Reverzování NFC EMV karet

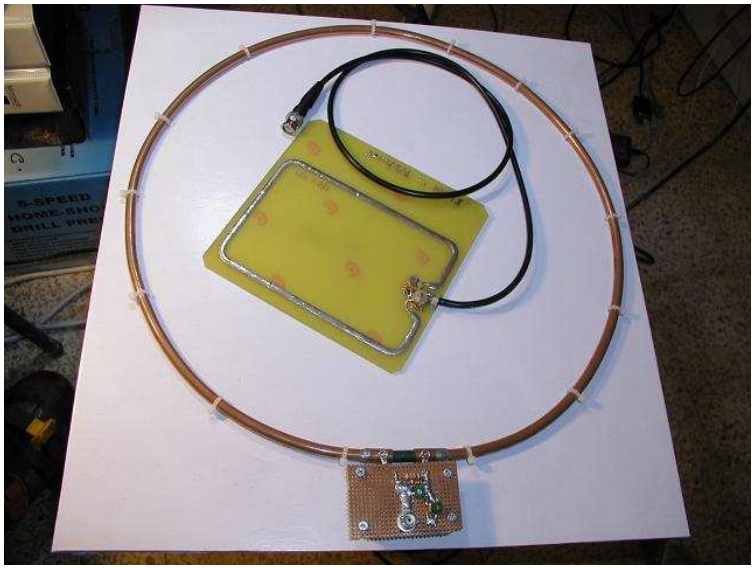
Ondrej Mikle • ondrej.mikle@nic.cz • 29.11.2014

Platební karty (EMV)

- čip je většinou JavaCard nebo Multos
- kolem 64-128 kB místa
- bezkontaktní část komunikuje protokolem ISO 14443A na 13.56 MHz
- NFC obvod se připojuje k stejnému čipu jako kontaktní část
- jsou i NFC „nálepky“ bez kontaktní části

Vzdálenost pro čtení a odposlech

- čtení z pasivního tagu (skimming)
  - 25 cm
  - ovlivněno velikostí a spotřebou tagu
- odposlech aktivní komunikace
  - 2.4 m
  - 18 m z vyšších harmonických
    - laboratorní podmínky



Mýtus „dvě karty vedle sebe se ruší“

- neplatí u ISO 14443 – má proces „antikolize“
- čtečka umí vybrat specifický tag

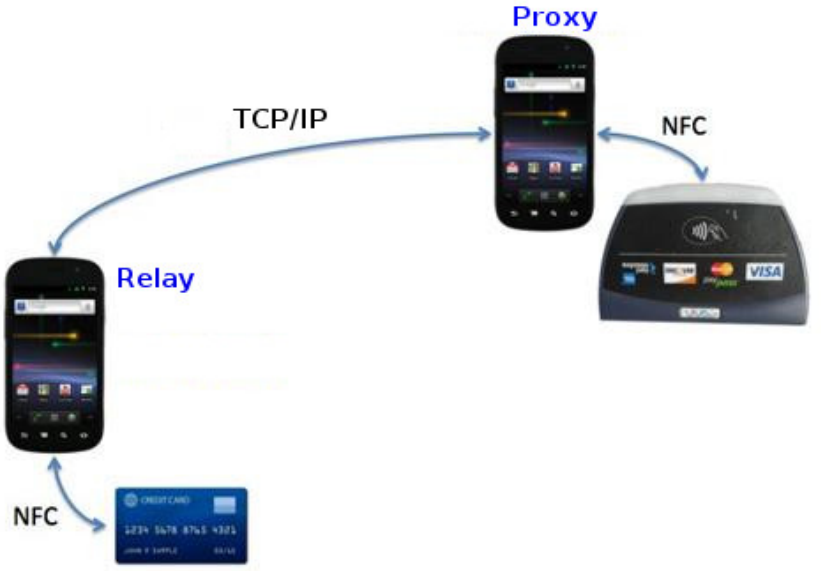
Zdroj	Data	Význam
čtečka	26 (7 bitů)	REQA
karta	44 00	ATQA
čtečka	93 20	SELECT – antikolize, kaskáda 1
karta	88 04 c2 4c 02	UID karty 4 byte + BCC 1 byte
čtečka	93 70 88 04 c2 4c 02 f3 08	SELECT 8804C24C + BCC + CRC
karta	04 da 17	SAK 1 byte + CRC 2 byte
...	...	... (kaskáda 2)

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
- např. SELECT, READ RECORD

Jak dostat data na reverzování

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



Lepší repeater

Androidí repeater/proxy

- vedlejší efekt TCP tunelu – karta může být na druhém konci světa
  - časování je velmi tolerantní
- telefony a tablety mají taky mizerné NFC antény
  - host card emulation funguje jen s některými chipsety

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
- APDU jdou ve vzduchu v plaintextu

Dekódovaní dat

- EMV je „napůl veřejné“
  - dost nepříjemná specifikace
- část jak se má chovat terminál je veřejná
- zpracování na straně vydavatele karty je tajné
- tip na nástroje:
  - dumpasn1, emvlab.org

Dekódované instrukce platby

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

PDOL

- Processing Options Data Object List
  - popisuje, co se posílá a podepisuje při platbě
- u Mastercard mnohem delší
  - obsahuje dvě verze – 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
???	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
  - na hraně
- downgrade na „contactless magnetic stripe data“ mód (MSD)

„Klonování“ karet (pre-play útok)

- terminálu budeme tvrdit, že nepodporujeme EMV mód
- způsobí fallback na MSD mód, který je povinný
- v MSD módu je unpredictable number jen 0-3 BCD číslice (Mastercard)
  - nejvíc 1000 možností
  - lze rychle enumerovat čtením z karty (1-2 minuty)

Simulace karty

- čtečka simulující kartu musí umět odpovědět na pár APDU instrukcí:
  - SELECT PSSE (statická odpověď)
  - SELECT payment application (statická odpověď)
  - GET PROCESSING OPTIONS (statická odpověď)
    - řekneme terminálu „neumím EMV přes NFC“ v AIP
  - READ RECORD magstripe (statická odpověď)
  - COMPUTE CRYPTOGRAPHIC CHECKSUM
    - 1000 možností CVC3 podle unpredictable number

Předgenerování odpovědí

- odpovědi na první čtyři instrukce stejné
- pro poslední instrukci se zeptáme karty na všech 1000 možností kryptogramu CVC3
- nyní máme všechna data potřebné k emulaci karty, můžeme ní alespoň jednou zaplatit
  - součástí CVC3 je i čítač transakce (ATC), který musí jít monotonně nahoru (banka jinak odmítne)
  - další transakce nám projde jenom když můžeme použít CVC3 s větším ATC než naposled

Děkuji za pozornost

Ondrej Mikle • ondrej.mikle@nic.cz