Nethemba
all about security

Nethemba s.r.o.

Bezpečnostná analýza zraniteľností slovenských a českých čipových RFID kariet založených na technológii Mifare Classic

Autori: Ing. Pavol Lupták, CISSP, CEH
Bc. Norbert Szetei

Dátum: 25. október 2009

Obsah

Zhrnutie

Analyzovali sme verejne používané karty na Slovensku a v Čechách založené na technológií Mifare Classic. Pomocou viacerých technologických postupov a na základe dostupných vedeckých publikácií sme prakticky demonštrovali možnosť kompletného získania prístupových kľúčov používaných na šifrovanie obsahu uvedených kariet.

Prakticky sme tiež overili možnosť plnej kontroly nad testovanými čipovými kartami vrátane kompletného prečítania, modifikácie a vyklonovania. Odhadli sme náklady na realizáciu samotného útoku ako aj navrhli vhodné bezpečnostné protiopatrenia – od najefektívnejších (kompletné stiahnutie zraniteľných kariet a nahradenie bezpečnejšími) až po menej efektívne (zviazanie UID karty s pasažierom, digitálne podpisovanie, „decrement counter“ riešenie).

Na demonštráciu závažnosti uvedenej zraniteľnosti a nevyhnutnosti súčasné karty prestať používať a nahradiť bezpečnejšími, sme vytvorili a zverejnili vlastnú implementáciu „offline nested“ útoku pomocou ktorého je možné útokom na kartu (bez použitia legitímnej RFID čítačky) získať všetky kľúče všetkých sektorov.

Ďalšie technické informácie ohľadom samotného útoku k dispozícii na:

https://www.nethemba.com/sk/research#zranitelnosti_v_mifare_kartach

Nethemba s.r.o. predstavuje spoločnosť certifikovaných bezpečnostných expertov zaoberajúcich sa širokým spektrom technologickej bezpečnosti od penetračných testov, detailných bezpečnostných auditov cez návrh a implementáciu ultrabezpečných systémov až po profesionálne bezpečnostné školenia, či konzultácie.

Zamestnanci Nethemba s.r.o. v minulosti odhalili a publikovali bezpečnostné zraniteľnosti v SMS lístkoch http://www.nethemba.com/SMS-ticket-hack4.pdf, ktoré prezentovali na viacerých svetových konferenciách:

- Confidence konferencia v Krakove / Poľsku
- Hacking At Random hackerskom kempe v Holandsku

1. História

Mifare Classic predstavujú čipové karty spoločnosti NXP Semiconductors, ktoré sa vďaka svojej nízkej cene masívne rozšírili po celom svete (súčasný odhad je niekoľko sto miliónov kariet v obehu). Na Slovensku a v Čechách sa uvedené karty používajú ako čipová električenka v Bratislave a v Prahe[1], univerzitné preukazy, ISIC preukazy, preukaz Slovak Lines, či parkovacie karty v platených parkoviskách.

Spoločnosť NXP už pred vyše rokom verejne priznala vážne kritické bezpečnostné zraniteľnosti v čipových kartách Mifare Classic[2].

Prvá verejná prezentácia Mifare zraniteľností bola už v roku 2007 na CCC konferencií v Berlíne p. Karstenom Nohlom[3].

Odvtedy sa bezpečnosťou Mifare kariet zaoberalo viacero výskumných tímov s najväčšou zásluhou tímu holandskej Univerzity Radboud Nijmegen, ktorí publikovali viacero vedeckých prác týkajúcich sa bezpečnosti čipových kariet Mifare Classic[4].

Holandskému výskumnému tímu sa ako prvému podarilo prakticky demonštrovať praktické zneužitie uvedenej karty na Londýnskej „Oyster“ karte používanou Londýnskym dopravným podnikom a v marci 2008 verejne publikovali uvedenú zraniteľnosť a popísali praktický útok[5].

Aj napriek tomu, že výrobca kariet NXP sa rozhodol zažalovať holandskú univerzitu za potenciálne finančné straty spojené so zverejnením uvedeného útoku, zvíťazili demokratické princípy a sloboda prejavu a Univerzita Radboud Nijmegen uvedený súdny proces vyhrala[6].

24.8.2009 firma Nethemba s.r.o. informovala hlavného dodávateľa slovenských Mifare kariet spoločnosť EMTEST, a.s. o uvedenej zraniteľnosti.

26.10.2009 firma Nethemba s.r.o. ako prvá na svete verejne publikovala funkčnú implementáciu „nested offline“ útoku pomocou ktorého je možné bez legitímnej čítačky s

---

1 V Pražskom DP bola nasadená bezpečnejšia technológia Mifare DESFire, staré OpenCard založené na zraniteľných Mifare Classic kartách sú ale naďalej akceptované

2 http://mifare.net/security/mifare_classic.asp

3 http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html

4 http://www.cs.ru.nl/F.Garcia/publications/Attack.MIFARE.pdf

http://www.cs.ru.nl/F.Garcia/publications/Dismantling.Mifare.pdf

http://www.cs.ru.nl/~flaviog/publications/Pickpocketing.Mifare.pdf

5 http://www.cs.ru.nl/B.Jacobs/PRESS/BBC-click-online-6-10-08.pdf

6 http://news.zdnet.co.uk/security/0,1000000189,39444421,00.htm

prednastavenými kľúčmi čisto „offline“ spôsobom zaútočiť na samotnú kartu a získať všetky kľúče pre všetky sektory.

Napriek všetkým verejne známym zraniteľnostiam Mifare Classic kariet a stanovisku ich výrobcu NXP, sú uvedené karty ale naďalej masívne používané ako na Slovensku, tak v Čechách.

2. Získanie prístupových kľúčov

Čipová karta Mifare Classic obsahuje 16 sektorov (prípad 1kB karty) alebo 40 (prípad 4 kB karty), každý sektor obsahuje 4 dátové bloky, pričom posledný dátovy blok v sektore obsahuje vždy prístupový kľúč A, prístupový kľúč B a samotné prístupové oprávnenia k jednotlivým blokom. Každá RFID čítačka, ktorá pristupuje k jednotlivých blokom musí mať nastavený správny prístupový kľúč. Samotný kľúč zabezpečuje, že čítačka má k danému sektoru povolený vždy presne definovaný prístup (buď na čítanie, zápis, inkrementovanie alebo dekrementovanie).

Overili sme dva odlišné spôsoby na získanie prístupových kľúčov na testovacích čipových kartách (Bratislavská električenka, Univerzitný STU preukaz a česká ISIC karta), pomocou ktorých bolo možné **získať všetky prístupové kľúče** do všetkých testovaných čipových kariet.

Odhalili sme, že funkčne odlišné karty (Bratislavská električenka, Univerzitný STU preukaz, preukaz Slovak Lines) od rovnakého dodavateľa (EMTEST, a.s.) používajú tie isté kľúče pre prvých 64 blokov (1024 bajtov), čo môže predstavovať ďalšie bezpečnostné riziko.

Získané kľúče pre naše testovacie karty po dohode so spoločnosťou EMTEST, a.s. v správe neuvádzame.

Je ich ale možné získať pomocou nášho zverejneného Mifare Classic „offline“ crackera.

2.1 Získanie kľúčov s použitím legitímnej RFID čítačky s prednastaveným kľúčom

V prípade, že je k dispozícií dostupná verejná RFID čítačka (terminál) s prednastavenými kľúčmi (prípad všetkých čipových električeniek, univerzitných preukazov atď), je možné získať kľúč odpočúvaním a prelomením zachytenej komunikácie medzi samotnou kartou a čítačkou. To sme realizovali na testovacích kartách pomocou špecializovaného zariadenia Proxmark III[7] s príslušnou vysokofrekvenčnou anténou. Zachytenie úvodnej komunikácie („challenge-response authentication“) stačí úplne k prelomeniu kľúču k sektoru, ku ktorému sa daná čítačka autentifikovala[8] .

Tento útok umožňuje získať kľúče iba k sektorom, ku ktorým pristupuje legitímna RFID čítačka, nie ku všetkým. Na vytvorenie funkčného klona je ale nevyhnutné získať všetky kľúče ku všetkým sektorom karty.

7 http://proxmark3.com/

8 http://code.google.com/p/crapto1/

2.2 Získanie kľúčov „offline“ útokom na samotnú kartu

Mifare Classic karty obsahujú množstvo rôznych bezpečnostných zraniteľností, ktoré umožňujú realizovať kompletný „offline“ útok bez potreby legitímnej RFID čítačky s prednastavenými kľúčmi[9].

Na demonštráciu závažnosti zraniteľností Mifare Classic kariet sme vytvorili a verejne publikovali vlastnú implementáciu „offline nested“ útoku (popísaný prvýkrát v publikácií „Wirelessly Pickpocketing a Mifare Classic Card[10], kapitola 4.4) pomocou ktorej je možné len útokom na samotnú kartu (bez potreby legitímnej RFID čítačky) získať všetky kľúče pre všetky sektory karty. Jediná podmienka na to, aby bolo možné útok úspešne realizovať a získať všetky kľúče je, aby samotná karta obsahovala minimálne jeden sektor šifrovaný „default“ kľúčom alebo tento kľúč bol dopredu známy. Na všetkých testovaných slovenských a českých kartách táto podmienka bola ale splnená a „offline nested“ útok vždy úspešne zbehol. V prípade, že by dané karty neobsahovali žiadny sektor šifrovaný „default“ kľúčom, stále je možné získať potrebný jeden kľúč odpočúvaním komunikácie medzi legitímnou RFID čítačkou a samotnou kartou (viď. predošlá sekcia) a potom realizovať „offline nested“ útok a získať všetky kľúče. Nicolas T. Courtois navrhoval vlastný multi-diferenciálny útok[11], kedy je možné aspoň jeden kľúč získať aj bez prelomenia komunikácie karty s legitímnou RFID čítačkou – tiež ide o „offline“ útok. Implementácia tohto útoku ale zatiaľ nie je zverejnená.

Tento útok umožňuje získať všetky kľúče ku všetkým sektorom, čo stačí na plnú kontrolu nad kartou (možnosť ju kompletne načítať, modifikovať, či vyklonovať).

9 http://www.cosic.esat.kuleuven.be/rfidsec09/Papers/mifare_courtois_rfidsec09.pdf
10 http://www.cs.ru.nl/~petervr/papers/grvw_2009_pickpocket.pdf
11 http://eprint.iacr.org/2009/137.pdf

3 Zneužitie čipovej karty

Znalosť uvedených kľúčov získaných buď odpočúvaním a prelomením komunikácie medzi kartou a legitímnou RFID čítačkou alebo „offline nested“ útokom umožňuje realizovať nad kartou nasledujúce druhy útokov:

- možnosť danú kartu kompletne načítať (v prípade fyzickej blízkosti cestujúcich vo verejných dopravných prostriedkov je možné získať kompletnú kópiu čipovej karty ľubovoľného cestujúceho, to znamená všetky informácie o ňom uložených na karte vrátane ich krstného mena, priezviska, študentského čísla, ..)
- možnosť modifikovať ľubovoľný sektor na karte (okrem nultého „read-only“ sektoru) a teda upraviť prípadný kredit na karte, meno vlastníka, alebo iné citlivé informácie
- možnosť vytvorenia 99.6% klonu karty (okrem nultého bloku v nultom sektore)
- možnosť vytvorenia 100% klonu karty (vrátane nultého bloku v nultom sektore) kompletnou emuláciou všetkých sektorov pomocou zariadenia Proxmark III

4 Náklady na prípadné zneužitie

V prípade, že útočník disponuje znalosťou prístupových kľúčov náklady na popisované zneužitie sú veľmi nízke – potenciálny útočník môže použiť ľubovoľnú lacnú RFID čítačku (prakticky sme overili Tikitag/Touchatag[12] v cene 30 € , čisté čipové Mifare Classic karty (trhová cena začína na 1 €/kus) a verejne dostupný softvér použiteľný na modifikáciu alebo klonovanie čipových kariet[13]. Náš implementovaný „nested offline“ útok bol vyladený a otestovaný na čítačkách Tikitag/Touchatag.

Náklady na získanie kľúčov pomocou zachytenia komunikácie medzi RFID čítačkou a čipovou kartou sú mierne vyššie – aktuálna cena zariadenia Proxmark III je $449[14].

Je nevyhnutné podotknúť, že **náklady na prípadne zneužitie potenciálnym útočníkom budú vždy klesať (nikdy nie rásť)** vďaka neustálemu zverejňovaniu novších a lepších rozbíjacích nástrojov ako aj znižovaniu ceny RFID hardvéru. Preto **pravdepodobnosť potenciálneho zneužitia bude s časom len narastať.**

12 http://www.touchatag.com/

13 http://www.libnfc.org/libnfc/examples/mftool

14 http://www.proxmark3.com/

5 Odporúčané spôsoby zabezpečenia

Vzhľadom na vážne implementačné chyby Mifare Classic kariet, **dôrazne odporúčame uvedené karty prestať vydávať a nahradiť ich bezpečnejšími** (napr. Mifare DESFire, na ktoré zatiaľ neboli publikované kritické zraniteľnosti).

Vzhľadom k tomu, že stiahnutie a nahradenie všetkých čipových kariet môže byť veľmi nákladné, uvádzame tiež čiastočne riešenia predstavujúce bezpečnostný kompromis, nakoľko nejde o plnohodnotné bezpečnostné riešenia.

Žiadne z týchto čiastočných riešení nedokážu ochrániť kartu voči prelomeniu kľúčov a kompletnému načítaniu citlivých údajov.

5.1 Zviazanie identity používateľa / pasažiera s UID sériovým číslom karty

Identitu každého používateľa karty / pasažiera odporúčame striktne zviazať s „read-only“ unikátnym identifikátorom karty (UID), čo predstavuje sériové číslo karty, ktoré je pri súčasných Mifare Classic kartách (zatiaľ) nemodifikovateľné.

Aby toto zviazanie bolo účinne, je nutné pri samotnej kontrole overovať, či dané UID je v systéme už zanesené a teda systém danú kartu pozná alebo ide o vyklonovanú kartu (tzv. „whitelisting“). Ďalšia možnosť je samotné UID karty použiť pri vytváraní digitálneho podpisu karty a následne ho overovať pri každej kontrole karty.

Vzhľadom k tomu, že pomocou Proxmark III je možné kompletne celú kartu odemulovať a je len otázka času, kedy budú na trhu nelicencované klony Mifare Classic s modifikovateľným nultým sektorom, silne odporúčame uvedené karty nepoužívať a nahradiť ich bezpečnejšími.

Treba podotknúť, že zviazanie identity používateľa / pasažiera s UID sériovým číslom jeho karty zabráni len prípadným lacným klonom, neznemožní ale útočníkovi modifikáciu karty (napríklad so zámerom obnoviť pôvodný kredit, teda pôvodnú kópiu karty).

5.2 Digitálne podpisy obsahu karty

Digitálne podpisy pomocou asymetrickej kryptografie výrazne znemožňujú modifikovať obsah čipovej karty. Bohužiaľ to ale neznamená, že karta je dokonale chránená - v prípade, že daná karta obsahuje „kredit“ v akejkoľvek forme, útočník dokáže pri nabitom stave získať jej kompletnú kópiu (tzv. „snapshot“ vrátane platného digitálneho podpisu), kartu použiť, kredit minúť a opätovne uvedenú kópiu obnoviť. V praxi to znamená, že aj napriek útočníkovej neznalosti daného digitálneho podpisu, útočník dokáže ovplyvňovať kredit podľa vlastnej ľubovôle a teda použitie akýchkoľvek digitálnych podpisov sa stáva neúčinné. Jediné riešenie, ktoré môže trvať niekoľko dní, je uvedené správanie odhaliť

centrálnou kontrolou (nakoľko nebude sedieť stav kreditu cestujúceho na karte a v centrálnom systéme) a zablokovať UID príslušnej vyklonovanej karty na všetkých koncových RFID čítačkách, čo môže byť veľmi pracné. V tomto prípade je ale nevyhnutné, aby jednotlivé čítačky overovali, či karta s daným UID je platná alebo nie, prípadne používali UID karty pri vytváraní digitálneho podpisu.

Aj napriek tomu, že identita cestujúceho bude zviazaná s UID karty a bude použité digitálne podpisovanie obsahu karty, stále hrozí reálne riziko zneužitia karty – t.j. útočník dokáže opätovne získať povodný kredit karty obnovením kópie karty, ktorá bola vytvorená pri plnom kredite. Toto riziko môže byť čiastočne eliminované centrálnou kontrolou, pokým ale uvedená kontrola nie je „online“, teda okamžitá, stále je priestor pre útočníka na potenciálne zneužitie.

Neodporúčame používať proprietárne algoritmy na vytváranie digitálneho podpisu, ani hashe, na ktoré sa objavili už kolízie (MD5, SHA1), ale bezpečné (Blowfish, SHA-2). Vzhľadom na kapacitné možnosti karty, v prípade asymetrického šifrovania odporúčame použiť algoritmy, ktoré používajú kratšie kľúče (napr. ECC[15]).

5.3 “Decrement counter” riešenie

Predstavuje riešenie, ktoré kombinuje výhody predošlých dvoch riešení a súčasne implementuje na karte špeciálne „počítadlo“, ktorého hodnotu je možné len načítať a dekrementovať (to je zabezpečené pomocou špeciálnych oprávnení kľúčov A/B, ktoré žiadne iné operácie nad uvedeným počítadlom neumožňujú). Súčasne je na karte zabezpečené, že uvedené oprávnenia kľúčov A/B je nemožné upravovať. Počítadlo je pri vydaní karty nastavené na maximálnu hodnotu (0xffffffff), pri každej autorizovanej operácií (dobitie, platba, zmena kreditu) je dekrementované. Celý obsah karty je digitálne podpísaný (pomocou kľúča, ktorým disponuje iba vydavateľ karty), pri digitálnom podpise sa ale tiež uplatňuje UID karty (znemožňuje jednoduché vyklonovanie) a „decrement counter“ (znemožňuje vytvorenie kópie karty a jej znovu obnovenie, nakoľko nie je možné obnoviť pôvodnú hodnotu počítadla).

Napriek tomu, že uvedené riešenie chráni kartu proti neautorizovanej modifikácii či klonovaniu, toto riešenie je ale neúčinné voči:

- kompletnému prelomeniu kľúčov a načítaniu celej karty (a citlivých informácií, ako krstné meno, priezvisko, či rodné číslo)
- proti 100% emulovanej karte pomocou zariadenia Proxmark III
- proti ďalším implementačným chýbam Mifare Classic, ktoré sa môžu objaviť v budúcnosti a budú umožňovať obnovenie pôvodnej hodnoty počítadla

15 http://en.wikipedia.org/wiki/Elliptic_curve_cryptography

6 Záver

Naša realizovaná analýza ukázala, že veľká časť čipových kariet na Slovensku a v Čechách používa zraniteľnú technológiu Mifare Classic, ktorej bezpečnostnú ochranu je možné kompletne prelomiť a získať kľúče ku všetkým sektorom danej karty, čo je možné následne zneužiť na kompletné načítanie karty, jej modifikáciu alebo vyklonovanie.

Zviazanie identity používateľa s UID sériovým číslom karty síce znemožní vytvárať jednoduché klony, nezabráni ale modifikácii obsahu karty a jej kompletnému načítaniu a odemulovaniu.

Digitálne podpisovanie obsahu síce znemožní modifikáciu obsahu karty, nezabráni ale jeho klonovaniu (pokým UID karty nebude súčasť digitálneho podpisu), vytvoreniu kópie karty (vrátane digitálneho podpisu) a jej opätovnému obnoveniu, kompletnému načítaniu karty a odemulovaniu.

„Decrement counter“ riešenie síce zabráni modifikácii obsahu karty a jej klonovaniu, nezabráni ale kompletnému načítaniu a odemulovaniu.

Preto za najbezpečnejšie riešenie pokladáme kompletné stiahnutie zraniteľných Mifare Classic kariet a ich nahradenie za bezpečnejšie.