Reverzování NFC karet

především platebních (EMV)

Ondrej Mikle • ondrej.mikle@gmail.com • 13.9.2014

Bezkonktatní (RFID) karty

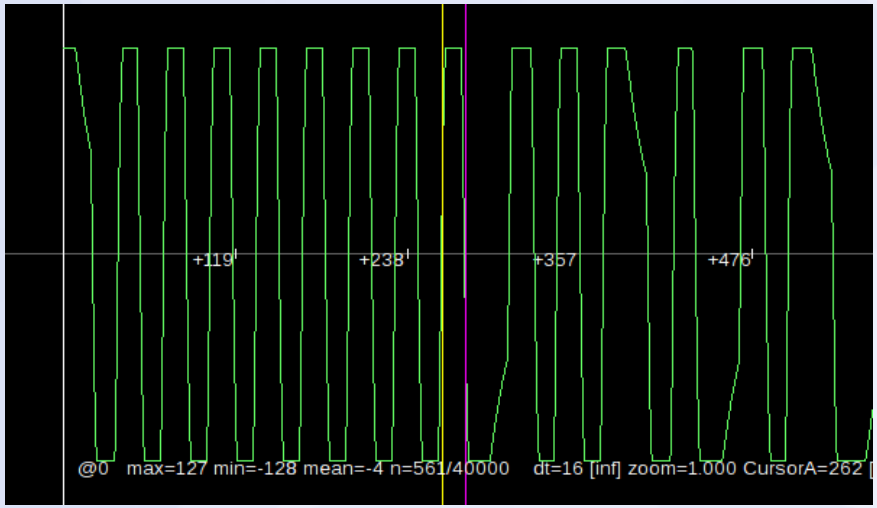
- 125kHz / 134.2kHz:
  - EM4x0x, Casi Rusco, HITAG 1, HITAG 2, HITAG S, MIRO, IDTECK, Pyramid, Q5, T55x7, Legic, Indala, HID Prox...
- 13.56 MHz ISO14443 A+B:
  - Mifare DESFire | Classic | Ultralight | ...
  - NFC platební karty
- 13.56 MHz ISO15693, ISO18092:
  - iCODE SLI, novější lyžařské turnikety

Nízkofrekvenční karty

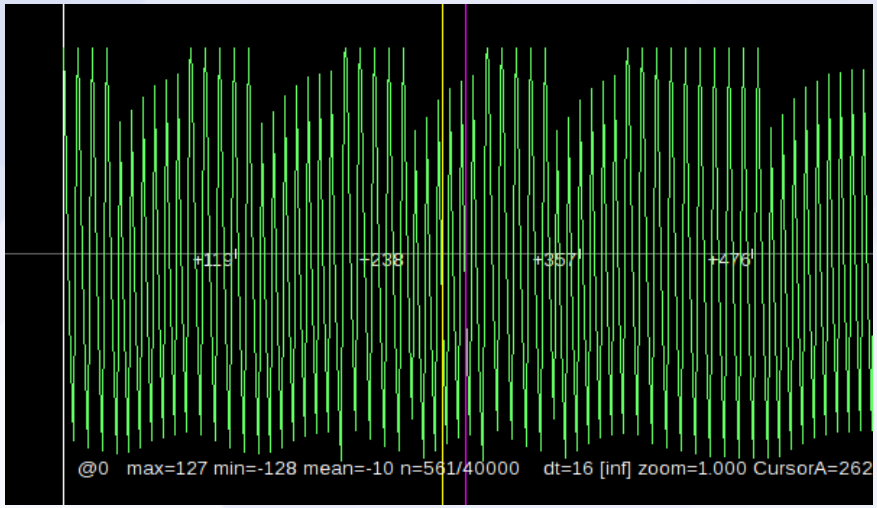
- 125-134 kHz, zřídkavě i jiné frekvence
- většinou velmi jednoduché
- čip vysílá v cyklu své UID, ~64 bitů
- EM410x
  - amplitudové klíčování (ASK)
  - kódování Manchester
- HID Prox
  - frekvenční klíčování (FSK)

Jednoduché RFID LF karty

EM410x



HID Prox



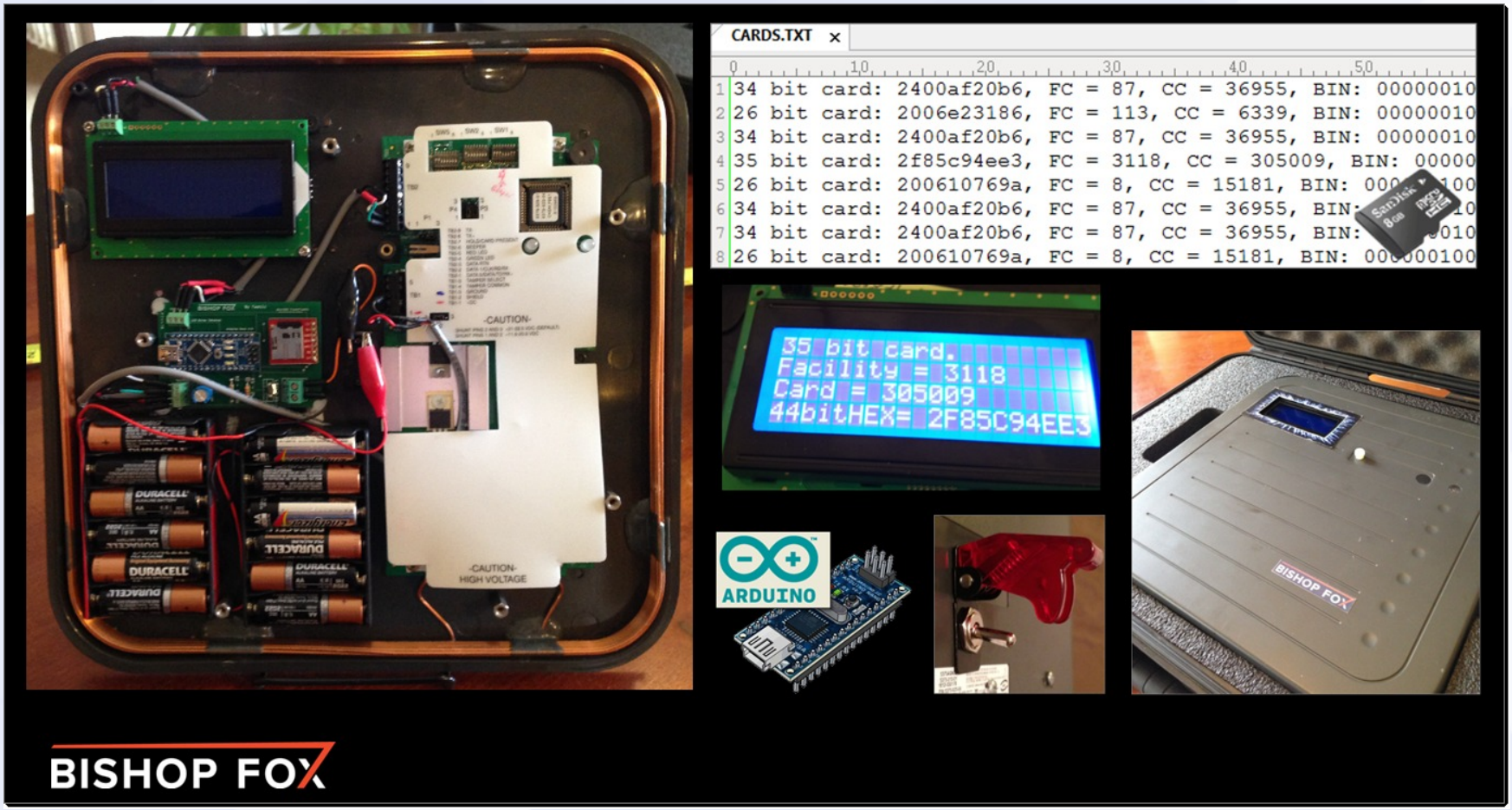
EM410x data

ASK po Manchester dekódování
0 0 1 0 1 1 1 1 0 1 0 1 1 1 1 0
1 1 1 1 1 1 0 0 0 1 1 1 0 0 1 1
1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1
1 0 0 0 0 0 1 0 0 0 1 0 1 1 1 1
0 0 1 0 1 1 1 1 0 1 0 1 1 1 1 0
1 1 1 1 1 1 0 0 0 1 1 1 0 0 1 1
1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1
1 0 0 0 0 0 1 0 0 0 1 0 1 1 1 1
0 0 1 0 1 1 1 1 0 1 0 1 1 1 1 0
1 1 1 1 1 1 0 0 0 1 1 1 0 0 1 1
1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1

EM410x UID

Terminator, data, parita
1 1 1 1 1 1 1 1 1
0 0 0 0	0	
0 0 0 1	1	
0 0 0 0	0	
1 0 0 0	1	
0 1 1 1	1	
0 0 1 0	1	
1 1 1 0	1	
0 1 1 1	1	
0 1 1 1	1	
1 1 0 0	0	

Tastic RFID pro HID Prox (1m dosah)



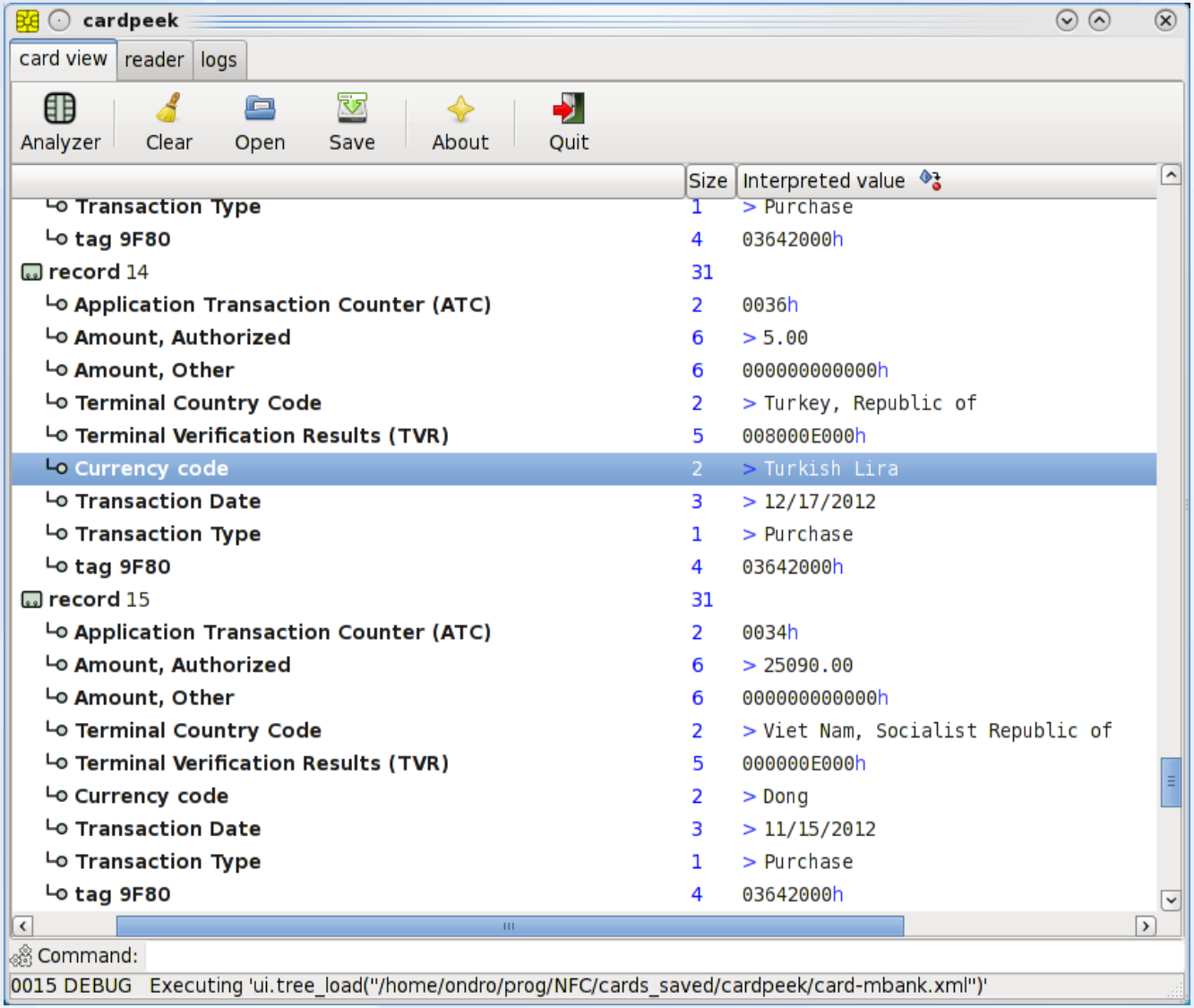
Platební karty (EMV)

- čip je většinou javacard
- ano, je to osekaná smartcard Java
- kolem 64-128 kB storage
- NFC obvod se připojuje k stejnému čipu jako kontaktní část
- jsou i NFC „nálepky“ bez kontaktní části

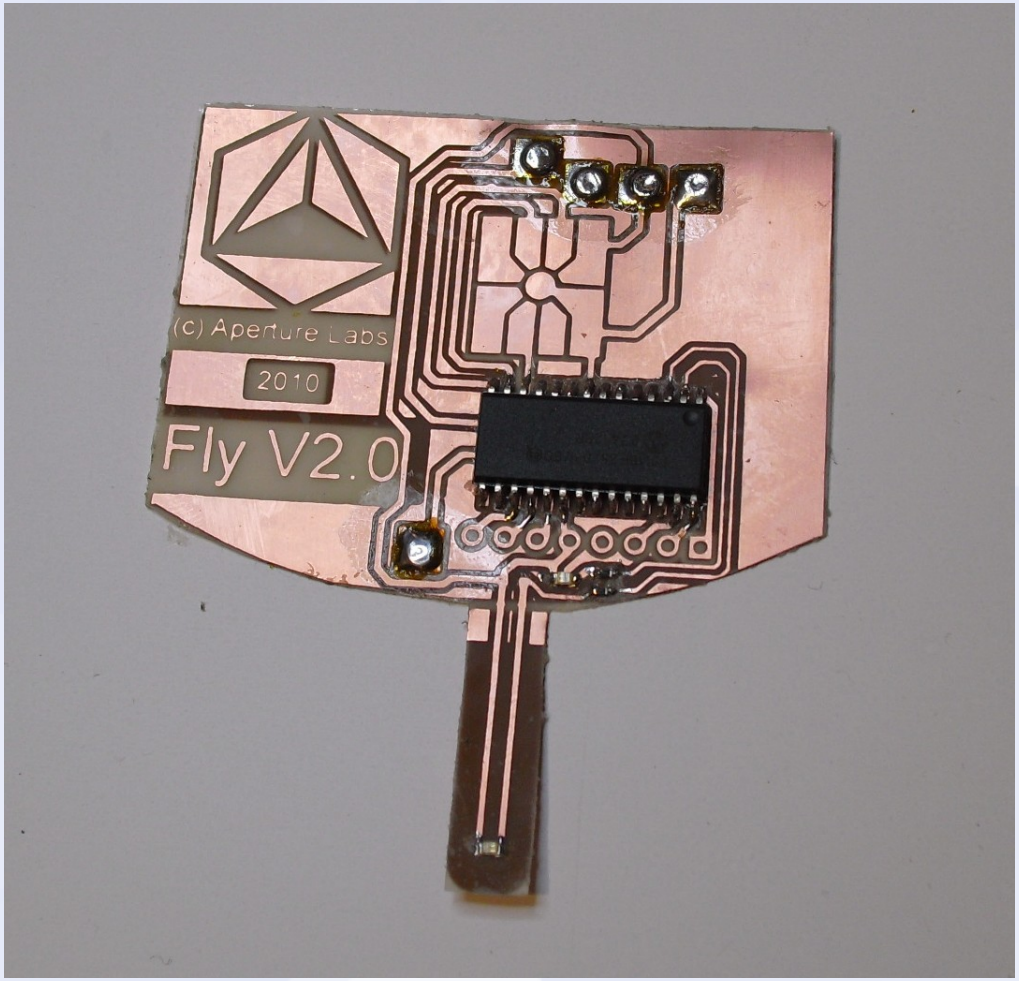
Komunikace smartkaret – APDU

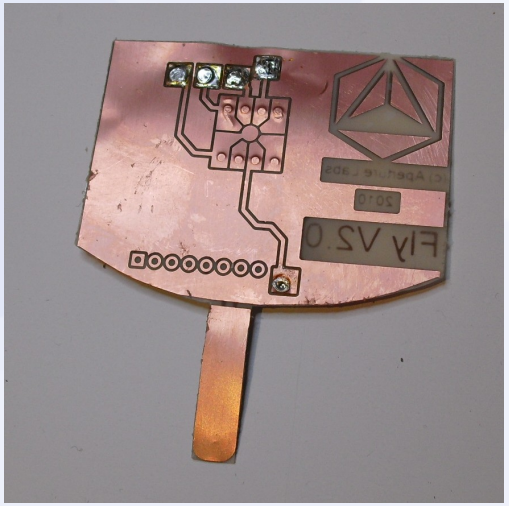
- APDU = „assembler“ smartkaret
- forma: **CLA INS P1 P2 [Lc] [Data] [Le]**
- CLA = class, 1 byte
- INS = opkód instrukce
- P1, P2 – parametry závislé na CLA/INS
- Lc, Data, Le – datové položky
- mnoho bichlí s referencí (EMV, SIM...)

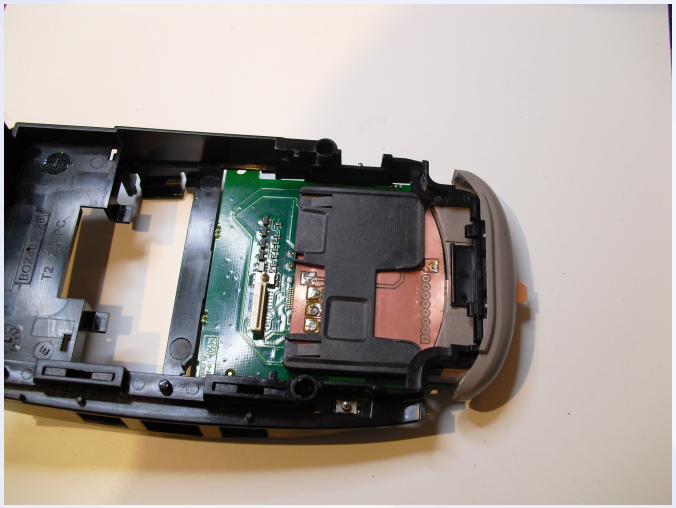
Co na EMV kartách je



EMV skimmer – MitM







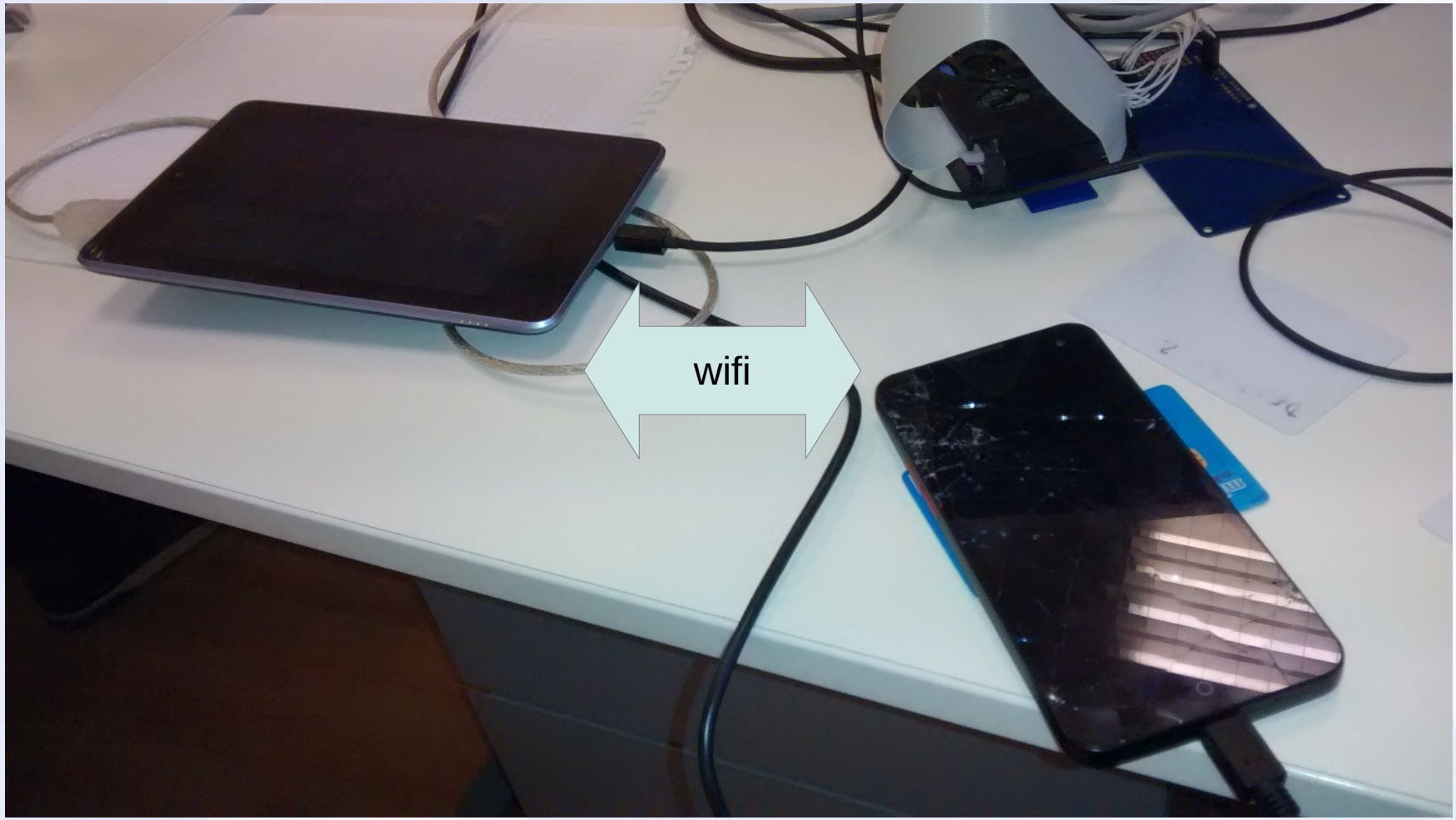
Vysokofrekvenční karty

- 13.56 MHz
- sdruženy pod standardy ISO 14443A/B, 18092, 15693
- lehce klonovatelné:
  - Mifare Classic, Mifare Ultralight
  - ISO 15693 (zatím nejsou „čínské magické“ s měnitelným UID)
- obtížně klonovatelné
  - Mifare Desfire, smartkarty

Jak dostat data na reverzování

- přímo sniffovat platby ze vzduchu lze
  - dost náchylné na chyby
  - platební karty mají dost mizerné antény
  - čipy mnoho žerou
- nejlepší je vyrobit „repeater“ nebo proxy

Lepší repeater



Androidí repeater/proxy

- telefony a tablety mají taky mizerné NFC antény
- vedlejší efekt wifi spojení – karta může být na druhém konci světa
  - ISO 14443 má jednu část velmi citlivou na časování (antikolize – naštěstí není podstatná)
  - zpracování samotných instrukcí (APDU) je naopak velmi časově benevolentní

Repeater z Raspberry Pi

Nahrání plateb

- Repeater postavený z Raspberry má mnohem lepší antény
  - Adafruit PN532
- opět by šlo rozšířit na 2 zařízení, které si budou forwardovat APDU přes internet
  - fixnul jsem to v libnfc, není ještě zamergováno
- APDU jdou ve vzduchu v plaintextu

Dekódovaní dat

- EMV je „napůl veřejné“
- část jak se má chovat terminál je veřejná
- zpracování na straně vydavatele karty a chování karty je tajné
- starší informace jsou někdy na čínských fórech leaknuté, zbytek je hádání
- paradoxně největší problém je přístup k terminálu na vyzkoušení

Dekódované instrukce platby

- Visa (3 instrukce)
  - SELECT AID „2PAY.SYS.DDF01“
  - SELECT VISA app (vrátí PDOL)
  - GET PROCESSING OPTIONS
- Mastercard (8 instrukcí)
  - 2x SELECT
  - GET PROCESSING OPTIONS
  - 4x READ RECORD (PDOL, pubkey, cert)
  - EXECUTE

PDOL

- Processing Options Data Object List
  - popisuje, co se posílá a podepisuje při platbě
- u Mastercard mnohem delší
  - obsahuje dvě verze pro online a offline – CDOL1, CDOL2 (Card Risk Management Data Object List)

Podepisování

- Visa karty používají pre-shared symetrický klíč, je nahrán na kartu od vydavatele
- Mastercard používá RSA na podepisování

VISA qVSCD PDOL

Velikost	Název	Tag
4	Terminal Transaction Qualifiers	9F66
6	Amount, Authorized	9F02
6	Amount, Other	9F03
2	Terminal Country Code	9F1A
5	Terminal Verification Result	95
2	Transaction Currency Code	5F2A
3	Transaction Date	9A
1	Transaction Type	9C
4	Unpredictable Number	9F37

Mastercard PDOL/CDOL1

Velikost	Název	Tag
6	Amount, Authorized	9F02
6	Amount, Other	9F03
2	Terminal Country Code	9F1A
5	Terminal Verification Result	95
2	Transaction Currency Code	5F2A
3	Transaction Date	9A
1	Transaction Type	9C
4	Unpredictable Number	9F37
1	Terminal Type	9F35
2	Data Authentication Code	9F45
8	ICC Dynamic Number	9F4C
3	Cardholder Verification Method results	9F34

VISA platba (GPO příkaz kartě)

Název	Hodnota	Význam
Terminal Transaction Qualifiers	83 21 36 20	typy protokolů
Amount, Authorized	40 00 00 00 00 00	40.0
Amount, Other	45 00 00 00 00 00	45.0
WTF???	00 00	
Terminal Country Code	02 03	Czech Republic
Terminal Verification Result	00 00 00 00 00	
Transaction Currency Code	02 03	CZK
Transaction Date	14 03 14	14. 3. 2014
Transaction Type	00	
Unpredictable Number	7c 9e d6 21	nonce

Odpověď VISA karty na GPO

Velikost	Název	Tag
18	Issuer Application Data	9F10
2	Cardholder Name	5F20
19	Track 2 Equivalent Data	57
1	Application Primary Account Number	5F34
2	Application Interchange Profile	82
2	Application Transaction Counter	9F36
8	Application Cryptogram	9F26
2	Card Transaction Qualifiers	9F6C

(obsah neukážeme, protože jsou tam citlivá data)

Lze s tím něco zajímavé dělat?

- nonce (unpredictable number) je jen 32-bit
  - birthday paradox u ~2^{16} plateb
- Visa application cryptogram jen 64-bit (!!!)
- přinutit kartu do „contactless magnetic stripe data“ módu nebo offline módu
- komunikace terminál↔karta končí dřív než se transakce ověří u vydavatele
- dCVV nemá žádné „unpredictable number“

Děkuji za pozornost

Ondrej Mikle • ondrej.mikle@gmail.com