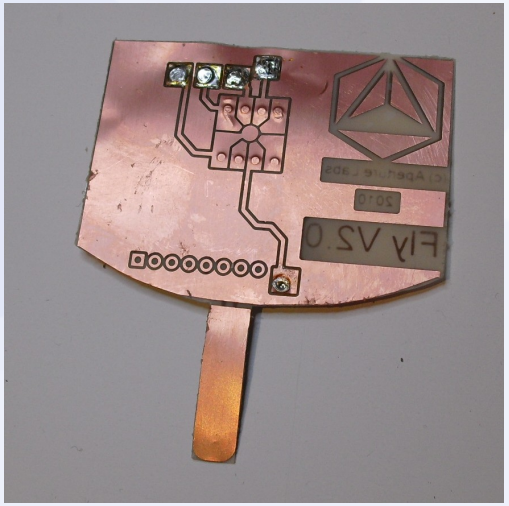
- demo čtení adresáře z SIM
  - používá APDU z přechozího slidu
- SIMTester + gsmmap
  - otestuje fuzzováním různé aplikace (TAR – toolkit application reference), jejich klíče
  - TAR 0 je card manager, umožňuje instalaci jiných aplikací (appletů)
  - funguje s PC/SC nebo OsmocomBB
  - našli jsme několik různě deravých SIM

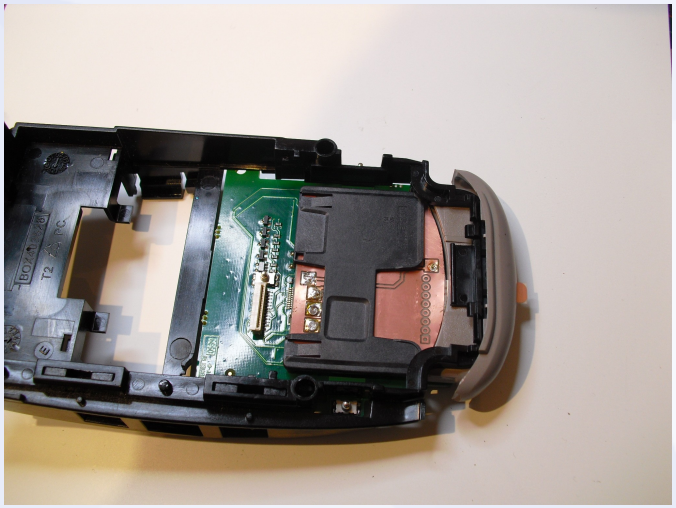
EMV karty

- předdefinované AID (application ID) pro karetní společnosti a typ karty, př.:
  - Visa credit/debit – A0000000031010
  - Visa electron – A0000000032010
  - MasterCard credit/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

EMV skimmer + MitM







EMV autentizace

- offline PIN verifikace vs offline transakce
  - dvě úplně rozdílné věci
  - bankomaty vždy online
- static data authentication (SDA)
  - offline PIN verifikace je v cleartextu
  - hack – úprava na bezPINovou „Yes“ kartu
- dynamic data authentication (DDA)
  - offline PIN může být v cleartextu
  - CVM downgrade

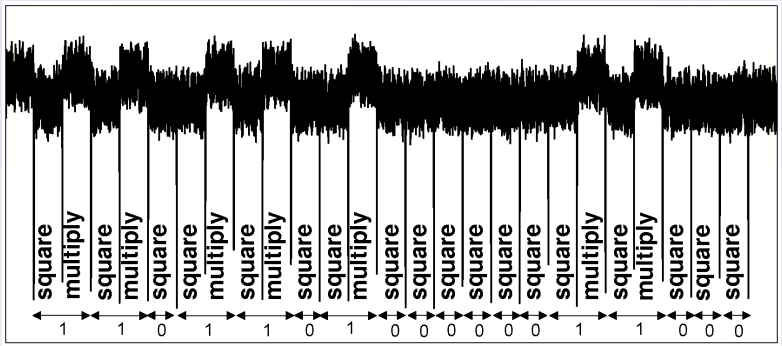
Implementace programů smartkaret

- nejčastěji je to javacard (JCOP)
  - „osekaná Java“ bez new, String, atd.
  - očekávatelně se to blbě debuguje
- exploity na embedded JVM
  - srlabs.de fixli 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

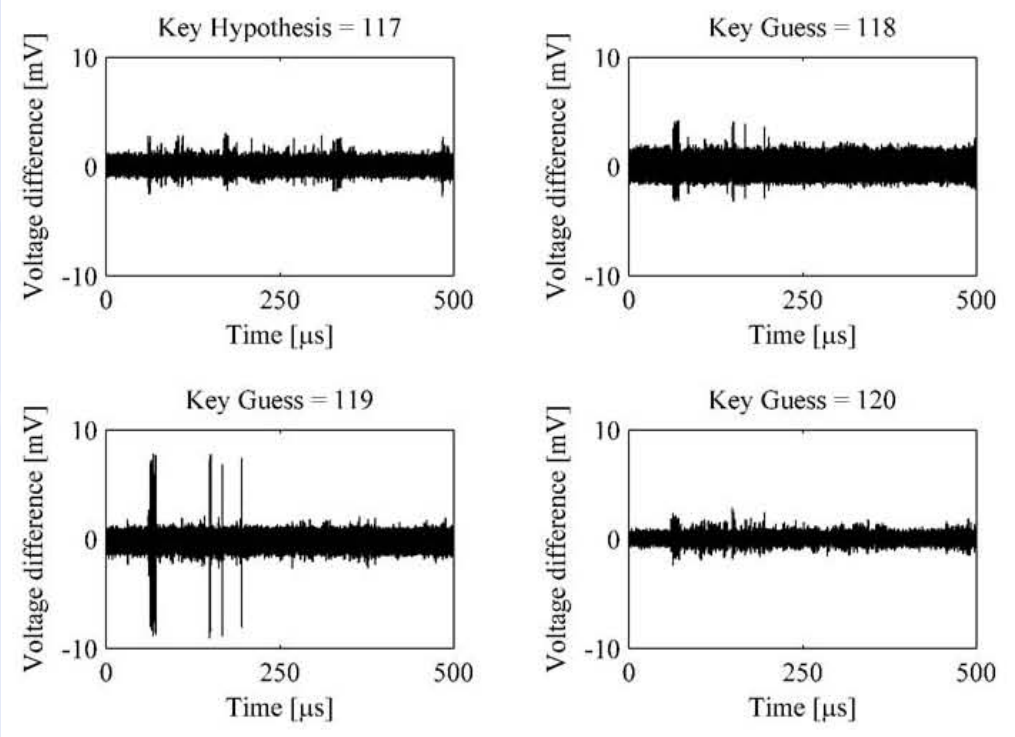
ISO-7816 „firewall“

- 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

Power analysis attacks



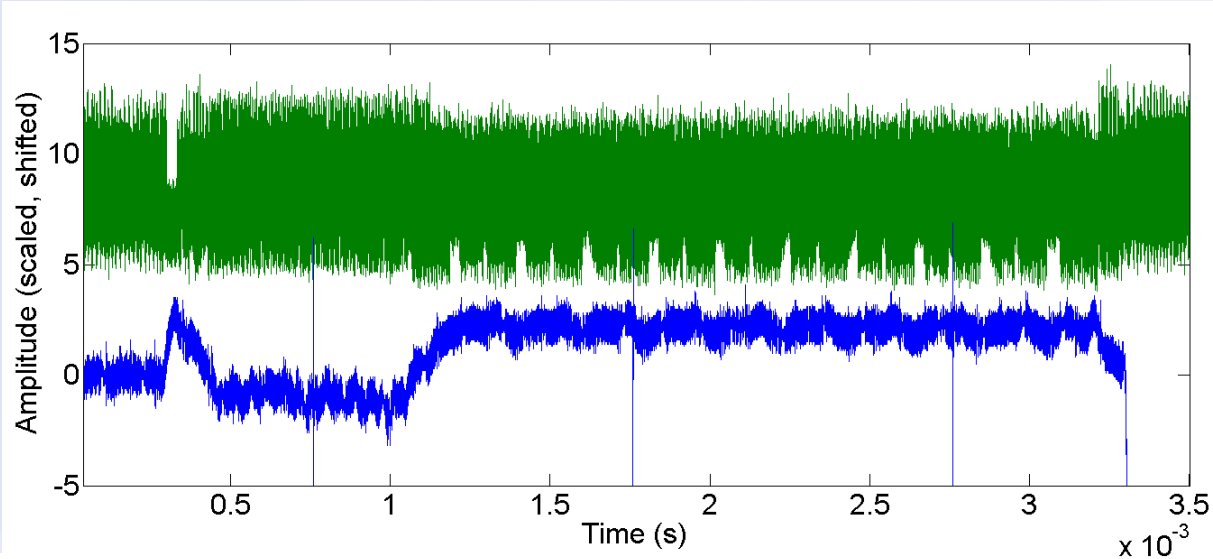
Simple power analysis

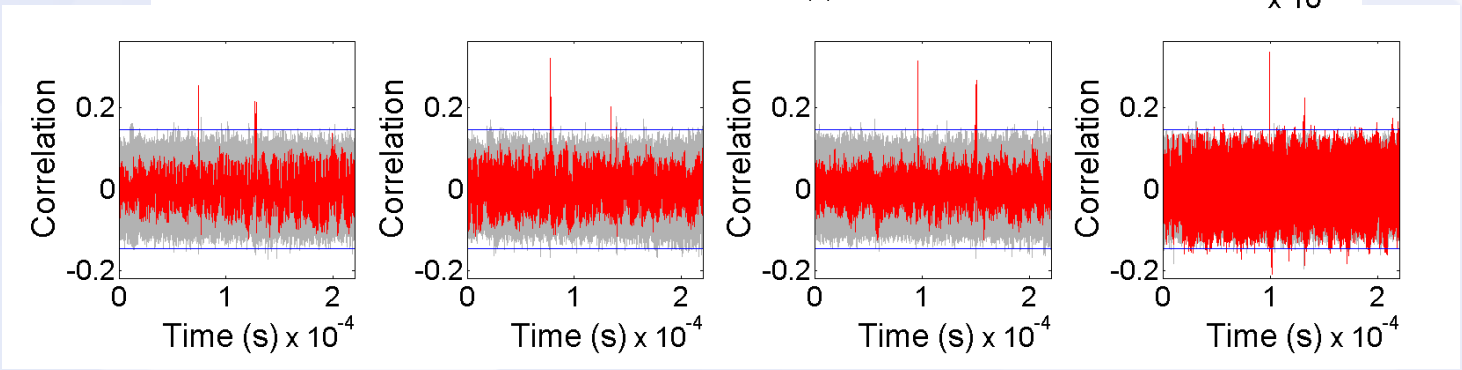


Differential power analysis

Yubikey extrakce klíče via PA

- starý firmware < 2.4 (30C3 přednáška)





Bezkonktatní karty

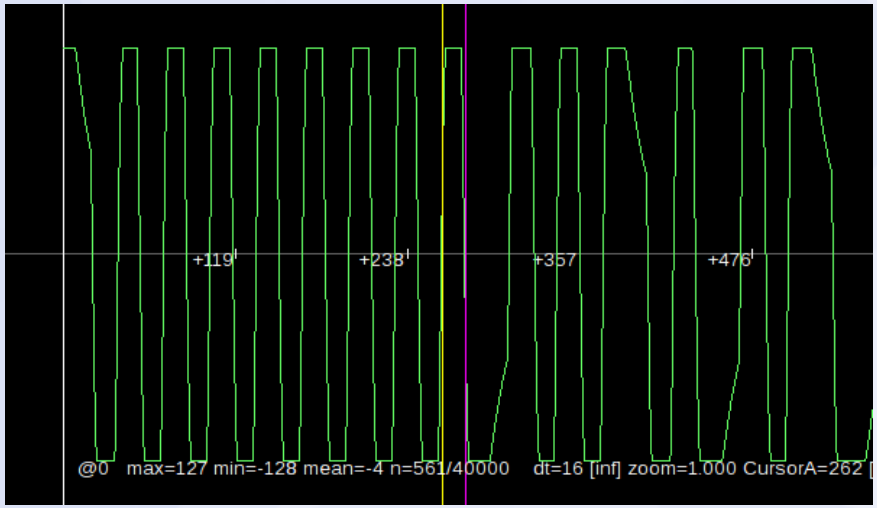
- 125kHz / 134.2kHz:
  - EM4x0x, Casi Rusco, HITAG 1, HITAG 2, HITAG S, MIRO, IDTECK, Pyramid, Q5, T55x7, Legic, Indala, HID Prox...
- ISO14443 A+B (kompatibilní s částí 4 - transmission protocol):
  - Mifare DESFire | Classic | Ultralight | ...
- ISO15693, ISO18092:
  - Tag-It, ICODE SLI, M24LR16/64, PicoPass, HID iCLASS, Sony Felica...

Nízkofrekvenční karty

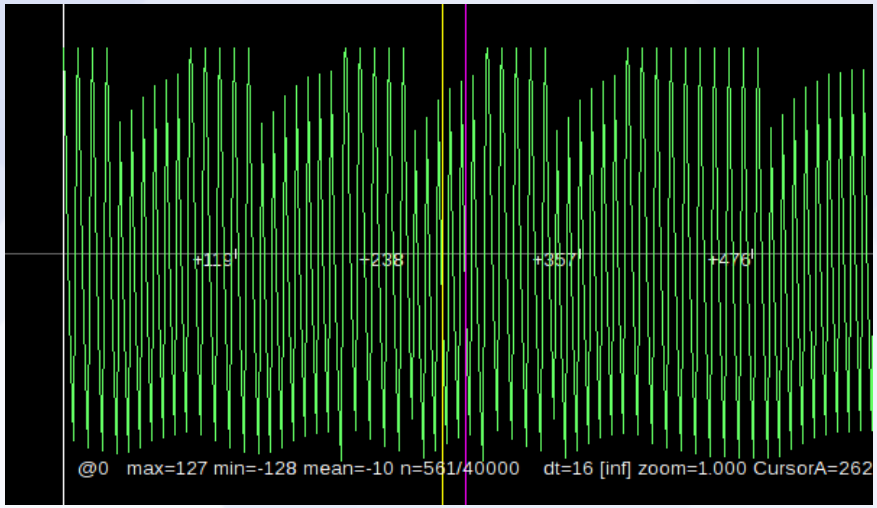
- 125-134 kHz, zřídkavě i jiné frekvence
- většinou velmi jednoduché
- čip vysílá v cyklu svůj obsah, ~64 bitů
- EM410x
  - amplitudové klíčování (ASK)
  - kódování Manchester
- HID Prox
  - frekvenční klíčování (FSK)

LF demo

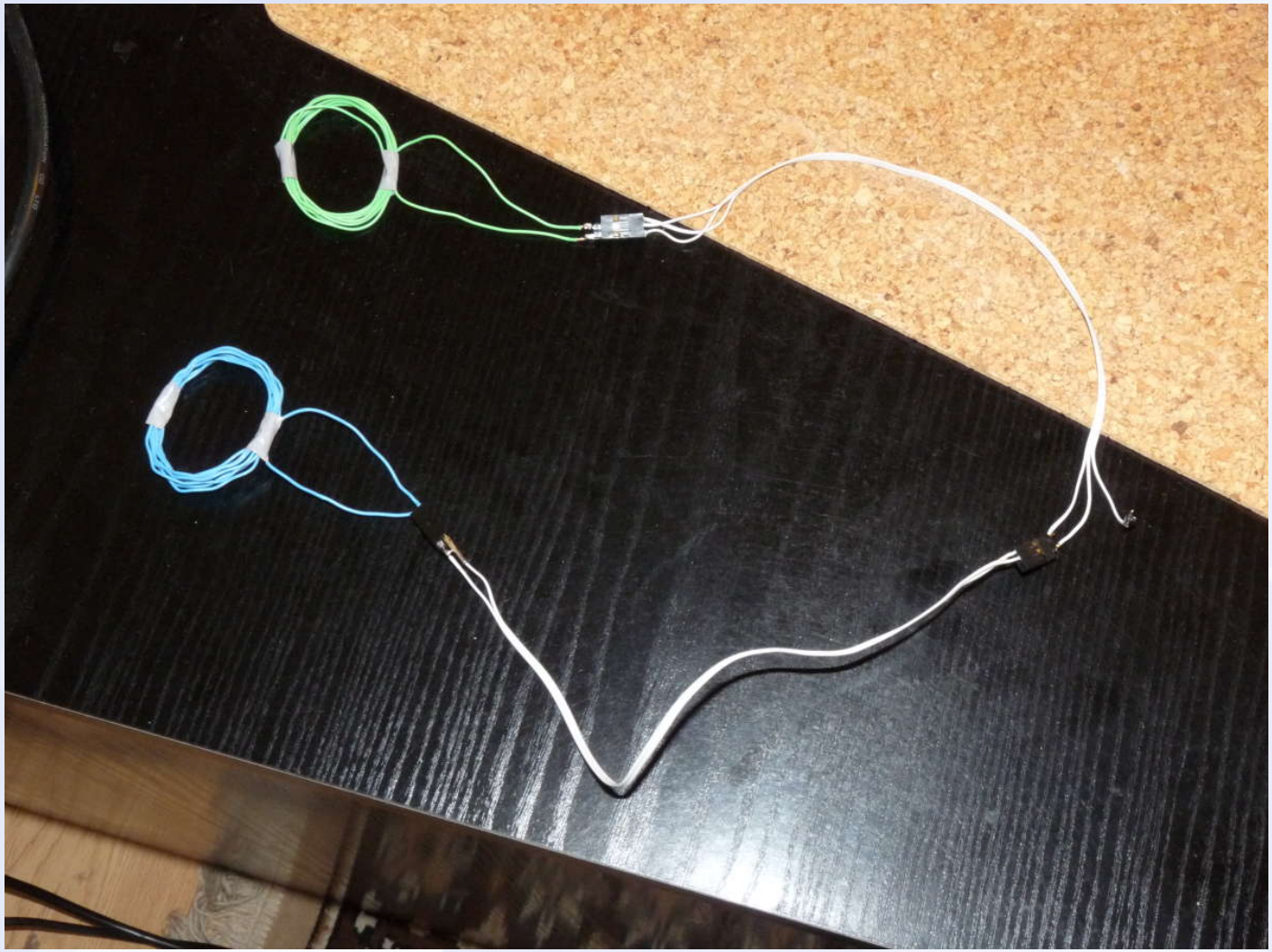
EM410x



HID Prox



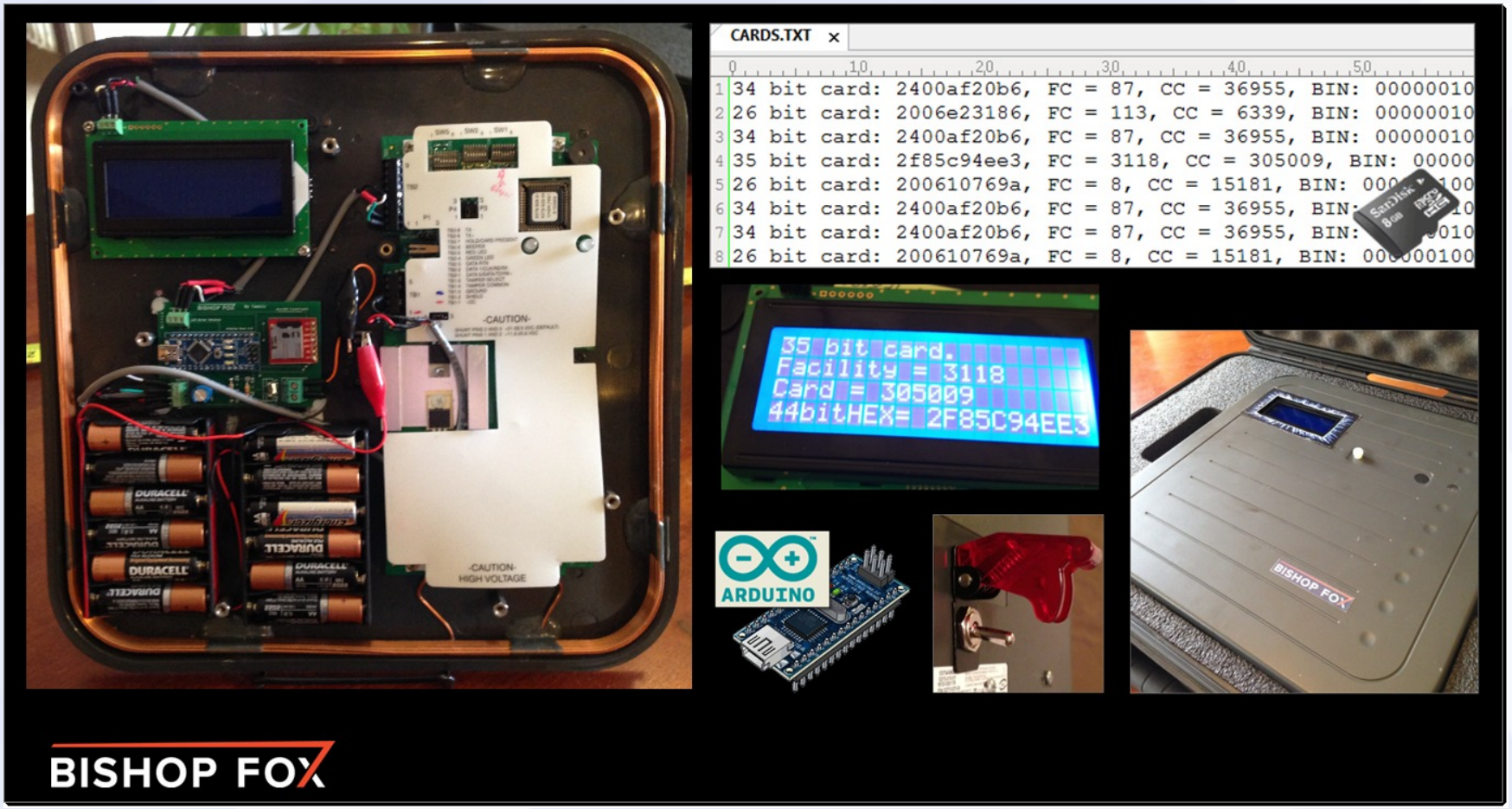
„Wormhole“ útok



Sniffing LF karet na dálku

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

Tastic RFID pro HID Prox (1m dosah)



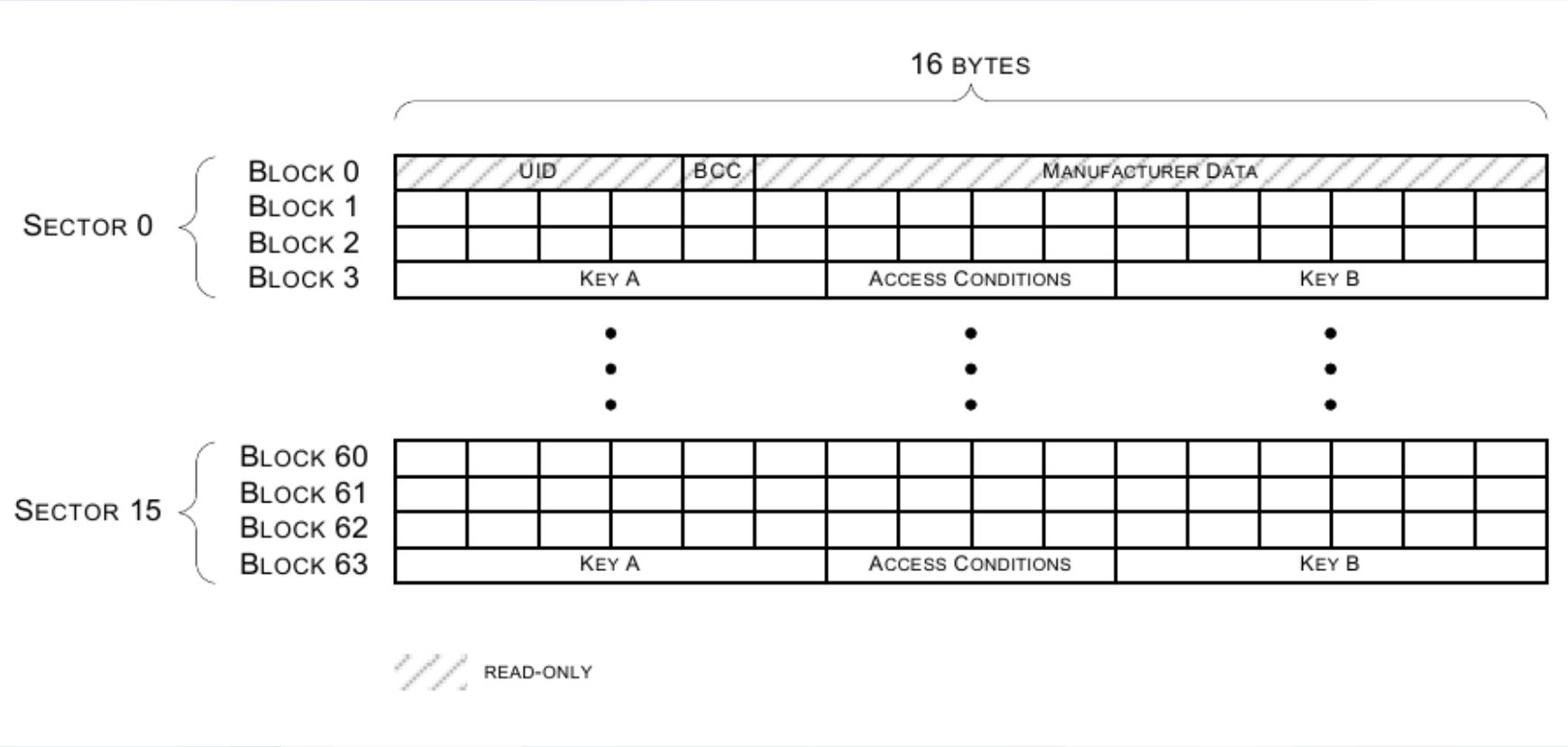
Vysokofrekvenční karty

- 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

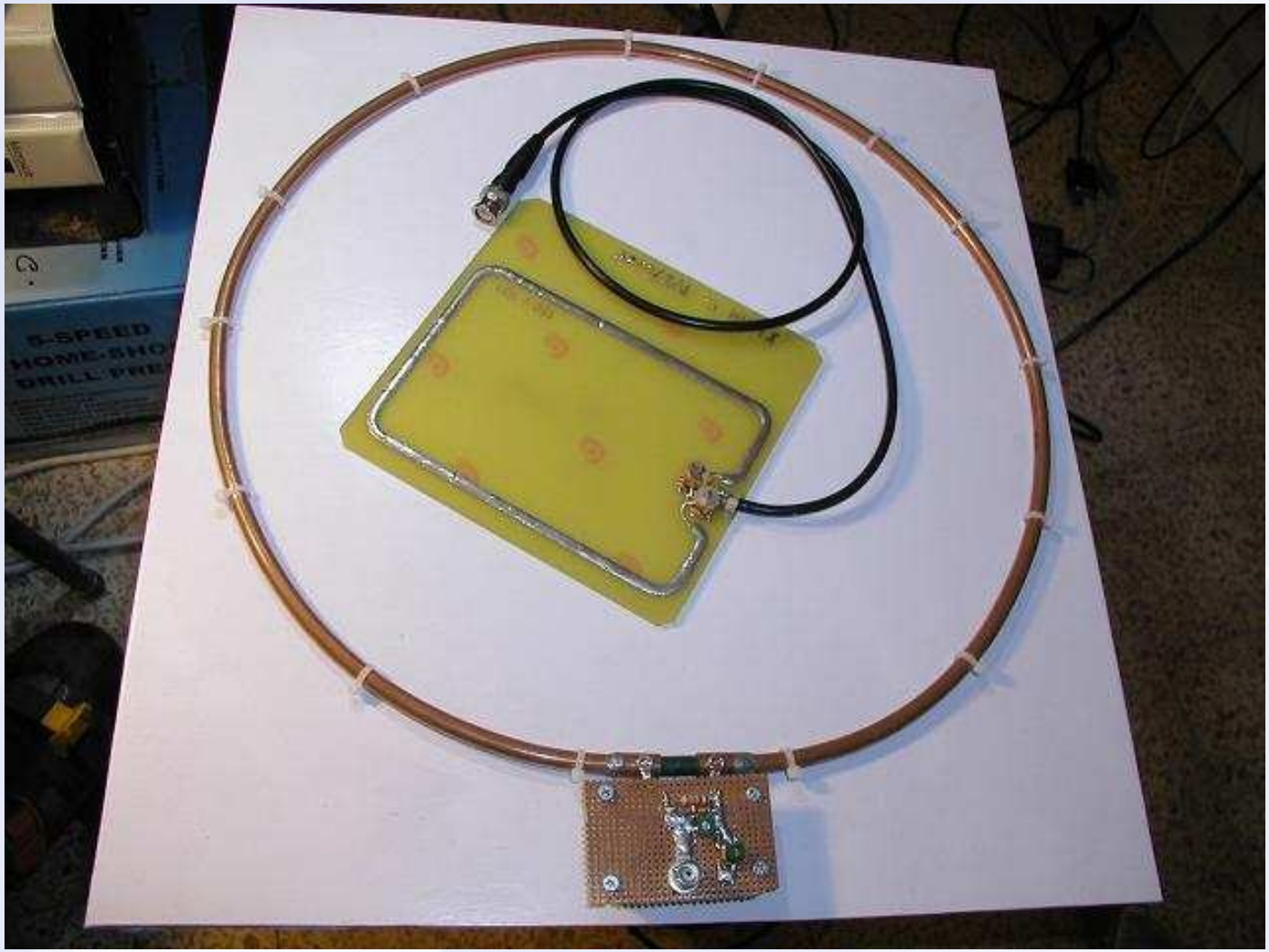


Sniffing ISO14443 provozu

Zdroj	Data	Význam
čtečka	26 (7 bitů)	REQA
karta	44 00	ATQA
čtečka	93 20	SELECT – antikolize, kaskáda 1
karta	88 04 c2 4c 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	e9 ad 27 80 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)

NFCProxy (APDU level)

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 přirazeno vícero klíčů s různými právami

Čínské „magické“ Mifare

- lze přepsat blok 0 s UID
  - prostě si v návrhu přidělali backdoor
  - jen 4 byte UID, neumí kaskádu s 7-10 B
  - uživatel musí dát pozor, aby sedělo BCC
- nestandardní příkazy u 1k varianty
  - 0x40 (7-bit) – „tajná“ varianta WAKEUP
  - 0x43 – „tajná“ varianta SELECT
  - 0xA0 0x00 – „unlocked“ write
    - nepožaduje znalost klíče k zápisu

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

ISO 15693

- 13.56 MHz, velmi podobné Mifare classic
- „vicinity“ tagy, na větší vzdálenost
- čipy méně žerou, jednodušší
- typické použití – turnikety (skipassy)

Děkuji za pozornost

Ondrej Mikle • ondrej.mikle@gmail.com