Autentizace platební kartou
- zkušenosti z penetračních testů

Tomáš Rosa

crypto.hyperlink.cz

Praha, 20.5.2010 SmartCard Fórum 2010

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 bankovnictví.
  - 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
  - buď sdílet tu samou aplikaci pro platební styk a pro elektronické bankovnictví,
  - 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 bankovnictví 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

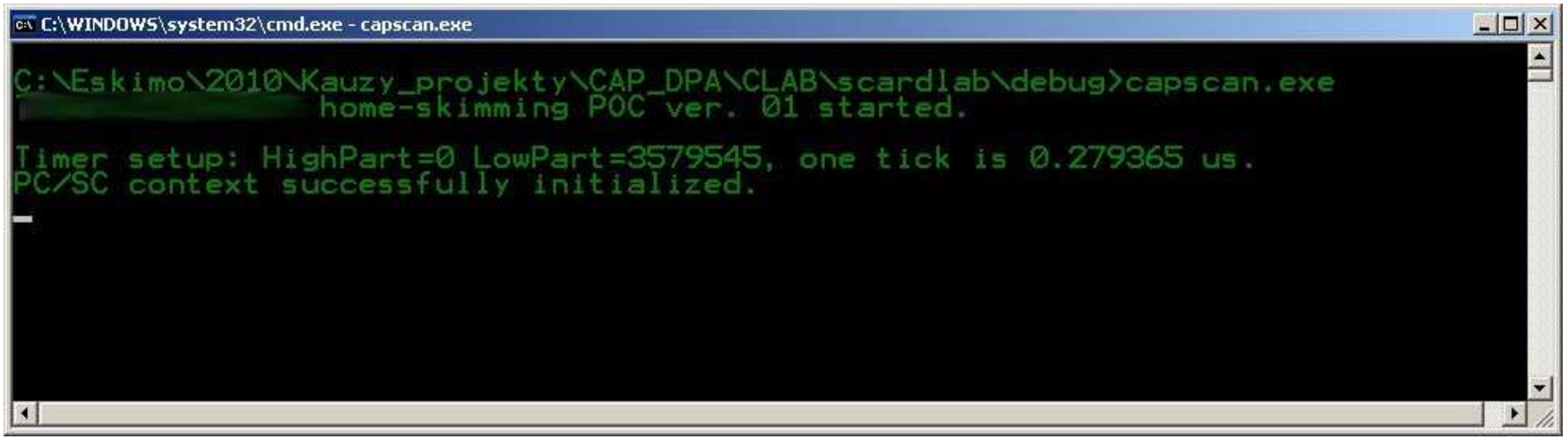
Aplikační firewall

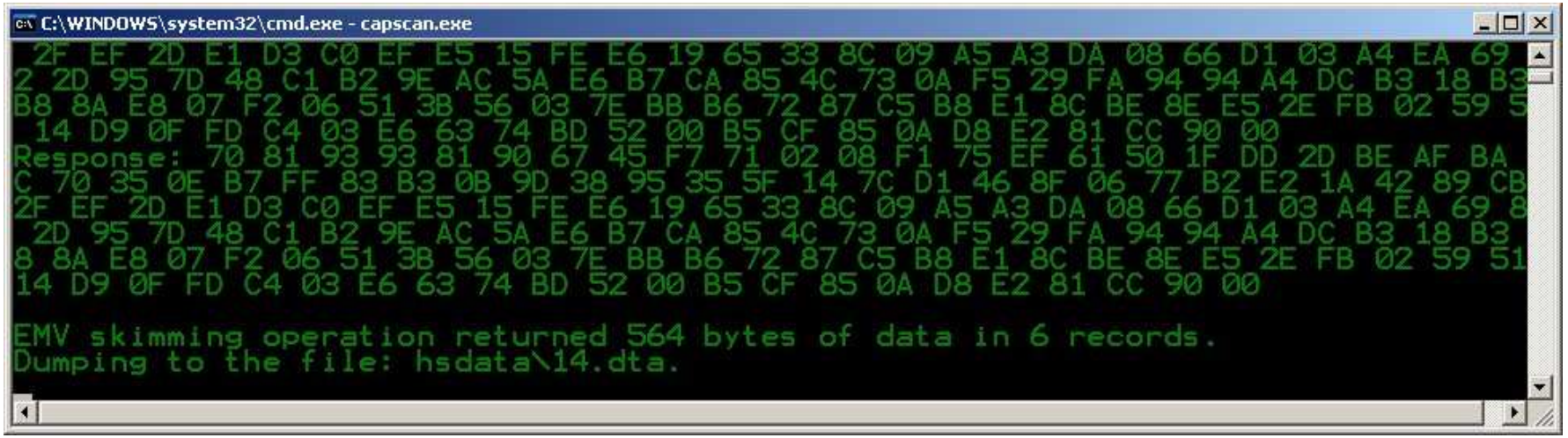
- Čtečka CAP/DPA je svého druhu most mezi počítačem klienta a jeho platební kartou.
  - Počítač však může být ovládán škodlivým kódem.
- Nějaký mechanizmus – aplikační firewall – musí zabránit škodlivému kódu v přímé komunikaci s platební kartou.
  - Jinak hrozí obdoba skimmingových útoků, říkejme jim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

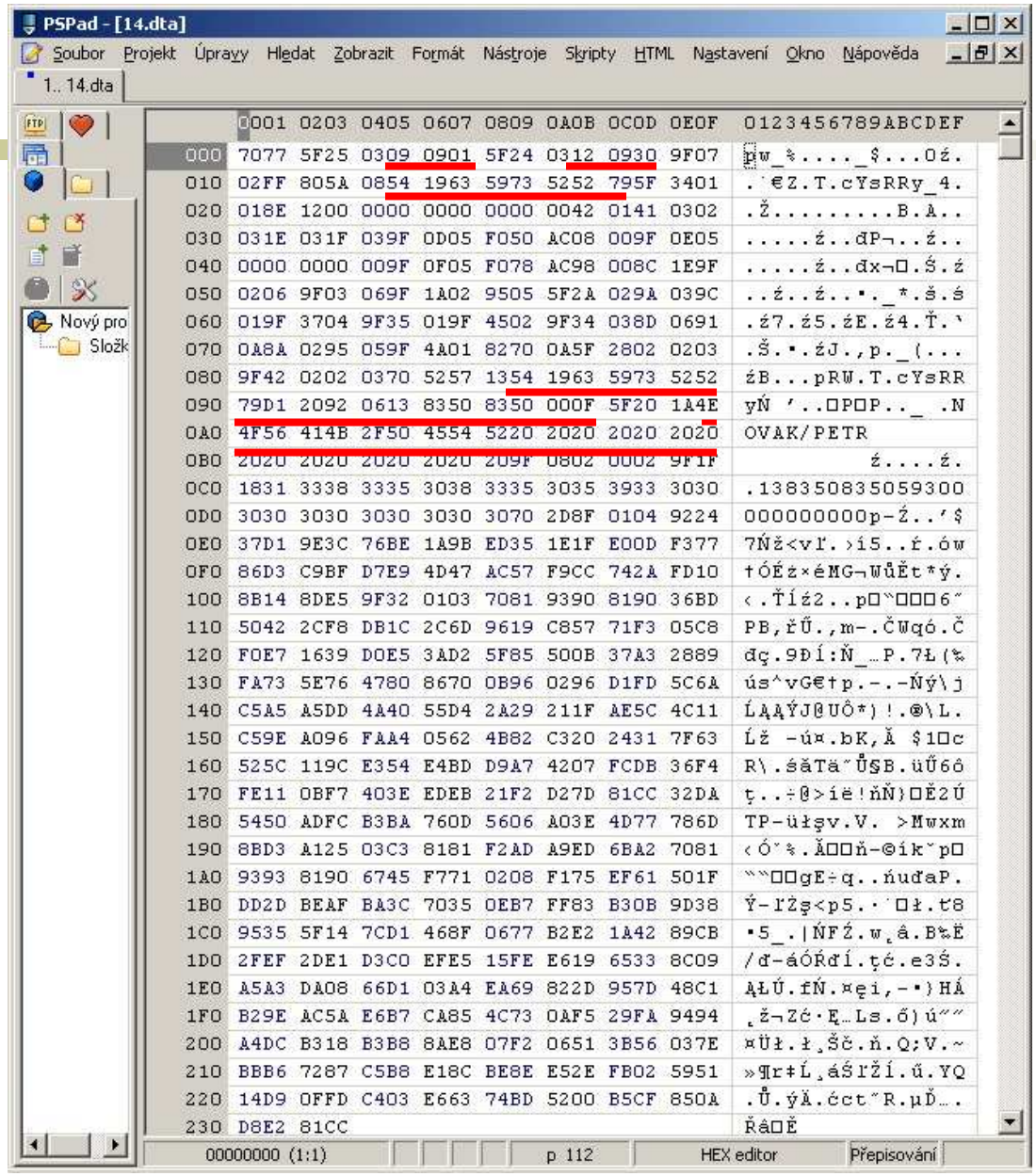
Realizace aplikačního firewallu

- 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







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 několiktisíckrát…
  - 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 bankovnictví.
  - 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

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