Bezpečnostní audit RFID systémů

Security audit of RFID systems

Bc. Stanislav Hubáček

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Stanislav HUBÁČEK**
Osobní číslo:	**A09504**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Bezpečnostní audit RFID systémů**

Zásady pro vypracování:

1. **Prostudujte známé způsoby útoků na dnes používané RFID systémy.**
2. **Analyzujte komunikaci mezi čtečkou a kartou u RFID systémů, dnes běžně používaných v ČR (např. přístupový systém na UTB ve Zlíně, elektronická peněženka ČSAD).**
3. **S použitím dostupných SW komponent demonstrujte funkční útok na vybraný špatně zabezpečený RFID systém.**
4. **Navrhněte možné úpravy zabezpečení kompromitovaných systémů, které by dokázaly Vámi provedeným útokům zabránit.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **THORNTON, Frank, et al. RFID Security [online]. 1st. ed. USA : SYNGRESS, 2005 [cit. 2011-01-17]. ISBN 978-1-59749-047-4.**
2. **GLOVER, Bill; BHATT, Himanshu. RFID essentials [online]. 1st. ed. USA : O'Reilly Media, Inc, 2006 [cit. 2011-01-17]. ISBN 987-0-596-00944-1.**
3. **ELLINGER, Frank. Radio Frequency Integrated. Second Edition. Berlin : Springer-Verlag Berlin Heidelberg, 2008. 515 s. ISBN 978-3-540-69324-6.**
4. **WANT, Roy. RFID Explained: A Primer on Radio Frequency Identification Technologies . USA : Morgan and Claypool Publishers , 2006. 94 s.**
5. **BROWN, Dennis E. RFID Implementation . USA : McGraw-Hill Osborne Media, 2006. 466 s. ISBN 978-0072263244.**

Vedoucí diplomové práce: **Ing. Tomáš Dulík**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **24. února 2011**

Termín odevzdání diplomové práce: **18. května 2011**

Ve Zlíně dne 24. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

ABSTRAKT

Tato práce se věnuje testování kvality bezpečnosti RFID systémů se zaměřením na nejrozšířenější a nejpoužívanější typy čipových RFID karet v České republice.

V teoretické části je krátké seznámení s principy funkčnosti rádio-frekvenční identifikace a zmínka o známých útocích, které byly do dnešní doby u RFID systémů zaznamenány. V dalších kapitolách je podrobnější pohled na protokoly tagů řady EM41xx a Mifare classic a nechybí zde ani analýza samotné komunikace mezi čtecím zařízením a zmíněnými typy tagů čipových karet.

Praktická část se zabývá testováním bezpečnosti čipových karet s pomocí dostupných hardwarových a softwarových komponent a názorným předvedením samotných útoků na vybrané RFID systémy. Dále jsou zde výsledky těchto testů analyzovány, a nakonec jsou doporučeny metody, jakým způsobem se lze těmto útokům bránit.

Klíčová slova: RFID, Mifare , čipová karta, tag, bezpečnostní audit, EM 41xx, manipulace, útok, emulace, simulace, zabezpečení.

ABSTRACT

This paper is dedicated to testing of quality and safety of RFID systems with focus on most common and used RFID chip cards in the Czech republic.

The academic part includes short introduction of utility of radio-frequence identification principals and reference to the known attacks that have been until these days recorded with the RFID systems. Following chapters show closer look at the tags of the EM41xx line and Mifare classic and even analisys of the communication between card reader and mentioned tags types of the chip card is included.

The practical part is focused on testing of security of chip cards with help of available hardware and software components and visual demonstration of the attacks thmeselves on the chosen RFID systems. Furthermore the results of these tests are analysed in this part and in the end the methods of how to prevent these kind of atacks are recommended.

Keywords: RFID, Mifare, smard card, tag, security audit, EM 41xx, manipulation, attack, emulation, simulation, security.

Poděkování

Chtěl bych tímto poděkovat panu Ing. Tomáši Dulíkovi, Ph.D. za jeho cenný čas věnovaný mé práci, ochotu a za rady, kterými mne neúnavně inspiroval.

Děkuji své rodině za její trpělivost a podporu, kterou mi umožnila poklidné studium.

Dále děkuji mému zaměstnavateli, firmě Impromat, za její podporu po celou dobu studia.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Žijeme v době, kdy si lidé snaží ulehčovat život, co nejlépe to jde a do této sféry patří i takzvané Rádio-frekvenční identifikační systémy neboli RFID. Hlavní myšlenkou tohoto řešení je bezdrátová identifikace čehokoli. Počínaje identifikací zboží a elektronickými pasy konče.

Mezi výhody patří již zmíněná bezkontaktní identifikace, možnost načítání více položek či osob v jednom okamžiku, malé rozměry nebo fyzické provedení takzvaného transpondéru, neboli čipové karty, neboli tagu, které může nabývat různých tvarů, a to i jednoduše ohebných či ve formě samolepek.

Bezkontaktní komunikace mezi takzvanou čtečkou a tagem, která je velkou výhodou se stává zároveň i velkou slabinou celého systému. Jedná se hlavně o slabinu bezpečnostní, neboť komunikaci je možno zachytit další neautorizovanou čtečkou a případné důležité informace z paměti čipové karty poskytnout třetí osobě, která tyto informace může různým způsobem zneužít.

Přestože existují různá provedení jednotlivých čipových karet, která mají různou úroveň zabezpečení, tak z ekonomického hlediska je tendence použití kompromisu, mezi cenou čipové karty a kvalitou jejího zabezpečení. V této práci se budeme věnovat testování kvality zabezpečení nejrozšířenějších čipových karet, které se používají k řízení přístupu osob do zabezpečených objektů či služeb, například tiskových, nebo pro bezhotovostní platby v přepravě osob, takzvaných elektronických peněženek.

Pro tyto účely byla vybrána čipová karta Univerzity Tomáše Bati ve Zlíně, používaná jako průkaz studenta s přístupem do menzy, knihovny, studovny a tiskovým službám. Tato karta pracuje na frekvenci 125 kHz s transpondérem EM 4100.

Čipová karta pracující na frekvenci 13,56 MHz bude v testu zastoupena transpondérem Mifare Classic 4k, která je využívána jako elektronická peněženka dopravní společnosti.

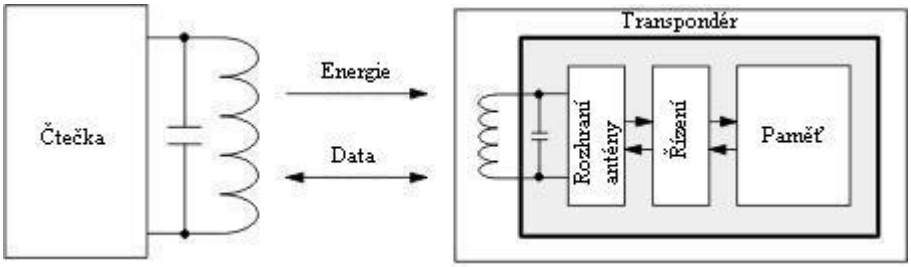
I. TEORETICKÁ ČÁST

1 ZNÁMÉ ZPŮSOBY ÚTOKŮ NA RFID SYSTÉMY

1.1 Princip RFID

Radio Frequency Identification, identifikace na rádiové frekvenci (RFID) je další generace identifikátorů navržených jednak k identifikaci zboží, dále pak k řízení přístupu osob do uzavřených objektů, nebo k bezhotovostním platbám v podobě elektronické peněženky [6]. Základní myšlenka RFID systému je založena na rádiovém přenosu dat mezi snímačem (čtečka), který funguje zároveň jako vysílač, a objektem (automobil, palety, osoby atd.). Objekt je vybaven takzvaným transpondérem, také označovaný jako RFID tag, který se skládá z elektronického obvodu obsahujícího anténu pro příjem i vysílání, nabíjecí kondenzátor, paměť a v případě takzvaného pasivního typu nepotřebuje napájení. Jedna z výhod transpondéru je, že může nabývat různých tvarů, které nejvíce odpovídají charakteru použití. Jsou to například klíčenky velikosti tablety, plastové kartičky velikosti kreditní karty, případně samolepky pro nalepení na jakékoli objekty různých tvarů.

Princip činnosti spočívá v tom, že vysílač (snímač) periodicky vysílá pulsy prostřednictvím antény do okolí. Jakmile se v dosahu antény objeví transpondér, přes jeho vlastní anténu přijme signál a ten využije k nabití svého kondenzátoru energií (pasivní tag), která je dostatečná k jeho aktivaci a následné odpovědi zpět snímači. Ten signál od transpondéru přijme a po jeho vyhodnocení jej předá k dalšímu zpracování (Obr. 1). Data mohou být předána ihned počítači ke zpracování, nebo mohou být uložena v paměti přenosných čteček a později nahrána do počítače. [7]



Obr. 1. Princip činnosti RFID. [11]

Vedle pasivní formy existuje ještě typ aktivního tagu, který má navíc i zdroj napájení a je schopen sám vysílat svou identifikaci. Toto provedení se většinou používá pro aktivní lokalizaci a je méně rozšířené.

Používané frekvence:

- 125 – 134 KHz LF (Low Frequency) tag
- 13.56 MHz HF (High Freguency) tag
- 860 – 930 MHz UHF (Ultra High Frequency) tag
- 2.45, 5.8 GHz Microwave tag

RFID tagy o vysokých frekvencích UHF a Microwave se využívají hlavě v logistice pro evidenci, sledování a třídění různých položek. Mnohem zajimavější jsou FRID tagy LF a HF, které se používají pro docházkové systémy, nebo jako elektronické peněženky.

Další důležité rozdělení je **podle typu zápisu do paměti:**

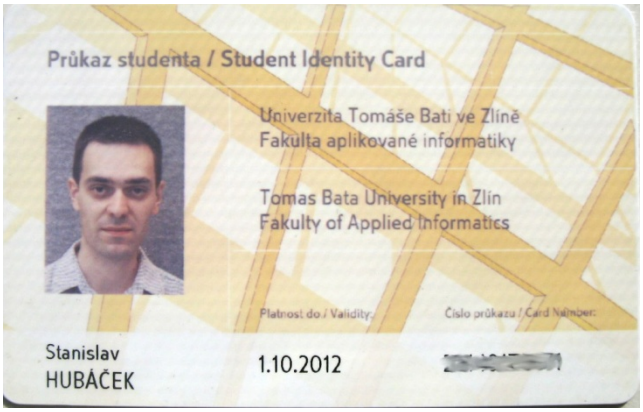
- Read only – pouze sériové číslo, uložené při výrobě
- WORM (jednou zapsatelné) – vhodné pro etiketu na zboží
- Read/Write – mnohokrát přepsatelné

1.2 RFID Tagy

Existuje celá řada RFID tagů, které se liší použitou nosnou frekvencí, provedením, zabezpečením, výrobcem a cenou. V další části se podrobněji podíváme na ty nejpoužívanější a nejrozšířenější provedení takzvaných čipových karet, které nás budou dále zajímat z hlediska zabezpečení.

1.2.1 EM 41XX

EM 41XX transpondér je jedna z nejrozšířenějších a nejjednodušších provedení čipové karty ISO (Obr. 2) používané hlavně k zabezpečení přístupu osob do budov či prostor, nebo k bezpečnému přístupu k určité službě, jako je například kopírka či tiskárna. Karta je vybavena 64 bitovou pamětí, které je v provedení pouze pro čtení a již z výroby obsahuje originální desetimístné sériové číslo. Formát dat v paměti je na obrázku 3. Komunikace se čtečkou probíhá na frekvenci 125 kHz.



Obr. 2. Příklad karty ISO EM41XX.

1 1 1 1 1 1 1 1 1 1		9 bitová hlavička, vše log 1
8 bitové číslo verze nebo ID výrobce	D00 D01 D02 D03	P0
	D04 D05 D06 D07	P1
	D08 D09 D10 D11	P2
	D12 D13 D14 D15	P3
Data o 32 bitech	D16 D17 D18 D19	P4
	D20 D21 D22 D23	P5
	D24 D25 D26 D27	P6
	D28 D29 D30 D31	P7
	D32 D33 D34 D35	P8
	D36 D37 D38 D39	P9
4 bitová parita	PC0 PC1 PC2 PC3	S0 1 stop bit (log 0)

Každou skupinu 4 bitů následuje paritní bit

Obr. 3. Formát dat paměti EM4100 tagu. [9]

1.2.2 MIFARE Ultralight

Nejlevnější varianta čipové karty s pracovní frekvencí 13,56 MHz je tak zvaná Ultralight varianta. Tag samotný neobsahuje žádnou metodu šifrování komunikace. Paměť má velikost 64 KB a je rozdělena do 16 bloků (pages) po 4 bytech. První dva bloky obsahují UID (Unique Identification) a BCC (Block Check Character). Obrázek 4 zobrazuje přehled dostupné paměti. Sektor 0x02 obsahuje lock-bity, pomocí kterých je možné zamknout paměťové bloky. Pokud toto provedeme, budou všechny příkazy o zápis do paměti zamítnuty. Nový tag má z výroby uzamčeny pouze první dva bloky, takže UID není možné změnit. Nastavení lock-bitu je možné pouze jednou, jakákoliv další změna již

není možná. Blok 0x03 je tak zvané One Time programovatelné počítadlo, které má jako výchozí hodnotu samé nuly a pokud je tento blok jednou nastaven, tak ho již nelze měnit. Toho lze využít například při sledování pohybu jízdenky v hromadné dopravě. Zbylé bloky paměti již lze standardně přepisovat. [13]

Číslo bytu	0x00	0x01	0x02	0x03	Blok
Sériové číslo	SN0	SN1	SN2	BCC0	0x00
Sériové číslo	SN3	SN4	SN5	SN6	0x01
Zámek	BCC1	Internal	Zámek0	Zámek1	0x02
Čítač	Č0	Č1	Č2	Č3	0x03
Data R/W	Data	Data	Data	Data	0x04
Data R/W	Data	Data	Data	Data	0x05
Data R/W	Data	Data	Data	Data	0x06
Data R/W	Data	Data	Data	Data	0x07
Data R/W	Data	Data	Data	Data	0x08
Data R/W	Data	Data	Data	Data	0x09
Data R/W	Data	Data	Data	Data	0x0A
Data R/W	Data	Data	Data	Data	0x0B
Data R/W	Data	Data	Data	Data	0x0C
Data R/W	Data	Data	Data	Data	0x0D
Data R/W	Data	Data	Data	Data	0x0E
Data R/W	Data	Data	Data	Data	0x0F

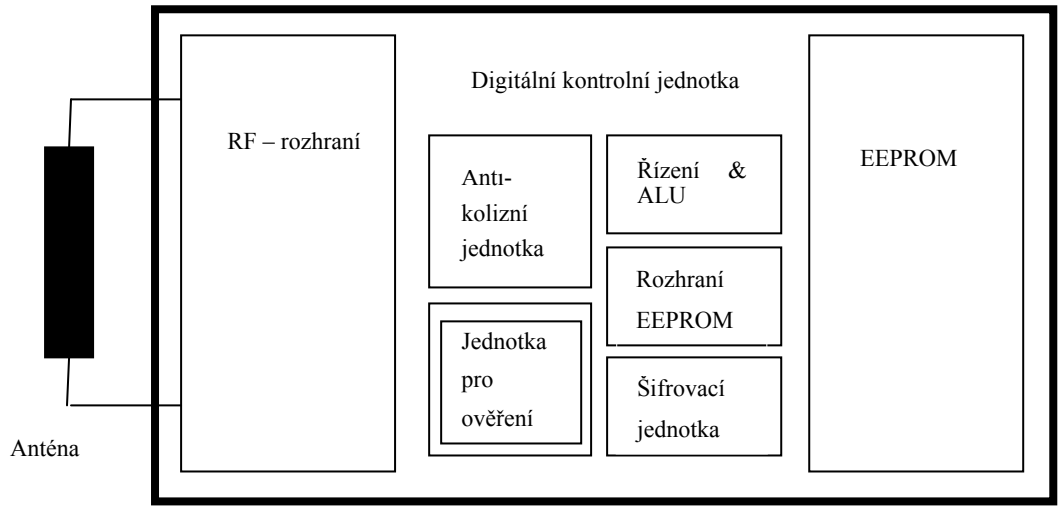
Obr. 4. Mapa paměti Ultralight tagu. [13]

1.2.3 MIFARE Classic

Je další velmi rozšířenou čipovou kartou nejčastěji ve formátu ISO (Obr. 2), která se vyrábí v provedení Classic 1K, 4K, 8K, podle velikosti paměti v kilobytech. Karta je v podstatě paměťové zařízení, kde paměť je rozdělena na segmenty a bloky s jednoduchými bezpečnostními mechanismy pro řízení přístupu. Provedení je na bázi ASIC (Application Specific Integrated Circuit) a mají omezený výpočetní výkon. Vzhledem k nízké ceně a přiměřené spolehlivosti jsou karty široce používané pro řízení přístupu, elektronické peněženky, firemní průkazy totožnosti a podobně.

MIFARE Classic 1K nabízí 1024 bytů pro uložení dat (Obr. 6), rozdělených do 16 sektorů. Každý sektor je chráněn dvěma různými klíči, označované klíč A, a klíč B. Je možné ji naprogramovat na operace čtení, zápisu, zvyšování hodnoty bloku atd. MIFARE Classic 4K nabízí 4096 bytů rozdělených do 40 sektorů. Pro každou z těchto karet je 16

bytů na sektor rezervováno pro klíče a metody přístupu, proto nemohou být standardně použity pro uživatelská data. Také prvních 16 bytů celé paměti obsahuje sériové číslo karty a některé další údaje výrobce, a také jsou jen pro čtení. Využitelná kapacita karty Classic 1K je pak 752 bytů a pro Classic 4K je to 3440 bytů.



Obr. 5. Blokové schéma MIFARE Classic. [12]

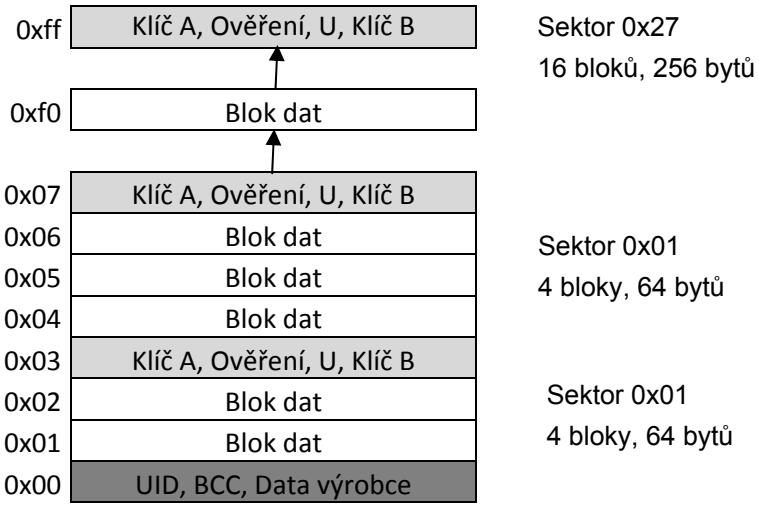
Popis blokového schématu

MIFARE Classic čip obsahuje paměť EEPROM, Rádio-frekvenční rozhranní a Digitální kontrolní jednotku. Energie a data jsou přenášeny přes anténu, která se skládá z cívky s několika závity a je připojena přímo k čipu.

- RF- rozhranní standard ISO/IEC 14443A
  - Modulátor – demodulátor
  - Usměrňovač
  - Generátor hodinových cyklů
  - Reset napájení
  - Regulátor napětí

- Antikolizní jednotka – je možné provozovat v dané oblasti několik karet v přiděleném pořadí.
- Jednotka pro ověření – pro ověření paměťových operací a zajištění, že přístup k bloku je možný pouze přes dva klíče stanovené pro každý blok.

- Řízení a Aritmetická logická jednotka – Hodnoty jsou uloženy ve speciálním redundantním formátu a mohou být inkrementovány a dekrementovány.
- Rozhranní EEPROM
- Šifrovací jednotka – Použití proudové šifry CRYPTO1 pro ověření a šifrování výměny dat.
- EEPROM – paměťový obvod.



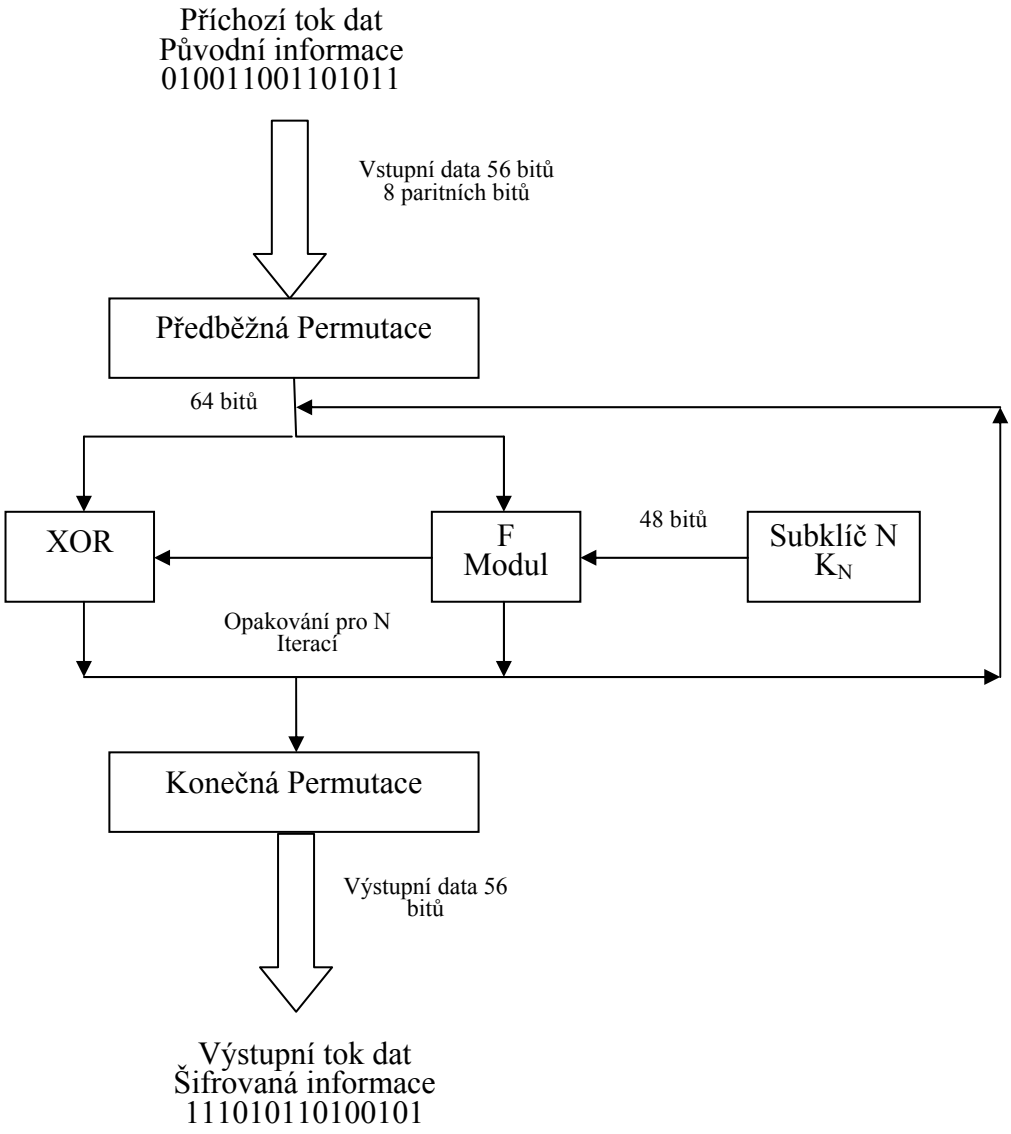
Obr. 6. Mapa paměti Mifare Classic tagu. [13]

1.2.4 MIFARE DESFire

K nejmodernější variantě RFID tagů, vyhovující standardu ISO/IEC 14443-4, patří provedení čipové karty DESFire, která již obsahuje procesorové jádro (8051) se standardně naprogramovaným univerzálním software (DESFire operační systém), nabízejícím jednoduchou adresářovou strukturu se soubory podobající se tomu, co se obvykle nachází na smart kartě a umožňují větší zabezpečení než varianta Classic. DESFire karty existují ve čtyřech variantách. Jedna z nich je varianta Triple-DES, využívající algoritmus symetrické blokové šifry DES, s kapacitou paměti 4 KB a další tři využívající symetrickou blokovou šifru AES o kapacitách 2, 4 a 8 KB. Tyto varianty mají také další bezpečnostní prvky jako je například CMAC (Cipher-based MAC) metoda ověření identity. Nevýhodou těchto karet jsou vyšší pořizovací náklady. [6]

Encryption Standard (DES) je jeden z nejstarších a nejznámějších šifrovacích algoritmů, který byl vyvíjen společností IBM a vlády USA od roku 1976 až do roku 2001. V roce 1999 byla šifra prolomena. Z toho důvodu byl algoritmus upraven na bezpečnější variantu, kdy se provádí vícenásobná aplikace šifry. Tato trojnásobná aplikace šifry DES je označována jako algoritmus Triple DES. Celková délka klíče tak vzrostla z původních 64 bitů u DES, na 168 bitů Triple DES.

Šifra DES byla v podstatě založena na algoritmu Lucifer vytvořeného panem Horstem Feistelem, který nikdy neviděl její velmi úspěšné nasazení. Jak již bylo zmíněno výše, šifra používá jediný 64-bitový klíč, z toho 8 bitů je kontrolních (paritních) a 56 bitů efektivních.



Obr. 7. Algoritmus šifrování DES.

Klíč je rozdělen na 16 samostatných subklíčů o velikosti 48 bitů pro každý cyklus algoritmu. Obrázek 7 zobrazuje blokové schéma aplikace algoritmu šifry.

Každá iterace cyklu se skládá ze substituční fáze, kdy jsou data nahrazena částmi klíče. V dalším kroku je provedena operace permutace, v níž jsou nahrazená data kódována (přeskupením).

Bezpečnost DES spočívá hlavně v tom, že operace substituce jsou nelineární a z toho důvodu nelze z šifrované zprávy bez příslušného klíče získat původní text.[1]

1.3 Útoky na RFID

Chceme-li určit možné útoky na RFID systémy, je třeba si uvědomit, co by mohlo být cílem této činnosti. Nejčastějším typem útoku je zcizení dat z RFID tagu, případně provedení 100% kopie původního tagu tak, aby bylo možné tuto původní kopii využít k prodloužení kreditu nebo k samotnému rozmnožení klonovaného tagu. Další příklad útoku může být zabránění komunikace mezi čtečkou a tagy, případně možnost vložení škodlivého kódu do komunikace pro zajištění přístupu do systémové databáze oběti.

1.3.1 Rádio-frekvenční manipulace

Rádio-frekvenční manipulace je nejjednodušší způsob útoku, který má za cíl zabránit komunikaci mezi tagem a čtečkou. Tohoto se využívá v případech, kdy je například zboží v obchodech označeno pomocí RFID tagů, a zároveň se tento způsob využívá i jako ochrana opuštění zboží z vyhrazené zóny bez předchozí deaktivace. K tomuto účelu se využívají některé kovy, které blokují rádiové frekvence, takže například stačí RFID tag zabalit do kovové fólie a tím je zabráněno možné komunikaci.

Tento způsob může být s výhodou použit i jako ochrana proti čtení například čipové karty nepovolanou třetí osobou. V praxi se můžeme setkat s takzvanými kovovými peněženkami, nebo se používají tašky s kovovou fólií.

Dalším bezpečnostním problémem je samotná rádiová komunikace mezi čtečkou a RFID tagem. V této souvislosti jsou známy čtyři typy útoků:

- Spoofing
- Insert
- Replay
- Denial of Service (DoS)

1.3.1.1 Spoofing

Spoofing je metoda, kdy útočník poskytuje podvržená data, která se pro systém zdají jako platná, takže jsou tímto systémem přijata. V případě RFID je vysíláno nesprávné Electronic Product Code™ (EPC)™ číslo v době, kdy je očekáváno právě platné číslo.

1.3.1.2 Insert

Insert je způsob vložení (maskování) příkazu do komunikace, která není zabezpečená, a to ve fázi přenosu dat. Typické použití pro tento útok je aplikace SQL příkazů do databáze.

1.3.1.3 Replay

U tohoto typu útoku se zachytí a uloží platná data komunikace (RFID signál) mezi tagem a čtečkou, která se mohou později znovu odeslat čtečce. Vzhledem k tomu, že tyto data jsou platná, systém je bude akceptovat.

1.3.1.4 Denial of Service

DOS útok, také známý jako **nedostupnost služby**, způsobuje zahlcení signálu více daty, než je systém schopen zpracovat. V oblasti RFID je variací tohoto útoku rádio-frekvenční rušení šumovým signálem pro dané frekvenční pásmo. To způsobí, že systému je odepřena schopnost správně rozpoznat příchozí data.

1.3.2 Manipulace s daty RFID tagu

V předchozím případě jsme byli schopni pracovat pouze se zachycenou komunikací, ale změna dat jako takových byla velmi omezená. V případě odečtení dat z paměti tagu, jejich analýze, případně úpravě a následnému uložení změněných dat zpět do paměti tagu, jsme schopni ovlivnit komunikaci v daleko širší míře. V praxi se můžeme setkat se situací, kdy je nabízené zboží v obchodě označeno špatně zabezpečeným RFID tagem a útočník je schopen upravit položku paměti, ve které je uložena cena. Je to možné z toho důvodu, protože oproti čárovému kódu, kde se cena ukládá do databáze systému, je cena uložena v paměti EEPROM, která dává širší možnosti manipulace s jednotlivými kusy oproti manipulaci cenou jedné položky. Pokud útočník tyto data změní, může získat obrovskou slevu, přičemž systém toto nerozpozná, dokud neproběhne inventurní kontrola. Jiným příkladem může být změna částky elektronické peněženky používané například pro přepravu osob v hromadné dopravě, pokud ovšem jsou tyto data uložena v paměti a nejsou porovnávána dálkově v systému dopravce.

1.3.3 Známé útoky na Mifare Classic

Jak již bylo napsáno, čipové RFID karty Mifare Classic patří mezi nejrozšířenější v České republice. Postupným testováním konstrukčního provedení byly zjištěny nedostatky v zabezpečení, které jsou popsány v kapitole 2.2.6.1 a 2.2.7.

Zatím jsou známi dvě metody, které vedou k zachycení komunikace, případně ke kompletnímu přečtení celého obsahu paměti tagu.

- Získání klíčů pomocí legitimního RFID čtecího zařízení s přednastaveným klíčem pomocí speciálního hardware a software.
- Získání klíčů pomocí „offline“ útoku na samotný tag (čipovou kartu). Pro tento typ útoku stačí jakékoliv jednoduché čtecí zařízení, pro příslušný typ RDIF systému, trochu času a speciální software.

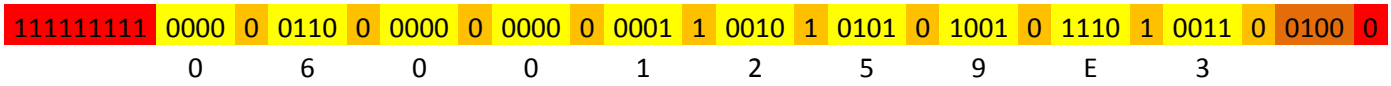
Pomocí těchto metod je možné data v paměti čipu nejen duplikovat, ale také číst, a dokonce provádět změny, jako je například změna uloženého kreditu.

Ukázce útoku na Mifare Classic 4k se budeme podrobněji věnovat dále v praktické části této práce.

2 POPIS KOMUNIKACE MEZI ČTEČKOU A KARTOU RFID SYSTÉMŮ

Tato kapitola se věnuje popisu protokolu a komunikace RFID systémů, které jsou v ČR nejběžnější. V současnosti se nejčastěji setkáváme s čipovými kartami série EM Marin 4100 od výrobce EM Microelectronics pracující na frekvenci 125 kHz a čipovými kartami Mifare Classic 4k, případně Mifare Classic 1k od výrobce NXP Semiconductors, pracující na frekvenci 13,56 MHz.

2.1 EM 4100 protokol



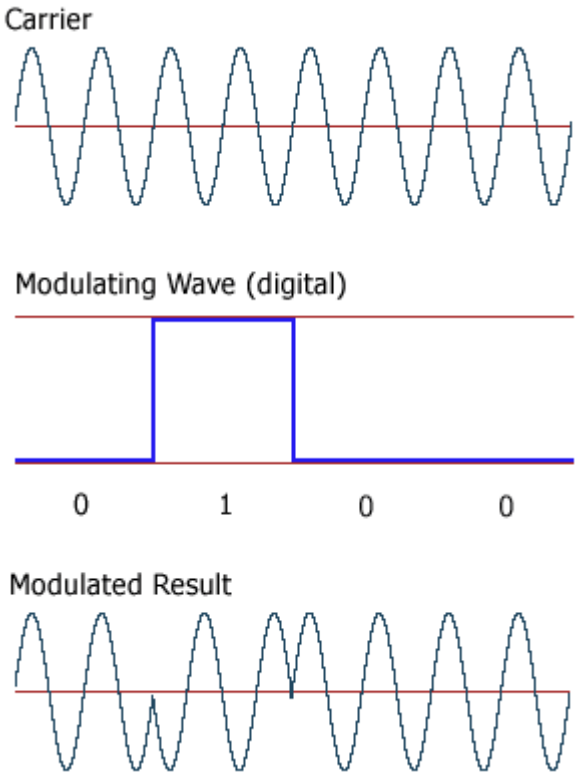
Obr. 8. Komunikace EM4100.

Pokud vložíme čipovou kartu do elektromagnetického pole vyzářeného RFID čtečkou, bude čip karty aktivován a začne vysílat údaje dle obrázku 8. Prvních 9 bitů je využito jako startovací sekvence k označení začátku řetězce, které systém očekává, aby mohl začít číst samotná data paměti karty. Tyto bity musí mít hodnotu log 1. Po přečtení neporušené startovní sekvence se začne číst 10 bloků po 4 bitech a jednom paritním bitu, která je ukončená sekvencí 4 paritních bitů a jedním stop bitem. Transpondér opakuje tuto sekvenci do vybití napájecí energie. Odesílaný řetězec podle obrázku 8 je číslo $06 (číslo výrobce) a $001259E3 jsou samotná uložená data, která udávají jedinečný identifikátor či sériové číslo. [9]

2.1.1 Modulace dat

RFID transponder je schopen přenášet data modulací RF pole čtecího zařízení.

Pro modulování signálu mezi čtecím zařízením a tagem (čipovou kartou) se u EM4100 nejčastěji používá modulace PSK – Phase Shift Keying (Obr. 9).



Obr. 9. Princip PSK modulace. [17]

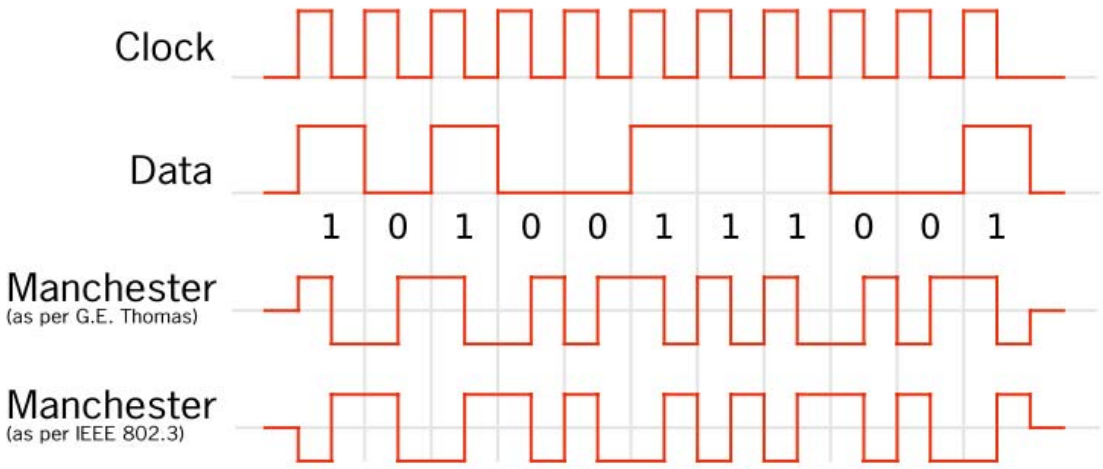
Kódování modulovaných dat jsou nejčastěji v těchto provedeních:

- **kódování Manchester**
- **kódování BiPhaze**
- **kódování PSK**

Transponder a čtecí zařízení používají pro synchronizaci přenosu dat mezi sebou jednotlivé cykly RF pole. Frekvence synchronizačního hodinového signálu je jednoduše převzata z frekvence použitého RF pole. RFID frekvence hodinového signálu se liší v závislosti na požadované aplikaci. V nízkých frekvencích a pro krátké vzdálenosti snímání se typicky používá pásmo mezi 100-150kHz. Pro větší čtecí vzdálenosti může být použita systémová frekvence 13,56 MHz, nebo případně jiné frekvence podle požadavku aplikace. Délka každého bitu je specifikována z hlediska počtu hodinových cyklů. Pro EM 4100 protokol může být délka jednoho bitu definovány buď 64, 32 či 16 hodinovými cykly.

2.1.1.1 Kódování Manchester

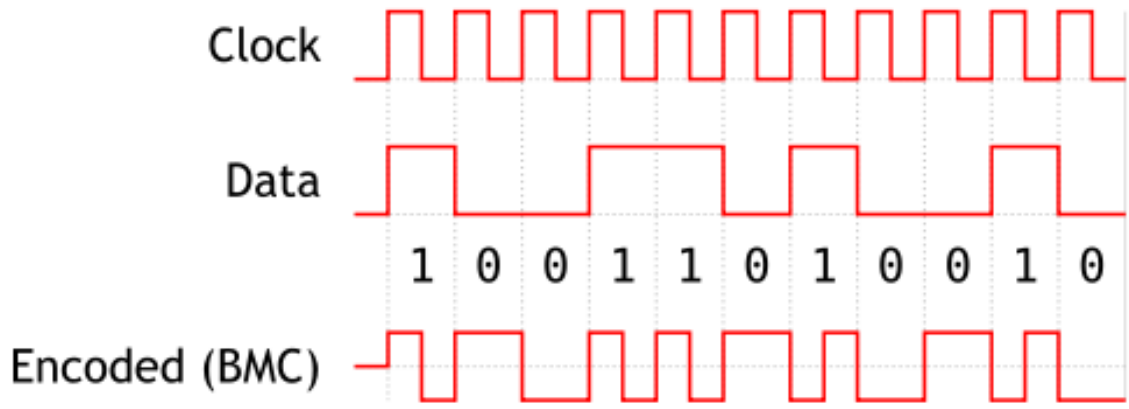
U kódování Manchester se hodnota bitu vyjadřuje vložením hrany (změny signálu) do bitového intervalu původního signálu. Pokud signál v této hraně přechází z vysoké úrovně na nízkou úroveň, pak vyjadřuje hrana hodnotu bitu 1. Pokud signál přechází z nízké úrovně na vysokou úroveň, pak vyjadřuje hodnotu bitu 0. Protože se hrana vždy nachází uprostřed každého bitového intervalu, může snadno sloužit k synchronizaci (Obr. 10).



Obr. 10. Kódování Manchester. [6]

2.1.1.2 Kódování BiPhaze

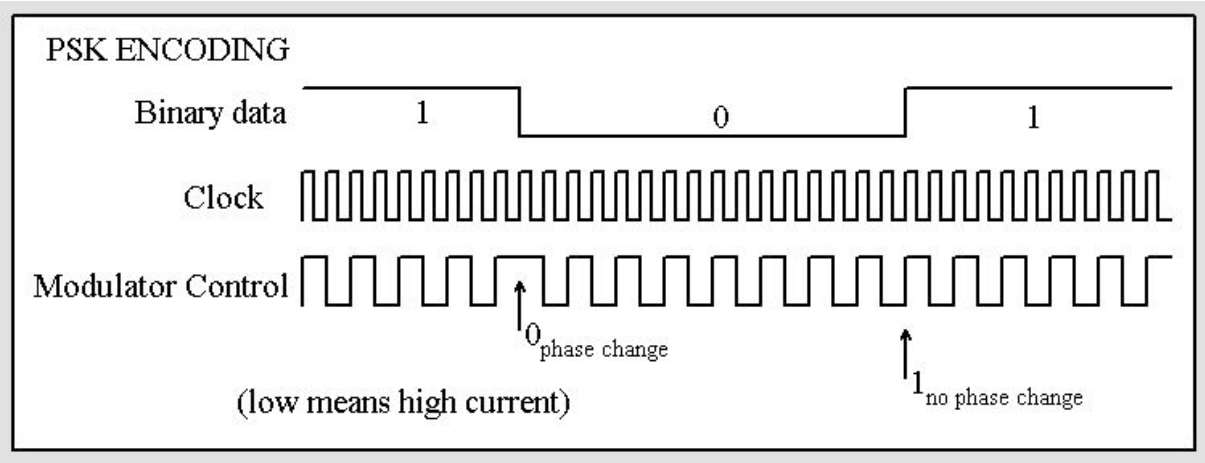
Oproti předchozímu případu je u kódování BiPhaze vložena hrana modulačního signálu na začátek intervalu bitového signálu. Hodnota bitu je dána tím, zda se během periody synchronizačního signálu změní hodnota modulačního signálu. Hodnota bitu 1 nastane v případě změny modulačního signálu v polovině periody a hodnota bitu 0 v případě, když se tento signál během periody nezmění nebo naopak (Obr. 11).



Obr. 11. Kódování BiPhaze. [6]

2.1.1.3 Kódování PSK

V případě kódování PSK (Phase Shift Keying) je princip ten, že modulační signál mění svoji hodnotu s periodou hodinového signálu a v závislosti na délce jednoho bitu podle počtu hodinových cyklů, mění nebo nemění svoji fázi. Pokud modulační signál změní fázi, po 64, 32 nebo 16 cyklech dle nastavené délky bitu datového signálu, objeví se na výstupu bit 0. Jestliže se fáze nezmění, zůstává na výstupu bit 1 (Obr.12).



Obr. 12. Kódování PSK.[9]

2.2 MIFARE Classic Tag protokol

Aktivace čipu probíhá podobným způsobem jako v předchozím případě. V okamžiku nabití kondenzátoru proběhne antikolizní operace zaručující výběr správného tagu čtečkou odesláním vlastního UID identifikátoru. Čtečka poté vybere tento tag dle specifikace ISO14443-A.

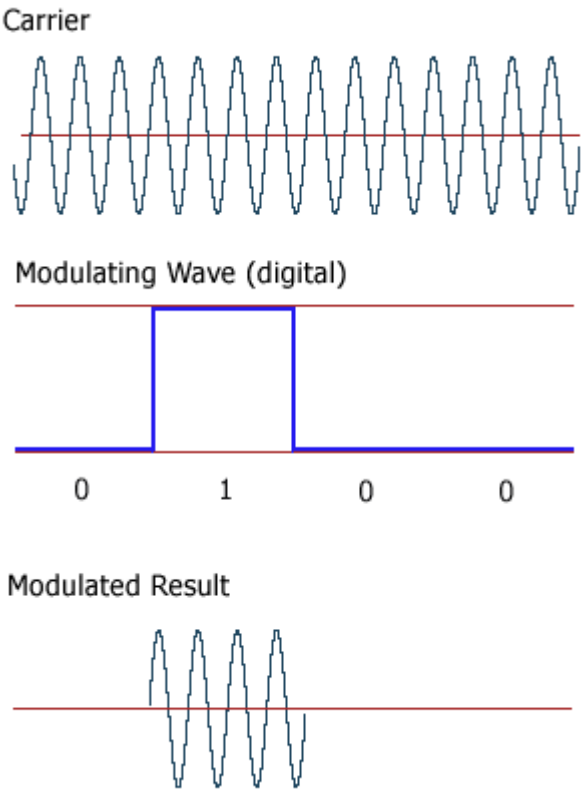
Podle dokumentace výrobce, čtečka poté pošle požadavek pro ověření konkrétního bloku. Tag odpoví výzvou nonce (number used once – číslo použito jen jednou) n_T odeslanou v čistě kódovém tvaru. Odpovědí čtečky je odeslání vlastní výzvy nonce n_R společně s odpovědí a_R na výzvu tagu. Tag ukončí proces ověření odpovědí a_T na výzvu čtečky. Počínaje n_R veškerá komunikace je šifrovaná. To znamená, že na n_R, a_R, a a_T je provedena logická operace eXclusive OR se sadou klíčů k_S1, k_S2, k_S3. Jednotlivé kroky komunikace jsou znázorněny v tabulce 1.

Tab. 1. Postup ověření MIFARE

Krok	Odesílatel	Hex hodnota	Popis
01	čtečka	26	žádost A
02	tag	04 00	odpověď
03	čtečka	93 20	výběr
04	tag	c2 a8 2d f4 b3	UID, BCC
05	čtečka	93 70 c2 a8 2d f4 b3 ba a3	výběr (UID)
06	tag	08 b6 dd	MIFARE 1k
07	čtečka	60 30 76 4a	ověření (blok30)
08	tag	42 97 c0 a4	n_T
09	čtečka	7d db 9b 83 67 eb 5d 83	n_R XOR k_{S1}, a_R XOR k_{S2}
10	tag	8b d4 10 08	a_T XOR k_{S3}

2.2.1 Modulace dat

Pro přenos signálu mezi čtecím zařízením a tagem se u Mifare Classic používá modulace ASK – Amplitude-Shift Keying (Obr. 13).



Obr. 13. Princip ASK modulace. [17]

2.2.2 Struktura Mifare Classic 4k

Podrobnější popis oblasti paměti Mifare Classic 4k, která je organizována do sektorů s čísly 0 až 39. Každý sektor obsahuje 4 nebo 16 bloků (blok 0 až 3 nebo blok 0 až 16). Blok 3 sektoru 0 až 31 a blok 15 sektoru 32 až 39 je označován jako hlavní blok sektoru a obsahuje informace, jako jsou řízení přístupu k sektoru (přístupové bity) či přístupové klíče (klíč A a klíč B). V závislosti na konfiguraci přístupových bitů musí čtecí zařízení provést autentizaci pomocí klíče A nebo klíče B k umožnění čtení či zápisu jednotlivých sekretů. Byte 9 hlavního bloku sektoru se označuje jako General Purpose Byte (GPB). Blok 0 sektoru 0 (někdy také označován jako tovární blok) obsahuje IC data výrobce a 4 byty označované jako Unique Identifier (jedinečný identifikátor UID, nebo také někdy označen jako sériové číslo tagu či čipové karty). [14]

2.2.3 Mifare application directory

Pro mapování dat v paměti Mifare Classic 1k či 4k se používá takzvaná Mifare application adresářová struktura (MAD). Tato aplikační adresářová struktura identifikuje, ke které aplikaci patří informace uložené uvnitř každého paměťového sektoru.

Existují dvě MAD specifikace:

1. Mifare application direcrory 1 (MAD1) pro Mifare Classic 1k.
2. Mifare application direcrory 2 (MAD2) pro Mifare Classic 4k.

MAD přiděluje každé aplikaci jedinečný aplikační identifikátor (Unique Application Identifier – AID). AID identifikátory jsou uloženy uvnitř sektoru 00h pro Mifare Classic 1k, a uvnitř sektorů 00h a 10h pro Mifare Classic 4k. Sektor 00h a sektor 10h (nebo sektor 0 a sektor 16) jsou označeny jako MAD sektory.

AID má velikost 2 byte a je rozdělen na dvě části každá po jednom byte. Jsou to:

1. Kód funkce clusteru (1 byte), který definuje cluster, ke které aplikaci patří.
2. Aplikační kód (1 byte), který definuje aplikaci v clusteru.

Devátý byte sektoru se označuje jako General Purpose Byte (GPB) a pro aktivaci MAD je nutné jeho první bit nastavit na logickou 1. Tímto bytem se mimo jiné nastavuje uvedení tagu jako multiaplikační či monoaplikační.

U všech dalších nepoužívaných sektorů se striktně doporučuje nastavení ochrany proti zápisu pomocí definovaného šifrovacího klíče, aby se zabránilo nežádoucí redefinici přístupových bytů a klíčů. Všechny další prázdné sektory by měli používat rozdílné šifrovací klíče, které v lepším případě nemají defaultní hodnotu. V praxi se ovšem stále setkáváme s pravým opakem. Je to dáno benevolencí a podceňováním ochrany RFID tagů ze strany provozovatelů systémů. [14]

2.2.4 Nastavení přístupu k Mifare Classic 1k/4k

Mifare Classic 1k/4k poskytuje mechanismus, který je založený na takzvaných přístupových bitech, které v kombinaci s klíči umožňují nastavit přístupová práva pro čtení či zápis.

Každý paměťový sektor má asociované dva klíče označené jako klíč A, klíč B, a dalších 12 přístupových bitů označených $C1_{0..3}$, $C2_{0..3}$ a $C3_{0..3}$. Nastavením těchto přístupových bitů je možné povolit nastavení přístupu pro čtení nebo zápis v závislosti s klíčem A nebo klíčem

B. Přístupové byte se nacházejí uvnitř sektoru na pozici 6 až 8 viz tabulka 2. Hodnoty a negované hodnoty každého přístupového bitu uvnitř sektoru jsou nastaveny například takto: $C1_0 = 0b$ a $\overline{C1_0} = 1b$.

Tab. 2. Čísla jednotlivých bytů v sektoru.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		klíč A				přístupové bity			GPB			klíč B			

Příklad obsazení Byte 6 až 8.

Byte 6 obsahuje jednotlivé bity 7-0 s označením: $\overline{C2_3}$, $\overline{C2_2}$, $\overline{C2_1}$, $\overline{C2_0}$, $\overline{C1_3}$, $\overline{C1_2}$, $\overline{C1_1}$, $\overline{C1_0}$.

Byte 7 obsahuje bity s označením: $C1_3$, $C1_2$, $C1_1$, $C1_0$, $\overline{C3_3}$, $\overline{C3_2}$, $\overline{C3_1}$, $\overline{C3_0}$.

Byte 8 obsahuje bity s označením: $C3_3$, $C3_2$, $C3_1$, $C3_0$, $C2_3$, $C2_2$, $C2_1$, $C2_0$.

2.2.5 Přístup k MAD sektoru

Paměťové sektory, kde jsou uloženy MAD1 a MAD2, jsou chráněny klíči A a B. Podle velikosti paměti jsou to sektory:

- Pro verzi 1k je to sektor 00h, neboli sektor 0.
- Pro verzi 4k jsou to sektory 00h a 10h, neboli sektor 0 a sektor 16.

Kdokoli by měl mít oprávnění číst sektor MAD. Toto je umožněno použitím veřejného klíče A (Tab. 3).

Tab. 3. Hodnota klíče A sektoru 0. [14]

Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5
A0h	A1h	A2h	A3h	A4h	A5h

Tab. 4. Konfigurace přístupových bitů pro MAD sektor s právy čtení i zápisu. [14]

Přístupové bity	**Hodnoty**	**Poznámka**
$C1_0\,C2_0\,C3_0$	100b	Blok 0 čtení s klíčem A a zápis s klíčem B
$C1_1\,C2_1\,C3_1$	100b	Blok 1 čtení s klíčem A a zápis s klíčem B
$C1_2\,C2_2\,C3_2$	100b	Blok 2 čtení s klíčem A a zápis s klíčem B
$C1_3\,C2_3\,C3_3$	011b	Hlavní blok sektoru: • Klíč A zapsán pomocí klíče B a nelze jej přečíst. • Přístupové bity jsou čteny pomocí klíče A nebo B a zapisovány pomocí klíče B. • Klíč B je zapsán pomocí klíče B a nelze jej přečíst

Tab. 5. Konfigurace přístupových bitů pro MAD sektor s právy pouze pro čtení. [14]

Přístupové bity	**Hodnoty**	**Poznámka**
$C1_0\,C2_0\,C3_0$	010b	Blok 0 čtení s klíčem A nebo s klíčem B
$C1_1\,C2_1\,C3_1$	010b	Blok 1 čtení s klíčem A nebo s klíčem B
$C1_2\,C2_2\,C3_2$	010b	Blok 2 čtení s klíčem A nebo s klíčem B
$C1_3\,C2_3\,C3_3$	110b	Hlavní blok sektoru: • Klíč A nelze nikdy zapsat ani číst • Přístupové bity jsou čteny pomocí klíče A nebo klíče B a nelze je nikdy zapsat • Klíč B nelze nikdy zapsat ani číst

2.2.6 Sada příkazů a odezev transpondéru

Mifare Classic 1k/4k tag přijímá následující sadu příkazů, zasílaných čtecím zařízením. Tabulka 6 popisuje sadu příkazů pro jednotlivé operace s pamětí.

Tab. 6. Sada příkazů pro operace s pamětí tagu.

Činnost	**Popis**
Identifikace a výběr	Identifikuje konkrétní tag a provede výběr.
Autentizace	Proces ověření. Tato operace vyžaduje právo čtení a zápisu do paměťového sektoru.
Čtení	Čtení jednoho paměťového bloku (16 bytů).
Zápis	Zápis jednoho paměťového bloku (16 bytů).

Popis jednotlivých operací

Identifikace a výběr – provede výběr konkrétního tagu vloženého do pole čtecího zařízení na základě anti-kolizního systému definovaného normou ISO/IEC 14443-3.

Autentizace – operace autentizace je založena na třístupňovém ověření použitím buďto klíče A nebo klíče B. Mifare Classic umožňuje přístup k paměti pouze v případě, pokud proběhlo úspěšně ověření přístupu ke konkrétnímu sektoru. Tato operace je specifická pro každý jednotlivý sektor. I v případě, že jsou některé sektory chráněny se shodnými klíči jako jiné sektory, bude se metoda ověření provádět pro tyto sektory znovu.

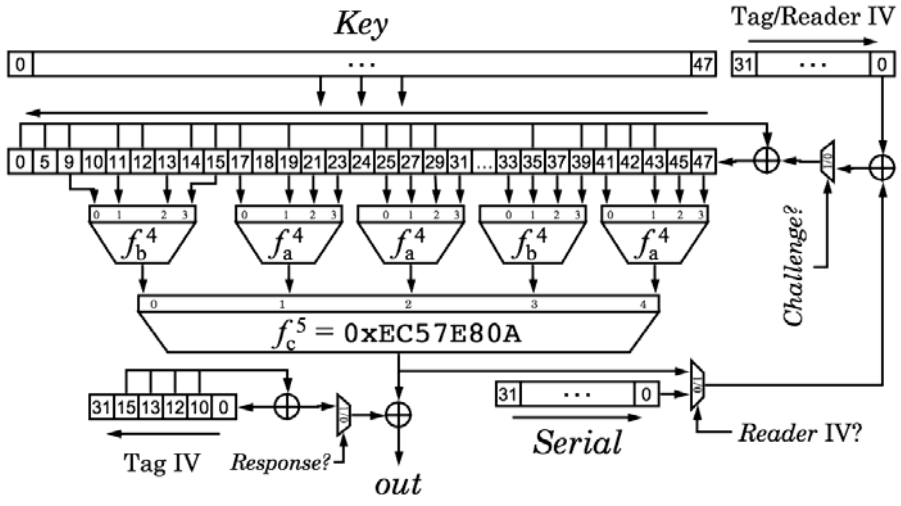
Pokud proběhne úspěšné ověření sektoru, tak podle nastavení přístupových bitů bude nebo nebude umožněno čtení či zápis do bloků sektoru.

Čtení – operace čtení umožňuje čtení jednotlivých bloků (16 bytů) sektoru.

Zápis – operace zápisu umožňuje zápis do jednotlivých bloků (16 bytů) sektoru. Zapisuje se vždy celých 16 bytů bloku. Jestli je vyžadována pouze změna části bloku, je nejprve třeba přečíst byty bloku, které se nemění, pokud nejsou známi předem, a poté provést zápis celého bloku.

2.2.7 Šifra Mifare CRYPTO1

Jádrem CRIPTO1 šifry je 48 bitový lineární zpětnovazební registr (linear feedback shift register – LFSR) (Obr. 14).



$f_a^4 = \texttt{0x9E98} = (a+b)(c+1)(a+d)+(b+1)c+a$

$f_b^4 = \texttt{0xB48E} = (a+c)(a+b+d)+(a+b)cd+b$

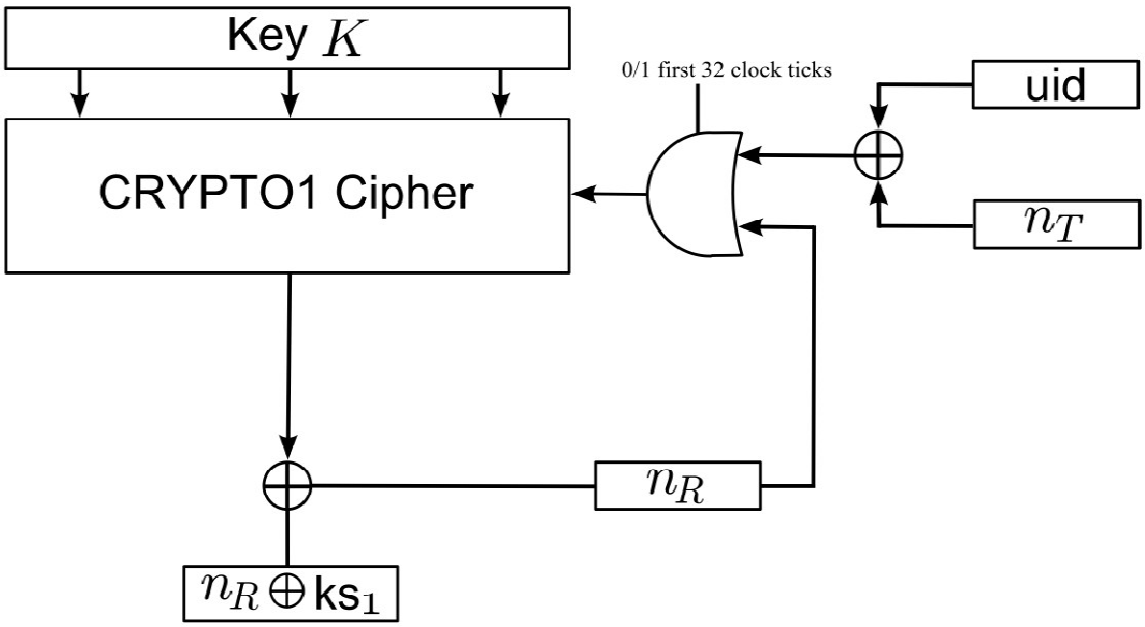
Obr. 14. Šifra CRYPTO1. [6]

Posuvný registr je popsán polynomem: $g(x) = x^{48} + x^{43} + x^{39} + x^{38} + x^{36} + x^{34} + x^{33} + x^{31} + x^{29} + x^{24} + x^{23} + x^{21} + x^{19} + x^{13} + x^{9} + x^{7} + x^{6} + x^{5} + 1$. V každém hodinovém cyklu dochází k posunu registru o jeden bit doleva. Bit nejvíce vlevo je vyřazen a bit pro zpětnou vazbu je vypočítán podle $g(x)$. Při inicializaci má LFSR registr připojen vstupní bit, na který je provedena logická operace XOR se zpětnou vazbou a výsledek je vložen zpět do registru z pravé strany. Přesněji, pokud stav registru LFSR v čase k je $r_k r_{k+1} \dots r_{k+47}$ a vstupní bit je i, potom stav v čase $k+1$ je $r_{k+1} r_{k+2} \dots r_{k+48}$, kde

$r_{k+48} = r_k \oplus r_{k+5} \oplus r_{k+9} \oplus r_{k+10} \oplus r_{k+12} \oplus r_{k+14} \oplus r_{k+15} \oplus r_{k+17} \oplus r_{k+19} \oplus r_{k+24} \oplus r_{k+27} \oplus r_{k+29} \oplus r_{k+35} \oplus r_{k+41} \oplus r_{k+42} \oplus r_{k+43} \oplus i.$ [15]

Pro šifrování jsou zvolené bity registru LFSR vloženy skrze filtrovací funkce f.

2.2.7.1 Inicializace



Obr. 15. Inicializační diagram [15]

Registr LFSR je inicializován během autentizace protokolu. Pokud hodnota n_T XOR UID zůstává konstantní, tak i šifrovaná odpověď čtecího zařízení zůstává konstantní. To naznačuje, že hodnota n_T XOR UID je jako první vložena do registru LFSR. Zajímavostí

je, že změnami zpětnovazebních bitů je možné modifikovat hodnotu n_T XOR UID a tajný klíč K takovým způsobem, že šifrovaný text po autentizaci zůstává také konstantní. Z toho vyplývá, že pokud hodnota $n_t \oplus UID \oplus K \oplus$ „zpětnovazební bity" zůstává konstantní, tak zašifrovaný řetězec znaků generovaný po autentizaci zůstává také konstantní. Zpětnovazební bity jsou vypočteny pomocí funkce $g(x)$. To naznačuje, že tajný klíč K je počátečním stavem registru LFSR.

V dalším kroku ověřovacího protokolu vyšle čtecí zařízení odpověď na výzvu tagu n_R, která je taktéž přivedena na vstup registru. Lze si povšimnout, že dříve zaslané odpovědi n_R mají vliv na šifrování pozdějších odpovědí n_R. V tuto chvíli je proces inicializace ukončen a vstupní bit registru již dále není využíván. Inicializační blokové schéma podle obrázku 9 zobrazuje diagram jak pro čtecí zařízení, tak pro tag samotný. Rozdílem je to, že čtecí zařízení generuje hodnotu n_R, poté provede výpočet a odesílá výsledek hodnoty $n_R \oplus KS_1$, zatím co tag přijímá hodnotu $n_R \oplus KS_1$, a poté provede výpočet n_R.[15]

2.2.8 Generátor náhodné hodnoty

Generátor náhodných hodnot (RNG – Random Number Generator) používaný u Mifare classic tagů je bezpečnostní riziko pro kryptografické aplikace, a dále zvyšuje šance případného útočníka tím, že zjednodušuje celý proces možných výpočtů bezpečnostních klíčů. Náhodné číslo tagu je generováno pomocí registru LFSR za konstantních počátečních podmínek. Generování každé náhodné hodnoty závisí pouze na počtu hodinových cyklů uplynulých mezi aktivací tagu (posun registru) a časem, kdy bylo číslo generováno. Hodnoty jsou generovány v maximální délce 16 bitů polynomem:

$$x^{16} + x^{14} + x^{13} + x^{11} + 1$$

Registr je taktovaný na 106kHz a obnovuje se každých 0,6 sekundy po vygenerování všech 65 535 výstupních hodnot. Z toho vyplývá, že rozmanitost náhodných čísel je velmi malá a nedostatečná. Zranitelnost generátoru navíc umocňuje fakt, že registr LFSR je po každém resetu nastaven do známého výchozího stavu pokaždé, než začne pracovat. Tento reset je zcela zbytečný, zvyšuje hardwarové režie a omezuje náhodnost.

V dnešní době již není problém zjistit toto náhodné číslo například použitím speciálního čtecího zařízení OpenPCD s uživatelským firmware. Dále je možné zajistit generování stejného „náhodného" čísla v každém dotazu, čímž se dokonale eliminuje náhodnost při procesu ověřování. Navíc bylo zjištěno, že stejná zranitelnost se objevuje i u 32 bitového

náhodného čísla generovaného čipem čtecího zařízení, což naznačuje podobnou hardwarovou implementaci v tagu a čtecím zařízení. [16]

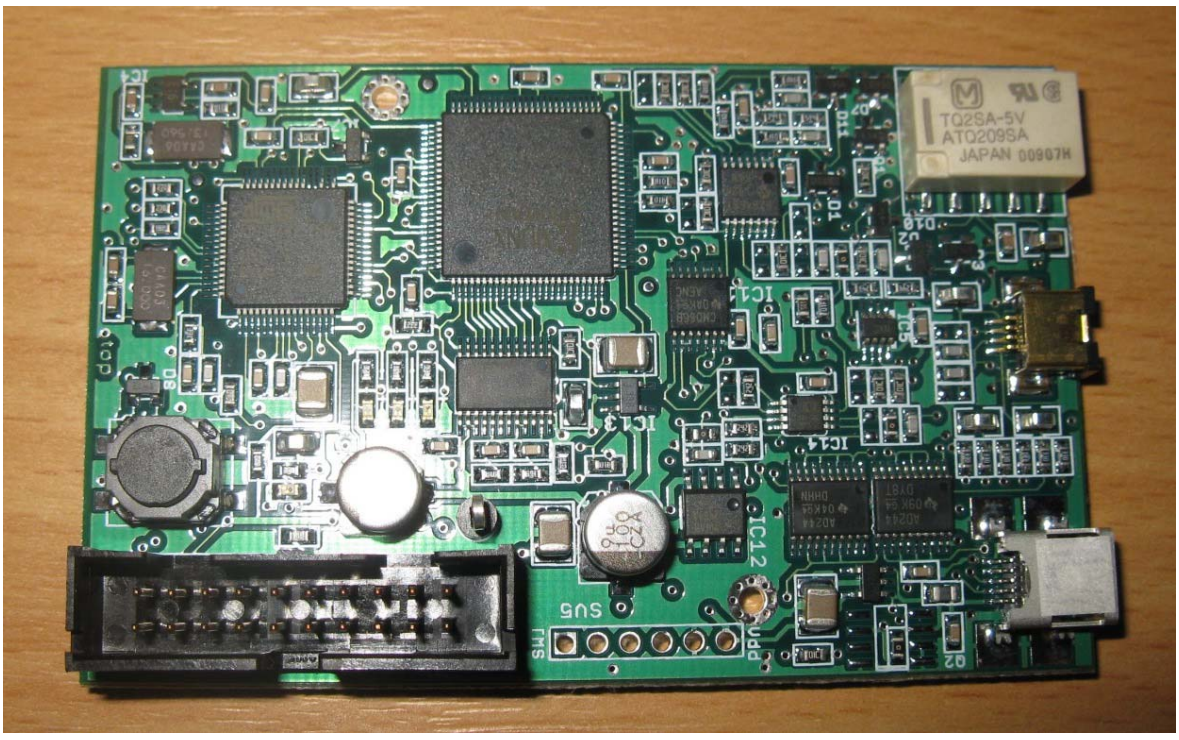
II. PRAKTICKÁ ČÁST

3 ÚTOK NA RFID SYSTÉM S EM4100 ČIPOVOU KARTOU

RFID systém s čipovými kartami EM4100 se používá pro přístupy do zabezpečených prostor UTB ve Zlíně, UTB knihovny, univerzitní menzy a k tiskovým službám. Útočník, který by se dostal k datům karty jiných uživatelů, by byl schopen například na úkor původního uživatele využívat tisková zařízení a tisknout „zdarma“.

3.1 Hardwarové prostředky

Pro provedení simulace a analýzu byl zvolen **PROXMARK III**. Jedná se o výkonný nástroj pro všeobecné použití RFID, jako je odposlouchávání komunikace mezi čtečkou a tagem, čtení různých typů tagů a emulace těchto tagů ve frekvenčním rozsahu 125kHz až 13,56 MHz. Zařízení je osazeno integrovaným obvodem řady Spartan vyráběného firmou Xilinx, který je velmi výkonným programovatelným obvodem typu FPGA (Field-Programmable Gate Arrays) řady XC2S30 s širokým rozsahem použití. Deska je dále osazena řídícím mikrokontrolerem ATMEL AT91SAM7S256, který je založen na 32 bitovém procesoru RISC ARM7TDMI. Pracuje na taktovací frekvenci 55MHz a obsahuje 256KB paměti typu flash a 64KB operační paměti SRAM. Zařízení původně navrhl pan Jonathanem Westhues a uvolnil jej pod GPL (General Public Licence – všeobecná veřejná licence) (Obr. 16).



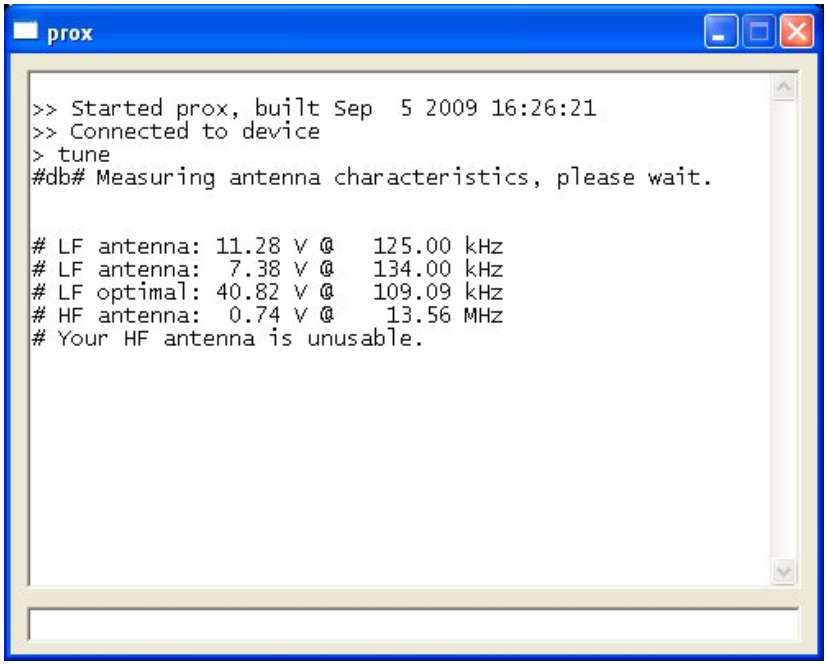
Obr. 16. PROXMARK III

Pro připojení napájení je dostupný USB Mini-A konektor, který je možné připojit přímo k PC, nebo lze připojit i externí zdroj napětí. Aby Proxmark mohl fungovat jako čtecí zařízení či emulátor čipových RFID karet, je třeba k němu připojit externí anténu. Pro HF frekvence byla zakoupena originální anténa speciálně určena k těmto účelům. Nicméně pro LF frekvence bylo třeba takovou anténu vyrobit. Originální anténa stojí v přepočtu 1500,- Kč, zatímco mnou vyrobená anténa vyjde na cca 90,- Kč (Obr. 17).

Obr. 17. LF anténa (125 kHz).

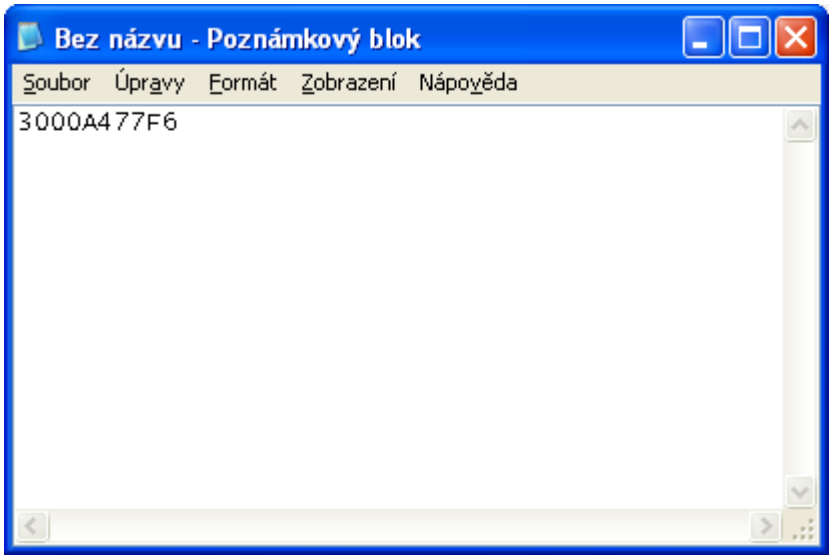
Obal antény je z plastu o velikosti 55 x 85 mm. Pro tyto rozměry bylo navinuto 100 závitů lakovaného drátu a připojeno pomocí USB kabelu na zařízení PROXMARK III. Pomocí softwarové komponenty (klienta) Prox GUI, která je vyvíjena a publikována pod GNU licencí, jsme schopni funkčnost antény ověřit (Obr. 18).

Příkazem „tune“ je možné provést měření vyladění antény. Z obrázku je patrné, že na frekvenci 125kHz anténa vrací 11,28 V. Tato hodnota je pro naše účely dostačující a čtecí vzdálenost se pohybuje kolem 7 centimetrů.



Obr. 18. Výsledek měření charakteristiky antény.

Pro kontrolní čtení čipových RFID karet je třeba zvolit referenční čtecí zařízení. Pro tyto účely bylo zvoleno zařízení Elatec – TWN3 Multi125 USB. Výhodou tohoto čtecího zařízení je, že používá nativní rozhraní USB-HID, a proto není potřeba speciální ovladač. Elatec se detekuje jako další USB klávesnice. Po vložení EM410x do elektromagnetického pole čtecího zařízení je možné ID čipu odečíst například z Poznámkového bloku ze systému Windows s přepnutou anglickou klávesnicí (Obr. 19).



Obr. 19. ID EM4100 přečtena čtečkou Elatec.

3.2 Emulace EM410x čipové karty

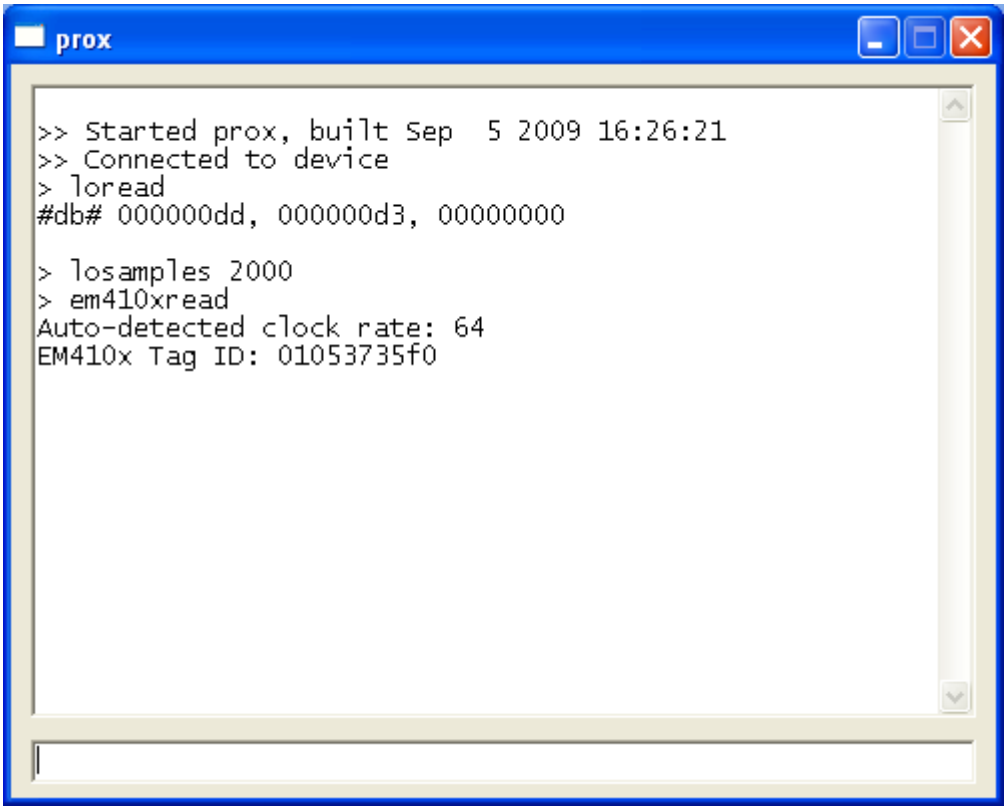
Systém využívající služeb čipových karet EM410x funguje na principu ověřování uživatele na základě ID čísla tagu v databázovém systému provozovatele. Pokud načtené ID číslo souhlasí se záznamem v databázi, je uživatel ověřen a na základě přidělených práv jsou mu zpřístupněny příslušné služby. V tomto případě je tedy dostačující, aby bylo jakýmkoli způsobem přečteno ID číslo uživatele, který se v databázi nachází, a toto ID poté emulovat například emulátorem PROXMARK III. Pro tyto účely můžeme využít například čtečku Elatec a ID číslo odečíst třeba z Poznámkového bloku systému Windows, nebo pro identifikaci tagu využijeme přímo PROXMARK III.

Pro využití emulátoru je třeba nejprve tento hardware „oživit“ uložením příslušného firmware do flash paměti zařízení. Firmware je vyvíjen na základě GNU licence komunitou uživatelů a existuje ve více verzích podle toho, jaký standard použití je vyžadován. Samotný firmware je rozdělen do tří logických částí: bootrom, fpga a operační systém. Bootrom (zavaděč) je relativně malá část kódu, která zabezpečuje základní inicializaci hardware, podporuje přeinstalování firmware přes USB rozhraní a zavádí spuštění operačního systému. Část FPGA se stará o zpracování, demodulaci a dekódování analogového signálu z antény. Operační systém je hlavní a největší část firmware zařízení, která implementuje požadovanou funkčnost a slouží jako rozhraní pro komunikaci se softwarovým klientem. Tato komunikace je opět zprostředkovávána pomocí USB rozhraní.

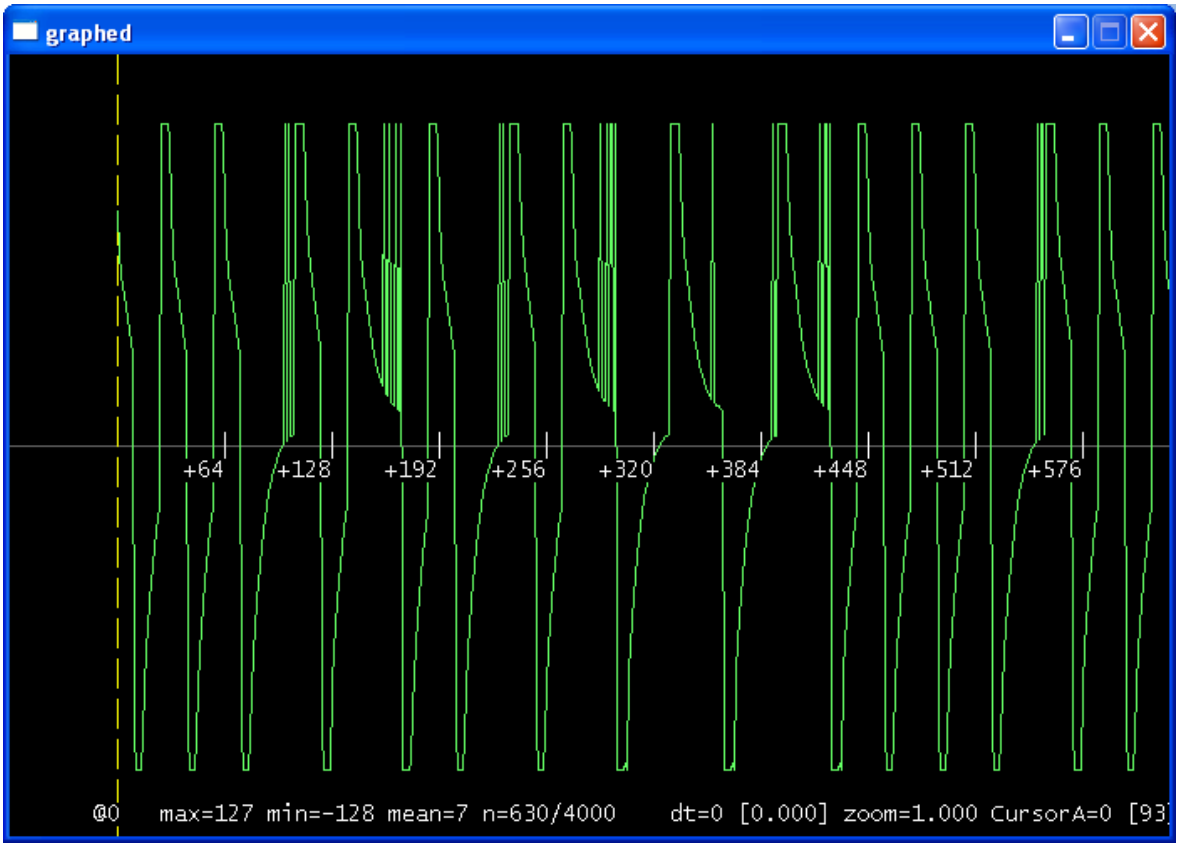
Pro naše účely byl vybrán firmware pm3-20090905-r216, který je dostupný z http://proxmark3.googlecode.com.

Po inicializaci a připojení hardware k USB rozhraní budeme využívat utilitu Prox, která je součástí softwarového balíčku společně se samotným firmwarem. Balíček obsahuje zdrojové kódy psané v jazyce C, a je možné je na základě GNU licence libovolně doplňovat či upravovat.

Pokud máme vše připraveno a víme, jaký typ karty budeme číst, připojíme vyrobenou anténu pro nízké frekvence a použijeme příkaz „loread“ pro konfiguraci komunikace a vytvoření simulace čtecího zařízení. Načtení samotného tagu je realizováno příkazem „losamples“ s parametrem, který nám udává počet načtených vzorků. Poslední fází je demodulace vzorků a dekódování ID čísla. V tomto případě víme, jaký typ tagu máme vložený do elektromagnetického pole simulovaného čtecího zařízení, a proto můžeme toto provést příkazem „em410xread“. Výsledek je patrný na obrázku 20 a 21.

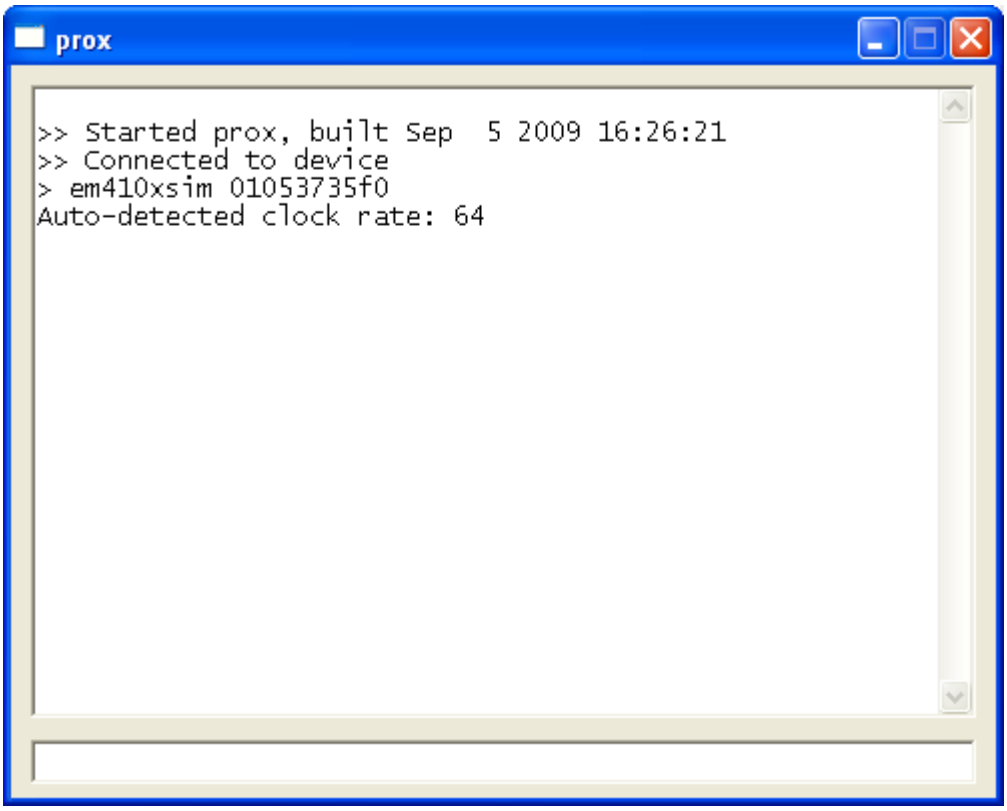


Obr. 20. Čtení EM410x tagu.



Obr. 21. Zachycená komunikace čtečka-EM410x tag.

Nyní máme zjištěné ID číslo EM410x karty a můžeme jednoduše zadáním příkazu „em410xsim“ provést simulaci samotného tagu (Obr. 22).



Obr. 22. Simulace EM410x tagu.

Pro předvedení reálného systému byla vybrána tisková služba SafeQ od společnosti YSOFT, která je implementována na UTB ve Zlíně. Na obrázku 23 je vidět načtení originální čipové karty vydané univerzitou a odblokování funkcí multifunkčního zařízení. Je evidentní, že kredit v systému je 999 Kč. Po nasimulování ID karty na zařízení PROXMARK III a vložení vyrobené LF antény do elektromagnetického pole se opět načte stejný uživatel se stejným kreditem a je možné bez problémů využívat služeb kopírování, jak je patrné z obrázku 24. Ten samý případ platí pro případný přístup do studovny či knihovny, nebo se může dotyčný útočník docela dobře najíst v univerzitní menze.

Obr. 23. Načtení originální čipové karty.

Obr. 24. Načtení emulované karty.

4 ÚTOK NA RFID SYSTÉM S MIFARE CLASSIC 4K ČIPOVOU KARTOU

V případě Mifare classic je situace už trochu zajímavější. Jednak lze kartu využít klasickým způsobem a použít pro identifikaci jen ID čísla karty. V tomto případě se dá velmi úspěšně použít i tag Mifare Ultralight, který se dodává i jako samolepka. Nebo jak bylo napsáno v kapitole 1.2.3 čipová karta Mifare classic obsahuje větší paměťový prostor, do kterého lze zapsat spoustu důležitých informací, které jsou ochráněny na základě dvou klíčů, a komunikace je šifrována.

4.1 Emulace Mifare classic na hardware PROXMARK III

V případě normy ISO 14443A je Proxmark schopen pracovat ve třech módech:

- Sniffing mode (odposlouchávání komunikace)
- Card emulation mode (emulace tagu)
- Reader mode (emulace čtecího zařízení)

Pro tuto část využijeme opět softwarového klienta Prox.exe, který byl vytvořen panem Jonathanem Westhuesem. Pro připojení k PC opět využijeme standardní HID (Human interface device) protokol. V případě čipových karet Mifare pracuje Winows klient se čtyřmi příkazy:

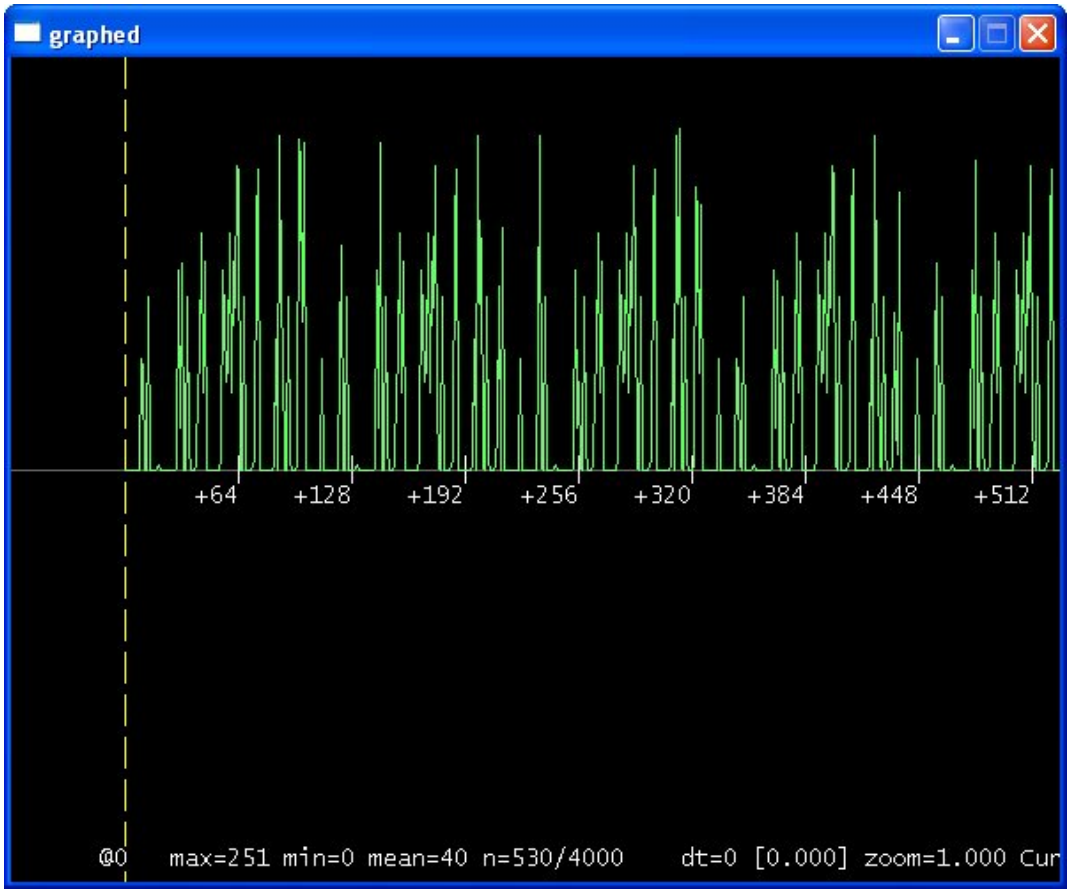
- **hi14asim –** Simulace ISO 14443-A tagu. Pomocí tohoto příkazu lze simulovat ID Mifare Classic 4k čipové karty.
- **hi14areader** – Pracuje jako čtecí zařízení. Proxmark zařízení generuje elektromagnetické pole, do kterého se vloží příslušná čipová karta. Případná komunikace mezi čtecím zařízením a tagem se uloží do bufferu na zařízení a je možné ji vyvolat příkazem hi14alist.
- **hi14asnoop –** Tento příkaz spustí odposlouchávání komunikace mezi autorizovaným čtecím zařízením a tagem. Tato komunikace je zachycena a uložena opět do bufferu, a jako v předchozím případě lze pro výpis komunikace použít příkaz hi14alist.
- **hi14alist –** Pomocí tohoto příkazu je možné zachycená data pomocí hi14areader a hi14asnoop stáhnout z bufferu a zobrazit v textové podobě v okně klientské aplikace.

Abychom mohli využít všechny funkčnosti hardware Proxmark je potřeba mít přístup k autorizovanému čtecímu zařízení, nebo alespoň referenčnímu čtecímu zařízení, na kterém si můžeme tuto komunikaci předvést. V tomto případě bylo využito nezávislého čtecího zařízení Touchatag od společnosti Altacel-Lucent (Obr. 25).

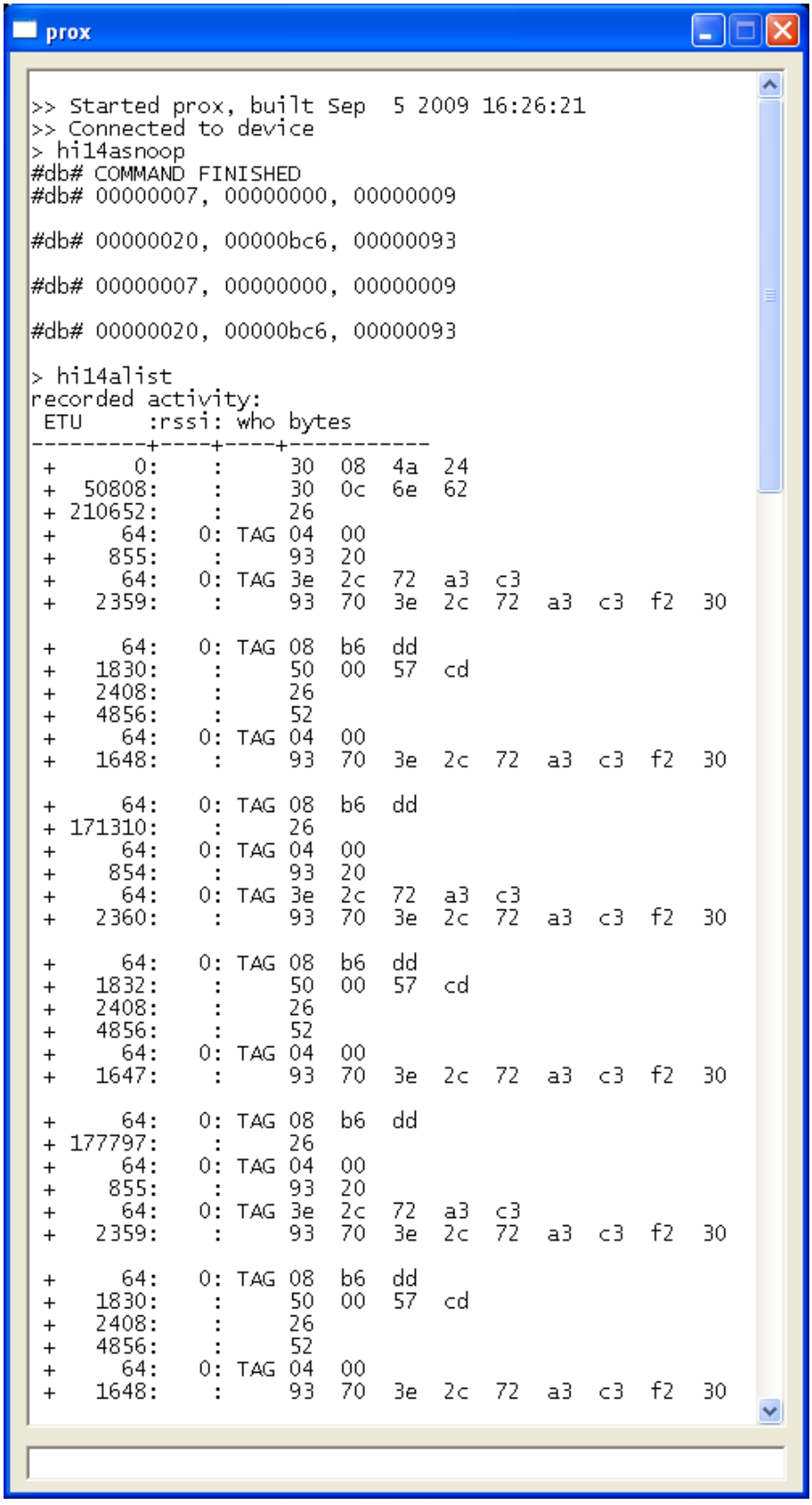
Obr. 25. Čtecí zařízení pro Mifare tagy.

Spuštěním příkazu hi14asnoop odstartujeme zachytávání komunikace mezi čtecím zařízením a tagem (CSAD Mifare Classic 1k – elektronická peněženka), která je načítána až do zaplnění bufferu. Pro bezproblémové zachycení této komunikace bylo třeba k zařízení Proxmark připojit příslušnou anténu konstrukčně vyrobenou pro pracovní frekvenci 13,56 MHz. Samotné provedení celé akce je zobrazeno na obrázku 26 a 27 na následující straně.

Obr. 26. Zachytávání komunikace Mifare classic čipové karty CSAD.



Obr. 27. Zachycený modulovaný signál mezi čtečkou a Mifare Classic.



Obr. 28. Komunikace čtečka - Mifare Classic čipová karta po demodulaci a dekódování.

Na obrázku 27 vidíme výpis průběhu zachytávání po zadání příkazu hi14asnoop. Proxmark III bude načítat data do naplnění bufferu. Podle analýzy je evidentní, že se jedná o zachycenou opakující se antikolizní smyčku. Z toho vyplývá, že simulované čtecí zařízení bude tak dlouho číst data, dokud bude tag v jejím dosahu. Jednotlivé kroky komunikace jsou následující:

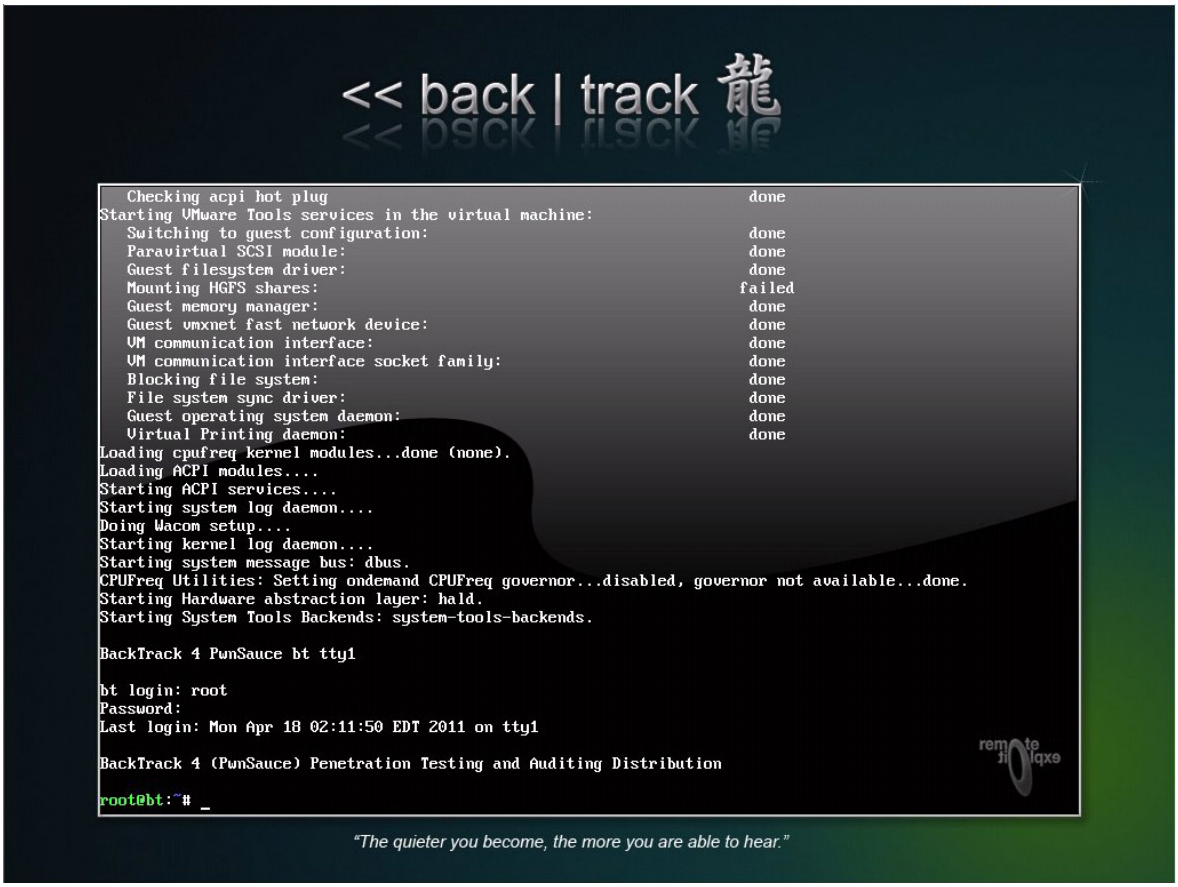
- **Čtečka: 26 -> Tag:04 00** – Čtecí zařízení vyšle do pléna příkaz „Request Standart" pod kódem hexa 0x26 a čeká na odezvu. Tag příjme příkaz a odpoví hodnotou 0x04 0x00, kterou informuje čtecí zařízení o své přítomnosti a svém typu.
- **Čtečka: 93 20 ->Tag:3e 2c 72 a3 c3 –** Čtecí zařízení kódem 0x93 0x20 spustí antikolizní proces pro výběr konkrétního tagu a vyžádá si jeho identifikační číslo. Tag odpoví svým identifikačním číslem 0x3e 0x2c 0x72 0xa3 a poslední byte je výsledkem hodnoty XOR prvních čtyř bytů identifikačního čísla tagu.
- **Čtečka: 93 70 3e 2c 72 a3 c3 f2 30 -> Tag: 08 b6 dd –** Čtecí zařízení vybere vložený tag odesláním kódu 0x93 0x70 následovaný jeho identifikačním číslem. Pokud je tag úspěšně vybrán odpoví kódem 0x08 0xb6 0xdd. Dále by podle softwarové implementace následovala autentizace a příkazy pro čtení či zápis.

Tuto komunikaci můžeme úspěšně simulovat příkazem hi14asim následovaný UID číslem simulovaného tagu. Nicméně tento způsob je použitelný pouze v případě identifikace dle ID čísla Mifare Classic tagu.

4.2 Offline útok na Mifare classic čipovou kartu

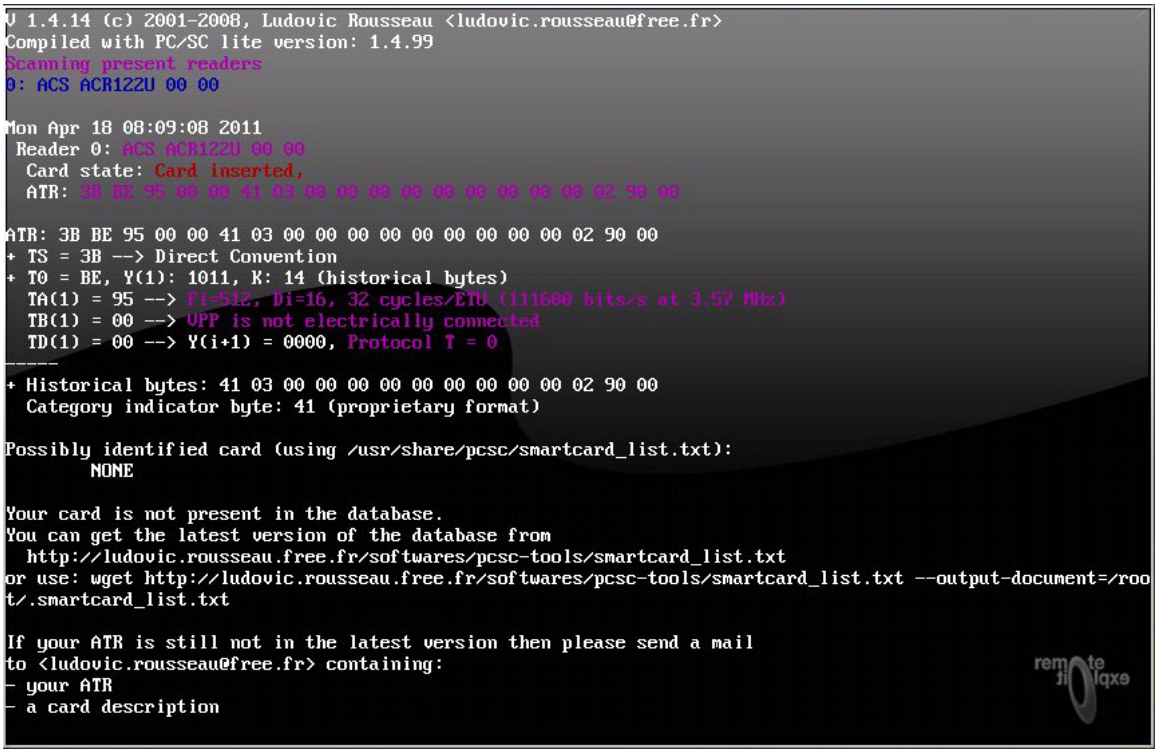
V případě, že budeme moci přečíst kompletní obsah paměti Mifare classic, naskytne se nám možnost data z paměti zálohovat či můžeme s těmito daty libovolně manipulovat. Abychom byli schopni toto provést, je třeba znát všechny klíče k sektorům, které máme v úmyslu číst či do kterých chceme zapisovat.

Pro práci s Mifare classic tagy se jako nevýhodnější jeví Open Source knihovna Libnfc vyvíjená komunitou pod GNU licencí a pracující na základě komunikační technologie NFC (Near Field Communication), která je rozšířením standardu ISO 14443. Knihovna Libnfc je psána v jazyce C++, a proto jsem vybral jako hostící operační systém Linux v distribuci BackTrack (Obr. 29).



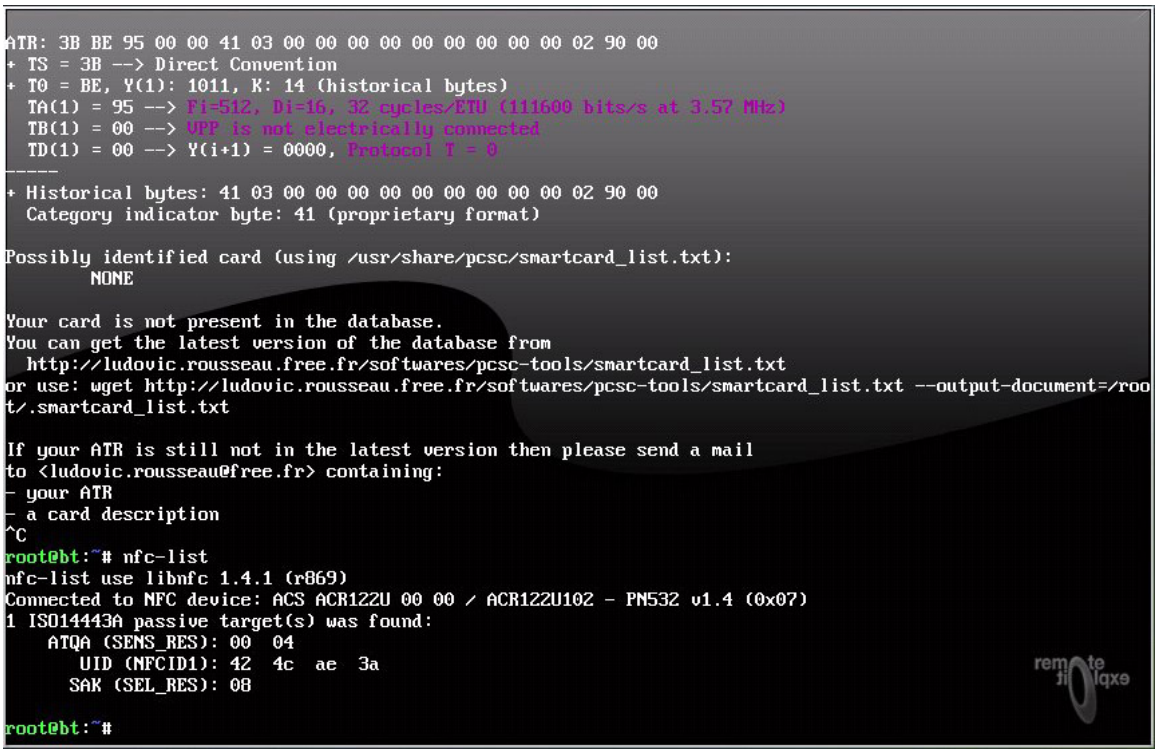
Obr. 29. OS Linux BackTrack.

Tato distribuce je výhodná hlavně proto, že již obsahuje softwarové balíčky, jako je například kompilátor GCC, potřebný pro překládání zdrojového C++ kódu. Samotná distribuce je zároveň oficiálně vydávána pro účely penetračních testů a auditů bezpečnosti. Jako čtecí zařízení použijeme nám již známý Touchatag od společnosti Altacel-Lucent. Obrázek 24. Čtecí zařízení potřebuje pro komunikaci ovladače, které jsou k dispozici v balíčku ACR122U_Package_Lnx_101_P, a balíček PCSC-Lite, který slouží jako prostředník pro přístup k čipové kartě a načtení hardware čtecího zařízení přes rozhranní USB. Jestliže máme všechny tyto potřebné balíčky nainstalované, ověříme správnou funkci čtecího zařízení pomocí příkazu PCSC_SCAN, který nám vypíše informace o tomto zařízení. Tyto informace jsou patrné z obrázku 30. na další straně.



Obr. 30. Aktivace čtecího zařízení Touchatag v Linuxu.

Po aktivaci čtecího zařízení již můžeme pomocí příkazu nfc-list zjistit, jaký typ karty je aktuálně vložen v elektromagnetickém poli zařízení. Na obrázku 31. vidíme příklad, kdy byla načtena čipová karta Mifare classic 1k.



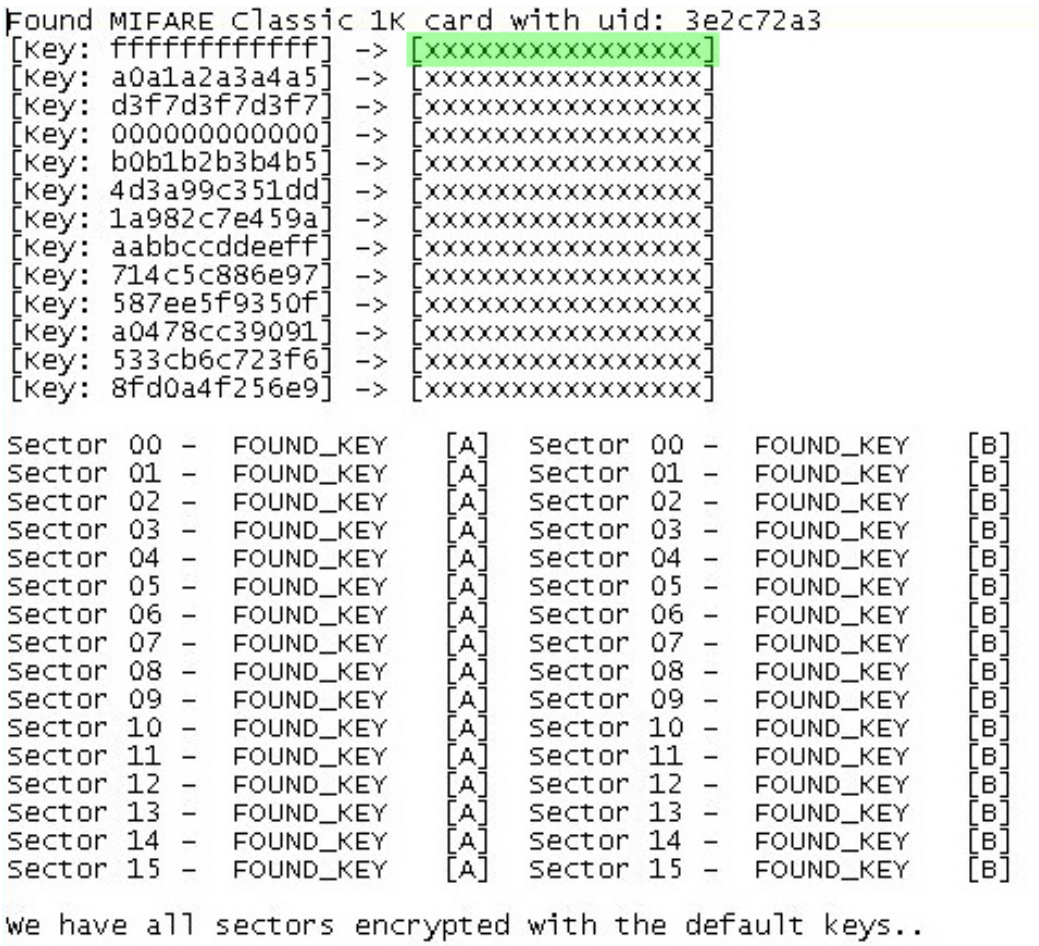
Obr. 31. Nfc_list Mifare Classic 1k UID: 42 4c ae 3a.

Nyní jsme již ve fázi, kdy máme plně funkční čtecí zařízení a jsme schopni rozpoznat Mifare Classic tag. Pro samotný offline útok využijeme kódu zveřejněného společností Nethemba dostupného z webových stránek zmíněné společnosti. Tento kód obsahuje samotnou implementaci nfc komunikace **nfc-utils.c**, implementaci CRYPTO1, **crapto1.c** a **crypto1.c**. Důležitou částí je identifikace Mifare Classic čipové karty, která je řešena v kódu **mifare.c,** a samotný výpočet šifrovacích klíčů, který je implementován v souboru **mfoc.c.** Abychom mohli výpočet pomocí MFOC použít, musí být splněna nutná podmínka, že některý ze sektorů na kartě musí obsahovat takzvaný defaultní klíč, který je předem známý (Tab. 7).

Tab. 7. Seznam defaultních klíčů.

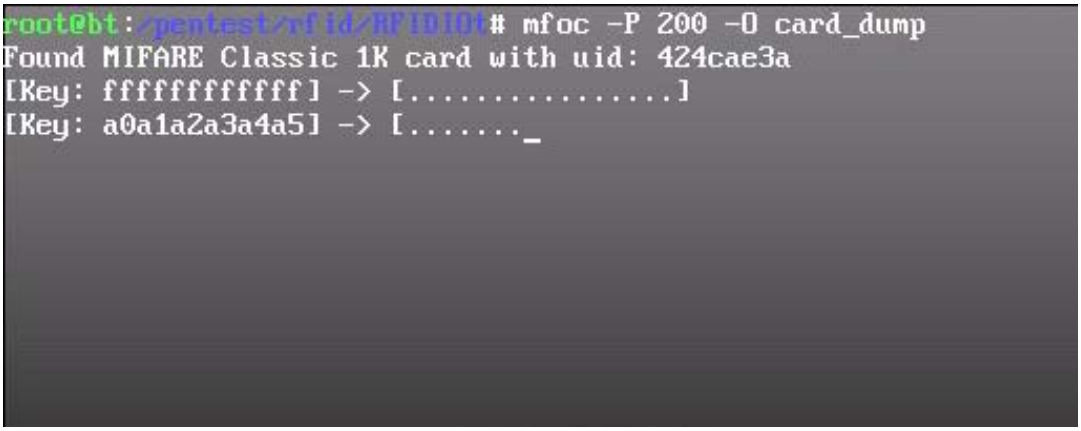
Hodnota klíče	Poznámka
A0 A1 A2 A3 A4 A5	MAD klíč
D3 F7 D3 F7 D3 F7	Content klíč
00 00 00 00 00 00	Prázdný klíč
B0 B1 B2 B3 B4 B5	
4D 3A 99 C3 51 DD	
1A 98 2C 7E 45 9A	
AA BB CC DD EE FF	
71 4C 5C 88 6E 97	
58 7E E5 F9 35 0F	
A0 47 8C C3 90 91	
53 3C B6 C7 23 F6	
8F D0 A4 F2 56 E9	

V případě, že ani jeden z těchto klíčů se v paměťových sektorech tagu nevyskytuje, je možné takový klíč získat odposlechem komunikace tagu a autorizovaného čtecího zařízení, který jsme si nastínili v kapitole 4.1. Na obrázku 31 je předvedeno, jak vypadá průběh hledání defaultních klíčů aplikovaný na prázdnou nenaprogramovanou Mifare classic 1k čipovou kartu. Z obrázku je patrné, že na tomto tagu je ve všech paměťových sektorech použito defaultního klíče FF FF FF FF FF FF. Tato karta je v tomto případě použitelná pouze pro identifikaci na základě svého UID čísla.



Obr. 32. Výstup MFOC pro Mifare S50 prázdnou kartu.

Pokud je příslušný klíč nalezen, je toto identifikováno na výstupu znakem x pro příslušný paměťový sektor (zelený řádek na obrázku 32). Jakmile prohledávání a případné počítání klíčů úspěšně skončí nalezením všech A i B klíčů, je celý obsah paměti uložen do souboru a je možné dále s tímto souborem manipulovat.



Obr. 33. Příklad aplikace příkazu „mfoc“.

Soubor důležitých parametrů MFOC je následující:

- Parametr B – Vyhodnocování klíče ‚B' místo klíče ‚A'.
- Parametr k – Použití specifického klíče místo vyhledávání defaultních klíčů.
- Parametr P – Udává počet realizací výpočtů pro jeden sektor – výchozí je 20.
- Parametr s – Specifikace pořadových čísel sektorů pro výpočet klíčů. Například: -s 0,1,3,5..
- Parametr O – Jako jediný povinný parametr. Tímto parametrem zadáváme vyhodnocovací soubor, který bude obsahovat samotné odhalené klíče jednotlivých sektorů.

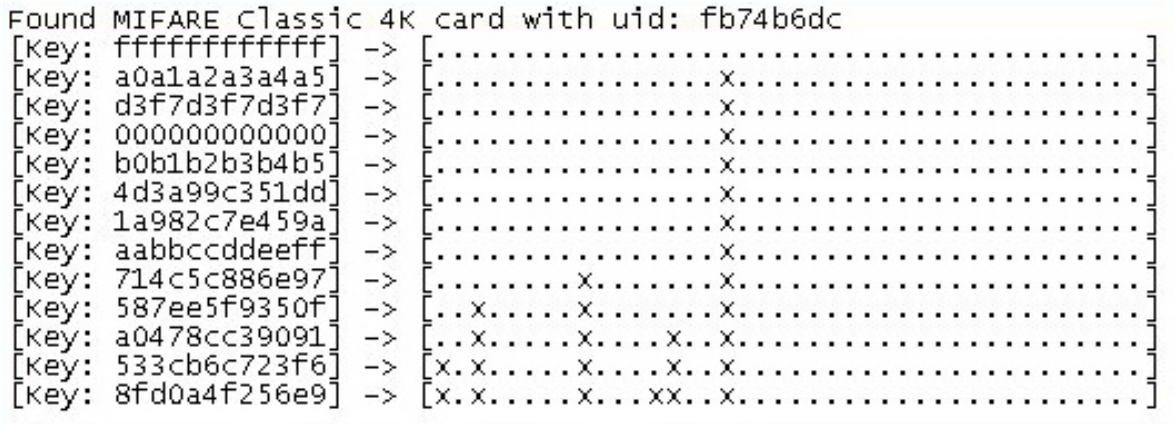
4.2.1 Analýza čipové karty ČSAD

Pro analýzu fyzicky nasazené a v praxi používané čipové RFID karty, jsem vybral takzvanou „Elektronickou peněženku společnosti ČSAD".

Obr. 34. RFID Mifare classic čipová karta ČSAD Vsetín.

Testovat budeme tři karty. Dvě nové karty Mifare classic 4k a jedna starší Mifare classic 1k.

Prvním krokem bude tedy otestování karty na defaultní známé klíče (tabulka 7).



Obr. 35. Proces vyhledávání defaultních klíčů na Mifare classic RFID čipové kartě.

Z obrázku 35 je patrné, že čipová karta obsahuje defaultní klíče ‚A', a to v sektoru 16 klíč: a0a1a2a3a4a5, v sektoru 8 klíč: 714c5c886e97, v sektoru 2 klíč: 587ee5f9350f, v sektoru 13 klíč: a0478cc39091, v sektoru 0 klíč: 533cb6c723f6 a v sektoru 12 klíč: 8fd0a4f256e9.

Byla tedy splněna podmínka pro vyhledávání neznámých klíčů, které může být nyní aplikováno. Aplikaci vyhledávání klíčů provedeme pro změnu na Mifare classic 1k kartě.

Na obrázku 35 vidíme, že všechny defaultní klíče použité u této čipové karty, jsou shodné s defaultními klíči, které byly nalezeny na předchozí variantě. Rozdíl je samozřejmě pouze v klíči, který se nachází na 4k kartě v sektoru 16, protože tento sektor se již v 1 kilobytové paměti testované karty nenachází. Pro výpočet „tajných" klíčů je provedeno ověření příslušného paměťového sektoru defaultním klíčem a je přečtena odpověď tagu Nt. Znovu je provedeno ověření toho samého paměťového sektoru a je přečtena odpověď tagu Nt. Nyní je ovšem tento proces ověření již šifrován. Proběhne výpočet času posunu LFSR zásobníku. Dalším krokem je pokus odhadu hodnoty Nt a ověření jiného paměťového sektoru. Počítání tabulky LFSR zásobníku znamená procházení 2^{36} hodnot 0 až FFFFFFFFF a adekvátní klíče ks2, ks3. Celková doba výpočtu může být podle typu tagu 4 až 18 hodin.

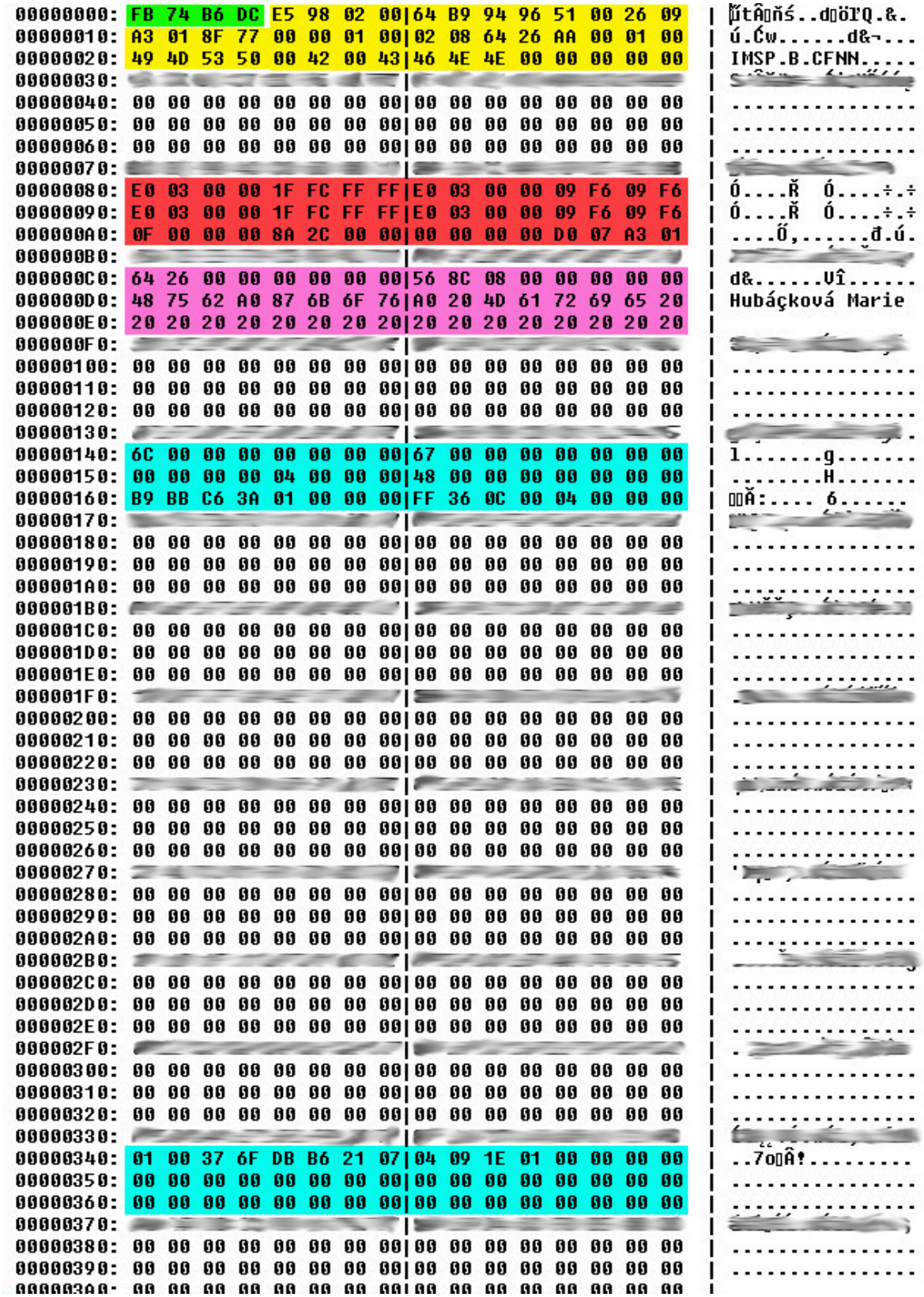
Vzhledem k tomu, že se jedná o citlivé informace, jsou hodnoty vypočítaných klíčů pro příslušné paměťové sektory na obrázku 36 kvůli bezpečnosti nečitelné. Proces vyhledávání tajných klíčů jsem nejprve realizoval na nejnověji pořízenou Mifare classic 4k čipovou kartu společnosti ČSAD Uherské Hradiště (Obr. 36).

```
Found MIFARE Classic 1K card with uid: 424cae3a
[Key: ffffffffffff] -> [................]
[Key: a0a1a2a3a4a5] -> [................]
[Key: d3f7d3f7d3f7] -> [................]
[Key: 000000000000] -> [................]
[Key: b0b1b2b3b4b5] -> [................]
[Key: 4d3a99c351dd] -> [................]
[Key: 1a982c7e459a] -> [................]
[Key: aabbccddeeff] -> [................]
[Key: 714c5c886e97] -> [........x.......]
[Key: 587ee5f9350f] -> [..x.....x.......]
[Key: a0478cc39091] -> [..x.....x....x..]
[Key: 533cb6c723f6] -> [x.x.....x....x..]
[Key: 8fd0a4f256e9] -> [x.x.....x...xx..]

Sector 00 -  FOUND_KEY   [A]  Sector 00 -  UNKNOWN_KEY [B]
Sector 01 -  UNKNOWN_KEY [A]  Sector 01 -  UNKNOWN_KEY [B]
Sector 02 -  FOUND_KEY   [A]  Sector 02 -  UNKNOWN_KEY [B]
Sector 03 -  UNKNOWN_KEY [A]  Sector 03 -  UNKNOWN_KEY [B]
Sector 04 -  UNKNOWN_KEY [A]  Sector 04 -  UNKNOWN_KEY [B]
Sector 05 -  UNKNOWN_KEY [A]  Sector 05 -  UNKNOWN_KEY [B]
Sector 06 -  UNKNOWN_KEY [A]  Sector 06 -  UNKNOWN_KEY [B]
Sector 07 -  UNKNOWN_KEY [A]  Sector 07 -  UNKNOWN_KEY [B]
Sector 08 -  FOUND_KEY   [A]  Sector 08 -  UNKNOWN_KEY [B]
Sector 09 -  UNKNOWN_KEY [A]  Sector 09 -  UNKNOWN_KEY [B]
Sector 10 -  UNKNOWN_KEY [A]  Sector 10 -  UNKNOWN_KEY [B]
Sector 11 -  UNKNOWN_KEY [A]  Sector 11 -  UNKNOWN_KEY [B]
Sector 12 -  FOUND_KEY   [A]  Sector 12 -  UNKNOWN_KEY [B]
Sector 13 -  FOUND_KEY   [A]  Sector 13 -  UNKNOWN_KEY [B]
Sector 14 -  UNKNOWN_KEY [A]  Sector 14 -  UNKNOWN_KEY [B]
Sector 15 -  UNKNOWN_KEY [A]  Sector 15 -  UNKNOWN_KEY [B]


Using sector 00 as an exploit sector
Sector: 1, type A, probe 0, distance 43630 .....
Sector: 1, type A, probe 1, distance 43576 .....
Sector: 1, type A, probe 2, distance 43579 .....
Sector: 1, type A, probe 3, distance 43585 .....
Sector: 1, type A, probe 4, distance 43579 .....
Found Key: A [            ]
Sector: 3, type A, probe 0, distance 43571 .....
Sector: 3, type A, probe 1, distance 43570 .....
Sector: 3, type A, probe 2, distance 43630 .....
Sector: 3, type A, probe 3, distance 43582 .....
Sector: 3, type A, probe 4, distance 45187 .....
Sector: 3, type A, probe 5, distance 43672 .....
Sector: 3, type A, probe 6, distance 43573 .....
Sector: 3, type A, probe 7, distance 45277 .....
Sector: 3, type A, probe 8, distance 43672 .....
Sector: 3, type A, probe 9, distance 43627 .....
Sector: 3, type A, probe 10, distance 43576 .....
Sector: 3, type A, probe 11, distance 43574 .....
Sector: 3, type A, probe 12, distance 43573 .....
Found Key: A [            ]
Sector: 4, type A, probe 0, distance 43520 .....
Sector: 4, type A, probe 1, distance 43627 .....
Sector: 4, type A, probe 2, distance 44104 .....
Sector: 4, type A, probe 3, distance 43197 .....
Sector: 4, type A, probe 4, distance 43528 .....
Sector: 4, type A, probe 5, distance 43576 .....
Sector: 4, type A, probe 6, distance 43568 .....
Sector: 4, type A, probe 7, distance 45131 .....
Sector: 4, type A, probe 8, distance 43585 .....
Sector: 4, type A, probe 9, distance 44528 .....
Sector: 4, type A, probe 10, distance 43531 .....
Sector: 4, type A, probe 11, distance 43576 .....
Sector: 4, type A, probe 12, distance 43582 .....
```

Obr. 36. Průběh odhadu a výpočtu tajných klíčů.



Obr. 37. Přečtený obsah paměti, obsahující data ČSAD čipové karty.

Na obrázku 37 je zobrazen obsah prvních 15 sektorů Mifare Classic 4k čipové karty. Další sektory jsou prázdné a nejsou proto důležité. Jak již bylo zmíněno výše, jedná se o takzvanou elektronickou peněženku ČSAD. Na obrázku 37 jsou barevně vyznačeny obsahy pro nás zajímavých sektorů. Identifikační číslo tagu je podbarveno zeleně. Žlutá barva označuje interní data společnosti a zůstávají neměnná. Červený sektor skrývá informace o kreditu uloženém v této části paměti. Do tohoto sektoru se zapisuje při každé uskutečněné jízdě. Obsahem fialového sektoru jsou data majitele elektronické peněženky a také tyto data zůstávají konstantní. Konečně dva azurové sektory obsahují data o zvýhodněné trase, kterou si zvolil zákazník. Tyto data jsou zapsána při prvním použití čipové karty. Zajímavostí je, že čipová karta vydaná ČSAD Vsetín před cca 7 lety má stejné přístupové klíče do odpovídajících sektorů jako nejnověji vydané karty ČSAD Uherské Hradiště. Toto vidím, jako velký bezpečnostní problém.

Soubor, který jsme touto akcí získali, je nazýván jako výpisový soubor („dump file“). Tento soubor můžeme posléze s výhodou použít jako zdroj přístupových klíčů pro čtení cizích čipových elektronických peněženek. S dostatečným vybavením a kvalitní RFID anténou jsme schopni celou kartu přečíst za 5 respektive 12 sekund, podle velikosti paměti (Obr. 38 a 39).

```
root@bt:/# nfc-mfclassic r a dump.mfd keys.mfd
Connected to NFC reader: ACS ACR122U 00 00 / ACR122U102 - PN532 v1.4 (0x07)
Found MIFARE Classic 1k card with UID: 3aae4c42
Reading out 64 blocks |................|
Done, 64 of 64 blocks read.
Writing data to file: dump.mfd ...Done.
```

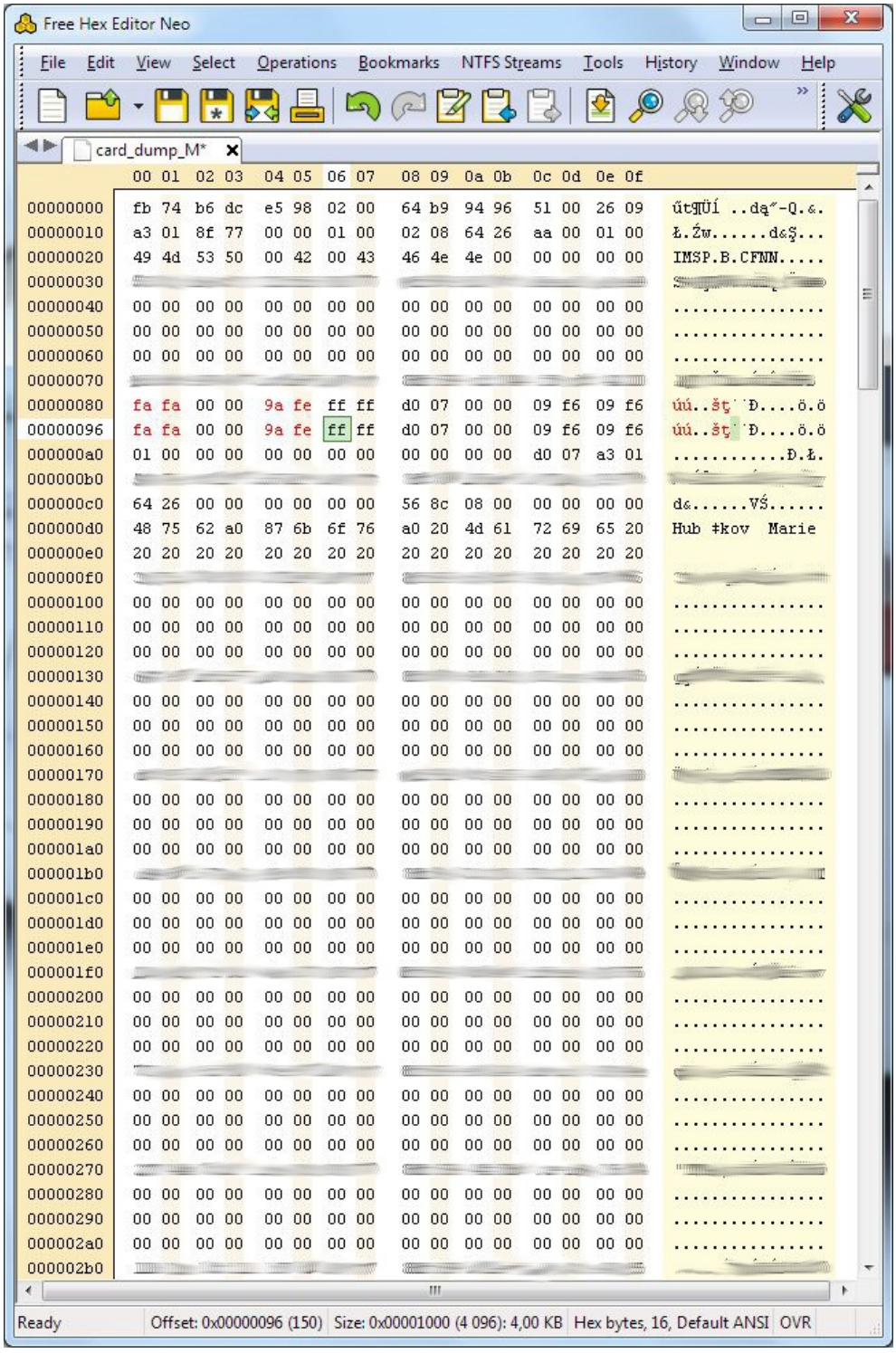
Obr. 38. Čtení Mifare classic na základě výpisového souboru.

```
root@bt:/# nfc-mfclassic w b dump.mfd keys.mfd
Connected to NFC reader: ACS ACR122U 00 00 / ACR122U102 - PN532 v1.4 (0x07)
Found MIFARE Classic 1k card with UID: 3aae4c42
Writing 64 blocks |................|
Done, 64 of 64 blocks written.
```

Obr. 39. Zápis na Mifare classic na základě výpisového souboru.

Jak je patrné z obrázků 38 a 39, pro čtení i zápis s výhodou využijeme nástroj „nfc-mfclassic“, který je součástí knihovny LIBNFC (Near Field Communication library). Z předchozích informací nám vyplývají různé možnosti, co všechno může být v souvislosti

s čipovou kartou Mifare classic zneužito. Předně je to možnost takovou kartu použít jako kartu s „nekonečným“ kreditem. Stačí přečíst a zálohovat kompletní obsah důležitých paměťových sektorů nabité karty a tuto paměť po vypotřebování kreditu těmito daty obnovit. Nebo můžeme jednoduše editovat obsah sektoru s kreditem a tento kredit navýšit.



Obr. 40. Free Hex Editor Neo.

Na obrázku 40 je zobrazen Free Hex Editor Neo, který je volně ke stažení a lze jej použít k výše zmíněným účelům. Editované položky jsou v souboru na adrese 90 a 96 v sektoru paměti určeném k uložení hodnoty kreditu. Červeně zvýrazněné hodnoty byly aktuálně editovány a takto pozměnění soubor se jednoduše uloží a přehraje do čipové RFID karty. Tímto způsobem lze získat až maximální kredit, který je 9999 Kč.

Poslední možností zneužití je krádež osobních údajů ostatních cestujících. Během jedné jízdy autobusem je možné získat data většiny cestujících a tato data mohou být různým způsobem zneužita.

5 NÁVRH ÚPRAV ZABEZPEČENÍ KOMPROMITOVANÝCH SYSTÉMŮ

Z výsledků auditu vyplývá, že v současné době používané systémy jsou velmi slabě zabezpečené a jenom trochu zdatný útočník se může k datům čipových karet jednoduše dostat. Proto je důležité apelovat na dodavatele karet, ale hlavně na provozovatele, kteří by si měli toto uvědomit a v co největší míře sjednat nápravu.

5.1 Zvýšení zabezpečení ověřování pomocí RFID tagů čipových karet EM 41xx

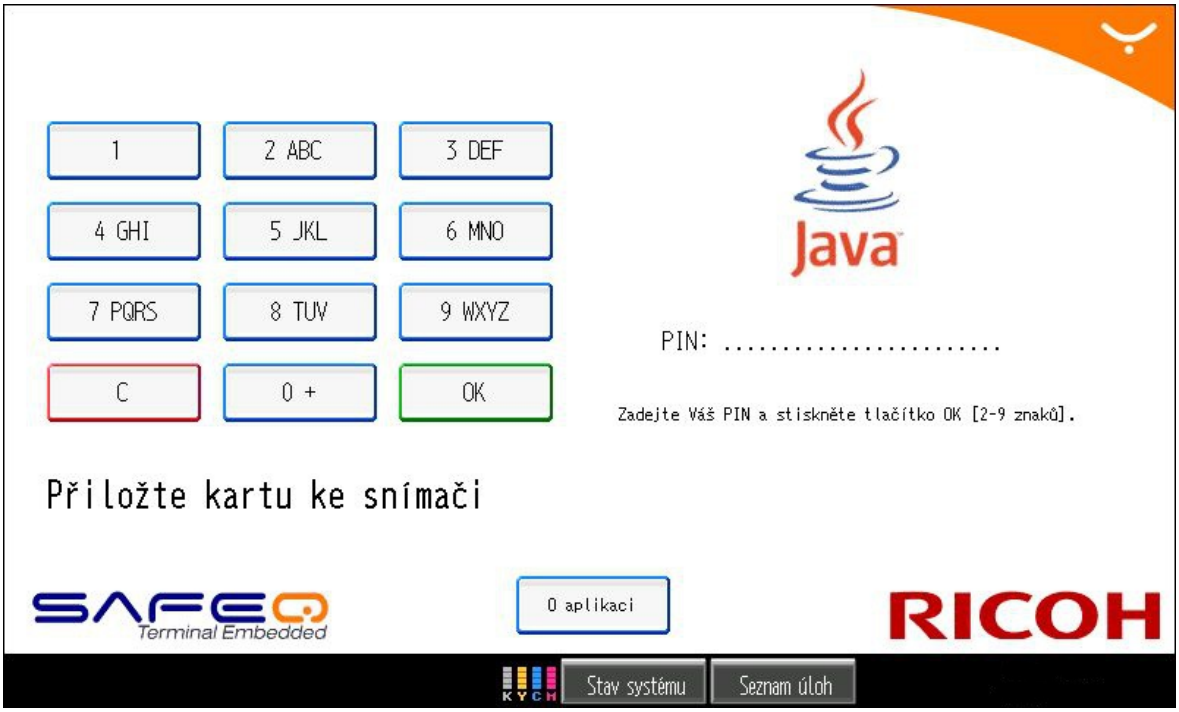
V případě karet EM41xx bude zabezpečení proti zcizení UID čísla trochu složitější. Předně je si potřeba uvědomit, že tyto tagy nemají žádné zabezpečení, a navíc ani není třeba fyzického kontaktu útočníka s kompromitovanou kartou. Stačí se dostat i jiným způsobem k databázi UID čísel karet a tyto tagy posléze naklonovat způsobem, který je popsán v kapitole 3.2.

Pokud se tyto čipové karty používají pro přístupy do zabezpečených prostor, je zneužití emulací karty podobné jako okopírování klíče vložky FAB. Tady se jde bránit například

Obr. 41. Peněženka pro RFID karty.

zamezením fyzického odposlechu karty používáním speciálních obalů či peněženek, které obsahují specifickou kovovou fólii pro vytvoření takzvané Faradayovy klece.

U kombinovaných systémů, kde se využívá čipových karet pro platby tiskových služeb a přístupů tak, jak to bylo prezentováno v kapitole 3.2, je možné zvýšit zabezpečení použitím zdvojené autentizace vyžadováním zadáním pinu v kombinaci s čipovou kartou, jak je to naznačeno na obrázku 42.



Obr. 42. Příklad kombinované metody přístupu ověření.

Samozřejmostí by mělo být monitorování citlivých přístupových míst pomocí kamerových systémů a fyzické ostrahy.

5.2 Úpravy zabezpečení systémů využívajících Mifare classic čipových karet

Čipové karty Mifare classic jsou stále velmi populární a vzhledem k této popularitě je firma NXP Semiconductors stále vyrábí a pravděpodobně v nezměněné podobě vyrábět bude i v budoucnosti. Nicméně vzhledem k vážné implementační chybě již není možné tyto čipové karty doporučit pro zavádění nových bezpečnostních systémů. U již zaběhnutých systémů je nejspolehlivějším řešením výměna všech těchto karet za novější, lépe zabezpečení Mifare DESFire karty, u kterých zatím nebyly zjištěny žádné kritické

zranitelnosti. Vzhledem k tomu, že by byla taková akce velmi finančně náročná, tak ani samotná výměna celého systému by se pravděpodobně neobešla bez velkých finančních ztrát.

Zneužití čipových karet obnovením kreditu či jeho svévolné navyšování je možné zamezit zavedením on-line čtecích terminálů, které by umožňovali kontrolu hodnoty kreditu v reálném čase z centrální databáze systému. Problém může nastat pouze v případě, kdy útočník použije 100% emulované čipové karty. Tady bohužel bude mít problém hlavně majitel originální karty, na jehož účet může útočník vybírat kredit. Ochrana proti zcizení dat originální karty, i když ne 100%, může být v případě použití speciálního obalu pro RFID karty (Obr. 41).

Problém modifikace obsahu karty lze řešit digitálním podpisem pomocí asymetrické kryptografie. Nicméně ani tato možnost nezabrání kompletnímu přečtení obsahu paměti a následnému obnovení tohoto obsahu na původní kartě.

Další možností by mohlo být zavedení speciálního počítadla implementovaného v paměťovém sektoru karty, které by bylo možné pouze načítat a jeho hodnotu po každé operaci automaticky odečíst. Tento proces nám zaručí oprávnění použitá u obou klíčů příslušného sektoru. Jiné operace by nebyly povoleny. Tímto a kombinací předchozích řešení lze zabránit jednoduchému klonování karty a její modifikaci i obnovení. Nezabrání ale samotnému přečtení a případnému emulování přečtené čipové karty.

Z předchozích zjištění vyplývá, že jediné 100% zabezpečení Mifare classic karty je její výměna za jiný lépe zabezpečený typ, jak již bylo napsáno výše.

ZÁVĚR

Tato práce není návodem jakým způsobem obejít ochrany, ani nezveřejňuje zjištěné tajné klíče. Je pouze auditem zabezpečení systémů používajících RFID čipové karty a upozorňuje na jejich nedostatky.

Teoretická část se věnuje popisu RFID (Radio Frequency Identification) systému jako celku. Nejprve popisuje samotný princip funkčnosti systému a jeho výhody či případné nevýhody. Dále se věnuje nejčastěji používaným typům jednotlivých tagů (EM41xx, Mifare, atd.), které se vyskytují v České republice. V dalších kapitolách je zmínka o známých typech útoků, které byly do dnešní doby zkoumány a zaznamenány. Kapitola 2 teoretické části se podrobněji věnuje čipovým kartám v souvislosti s analýzou komunikace protokolů mezi čtečkou a čipovou kartou tagů EM4102 a Mifare classic.

Praktická část se již zabývá konkrétním testováním samotné bezpečnosti vybraných tagů. Nejprve jsou uvedeny hardwarové prostředky, které bylo nutno využít pro tyto účely. Jako první byla testována čipová karta EM4102, která se používá na Univerzitě Tomáše Bati, pro umožnění přístupů do zabezpečených prostor univerzity, a zároveň slouží i k provádění plateb tiskových a jiných služeb, které využívají nejen studenti.

RFID čipová karta Mifare classic byla zastoupena takzvanou elektronickou peněženkou firmy ČSAD Uherské Hradiště a ČSAD Vsetín, přičemž se jednalo o varianty s pamětí 1 kilobyte respektive 4 kilobyty.

Poslední kapitola praktické části je věnována metodám, pomocí kterých by bylo možné bezpečnost kompromitovaných čipových karet zvýšit.

Bylo zjištěno, že zabezpečení karet řady EM41xx je na velmi nízké úrovni. Hlavně se jedná o nebezpečí zcizení identifikačního čísla tagu, které je možné u těchto karet získat velmi jednoduchým způsobem. Vzhledem k tomu, že tento typ čipových karet má paměť, ze které lze pouze číst, není možné paměť této karty přepisovat či jakýmkoliv způsobem pozměňovat. Způsob jaký lze nasimulovat tag této čipové karty, je použití speciálního hardwarového emulátoru, který lze pořídit řádově v jednotkách tisíc korun. Na zahraničních trzích se již ovšem začínají objevovat čipové karty s prázdnou pamětí, do kterých bude možné zapsat jedinečné ID klonované karty. Nebezpečí klonování spočívá hlavně v tom, že útočník má možnost vybírat kredit oběti bez jejího vědomí. Tomuto lze částečně zabránit způsobem, který byl popsán v kapitole 5.1.

Situace u karet Mifare classic je podobná té předchozí, nicméně tyto typy tagů jsou zabezpečeny trochu lépe a manipulace s pamětí čipových karet je již obtížnější a vyžaduje větší úsilí. Pro získání přístupových klíčů používaných čipových karet je třeba dodržet určitých popsaných postupů, nicméně kompletní získání všech přístupových klíčů kompromitovaných karet zabere méně než 24 hodin. Velkou slabinou testovaných karet bylo to, že všechny karty, i od různých provozovatelů a s různým časem vydání, používalo stejné přístupové klíče pro ekvivalentní paměťové sektory, což je velmi laxní přístup jak dodavatele těchto karet, tak samotných provozovatelů celého systému. Po získání tajných klíčů může útočník přečíst obsah paměti jakékoliv používané čipové karty během několika sekund a tyto data na kartách pozměňovat, nebo využít pro své vlastní potřeby. Proti těmto nedostatkům v bezpečnosti byly navrženy metody, které by zamezily či alespoň omezily možnosti manipulace s Mifare classic čipovými kartami, ale je nutná spolupráce s dodavateli a provozovateli těchto systémů, neboť se může jednat o velmi ekonomiky nákladné řešení a je třeba hledat i určité kompromisy, které by se ovšem v budoucnosti určitě všem vyplatily.

CONCLUSION

This abstract is not a clue of how to pass the protection nor is it publishing detected secret keys. It is solely an audit of securing of systems using RFID chip cards and shows their defects.

Theoretical part is focused on the description of RFID (Radio Frequency Identification) system in general. In the first instance it describes a principle of functioning of the system alone and its advantages or possible disadvantages. Furthemore it shows the most often used types of tags (EM41xx, Mifare, etc.) that are being used in the Czech republic. Following chapters mention known types of attacks that have been recorded and examined until these days. Chapter 2 of the theoretical part is closely focused on the chip cards in connection with analysis of the communication of protocols between the card reader and the chip card of tags EM4102 and Mifare classic.

Practical part is focused on the particular testing of the safety of the chosen tags. First the hardware instruments that were necessary to be used for this purpose are listed. First the EM4102 chip card, that is being used at the Tomas Bata University for accessing of the secured premises of the university and is also used for conducting of payments for printing and other services used not only by students, was tested.

RFID chip card Mifare classic was represented by so called electronic wallet of the ČSAD Uherské Hradiště and ČSAD Vsetín companies whilst the 1 kilobyte or 4 kilbytes options were concerned.

The last chapter of the practical part is focused on the methods with help of which it would be possible to increase the safety of the committal chip cards.

It was found out that securing of the cards of EM41xx line is at a very low level. Mainly the danger of alienation of the ID number of the tag is concerned as this is very easy with this type of cards. With regards to the fact that this type of the chip cards has read only memory it is not posible to overwrite or change the memory in any way. The way how to simulate tag of this chip card is using of special hardware emulator that can be generally purchased in the units of thousands Czech crowns. On the foreign markets the types of the chip cards with empty memory are being introduced, this cards will be able to carry unique ID of the cloned card. The danger of cloning is that the assailant has possibility to

withdraw credit of the victim without the victims awareness. This can be partialy prevented by means described in the chapter 5.1.

The situation with Mifare classic cards is similar to the previous one nontheless these types of tags are secured a bit better and manipulation with memory of the chip cards is more difficult and demands greater effort. For obtaining of all the access keys of the used chip cards it is necessary to keep some described processes however complete obtaining of all of the access keys of committal cards takes less than 24 hours. The big weakness of the tested cards was that all the cards even from various operators with different time of issue were using same access keys for equivalent memory sectors which is very lax approach from both supplier of these cards as well as operators of the whole system. After obtaining of the secret keys the attacker can read the containts of the memory of any used chip card within seconds and either change these data on the cards or usem them for his own purpose. Methods that would stop or reduce the possibilites of manipulation with Mifare classic cards were proposed against the safety deficiencies but the cooperation with suppliers and operators fo these systems is necessary as the solution can be very expensive in the economy way and is is also important to look for certain compromises that would however certainly payoff to all the parties in the future.

SEZNAM POUŽITÉ LITERATURY

[1] THORNTON, Frank, et al. *RFID Security* [online]. 1st. ed. USA : SYNGRESS, 2005 [cit. 2011-01-17]. ISBN 978-1-59749-047-4.

[2] GLOVER, Bill; BHATT, Himanshu. *RFID essentials* [online]. 1st. ed. USA : O´Reilly Media, Inc, 2006 [cit. 2011-01-17]. ISBN 987-0-596-00944-1.

[3] ELLINGER, Frank. *Radio Frequency Integrated*. Second Edition. Berlin : Springer-Verlag Berlin Heidelberg, 2008. 515 s. ISBN 978-3-540-69324-6.

[4] WANT, Roy. *RFID Explained: A Primer on Radio Frequency Identification Technologies* . USA : Morgan and Claypool Publishers , 2006. 94 s.

[5] BROWN, Dennis E. *RFID Implementation* . USA : McGraw-Hill Osborne Media, 2006. 466 s. ISBN 978-0072263244.

[6] RFID. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 27.3.2006, last modified on 1.3.2011 [cit. 2011-04-28]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/RFID>.

[7] HRUŠKA, František. *Technické prostředky informatiky a automatizace*. Zlín : Univerzita Tomáše Bati ve Zlíně, 2007. 193 s. ISBN 978-80-7318-535-0.

[8] *RFID - EPC portal* [online]. 2007 [cit. 2011-04-28]. Dostupné z WWW: <http://www.rfid-epc.cz/>.

[9] *Priority 1 Design* [online]. 2007 [cit. 2011-04-28].EM4100 Protocol description. Dostupné z WWW: <http://www.priority1design.com.au/em4100_protocol.html>.

[10] VAN ROSSUM, Peter. Mifare Classic Troubles. In *Digital Security* [online]. Radbound University Nijmegen : Radbound University Nijmegen, 2007 [cit. 2011-04-28]. Dostupné z WWW: <http://www.ict-forward.eu/media/workshop2/presentations/rossum-mifare.pdf>.

[11] *RFID* [online]. 2005 [cit. 2011-04-28]. Princip. Dostupné z WWW: <http://rfid.wz.cz/princip.htm>.

[12] MF1|CS50 : Functional specification. In *Mifare_NXP.pdf* [online]. [s.l.] : NXP B.V., 2010 [cit. 2011-04-28]. Dostupné z WWW: <http://www.nxp.com>.

[13] VERDULT, Roel. *Security analysis of RFID tags* [online]. [s.l.] : [s.n.], 25.6.2008 [cit. 2011-04-28]. Dostupné z WWW: <http://www.sos.cs.ru.nl/applications/rfid/2008-verdult-thesis.pdf>.

[14] *NXP Type MF1K/4K Tag Operation : Storing NFC Forum data in Mifare Standard 1k/4k* [online]. [s.l.] : NXP Semiconductors, 2007 [cit. 2011-04-28]. Dostupné z WWW: <http://www.nxp.com>.

[15] D. GARCIA, Flavio, et al. *Dismantling Mifare Classic* [online]. The Netherlands : Radbound University Nijmegen, 2008 [cit. 2011-04-28]. Dostupné z WWW: <http://www.sos.cs.ru.nl/applications/rfid/2008-esorics.pdf>.

[16] NOHL, Karsten, et al. *Reverse-Engineering a Cryptographic RFID Tag* [online]. San Jose : USENIX Security Symposium, 31.7.2008 [cit. 2011-04-28]. Dostupné z WWW: <http://www.cs.virginia.edu/~evans/pubs/usenix08/usenix08.pdf>.

[17] FREEDMAN, Alan. *Computer Desktop Encyclopedia*. New York, USA : American Management Assoc., Inc., 1996. 1082 s. ISBN 0814400116

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AID	(Unique Application Identifier). Jedinečný identifikátor aplikace v paměti.
ASK	(Amplitude Shift Keying). Amplitudová modulace.
BCC	(Block Check Character). Detekce chyb přenosu dat paměťového sektoru.
CMAC	(Cipher-based MAC). Metoda ověření identity.
CRYPTO1	Proprietární šifrovací algoritmus vytvořený NXP Semiconductors speciálně pro Mifare RFID tagy.
DES	(Data Encryption Standard). Symetrická šifra vyvinutá v 70. letech.
DoS	(Denial-of-Service). Nedostupnost služby.
EEPROM	(Electrically Erasable Programmable Read-Only Memory). Elektricky mazatelná semipermanentní paměť.
EM 41xx	Označení pro RFID tag řady 41xx, pracující na frekvenci 125kHz od výrobce EM Microelectronic Marin SA.
EPC	(Electronic Product Code). Unikátní kód rádio-frekvenční identifikace fyzických objektů.
FPGA	(Field-Programmable Gate Arrays). Programovatelná hradlová pole.
FAB	Označení mechanické vložky zámku.
GNU	Označení pro svobodný software.
GPB	(General Purpose Byte). Byte v sektoru paměti pro nastavení povolení více aplikací na jedné čipové kartě.
GPL	(General Public License). Všeobecná veřejná licence pro software.
HF	(High Frequency). Označení pro rádio-frekvenční pásmo v rozmezí 3-30 MHz.
ID	Identifikace ve výpočetní technice
IEC	(International Electrotechnical Commission). Označení ustanovení mezinárodní normy.
ISO	(International Organization for Standartization). Mezinárodní organizace pro certifikaci a normalizaci.
LF	(Low Frekvency). Označení pro rádio-frekvenční pásmo v rozmezí 30-300 kHz.

LFSR	(Linear Feedback Shift Register). 48 bitový zpětnovazební registr.
LIBNFC	(Public Platform Independent Near Field Communication library). Otevřená knihovna zdrojových kódů pro ovládání bezdrátové komunikace.
MAD	(Mifare application direcrory). Adresářová aplikační struktura Mifare classic tagů.
NFC	(Near Field Communication). Technologie k bezdrátové komunikaci mezi elektronickými zařízeními na krátké vzdálenosti (do 20 cm).
PCSC	Personal Computer Smart Card). Specifikace integrace čipových karet do počítačového prostředí.
PSK	(Phase-shift keying). Fázová modulace.
RFID	(Radio Frequency Identification). Rádio-frekvenční identifikace.
SQL	(Structured Query Language). Dotazovací jazyk pro práci s daty relačních databází.
UID	(Unique Identification Number). Jedinečný číselný identifikátor.
UHF	(Ultra High Frequency). Označení pro rádio-frekvenční pásmo v rozmezí 300 MHz až 3 GHz.
USB	(Universal Seriál Bus). Univerzální sériová sběrnice.
USB-HID	(USB Human Interface Device Class). Popisuje zařízení pro lidské uživatelské rozhraní komunikující přes univerzální sériovou sběrnici.
UTB	Univerzita Tomáše Bati.
WORM	(Write Once Read Many). Označení paměti s možností jediného zápisu a neomezeného čtení.
XOR	(eXclusive OR). Exkluzívní logický součet.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: MAPA PAMĚTI TAGU MIFARE CLASSIC 4K ČSAD

```
00000000: FB 74 B6 DC E5 98 02 00|64 B9 94 96 51 00 26 09 | ûtÂ▄ńś..d┤öľQ.&.
00000010: A3 01 8F 77 00 00 01 00|02 08 64 26 AA 00 01 00 | ú.Ćw......d&¬...
00000020: 49 4D 53 50 00 42 00 43|46 4E 4E 00 00 00 00 00 | IMSP.B.CFNN.....
00000030: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000040: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000050: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000060: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000070: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000080: E0 03 00 00 1F FC FF FF|E0 03 00 00 09 F6 09 F6 | Ó....Ř Ó.... ÷.÷
00000090: E0 03 00 00 1F FC FF FF|E0 03 00 00 09 F6 09 F6 | Ó....Ř Ó.... ÷.÷
000000A0: 0F 00 00 00 8A 2C 00 00|00 00 00 00 D0 07 A3 01 | ....Ő,.......đ.ú.
000000B0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
000000C0: 64 26 00 00 00 00 00 00|56 8C 08 00 00 00 00 00 | d&......Vî......
000000D0: 48 75 62 A0 87 6B 6F 76|A0 20 4D 61 72 69 65 20 | Hubáçková Marie
000000E0: 20 20 20 20 20 20 20 20|20 20 20 20 20 20 20 20 |
000000F0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000100: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000110: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000120: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000130: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000140: 6C 00 00 00 00 00 00 00|67 00 00 00 00 00 00 00 | l.......g.......
00000150: 00 00 00 00 04 00 00 00|48 00 00 00 00 00 00 00 | ........H.......
00000160: B9 BB C6 3A 01 00 00 00|FF 36 0C 00 04 00 00 00 | ┤┐Ă:.... 6......
00000170: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000180: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000190: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000001A0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000001B0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
000001C0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000001D0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000001E0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000001F0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000200: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000210: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000220: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000230: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000240: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000250: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000260: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000270: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000280: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000290: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000002A0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000002B0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
000002C0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000002D0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000002E0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000002F0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000300: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000310: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000320: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000330: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000340: 01 00 37 6F DB B6 21 07|04 09 1E 01 00 00 00 00 | ..7o▄Â!.........
00000350: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000360: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000370: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000380: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
```

```
00000390: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000003A0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000003B0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
000003C0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000003D0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000003E0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000003F0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000400: 16 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000410: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000420: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000430: FF FF FF FF FF FF 78 77|88 C2 FF FF FF FF FF FF | xwł┬
00000440: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000450: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000460: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000470: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000480: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000490: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000004A0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000004B0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
000004C0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000004D0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000004E0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000004F0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000500: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000510: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000520: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000530: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000540: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000550: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000560: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000570: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000580: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000590: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000005A0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000005B0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
000005C0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000005D0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000005E0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000005F0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000600: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000610: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000620: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000630: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000640: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000650: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000660: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000670: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000680: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000690: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000006A0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000006B0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
000006C0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000006D0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000006E0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000006F0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000700: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000710: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000720: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000730: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
```

```
00000740: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000750: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000760: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000770: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wÇi
00000780: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000790: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000007A0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000007B0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wÇi
000007C0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000007D0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000007E0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000007F0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wÇi
00000800: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000810: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000820: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000830: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000840: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000850: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000860: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000870: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000880: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000890: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000008A0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000008B0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000008C0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000008D0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000008E0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000008F0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wÇi
00000900: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000910: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000920: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000930: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000940: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000950: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000960: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000970: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000980: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000990: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000009A0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000009B0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000009C0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000009D0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000009E0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
000009F0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wÇi
00000A00: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000A10: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000A20: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000A30: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000A40: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000A50: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000A60: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000A70: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000A80: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000A90: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000AA0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000AB0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000AC0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000AD0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000AE0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
```

```
00000AF0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wÇi
00000B00: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000B10: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000B20: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000B30: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000B40: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000B50: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000B60: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000B70: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000B80: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000B90: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000BA0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000BB0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000BC0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000BD0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000BE0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000BF0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wÇi
00000C00: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000C10: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000C20: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000C30: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000C40: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000C50: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000C60: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000C70: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000C80: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000C90: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000CA0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000CB0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000CC0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000CD0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000CE0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000CF0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wÇi
00000D00: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000D10: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000D20: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000D30: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000D40: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000D50: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000D60: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000D70: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000D80: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000D90: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000DA0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000DB0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000DC0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000DD0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000DE0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000DF0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wÇi
00000E00: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000E10: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000E20: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000E30: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000E40: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000E50: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000E60: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000E70: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000E80: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000E90: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
```

```
00000EA0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000EB0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000EC0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000ED0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000EE0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000EF0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
00000F00: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000F10: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000F20: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000F30: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000F40: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000F50: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000F60: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000F70: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000F80: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000F90: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000FA0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000FB0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000FC0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000FD0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000FE0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00 | ................
00000FF0: FF FF FF FF FF FF 08 77|8F 69 FF FF FF FF FF FF | .wĆi
```

PŘÍLOHA P II: MAPA PAMĚTI TAGU MIFARE ULTRALIGHT

```
00000000: 04 FB 84 F3 19 3E 25 80|82 48 FF 7F E1 10 06 00 | .ûä˘.>%ÇéH _ß...
00000010: 03 1D D1 01 19 55 01 74|74 61 67 2E 62 65 2F 6D | ..Ð..U.ttag.be/m
00000020: 2F 30 34 46 42 38 34 31|39 33 45 32 35 38 30 3B | /04FB84193E2580;
00000030: 01 18 D4 C0 03 31 38 69|9A 4F 01 1D 00 00 00 00 | ..đ └.18iÜO......
```