

A decorative graphic consisting of a thin yellow circle. A thick black left square bracket is positioned on the left side of the circle, and a thick yellow right square bracket is on the right side. A horizontal bar with a light green-to-white gradient is overlaid across the middle of the circle, containing the title text.

# Autentizace platební kartou

- zkušenosti z penetračních testů

Tomáš Rosa

[crypto.hyperlink.cz](http://crypto.hyperlink.cz)

# [ Osnova ]

---

- Základy technologie CAP/DPA
- Trojští koně vs. nepřipojené terminály (čtečky)
- Trojští koně vs. připojitelné terminály (čtečky)
  - Home-skimming
  - DoS
  - Sociální inženýrství
  - Firmware pod lupou



**Část první**  
**Základy technologie CAP/DPA**

# [ Technologie CAP/DPA ]

- Cílem je umožnit autentizaci identity klientů a původu bankovních příkazů pomocí existující infrastruktury čipových platebních karet.
- MasterCard – CAP (Chip Authentication Program)
- VISA – DPA (Dynamic Passcode Authentication)
- Dále se soustředíme zejména na internetové bankovníctví.
  - Poněkud stranou necháme problematiku 3-D Secure.

# [ Myšlenka využití EMV ICC ]

- Standard EMV pro čipové karty definuje jistou aplikaci s řadou služeb pro platební styk.
  - Jde o aplikaci ve smyslu ISO 7816-4.
- Pro účely CAP/DPA je využito zejména:
  - služby ověření off-line PIN (příkazy VERIFY),
  - služby online autentizace čipu karty (příkaz GENERATE AC).
- Ostatní služby hrají roli víceméně podružnou.
  - Jde například o metody SDA/DDA/CDA.

# [ Uspořádání aplikací na čipu ]

- Koncept CAP/DPA dovoluje
  - bud' sdílet tu samou aplikaci pro platební styk a pro elektronické bankovníctví,
  - anebo použít dvě do jisté míry nezávislé aplikace.
- Obvykle je prosazován koncept dvou aplikací s jistým datovým přesahem.
  - Sdílí se: off-line PIN, PAN, atp.
  - Nezávislé jsou: ATC, klíče pro autentizaci čipu, datové lokátory, atp.

# [ Slabiny základního konceptu ]

- Ačkoliv je bezpečnost CAP/DPA často kritizována [1], dosud nebyl publikován žádný útok, kterému by se dobře navržený systém nedokázal vyhnout.
  - Spíše než o útocích bychom zrovna v případě [1] mohli mluvit o implementačních doporučeních.
- I přes těsnou vazbu na EMV se řada útoků na platební systémy netýká CAP/DPA.

# [ CAP/DPA se **netýká** zejména ]

- Klasický skimming magnetického proužku.
- Útok na off-line PIN z Cambridge [7].
  - CAP/DPA totiž implicitně aplikuje účinné protiopatření, kterým je křížová kontrola kryptograficky chráněného vektoru CVR.





## **Část druhá**

### **Hrozby, které je radno zvážit**

# [ Koncept MITM a MITB ]

---

- Základní hledisko hodnocení jakékoliv bezpečnosti je dáno modelem hrozeb.
- Významnou hrozbou elektronického bankovníctví je aktivita škodlivého kódu.
  - Trojští koně, červi, viry, atp.
- Cílem je ovlivnit chování „důvěryhodné“ výpočetní platformy.
  - MITM – Man In The Middle
  - MITB – Man In The Browser (zvláštní případ MITM)

# [ Nepřipojená čtečka CAP/DPA ]

- Základní pravidla:
  - Náhodná výzva banky při přihlašování klienta
  - Ochrana sémantických kolizí
    - Kód CAP/DPA je použit k jiné operaci, než si klient myslí.
  - U platebního příkazu musí klient jasně vidět jeho data na displeji čtečky.
- Časté prohřešky:
  - Přihlašovací kód nezávisí na výzvě banky.
  - Autentizace identity a původu příkazů koliduje.
  - Uživatel vidí jen otisk platebního příkazu.

# [ Evoluce ]

---

- Bezpečné použití nepřipojené čtečky může někomu připadat příliš komplikované.
- Spásou se zdá být **připojitelná čtečka**.
  - Klient opisuje co nejméně údajů.
  - Místo opisování se klient soustředí na potvrzování.
- Nic však není samospasitelné.
  - Nová technologie obvykle eliminuje stará, avšak zároveň zavádí některá nová rizika...



# **Část třetí**

## **Bezpečnost připojitelné čtečky**

# [ Aplikační firewall ]

- Čtečka CAP/DPA je svého druhu most mezi počítačem klienta a jeho platební kartou.
  - Počítač však může být ovládán škodlivým kódem.
- Nějaký mechanismus – aplikační firewall – musí zabránit škodlivému kódu v přímé komunikaci s platební kartou.
  - Jinak hrozí obdoba skimmingových útoků, říkejme jim **home-skimming**.

# [ Realizace aplikačního firewallu ]

- Totální ochrana
  - Za žádných okolností nelze „skrz čtečku“ poslat APDU na vloženou kartu.
  - Čtečku nelze využít například pro elektronický podpis.
- Selektivní ochrana karty
  - Totální ochrana aktivována jen v případě pozitivní detekce platební aplikace na vložené kartě.
  - Rozumný kompromis.
- Filtrování jednotlivých příkazů APDU
  - Sází na rozpoznání, který příkaz lze bezpečně předat.
  - Úspěšně prolomeno na několika čtečkách.

# [ Home-skimming PoC ]

```
C:\WINDOWS\system32\cmd.exe - capscan.exe
C:\Eskimo\2010\Kauzy_projekty\CAP_DPA\CLAB\scardlab\debug>capscan.exe
home-skimming PoC ver. 01 started.

Timer setup: HighPart=0 LowPart=3579545, one tick is 0.279365 us.
PC/SC context successfully initialized.

-
```

```
C:\WINDOWS\system32\cmd.exe - capscan.exe
2F EF 2D E1 D3 C0 EF E5 15 FE E6 19 65 33 8C 09 A5 A3 DA 08 66 D1 03 A4 EA 69
2 2D 95 7D 48 C1 B2 9E AC 5A E6 B7 CA 85 4C 73 0A F5 29 FA 94 94 A4 DC B3 18 B3
B8 8A E8 07 F2 06 51 3B 56 03 7E BB B6 72 87 C5 B8 E1 8C BE 8E E5 2E FB 02 59 5
14 D9 0F FD C4 03 E6 63 74 BD 52 00 B5 CF 85 0A D8 E2 81 CC 90 00
Response: 70 81 93 93 81 90 67 45 F7 71 02 08 F1 75 EF 61 50 1F DD 2D BE AF BA
C 70 35 0E B7 FF 83 B3 0B 9D 38 95 35 5F 14 7C D1 46 8F 06 77 B2 E2 1A 42 89 CB
2F EF 2D E1 D3 C0 EF E5 15 FE E6 19 65 33 8C 09 A5 A3 DA 08 66 D1 03 A4 EA 69 8
2D 95 7D 48 C1 B2 9E AC 5A E6 B7 CA 85 4C 73 0A F5 29 FA 94 94 A4 DC B3 18 B3
8 8A E8 07 F2 06 51 3B 56 03 7E BB B6 72 87 C5 B8 E1 8C BE 8E E5 2E FB 02 59 51
14 D9 0F FD C4 03 E6 63 74 BD 52 00 B5 CF 85 0A D8 E2 81 CC 90 00

EMV skimming operation returned 564 bytes of data in 6 records.
Dumping to the file: hsdata\14.dta.
```



```

0001 0203 0405 0607 0809 0A0B 0C0D 0E0F 0123456789ABCDEF
000 7077 5F25 0309 0901 5F24 0312 0930 9F07 00w_%. . . . $ . . . 0ž.
010 02FF 805A 0854 1963 5973 5252 795F 3401 . '€Z.T.cYsRRy_4.
020 018E 1200 0000 0000 0000 0042 0141 0302 . Ž . . . . . . . . . . B . A . .
030 031E 031F 039F 0D05 F050 AC08 009F 0E05 . . . . . ž . . . dP . . . ž . .
040 0000 0000 009F 0F05 F078 AC98 008C 1E9F . . . . . ž . . . dx - □ . Š . ž
050 0206 9F03 069F 1A02 9505 5F2A 029A 039C . . ž . . ž . . . . * . š . š
060 019F 3704 9F35 019F 4502 9F34 038D 0691 . ž 7 . ž 5 . ž E . ž 4 . Ť . ˇ
070 0A8A 0295 059F 4A01 8270 0A5F 2802 0203 . Š . * . ž J . , p . _ ( . . .
080 9F42 0202 0370 5257 1354 1963 5973 5252 ž B . . . pRW.T.cYsRR
090 79D1 2092 0613 8350 8350 000F 5F20 1A4E yŇ ' . . . □ P □ P . . . . N
0A0 4F56 414B 2F50 4554 5220 2020 2020 2020 OVAK/PETR
0B0 2020 2020 2020 2020 209F 0802 0002 9F1F ž . . . . ž .
0C0 1831 3338 3335 3038 3335 3035 3933 3030 . 138350835059300
0D0 3030 3030 3030 3030 3070 2D8F 0104 9224 0000000000p-Ž . ' $
0E0 37D1 9E3C 76BE 1A9B ED35 1E1F E00D F377 7Ňž<vI' . >i5 . . ř . ów
0F0 86D3 C9BF D7E9 4D47 AC57 F9CC 742A FD10 tÓĚžxéMG-WŮĚt*ý.
100 8B14 8DE5 9F32 0103 7081 9390 8190 36BD < . Ť í ž 2 . . p □ ~ □ □ □ 6 ~
110 5042 2CF8 DB1C 2C6D 9619 C857 71F3 05C8 PB,řŮ . , m - . ČWqó . Č
120 F0E7 1639 D0E5 3AD2 5F85 500B 37A3 2889 dç.9DÍ:Ň _ . P . 7ł (%
130 FA73 5E76 4780 8670 0B96 0296 D1FD 5C6A ús^vG€+p . - . - Ňý \ j
140 C5A5 A5DD 4A40 55D4 2A29 211F AE5C 4C11 LĀĀŸJ@UŌ*) ! . @ \ L .
150 C59E A096 FAA4 0562 4B82 C320 2431 7F63 Lž - úw . bK , Ā $ 1 □ c
160 525C 119C E354 E4BD D9A7 4207 FCDB 36F4 R \ . š ā T ā ~ Ů Š B . ů Ů 6 ó
170 FE11 0BF7 403E EDEB 21F2 D27D 81CC 32DA t . . ÷ @ > i ē ! ň Ň } □ Ě 2 Ů
180 5450 ADFC B3BA 760D 5606 A03E 4D77 786D TP - ů ž v . V . > Mwxm
190 8BD3 A125 03C3 8181 F2AD A9ED 6BA2 7081 < Ó * % . Ā □ □ ň - @ i k ~ p □
1A0 9393 8190 6745 F771 0208 F175 EF61 501F ~ ~ □ □ g E ÷ q . . ň u d a P .
1B0 DD2D BEAF BA3C 7035 0EB7 FF83 B30B 9D38 Ÿ - l ž ž < p 5 . . □ ł . t 8
1C0 9535 5F14 7CD1 468F 0677 B2E2 1A42 89CB * 5 _ . | Ň F Ź . w _ á . B % Ě
1D0 2FEF 2DE1 D3C0 EFE5 15FE E619 6533 8C09 / d - á Ó Ť í . t č . e 3 Š .
1E0 A5A3 DA08 66D1 03A4 EA69 822D 957D 48C1 A Ľ Ů . f Ň . x e i , - - } H Ā
1F0 B29E AC5A E6B7 CA85 4C73 0AF5 29FA 9494 _ ž - Z c . Ě _ L s . ō ) ú ~ ~
200 A4DC B318 B3B8 8AE8 07F2 0651 3B56 037E x Ů ł . ł . Š č . ň . Q : V . ~
210 BBB6 7287 C5B8 E18C BE8E E52E FB02 5951 » q r + L _ á Š r Ž í . ů . Y Q
220 14D9 OFFD C403 E663 74BD 5200 B5CF 850A . Ů . ý Ā . é c t ~ R . μ Ď . .
230 D8E2 81CC Ě Ā □ Ě
  
```

## Zvýrazněno jest:

- Platnost od - do
- PAN
- Track 2 equiv. data
- Jméno držitele

# [ Útoky DoS ]

---

- Hrozí zejména vůči položce ATC (tag 9F36).
  - Jakmile čtečka zahájí (kvazi)platební operaci s kartou, je ATC nevratně a nevyhnutelně inkrementován.
  - Při dosažení hodnoty 65535 je daná aplikace CAP/DPA nevratně zablokována.
- Místem uplatnění jsou příkazy, které mohou během operace CAP/DPA selhat.
  - Například autentizace dat ve volném formátu, atp.
  - Obecně je také žádoucí, aby existoval nějaký druh příkazu „Abort“...

# [ Obrana proti DoS ]

- Vyjděme z předpokladu užitečnosti.
  - Útočník musí být schopen nepozorovaně zahájit (a nějak ukončit) řadu CAP/DPA operací.
- Opatřením je potom vhodně zapojit lidskou obsluhu (klienta).
  - Například po 10 automatických přerušeních je nutno vyjmout a znovu vložit kartu do čtečky.
  - Málokdo má trpělivost udělat toto několikrátisíkrát...
  - Navíc je aktivita škodlivého kódu rozpoznána klientem a nahlášena bance (coby reklamace).

# [ Sociální inženýrství ]

- Klient bude mít patrně velkou důvěru v data zobrazená na displeji čtečky CAP/DPA.
  - Pokud útočník dokáže toto médium infiltrovat, pak může zmást a ovládnout klienta.



# [ Opatření proti SI ]

---

- Důsledně používat kryptograficky chráněný protokol mezi bankou a čtečkou.
  - Příkladem budiž standard bank@home od MasterCard.
  - Různí výrobci mají i své proprietární metody (ze kterých bank@home mj. čerpal inspiraci).
  - Vhodná je nezávislá kryptologická expertiza.

# [ Firmware pod lupou ]

---

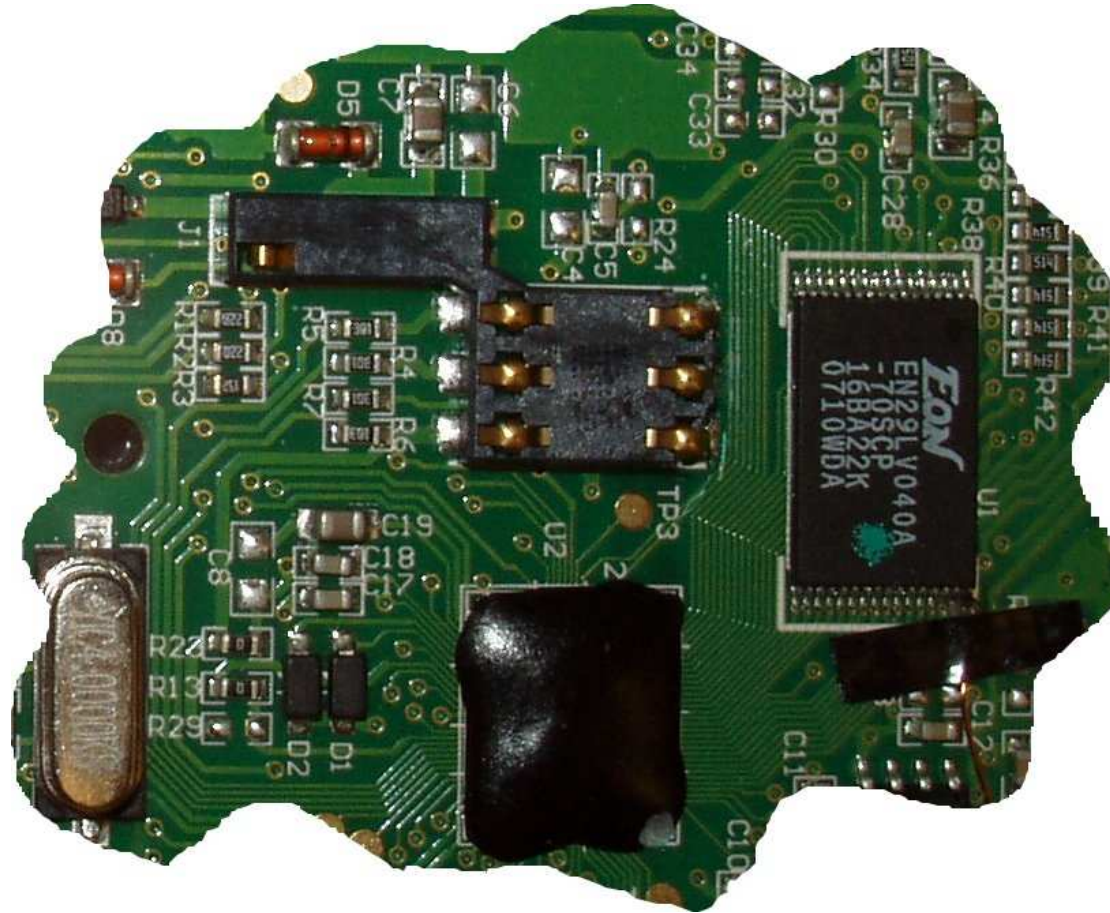
- HW i SW jakéhokoliv typu může obsahovat chyby.
  - Platí i pro čtečky CAP/DPA.
- Konstrukce čtečky by neměla umožnit jejich snadné hledání.
  - Toto samozřejmě není primární opatření, nýbrž vhodná doplňková ochrana.

# [ Příklad z praxe ]

---

- Jisté čtečky měly detašovanou Flash ROM s volně přístupnou sběrnicí.
  - Bylo možné snadno identifikovat načítání jednotlivých instrukcí obslužného programu.
  - Pomocí FPGA přípravku šlo sledovat jeho běh.
- Údajně se jednalo o marketingové vzorky.
  - Ostrá produkce detašovanou paměť nemá.
  - Jenže velká část kódu bude jistě společná a marketingové vzorky jsou široce dostupné...

# [ Marketingový vzorek... ]





# [ HW trojský kůň ]

---

- Aneb home-skimming jinou cestou.
- Cílem je výměna části nebo celé čtečky tak, aby útočník získal nechráněný přístup k čipové platební kartě.
  - Dnes poněkud futuristická představa, avšak pro cílené útoky jistě lákavá alternativa.
  - Je vhodné zamýšlet se už nyní nad možnou obranou.
  - Personalizovaný „pozdrav“ čtečky, kryptografická autentizace čipu mikrořadiče, atp.

# [ Závěr ]

- **CAP/DPA je bezesporu slibnou technologií.**
  - Mimo jiné nabízí těsnější propojení aplikací platebních karet a elektronického bankovníctví.
  - Při jejím zavádění však nelze sázet na „druhý pokus“, systém musí fungovat napoprvé, a to bezpečně.
- **Výše uvedené příklady nemají za cíl CAP/DPA deklasovat, ale upozornit na místa hodná pozornosti.**
  - Zde jsme se soustředili téměř výhradně na koncová zařízení.
  - Další aspekty se týkají personalizace karet, volby konkrétních schémat, atp. – těm jsou zase adresovány podrobné manuály karetních asociací [6], [8] a studie [1].

[ Děkuji za pozornost... ]

---



Dr. Tomáš Rosa  
[crypto.hyperlink.cz](http://crypto.hyperlink.cz)

# [ Zdroje ]

---

1. Drimer, S., Murdoch S.-J., and Anderson, R.: *Optimised to Fail: Card Readers for Online Banking*, Financial Cryptography 2009, <http://www.cl.cam.ac.uk/~sjm217/papers/fc09optimised.pdf>
2. EMV Integrated Circuit Card Specification for Payment Systems, Book 1 – Application Independent ICC to Terminal Interface Requirements, version 4.1, May 2004
3. EMV Integrated Circuit Card Specification for Payment Systems, Book 2 – Security and Key Management, version 4.1, May 2004
4. EMV Integrated Circuit Card Specification for Payment Systems, Book 3 – Application Specification, version 4.1, May 2004
5. EMV Integrated Circuit Card Specification for Payment Systems, Book 4 – Cardholder, Attendant, and Acquirer Interface Requirements, version 4.1, May 2004
6. MasterCard: Chip Authentication Program, soubor neveřejných standardů MasterCard
7. Murdoch S.-J., Drimer, S., Anderson, R., and Bond, M.: Chip and PIN is Broken, to appear at the 2010 IEEE Symposium on Security and Privacy, draft available at <http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf>
8. VISA: Dynamic Passcode Authentication, soubor neveřejných standardů VISA