elektrorevue
ISSN 1213 - 1539

Rok / Year:	Svazek / Volume:	Číslo / Number:	Jazyk / Language
2019	21	1	CZ

Bezpečnost autentizačních systémů založených na kartách Mifare Classic a ověřování pomocí UID

Security of authentication systems based on Mifare Classic and UID verification

Tomáš Lieskovan

tomas.lieskovan@vut.cz

Fakulta elektrotechniky a komunikačních technologií VUT v Brně

DOI: -

Abstract: The article describes the technology of user authentication using Mifare Classic access cards. As an introduction, the types of access cards are presented and then the most common access cards Mifare Classic, their security mechanisms and attack possibilities, are explained. The principle of authentication systems using the invariant UID, as the main security mechanism, the pitfalls of this system, and an attack on the UID-changeable card, in three possible ways, are explained in more detail.

elektrorevue
ISSN 1213 - 1539

Bezpečnost autentizačních systémů založených na kartách Mifare Classic a ověřování pomocí UID

Ing. Tomáš Lieskovan

Fakulta elektrotechniky a komunikačních technologií VUT v Brně
Email: tomas.lieskovan@vut.cz

Abstrakt *– Článek přibližuje technologii autentizace uživatelů pomocí přístupových karet Mifare Classic. Na úvod jsou představeny druhy přístupových karet a následně je vysvětlena problematika nejrozšířenějších přístupových karet Mifare Classic, jejich bezpečnostní mechanismy a možnosti útoku. Blíže je vysvětlen princip autentizačních systémů používající neměnný identifikátor karty UID jako hlavní bezpečnostní mechanismus, úskalí tohoto systému a je demonstrován útok pomocí karet se zapisovatelným UID třemi možnými způsoby.*

1 Úvod

Při výběru autentizačního mechanismu uživatelů jsou vždy brány v potaz požadavky na bezpečnost, praktičnost, rychlost, cenu a složitost implementace do stávajícího systému. Každá organizace či firma klade důraz na jiný požadavek a tak situace často dopadá, že bezpečnost ustupuje ceně, popřípadě náročnosti implementace do stávajícího systému. Tyto ústupky při volbě autentizačního mechanismu poté mohou vést až k drastickým bezpečnostním trhlinám [1].

Častou situací u velkých institucí je využívání autentizačních mechanismů, které byly implementovány již před mnoha lety. Nezřídka se stává, že je implementováno řešení, které již v době instalace nevyužívá všechny své bezpečnostní technologie. V tomto případě může být spoléháno na to, že útočník nedisponuje potřebným technickým vybavením a útok tedy není možné provést. Postupem času se vybavení útočníka zlepšuje, spoléhat tedy na technicky obtížně proveditelný útok je velmi lehkomyslné. Tento článek si klade za cíl přiblížit technologii autentizace pomocí karet Mifare Classic, její bezpečnostní mechanismy a možné zneužití chybné implementace, spočívající zejména v ověřování uživatelů na základě neměnného identifikátoru UID.

2 Mifare

Historie karet Mifare sahá až do roku 1994, kdy firma Philips tyto karty začala vyrábět. Nejstaršími produkty firmy z této doby jsou Mifare Classic (v té době nejrozšířenější po celém světě), dále Mifare Pro, obsahující 3DES (Triple DES) koprocesor a v roku 1999 již byla vyráběna karta Mifare PROX obsahující PKI (Public Key Infrastructure) koprocesor. V roce 2001 přišly Mifare Ultrlight a o rok později DESfire splňující normu ISO 14443A [2].

Tabulka 1: Porovnání karet Mifare Classic.

Název Karty	Velikost paměti	Počet sektorů
Mifare mini	320 bajtů	5
Mifare 1K	1024 bajtů	16
Mifare 4K	4096 batů	40

2.1 Mifare Classic

Mifare Classic jsou jedny z nejstarších karet na světě. Bezkontaktní karty Mifare Classic operují na pracovní frekvenci 13,56 MHz a jsou dostupné ve třech variantách (viz tabulka 1): 1K, 4K a mini [3].

Pro většinu karet Mifare Classic platí, že první 4 bajty jsou vyhrazeny pro identifikátor karty (UID) a zbytek sektoru 0 bloku 0 obsahuje informace definované výrobcem. Tato data jsou chráněna proti přepsání a jsou na tvrdo zapsána do paměti Mifare karty při procesu výroby. Struktura nultého sektoru je vyobrazena na Tabulce 2. Pro speciální účely jsou vyráběny Mifare Classic karty, které využívají celkem 7 bajtů pro UID identifikátor karty [4]. Těmito kartami se ale článek zabývat nebude.

Paměť karty Mifare Classic 1K je rozdělena do 16ti sektorů, každý z těchto sektorů je rozdělen do čtyř 16bajtových bloků. Sektory 1 až 15 jsou rozděleny na čtyři bloky, kde bloky 0,1 a 2 jsou určené pro data. Blok 3 uchovává klíč A, bity přístupu a klíč B [3].

Sektor 0 je od ostatních sektorů odlišný. Blok 0 je rozdělen na první čtyři bajty reprezentující číslo karty (UID), následující bajt slouží jako kontrolní. Ostatní bajty obsahují tovární data.

2.2 Mifare DESfire

Druhou nejrozšířenější kartou je Mifare DESfire, která byla poprvé uvedena v roce 2002 ve své první verzi EV1. Jedná se o aktualizaci velmi úspěšné karty Mifare Classic, pracující na stejné frekvenci a disponující pokročilými hardwarovými i softwarovými funkcemi. Karty se vyrábí ve třech paměťových kapacitách 2 kB, 4 kB a 8 kB. Karty DESfire obsahují kryptografický koprocesor podporující šifrování DES a AES-128. Karta zároveň umožňuje generování náhodných čísel, což umožnilo rozvoj a implementaci nových

elektrorevue
ISSN 1213 - 1539

Tabulka 2: Struktura nultého sektoru karet Mifare 1K [4].

Číslo bajtu	**0**	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Blok 0	UID				X	Tovární data											
Blok 1																	
Blok 2																	
Blok 3	Klíč A						Bity přístupu					Klíč B					

Tabulka 3: Přehled šifrovacích algoritmů karet Mifare [3].

Typ karty	**crypto1**	**3DES**	**AES**	**PKE**
Mifare Ultralight				
Mifare Ultralight C		✓		
Mifare Classic mini	✓			
Mifare Classic 1K	✓			
Mifare Classic 4K	✓			
Mifare Plus	✓		✓	
Mifare DESFire		✓	✓	
Mifare ProX	✓	✓		✓
SmartMX	✓	✓	✓	✓

kryptografických algoritmů. Kompletní přehled je znázorněn na tabulce 3.

3 Zabezpečení karet Mifare Classic

Karty Mifare Classic již od svého vydání umožňují podmíněný přístup k hodnotám v blocích. Klíče A a B jednotlivých sektorů umožňují čtení nebo zápis do těchto sektorů pouze za předpokladu znalosti správného klíče.

3.1 Proudová šifra CRYPTO1

Proprietární algoritmus CRYPTO1, vyvinut firmou NXP, zajišťuje zabezpečení informací v čipu Mifare Classic. Tento algoritmus nebyl nikdy zveřejněn, nicméně o rekonstrukci se již mnoho výzkumníků pokusilo a již se podařilo sestavit funkční model algoritmu. V principu se jedná o proudovou šifru s posuvným registrem s délkou 48 bitů. Dále je v čipu implementován 32 bitový pseudonáhodný generátor čísel, který ale nepracuje s prvními 16ti bity, jedná se tedy pouze o 16 bitový generátor [5].

3.2 Autentizace a inicializace šifrování

K tomu, aby se karta dozvěděla, že je čtečka připravena na proces autentizace, je potřeba zaslat příkaz AUTH. Následuje autentizace v tomto pořadí [5]:

1. Terminál nešifrovaně zašle žádost s číslem bloku a typem klíče (A nebo B), kterým se chce autentizovat
2. Karta vygeneruje pomocí pseudonáhodného generátoru hodnotu, kterou spolu s UID odešle terminálu jako výzvu. Obě strany od teď znají šifrovací klíč. Mezi tím zapíše klíč do registru a spočítá odpověď terminálu.
3. Terminál vygeneruje svoji výzvu a spočítá odpověď na výzvu karty a obojí odešle kartě.
4. Karta příjme výzvu a odpověď a provede dešifrování. Pokud je odpověď terminálu shodná s vypočítanou odpovědí, autentizace byla úspěšná.

4 Útoky na Mifare Classic

První Mifare Classic karty přišly na trh již koncem 20. století. Od té doby bylo nalezeno mnoho bezpečnostních zranitelností.

4.1 Útok hrubou silou

První možností je útok hrubou silou, tzv. brute-force. Útočník odhaduje přístupová hesla a zkouší přečíst některý sektor. Pokud uvažujeme nejhorší případ, že se hledaný klíč nachází na konci testovací množiny o velikosti 2^{48} a zároveň, že vyzkoušení jednoho přístupového klíče trvá 25 ms, by nalezení takového klíče trvalo přibližně 223 tisíc let. Útok hrubou silou tedy není z časového hlediska proveditelný.

4.2 Pseudonáhodný generátor

Karty Mifare Classic obsahují pseudonáhodný generátor, určený ke generování náhodných výzev. Tento generátor má za úkol generovat 32 bitů dlouhé číslo, avšak generuje pouze druhou polovinu tohoto čísla, tedy se jedná pouze o množinu čísel 2^{16}. Aby toho nebylo málo, po zapnutí napájení čipu se generátor nastaví do původního konkrétního stavu, to znamená, že je možné manipulovat generátorem pomocí časové odezvy mezi sepnutím napájení a přijatou výzvou [6].

4.3 Zachycení klíče

Tato metoda se také nazývá Key Recovery Attack a využívá slabiny lichých bitů v posuvném registru. Výzkumníci Gerhard de Koning Gans a Roel Verdult z univerzity Radboud University Nijmegen ve svém článku demonstrují, jak lze tento útok provést. Využívají k tomu zařízení Proxmark 3 s anténou, kterou je nutné vložit mezi terminál a kartu [5].

4.4 Útok postranními kanály

Další metodou je útok pomocí postranních kanálů. Karty Mifare jsou kartami bezkontaktními, to znamená, že po-

elektrorevue
ISSN 1213 - 1539

třebnou energii je nutné čipu dodat pomocí elektromagnetického pole, které čtečka generuje. To umožňuje velmi efektivně měřit proudovou spotřebu procesoru karty při vykonávání výpočetně náročných instrukcí (typicky XOR) bez jakéhokoli zásahu do vnitřního uspořádání.

5 Bezpečnost autentizačních systémů založených na ověřování UID

Karty Mifare 1K, 4K a mini obsahují v prvním sektoru továrně nastavené UID karty. Toto UID je neměnné a vždy náhodně generované. Množina těchto hodnot se sestává z $2^{32} = 4294967296$ kombinací. To je poměrně dobrá množina možných hodnot. V případě využití těchto karet podnikem nebo organizací o 1000 přístupových kartách je pravděpodobnost kolize karty se stejným UID z jiného karetního systému přibližně 1 : 4294967, což je hodnota, kterou můžeme označit za bezpečnou.

Systémy založené na ověřování UID karty zašlou kartě výzvu, aby zjistily UID. Karta odpoví svou výzvou, která obsahuje UID. Toto UID je v koncovém systému spárováno s konkrétním uživatelem, který má v systému přidělena konkrétní práva. Na základě těchto informací je poté uživateli přístup povolen nebo zamítnut. Vzhledem k tomu,

Obrázek 1: UID měnitelné Mifare 1K karty a čipy.

že karty Mifare sektor 0 blok 0 mají neměnný, tento systém nepočítá s podvržením UID. Na trhu se ale objevují speciální typy Mifare karet, které mají sektor 0 blok 0 zapisovatelný. Některé přímo, některé pomocí tzv. backdooru. Tímto pojmem se rozumí speciální instrukce naprogramovaná výrobcem(typicky 0x60 [7]), která odemkne sektor 0 blok 0 k zápisu a tím umožní pozměnit UID karty. Ukázka běžně dostupných karet je na Obrázku 1.

Nebezpečí této slabiny je zejména v tom, že s dnešní dostupností hardwarových nástrojů je velmi levné sestavit čtečku / zapisovačku UID, popřípadě zcela zdarma využít nějakou již dostupnou aplikaci pro mobilní telefony vybavené technologií NFC. Tyto telefony již také umožňují tzv. emulaci Mifare karet, to znamená, že se telefon chová jako Mifare karta a autentizuje se proti terminálu.

5.1 nfctool + ARC122U

Nejdostupnější variantou je využití čtečky / zapisovačky ARC122U s rozhraním USB. ARC122U je potřeba připojit do počítače s operačním systémem Linux a nainstalovat balíček *nfclib* [8]. Celý proces spočívá v načtení obsahu celé karty do souboru a následném zápisu obsahu souboru do nové karty. Uložení obsahu karty lze provést pomocí:

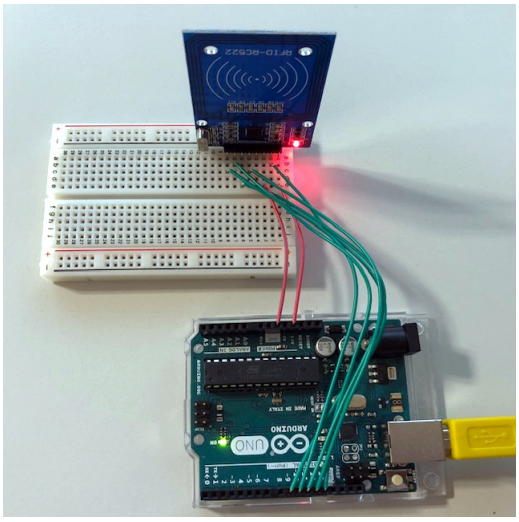
```
nfc-mfclassic R a u /tmp/mifare1k.dmp
```

Po přiložení nové karty ke čtečce provedeme zápis pomocí příkazu:

```
nfc-mfclassic W a u /tmp/mifare1k.dmp
```

Tím jsme docílili vytvoření duplicitní karty i s totožným obsahem.

5.2 Arduino + MFRC522



Obrázek 2: Arduino UNO + MFRC522.

Další vhodnou variantou, jak tento útok provést je využít platformu Arduino (založenou na ATMega) spolu s NFC čtečkou MRFC522, jak demonstruje obrázek 2. Po připojení čtečky k desce Arduino je možné využít knihovnu MFC522 dostupnou ze stránek výrobce. Potom, co do programu zahrneme naši MFC522 knihovnu, je možné přistoupit k samotnému čtení UID karet. Pro čtení UID karty je nutné využít funkci:

```
mfrc522.PCD_DumpVersionToSerial();
```

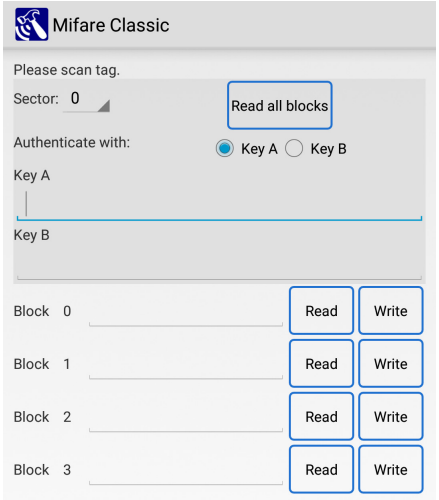
Po zjištění UID karty je toto UID potřeba zapsat na novou (UID měnitelnou) kartu. Nejčastější řešení zápisu do sektoru 0 bloku 0 je pomocí přímého přístupu, který je možné provést pomocí:

```
byte newUid[] = {0x01, 0x23, 0x45, 0x67};
mfrc522Hack.MIFARE_SetUid(newUid, (byte)4, true);
```

kde pole *newUid[]* reprezentuje 4 byty identifikátoru UID. Druhý řádek poté provede samotnou změnu UID. Původní UID karty bylo přepsáno, hodnoty v ostatních segmentech ale nebyly pozměněny.

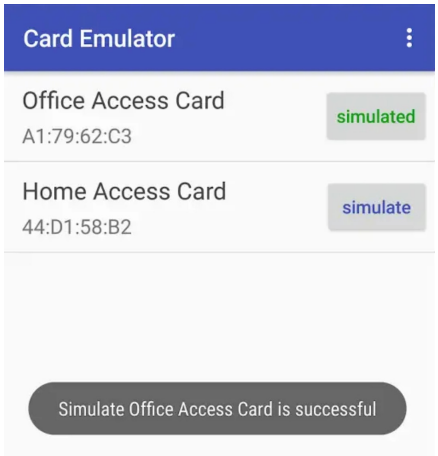
elektrorevue
ISSN 1213 - 1539

5.3 Mobilní aplikace



Obrázek 3: Náhled aplikace RFID NFC Tool.

Ještě jednodušší situace je v oblasti využití mobilních aplikací pro platformu Android. Nejvhodnější aplikací ke klonování se jeví aplikace RFID NFC Tool (viz obrázek 3) [9]. Tato aplikace umožňuje čtení a zápis karet Mifare Classic. K tomu, aby aplikace měla přístup k NFC modulu mobilního zařízení je nutné provést odblokování telefonu (tzv. root). Po spuštění aplikace vybereme možnost *Read* a vyčteme původní UID. Toto UID je poté možné pomocí funkce *Write* zapsat na UID měnitelný Mifare čip. Zapsání



Obrázek 4: Náhled aplikace NFC RFID Tag Emulator. [10]

UID do UID měnitelné karty není ale jediný způsob, jak dosáhnout klonování karty. Jakmile útočník disponuje UID karty oběti je možné využít například aplikaci NFC RFID Tag Emulator (viz obrázek 4) [10], která dokáže NFC modul mobilního zařízení přepnout do režimu emulace, což způsobí, že se bude NFC čip telefonu chovat jako karta. Telefon se poté autentizuje vůči čtečce podvrženým UID.

6 Závěr

Bezpečnost karet Mifare Classic je implementována pomocí šifrování přenosu pomocí proudové šifry CRYPTO1 a poté autentizačních klíčů A a B ke každému sektoru paměti. Bezpečnosti bylo dosaženo zejména utajováním šifrovacího algoritmu. Pomocí reverzního inženýrství se již několika výzkumným skupinám podařilo sestavit možný model tohoto algoritmu [11].

Dále se článek zabýval bezpečností autentizace pomocí neměnného UID karty. Systémy založeny na tomto systému nepočítají s možností úpravy UID karty, jelikož toho standardní Mifare čip není schopen. Na trhu se ale nachází speciálně upravené Mifare Classic čipy, které umožňují přímý zápis UID karty a tím vytvořit klon karty [5]. Navíc, při přenosu není možné šifrovat UID, jelikož je nutné k výpočtu odpovědi terminálu na výzvu karty. Nebezpečí zejména spočívá v dostupnosti komponent umožňující UID karty přečíst. Takové zařízení je možné sestrojit do velikosti běžné peněženky a tímto zařízením provádět odcizení identifikátoru karty v prostředcích veřejné dopravy, popřípadě ve frontách atp.

Jako další velké nebezpečí tohoto typu autentizace článek hodnotí kompatibilitu tohoto autentizačního mechanismu s technologií NFC, která je běžně dostupná v mobilních telefonech. Mobilní telefon vybavený technologií NFC je možné využít k přečtení UID a následně NFC čip přepnout do režimu emulace, což umožní autentizovat telefon vůči terminálu. Útočník v tomto případě nepotřebuje žádné speciální vybavení a vystačí si pouze s mobilním telefonem.

Autentizace pomocí Mifare Classic s sebou přináší jistá omezení a bezpečnostní rizika. Mifare Classic spolu s proudovou šifrou CRYPTO1 zabezpečuje pouze nízkou úroveň bezpečí, nicméně stále je tato úroveň vyšší, než autentizace uživatelů pomocí UID.

Jako určité doporučení se v této situaci jeví přejít na jiný, bezpečnější způsob autentizace. Pokud je z nějakého důvodu nutné zachovat systém založený na Mifare Classic, je nutné počítat pouze s částečnou bezpečností.

Literatura

[1] NEMEC, Matus, et al. *The return of coppersmith's attack: Practical factorization of widely used rsa moduli. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security.* ACM, 2017. p. 1631-1648.

[2] RANKL, Wolfgang. *Smart card applications. Design Models forusing and programming smart cards, Springer-Verlag*, 2007

[3] DE KONING GANS, Gerhard; HOEPMAN, Jaap-Henk; GARCIA, Flavio D. A practical attack on the MIFARE Classic. In: *International Conference on Smart Card Research and Advanced Applications.* Springer, Berlin, Heidelberg, 2008. p. 267-282.

elektrorevue
ISSN 1213 - 1539

[4] FINKENZELLER, Klaus. *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication.* John Wiley Sons, 2010.

[5] GARCIA, Flavio D., et al. Wirelessly pickpocketing a Mifare Classic card. In: *2009 30th IEEE Symposium on Security and Privacy*. IEEE, 2009. p. 3-15.

[6] TAN, Wee Hon. Practical attacks on the Mifare Classic. *Imperial College London*, 2009.

[7] MIFARE Classic 1K MODIFIABLE [Online]. Retrieved February 23, 2019, from https://lab401.com/products/mifare-compatible-1k-direct-write-uid

[8] VAN DULLINK, Wouter; WESTEIN, Pieter. *Remote relay attack on RFID access control systems using NFC enabled devices*. 2013.

[9] RFID NFC Tool [Online]. Retrieved February 23, 2019, from https://play.google.com/store/apps/details?id=tw.com.method.rfidtoolhl=cs

[10] NFC Card Emulator Pro (Root) [Online]. Retrieved February 23, 2019, from https://play.google.com/store/apps/details?id=com.yuanwofei.cardemulator.pro

[11] COURTOIS, Nicolas; NOHL, Karsten; O'NEIL, Sean. Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards. *IACR Cryptology ePrint Archive*, 2008, 2008: 166.