VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

BEZPEČNOST TECHNOLOGIE RFID

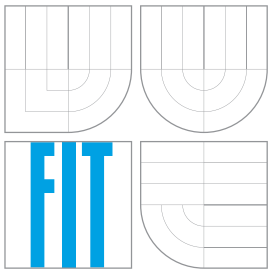
DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. STANISLAV BOŘUTÍK

BRNO 2013

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

BEZPEČNOST TECHNOLOGIE RFID

SECURITY OF THE RFID TECHNOLOGY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. STANISLAV BOŘUTÍK
AUTHOR

VEDOUCÍ PRÁCE — Ing. PAVEL BARTOŠ
SUPERVISOR

BRNO 2013

Abstrakt

Práce se zabývá bezpečností RFID systémů, možnými útoky na ně a opatřeními proti těmto útokům. V rámci práce byl také implementován útok pro získání klíče z karty Mifare Classic. Dále jsou popsány možnosti odposlechu komunikace, bezpečnost technologie NFC a biometrických pasů.

Abstract

This paper is about security of the RFID systems, attacks on them and countermeasures. Attack to obtain secret key from Mifare Classic card was implemented. Options for eavesdropping RFID communication, security of the NFC technology and biometric passports are descibed too.

Klíčová slova

RFID, bezpečnost, Mifare, odposlech, NFC, biometrický pas

Keywords

RFID, security, Mifare, eavesdropping, NFC, biometric passport

Citace

Stanislav Bořutík: Bezpečnost technologie RFID, diplomová práce, Brno, FIT VUT v Brně, 2013

Bezpečnost technologie RFID

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením pana Ing. Pavla Bartoše.

.....
Stanislav Bořutík
10. května 2013

Poděkování

Tímto bych chtěl poděkovat vedoucímu práce Ing. Pavlovi Bartošovi, rodině a přátelům za trpělivost a pomoc, kterou mi poskytli.

Obsah

Úvod

Technologie RFID (Radio Frequency Identification) je nejen nástupce čárových kódů a papírových jízdenek, oproti nimž má mnohem širší možnosti, ale také další generací přístupových systémů a způsobu komunikace mezi zařízeními. V některých oblastech lidské činnosti je běžně používána již několik let, zatímco v jiných se ještě nerozšířila, ač by i v nich byla přínosem a vylepšením stávajících řešení. Jedním z hlavních důvodů je úroveň zabezpečení, která je oproti jiným oblastem informačních technologií značně pozadu. Navíc je vzhledem k bezdrátovému přenosu dat komunikační médium snadněji dostupné útočníkovi, což sebou přináší nové typy útoků.

První kapitola se zabývá historií, využitím, vlastnostmi a popisem architektury RFID systému. Ve druhé kapitole je popsán princip přenosu dat mezi čtečkou a RFID tagem. Ve třetí kapitole je podrobný přehled možných bezpečnostních útoků na RFID systém a opatření pro zabránění těmto útokům. Čtvrtá kapitola popisuje bezpečnostní metody, použitelné proti útokům na RFID systém a stav zabezpečení nejpoužívanějších standardů i řešení výrobců na nich postavených. V páté kapitole čtenář nalezne informace o možnostech odposlechu komunikace mezi RFID čtečkou a tagem a o přečtení obsahu tagu čtečkou útočníka. Šestá kapitola popisuje implementovaný útok na zabezpečení dat uložených v tagu Mifare Classic. Sedmá kapitola se zabývá technologií NFC, která je nadstavbou technologie RFID a rozšiřuje možnosti a snadnost jejího použití. V osmé kapitole jsou stručně popsány metody zabezpečení biometrických pasů a možné bezpečnostní hrozby. Závěr shrnuje poznatky o bezpečnosti technologie RFID a vhodnosti jejího použití v aplikacích, kde je bezpečnost dat kriticky důležitá.

Kapitola 1

Popis RFID

1.1 Historie RFID

Počátek technologie RFID je v období 2. světové války, kde byla použita pro rozlišování přátelských a nepřátelských letadel. Pozemní stanice vyslala rádiový signál s dotazem, transpondér na letadle jej dekódoval a vyslal zpět zašifrovanou zprávu se svou identifikací. Později byla použita pro identifikaci vojenského vybavení a personálu. V 70. letech byly vyvinuty první systémy pro ochranu zboží proti krádeži v prodejnách a identifikaci dobytka. V 80. letech se objevily systémy pro výběr mýta, v 90. letech následované prvními přístupovými systémy. Na počátku 21. století se začaly RFID tagy objevovat coby budoucí náhrada čárových kódů. [15]

1.2 Oblasti použití

Technologie RFID má široké možnosti využití, mezi nejčastější aplikace patří [36][31]:

- evidence zboží ve skladu, logistika, knihovny
- sledování zboží v řetězci zásobování a prodeje
- identifikace osob (přístupové karty, elektronické pasy)
- identifikace zvířat
- platební systémy, jízdenky, vstupenky
- sledování zavazadel na letišti
- ochrana zboží proti krádeži
- telemetrické systémy

1.3 Vlastnosti

Výhodou je možnost snadno strojově přečíst obsah tagu bez nutnosti přímé viditelnosti, zarovnání, případně natočení (jako je tomu například při čtení čárových kódů). Díky tomu odpadá nutnost zásahu člověka, který by musel objekty natáčet apod. Tato vlastnost je ovšem zároveň nevýhodou, jelikož usnadňuje i nežádoucí přečtení tagu (např. útočníkem).

Oproti identifikaci osob biometrickými vlastnostmi odpadají problémy s protisvětlem, hlukem a jiným rušením.[11][8]
Dalšími výhodami jsou:

- množství uložených dat
- možnost přečtení obsahu tagu i na větší vzdálenosti
- možnost identifikace každého objektu zvlášť
- vysoká rychlost přečtení velkého množství tagů
- odolnost vůči vnějším vlivům
- vysoká rychlost čtení

Nevýhody:

- vyšší cena v porovnání s čárovým kódem
- možnost odstínění tagu
- nečitelnost dat pro člověka

1.4 Dělení RFID systémů

Existuje mnoho různých RFID systémů vhodných pro různé konkrétní aplikace. Nejdůležitější kritéria, podle kterých je můžeme dělit, jsou:

- komunikační frekvence (135 kHz - 5,8 GHz)
- dosah
- způsob komunikace (plně duplexní, poloduplexní, sekvenční)
- typ tagů (pasivní/aktivní)
- fyzické provedení tagů (karta, klíčenka, etiketa)
- kapacita paměti tagu
- modifikovatelnost obsahu paměti tagu
- fyzikální způsob vazby

1.5 Architektura RFID systému

Kompletní RFID systém se obvykle skládá z RFID tagů, které slouží pro identifikaci fyzického objektu, čtečky, která s tagy bezdrátově komunikuje, a řídicího systému s databází, ve které jsou uloženy informace o každém tagu.[36]

1.5.1 RFID tag (transpondér)

Rádiový transpondér se skládá z antény, paměti, kódovacího a dekódovacího obvodu, řadiče, pouzdra, případně kryptografického koprocesoru a v případě aktivních tagů i zdroje napájení (baterie, solární článek). Činnost jednoduchého tagu je řízena stavovým automatem, v případě výkonnějších tagů (Smart Cards) programovatelným mikroprocesorem s operačním systémem, který řídí přístup k paměti a souborům, spouští programový kód a kryptografické funkce. Mezi nejrozšířenější operační systémy, které se používají pro smart karty, patří MULTOS a JavaCard. Pro výrobu RFID tagů se používají sloučeniny křemíku, měď a hliník. Ve stadiu výzkumu je výroba tagů z organických, biologicky rozložitelných materiálů. Jelikož je potřeba dosáhnout co nejnižší ceny tagu, vyvíjí se i technologie pro jednoduchý tisk tagů, čímž odpadne jejich kompletace z jednotlivých komponent. Tyto nové technologie budou přínosné zejména pro jednoduché tagy, které slouží jako náhrada čárového kódu. Tagy rozlišujeme podle zdroje energie na pasivní, aktivní a semipasivní:

Pasivní tagy

Neobsahují žádný zdroj napájení, elektrickou energii pro napájení všech obvodů získávají z rádiového signálu vyslaného anténou čtečky. Protože takto přenesený výkon není vysoký, mohou pracovat pouze v malé vzdálenosti od čtečky. Pasivní tagy jsou malé, levné a mají dlouhou životnost. Anténa čtečky je napájena signálem s frekvencí nosné, čímž vzniká v jejím okolí elektromagnetické pole. Pokud je tag v tzv. pásmu „near field“ (cca do vzdálenosti $\lambda/2\pi$ od antény čtečky), je magnetická složka pole dostatečně silná na to, aby v přijímacím LC obvodu tagu naladěném na stejnou frekvenci nosné indukovala napětí. Toto napětí je usměrněno, vyfiltrováno, stabilizováno a je jím napájen samotný integrovaný obvod. Množství a stabilita takto přenesené energie je závislá na vzdálenosti tagu od čtečky, velikosti a tvaru antén, přesnosti shody frekvence, na kterou jsou tag a čtečka naladěny, modulaci signálu, vlivech okolí atd.

Aktivní tagy

Obsahují baterii nebo solární článek coby vlastní zdroj elektrické energie. Mohou tedy se čtečkou komunikovat na větší vzdálenost, neboť nejsou závislé na jejím poli. Mohou také být vybaveny více funkcemi. Pochopitelně jsou však oproti pasivním tagům dražší a rozměrnější. Jejich životnost je omezena životností baterie nebo solárního článku.

Semipasivní tagy

Obsahují podobně jako aktivní tagy vlastní zdroj elektrikcé energie. Narozdíl od nich ji však používají pouze pro napájení paměťového obvodu tagu, rádiová (komunikační) část je napájena polem čtečky jako v případě pasivních tagů.

Fyzické formáty tagů jsou rozličné, od přívěsků a karet přes válečky a hřebíčky až po samolepící etikety a miniaturní čipy pro implantaci pod kůži. Příklady tagů jsou na obr. 1.2.

Počet závitů antény tagu závisí na pracovní frekvenci. Čím je frekvence vyšší, tím méně závitů antény je potřeba. Např. antény pro frekvenci 135 kHz mají 100 až 1000 závitů, antény tagů pracujících na frekvenci 13,56 MHz jen 3 až 10 závitů.[8]

Obrázek 1.1: Příklady fyzických formátů tagů (zdroj: www.hidglobal.com)

Velikost paměti tagů se obvykle pohybuje od několika bajtů po několik kilobajtů. Výjimkou jsou systémy proti krádežím zboží v obchodech (EAS - Electronic Article Surveillance), kterým stačí velikost paměti 1 bit, postačující pro uložení informace, zda zboží bylo zaplaceno či nikoliv. Tyto tagy ale ukládají informaci na fyzikálním principu bez použití řadiče a paměti, nebudeme se jimi proto dále zabývat.

Tagy dělíme dle paměťových funkcí na:

- **Tagy pouze pro čtení (Read-Only)** umožňující pouze identifikaci objektů. Jejich paměť většinou obsahuje pouze unikátní identifikátor - sériové číslo, případně další data. Ta jsou do paměti zapsána při výrobě a nejsou uživatelem editovatelná. Pokud se takový tag ocitne v dosahu pole čtečky, začne svou identifikaci a případná další data opakovaně vysílat. Výhodou je malá velikost, nízká spotřeba a hlavně nízká cena. Používají se jako náhrada čárového kódu.

- **Zapisovatelné tagy**, na které může uživatel zapisovat data, např. dekrementovat kredit uživatele apod. Velmi často je pamět rozdělena na bloky o pevném počtu bajtů. Čtení a zápis dat se pak provádí právě po blocích jakožto nejmenší adresovatelné jednotce paměti. Při změně i jediného bajtu je tak nutné přečíst celý příslušný blok, změnit hodnotu bajtu a zapsat celý blok zpět do paměti. Nejčastější velikosti bloků jsou 2, 4 nebo 16 bajtů.

Trvalá paměť tagu pro uložení dat po delší dobu může být typu:

- Read-Only (obsah paměti je zapsán výrobcem při výrobě tagu)
- WORM - Write Once Read Many (obsah paměti je zapsán uživatelem při aplikaci tagu na objekt, dále lze obsah již pouze číst)
- Read/Write (Write Many) - umožňují opakované přepisování uživatelem

Dále tag obsahuje operační paměť pro různé operace (inkrementace hodnot v paměti, kryprografické funkce apod.), která při přerušení napájení ztrácí svůj obsah.

Pro trvalou paměť se používají paměti typu EEPROM (Electrically Erasable Programmable Read-Only Memory), jejichž nevýhodami jsou vyšší spotřeba při zápisu a omezený počet (100 000 - 1 000 000) zápisů, životnost dat je typicky 10 let. Nahradit by je měly paměti typu FRAM (Ferroelectric RAM) pracující na základě feroelektrického efektu. Tyto paměti jsou menší, rychlejší, mají milionkrát menší spotřebu energie potřebné pro zápis oproti EEPROM a delší životnost. Jsou ovšem problémy s jejich umístěním na jednom čipu společně s CMOS mikroprocesory a analogovými obvody.

Paměti typu SRAM (Static Random Access Memory) mají velkou rychlost zápisu, vyžadují ovšem neustálou přítomnost napájení (volatile memory), pro dlouhodobé uložení dat je lze tedy použít pouze v případě aktivních nebo semi-pasivních tagů. U pasivních tagů se používají jako operační paměť.

Základní operace tagu jsou:
READ - přečtení obsahu paměti čtečkou
WRITE - zápis dat do paměti tagu čtečkou (pokud tag zápis podporuje)
INCREMENT/DECREMENT - Některé tagy také nabízí operace inkrementace a dekrementace hodnoty proměnné v paměti.

Tag může také implementovat další funkce:
Bezpečnostní funkce - tag umožňuje šifrovanou komunikaci se čtečkou nebo autentizaci čtečky pomocí hesla
KILL (disable) funkce - tag umožňuje svou stálou deaktivaci, po které již dále neodpovídá na požadavky čtečky. Deaktivace tagu se provede zasláním příkazu KILL a tzv. KILL hesla, které je nastaveno při výrobě. Zároveň mohou být smazána některá nebo všechna data z paměti tagu. Tato funkce je využívána zejména pro ochranu soukromí.
LOCK funkce - stálý nebo dočasný zámek paměti tagu, data v tagu tedy nelze změnit. Je také chráněna předdefinovaným heslem.

Existují také tagy, které neslouží pouze k identifikaci a ukládání dat. Mohou být vybaveny např. dotykovými (tlačítka) nebo teplotními senzory.

1.5.2 Čtečka (terminál, transceiver)

Obsahuje kromě rádiové části s anténou i obvody implementující komunikační protokol, správu kolizí, autentizaci, šifrování a rozhraní pro komunikaci s backendem. Anténa může být přímo její součástí (ruční a nástěnné čtečky) nebo mohou být fyzicky odděleny (čtecí brána ve skladu). Čtečka buďto data ukládá do své paměti, ze které jsou později data stažena

např. do PC (ruční čtečky) nebo je přes Ethernetové, RS-232, RS-485 či USB rozhraní ihned posílá dále ke zpracování.

Obrázek 1.2: Příklad stolní a nástěnné čtečky (zdroj: www.hidglobal.com)

1.5.3 Middleware, backend, databáze

Middleware software slouží pro řízení toku dat mezi čtečkou a backend systémem, řídí čtečku, filtruje užitečná data z tagů[11]. Backend systém implementuje business logiku celého RFID systému, čte a ukládá data z databáze, udržuje historii transkací, provádí správu klíčů, komunikuje s jinými systémy a provádí různé akce jako je např. tisk faktur apod. Jako databáze slouží široce používané produkty Oracle, MS SQL Server, MySQL, PostgreSQL a jiné databázové systémy.

1.5.4 RFID tiskárny, aplikátory

Jako součást systému můžeme zahrnout i RFID tiskárny a aplikátory. Tiskárny slouží k potisku prázdného tagu (Smart Labelu) čárovým kódem a dalšími informacemi a zároveň k zápisu dat do RFID tagu a jejich kontrole. Smart Label je tenký tag formátu samolepicího štítku, který ma horní papírovou vrstvu s možností potisku čárovým kódem apod. Aplikátory v sobě kombinují RFID tiskárnu a mechanismus pro automatickou aplikaci tagu například na krabici nebo paletu, jsou součástí automatizované balicí linky.

Kapitola 2

Komunikace mezi čtečkou a tagem

2.1 Referenční komunikační model

Obrázek 2.1: Referenční komunikační model

Fyzická vrstva definuje rádiové rozhraní - frekvenci, typ modulace, kódování atd.
Komunikační vrstva[1] definuje datové rámce a algoritmy pro mnohonásobný přístup k médiu (antikolizní metody výběru konkrétního tagu pro komunikaci).
Aplikační vrstva definuje zprávy pro čtení/zápis dat z/do tagu a autentizační algoritmy.
Fyzická a komunikační vrstva jsou pro zajištění interoperability mezi čtečkami a tagy různých výrobců definovány ve standardech. Aplikační vrstva se liší dle konkrétní aplikace.

2.2 Rádiové rozhraní

Čtečka a tag spolu komunikují bezdrátově pomocí rádiových vln. Jsou používány různé frekvence, na kterých vysílají čtečky (frekvence, na které odpovídají tagy, se od ní může lišit - viz dále). Volba frekvence závisí na požadovaném dosahu, rychlosti (čím vyšší frekvence, tím vyšší rychlost přenosu) a objektu, ke kterému bude RFID tag připevněn (například systémy v pásmu LF jsou schopny komunikovat v prostředí s kapalinou, UHF tagy není vhodné připevňovat na kovové předměty apod.).

[1] Některá literatura označuje komunikační vrstvu jako spojovou nebo síťově-transportní

RFID systémy se dělí podle dosahu na:
Systémy s těsnou vazbou (close coupling) s dosahem do 1 cm. Tag musí být vložen do čtečky nebo přiložen na její čtecí plochu. Používají elektrickou (kapacitní) i elektromagnetickou (indukční) vazbu a pracují na frekvenci do 30 MHz. Mohou používat i tagy s vyššími nároky na napájení. Hodí se pro použití v aplikacích, kde hraje velmi důležitou roli bezpečnost a nevadí krátký dosah (platební a přístupové systémy). Tagy mají podobu plastikové karty formátu ID-1.
Systémy se vzdálenou vazbou (remote coupling) mají dosah do 10 cm (tzv. proximity systémy) resp. do 1 m (tzv. vicinity systémy). Drtivá většina z nich používá indukční vazbu, pouze některé kapacitní. Pracují na frekvencích do 135 kHz nebo na 13,56 MHz.
Systémy velkého dosahu (long-range) používají frekvence v UHF nebo mikrovlnném pásmu a mají dosah nad 1 m. Většina jich pracuje na principu backscatter vazby, některé na principu SAW (Surface Acoustic Wave)[1]

V pásmech LF a HF je využito indukční vazby, kdy antény čtečky i tagu mají tvar cívek, čímž tvoří systém podobný transformátoru se slabou vazbou. V UHF a mikrovlnném pásmu je využito elektromagnetické „backscatter“ vazby, antény mají tvar dipólu.

RFID systémy pracují v následujících frekvenčních pásmech:

Pásmo LF

Frekvence: 125 - 134 kHz
Čtecí dosah: do 0,5 m
Výhody: odolné vůči rušení, lze upevnit na kovové podložky i v blízkosti tekutin
Nevýhody: malý dosah a rychlost, velká anténa a tady velký a drahý tag
Použití: identifikace zvířat a kovových předmětů, přístupové systémy

Pásmo HF

Frekvence: 13,56 MHz
Čtecí dosah: do 1 m
Výhody: nejvíce rozšířené, nízká cena, celosvětově standardizovaná frekvence
Nevýhody: kovové podložky a tekutiny v blízkosi tagu snižují dosah
Použití: Smart Cards, Smart Labels, bezkontaktní placení, identifikace zavazadel, přenos naměřených dat
Protokoly: ISO 14443, ISO 15693, Tag-IT, I-Code

Pásmo UHF

Frekvence: 860 - 960 MHz
Čtecí dosah: do 3 m
Výhody: čtení na větší vzdálenosti, velká přenosová rychlost, levné tagy
Nevýhody: nelze číst přes kapaliny, odstínění signálu při aplikaci na kovové podložky, celosvětově nejednotná frekvence
Použití: identifikace zboží, sledování palet, elektronické mýtné, parkovací karty

[1] Tagy SAW obsahují piezoelektrický materiál, který na základě do něj zakódovaných dat (pomocí kovových reflektorů) odráží vyslanou rádiovou vlnu, ze které lze data dekódovat.

Protokoly: ISO 18000-6A/B, EPC Class 0/1

UHF/mikrovlnné pásmo

Frekvence: 2,4 - 5,8 GHz
Čtecí dosah: 3 m (pasivní tag), 15 m (aktivní tag)
Výhody: vysoká přenosová rychlost, malé tagy
Nevýhody: složitá konstrukce, drahé tagy, velký stínící vliv kovu a kapalin
Použití: elektronické mýtné, identifikace zavazadel, přenos dat v reálném čase

Pásmo UHF je velmi využívané zejména v oblasti logistiky pro sledování celých palet a položek v nich, kde je nutný větší dosah. Díky hustému využití tohoto pásma byly v různých částech světa regulačními institucemi uvolněny různé frekvence. To vede k nekompatibilitě tagů a čteček, což je v době celosvětového obchodu nepříjemné. Vývoj směřuje k multifrekvenčním tagům, schopným pokrýt celé pásmo a tedy odstranit tuto nekompatibilitu[38].

2.3 Přenos dat ze čtečky do tagu - downlink/forward kanál

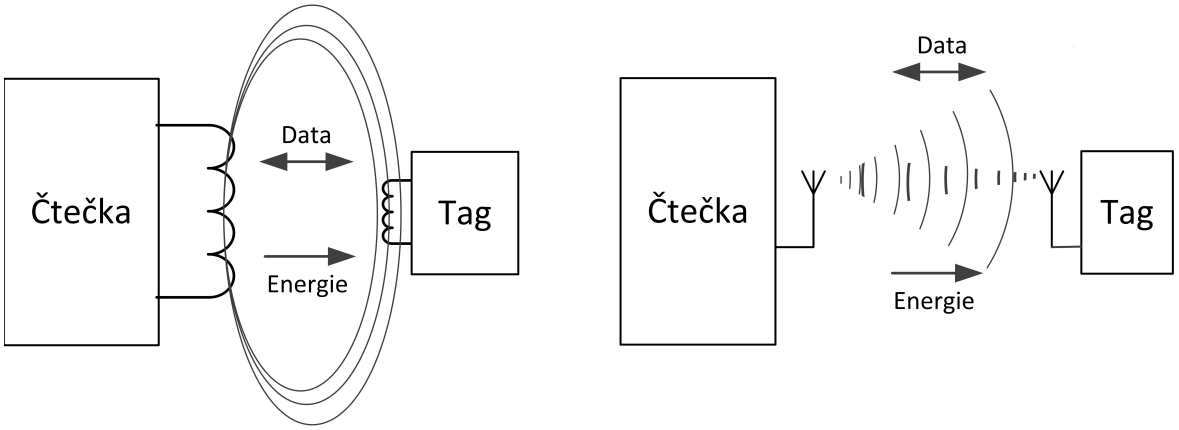
Nosná je modulována kódovaným binárním tokem dat. Lze použít amplitudovou, frekvenční i fázovou modulaci. Parametry modulace však musí být nastaveny tak, aby neovlivňovaly funkci napájení pasivních tagů a po celou dobu komunikace jim čtečka dodávala dostatek energie k provozu. Kvůli jednoduchosti demodulace (a tím jednoduchosti a nižší ceně tagů) je v drtivé většině používána amplitudová modulace.

2.4 Přenos dat z tagu do čtečky - uplink/back kanál

Většinou je používána zátěžová modulace (typ amplitudové modulace) pomocí změny rezistivity anténního obvodu tagu. Nyní si vysvětlíme přenos při využití indukční vazby. Čtečka se po ukončení vysílání dat přepne do módu naslouchání, kdy vysílá nemodulovanou nosnou a čeká na příjem dat od tagu. Tag mění podle vysílaných dat rezistivitu anténního obvodu a tím také spotřebu proudu. To se projeví změnami magnetického pole a dále změnami proudu v obvodu antény čtečky. Tyto změny jsou čtečkou detekovány a dekódovány, čímž jsou získána data vyslaná tagem. Tyto změny jsou však velmi malé a bylo by velmi složité je detekovat, pokud by čtečka i tag vysílali na stejné frekvenci. Proto tag odpovídá na frekvenci jiné, odvozené od frekvence čtečky. Používá se metoda subnosných, kdy tag odpovídá na jedné nebo dvou frekvencích blízko frekvence nosné, nebo metoda subharmonických frekvencí, kdy tag odpovídá na frekvenci, jejíž hodnota vznikne poděleníím hodnoty nosné dělitelem, který má nejčastěji hodnotu 2. Obě tyto metody umožňují díky použití odlišných frekvencí plně duplexní komunikaci, čtečka i tag tedy mohou vysílat současně.

Dále se používá také sekvenční metoda, při které čtečka vyšle data tagu a poté přestane vysílat. Tag si poté vytvoří vlastní magnetické pole a na stejné frekvenci odešle data zpět čtečce. Díky tomu, že je magnetické pole čtečky vypnuté, lze snadno detekovat pole tagu. Protože po dobu vysílání není tag napájen pomocí pole čtečky, musí si pomocí kondenzátoru uschovat po dobu vysílání čtečky dostatek energie pro vlastní vysílání. Místo zátěžové je zde použita frekvenční modulace, komunikace je poloduplexní.

U vyšších frekvencí se využívá zpětného odrazu elektromagnetického vlnění, tzv. backscatter vazby. Ta používá stejný princip jako radar. Čtečka vysílá nosnou, která je odrážena zpět anténou tagu. Změnou rezistivity anténního obvodu je amplitudově modulována (platí nepřímá úměra mezi rezistivitou a velikostí amplitudy) a odražena zpět ke čtečce, kde je signál vyhodnocen. Tento přenos je poloduplexní.



Obrázek 2.2: Indukční a backscatter vazba

2.5 Inicializace komunikace

Komunikace mezi čtečkou a RFID tagem probíhá bezdrátově pomocí rádiových vln. Podle toho, zda jako první vysílá data čtečka nebo tag, rozlišujeme dva typy inicializace komunikace[19]:

- **Reader Talks First (RTF)** - čtečka vyšle příkaz a tag jej vykoná (vyšle odpověď)
- **Tag Talks First (TTF)** - Pasivní tag zašle informace o své přítomnosti čtečce, jakmile začne být napájen jejím polem. Aktivní tag tyto informace periodicky vysílá.

2.6 Kódování bitů

Bit lze pro přenos zakódovat různými kódy. V RFID systémech se používají například tyto:

- NRZ (Non Return to Zero)
- Manchester
- Unipolární RZ (Return to Zero)
- DBP kód
- Millerův kód
- Diferenční kód

Při výběru kódu je nutno zvážit jeho vliv na kmitočtové spektrum (vyšší počet změn - vyšší počet harmonických - větší zabraná šířka frekvenčního pásma) a také vliv na funkci napájení pasivních tagů, která může být narušena nevhodnou kombinací modulace a kódování. Nežádoucí je delší dobu trvající nízká amplituda signálu, která způsobí výpadek napájení pasivního tagu.

2.7 Vícenásobný přístup a řešení kolizí

Při reálném použití (obzvláště u systémů s velkým dosahem) je běžné, že se v dosahu čtečky nachází více než jeden tag. Obvykle jsou všechny tagy postaveny na stejném standardu a pracují na stejné frekvenci, na dotaz čtečky by tedy odpověděly všechny najednou. To by samozřejmě vedlo k zarušení a ztrátě dat. Proto je nutné použít některou z metod, která umožní pomocí zamezení kolize přístup k více tagům a bezproblémovou komunikaci s nimi. K tomu se používá metoda TDMA (Time Division Multiple Access), která v čase postupně přiděluje pásmo jednotlivým tagům. Pro předcházení kolizím se používají pravděpodobnostní a deterministické algoritmy. Pravděpodobnostní algoritmy jsou založeny na protokolu ALOHA (předchůdci CSMA/CD protokolu používaného v Ethernet sítích). Každý tag při detekci kolize čeká náhodnou dobu a až poté opakuje vysílání. Tyto algoritmy jsou efektivní do určitého počtu současně dostupných tagů, od kterého se už neúnosně prodlužuje doba přečtení jednoho tagu. Deterministický algoritmus procházení binárního stromu je založen na existenci unikátního identifikátoru každého tagu. Komunikace je řízena čtečkou následovně: Čtečka pošle výzvu všem tagům, jejichž identifikátor začíná bitem hodnoty 0. Pokud žádný tag neodpoví, vyšle výzvu s prefixem identifikátoru "1", pokud odpoví více tagů a dojde tedy ke kolizi, čtečka zpřesní dotaz na identifikátor začínající "00". Zpřesňování probíhá, dokud neodpoví pouze jeden tag. Stejným způsobem se prohledají i ostatní větve stromu. Na konci algoritmu čtečka zná identifikátory všech tagů v dosahu a může s nimi komunikovat individuálně pomocí identifikátoru. Výběr konkrétního tagu se provádí pomocí příkazu SELECT následovaného identifikátorem tagu[15][33].

Kapitola 3

Útoky na RFID systémy

Bezpečnost systému je jeho schopnost zachovat si svou funkci i v podmínkách, které mají snahu ji narušit, např. při pokusu o úmyslný útok na systém. Bezpečnost informačního systému má následující cíle: [15]

- **Důvěrnost** - informace v systému jsou dostupné pouze autorizovaným osobám. Může být zajištěna řízením přístupu a použitím kryptografie pro zabezpečení přenosu dat.
- **Integrita** - informace v systému nemohou být neoprávněně modifikovány a systém nemůže být převeden do nežádoucího stavu. Při přenosu dat je možno ověřit jejich původ a také to, že nebyla během přenosu modifikována ať už náhodně (např. rušením) či úmyslně (útokem).
- **Dostupnost** - autorizovaným uživatelům je kdykoliv zajištěn přístup k datům a službám. Může být narušena náhodně (např. selhání hardwaru) nebo úmyslně (útočníkem).

Útokem na bezpečnost systému rozumíme nežádoucí aktivitu, která má za cíl získat z něj důvěrná data, modifikovat je nebo narušit jeho funkci. Objektem útoku může být kterákoliv část systému: tag, čtečka, middleware, backend databáze nebo kterýkoliv z komunikačních spojů mezi nimi. Útok na různé části systému má různý dopad, např. změna jednoho tagu ovlivní pouze jeden konkrétní objekt, změna celé databáze nebo útok na middleware bude však mít pro systém fatálnější následky. Následující útoky na RFID systémy [15][39][36] jsou seskupeny podle vrstev komunikačního modelu dle [22].

3.1 Útoky na fyzickou vrstvu

3.1.1 Deaktivace tagu

Jedná se o zabránění rozpoznání přítomnosti tagu. Rozlišujeme dočasnou a trvalou deaktivaci. Dočasná deaktivace může být provedena pasivně odstíněním objektu na principu Faradayovy klece (např. jeho zabalením do kovové fólie) nebo blokováním signálu pomocí kovových předmětů, vody nebo ledu. Při aktivním rušení (RF jammingu) je rádiové pásmo v blízkosti čtečky zarušeno silným šumem (ať již konstantním nebo nějakým způsobem modulovaným), který je vysílán útočníkovým oscilátorem. Trvale deaktivovat tag lze pomocí mechanické (odlomení antény), elektronické (silný elektrostatický výboj) či chemické destrukce tagu nebo jeho odstraněním z objektu a umístěním mimo dosah čtečky. Další

z možností trvalé deaktivace je příkaz KILL, jehož zneužití je obzvláště nebezpečné v případě sdílení stejného KILL hesla velkým množstvím tagů.

Protiopatření: Proti odstínění, odstranění a destrukci tagu se lze bránit zvýšenou fyzickou bezpečností (ostraha, kamerový systém, ploty), odolnější aplikací tagů na objekty (silné lepidlo, odolné mechanické připevnění), neviditelným nebo pro útočníka hůře dostupným umístěním tagu (např. dovnitř objektu) a detekcí manipulace s tagem pomocí senzorů. Proti aktivnímu RF rušení může pomoci odstínění zdí, proti zneužití příkazu KILL pomůže efektivní správa hesel.

3.1.2 Krádež a destrukce čtečky

Motivem pro krádež čtečky může být získání tajných klíčů pro přístup k tagům s kryptografickými funkcemi nebo dokonce získání přístupu do systému či přímo do databáze, což může mít podstatně horší následky.

Protiopatření: Zvýšená fyzická bezpečnost (podobně jako u tagů).

3.1.3 Relay útoky

Útočník umístí své zařízení mezi čtečku a tag, jedná se tedy o útok *man-in-the-middle*. Zařízení přijímá data od jedné strany, v některých případech je pozmění a odešle druhé straně. Tag i čtečka se tedy domnívají, že spolu komunikují přímo. Útočník také může použít dvě útočná zařízení, jedno v blízkosti čtečky a druhé v blízkosti tagu. Tato zařízení od sebe mohou být teoreticky velmi daleko od sebe a může mezi nimi existovat jiné datové propojení (např. GSM síť či internet).

Protiopatření: šifrování komunikace se zajištěním integrity dat proti jejich modifikaci, zavedení sekundární autentizace (heslo, PIN, biometrická vlastnost), použití distance bounding protokolu, který na základě rychlosti odpovědi protistrany dokáže zjistit přítomnost nežádoucího komunikačního kanálu mezi čipem a čtečkou.

3.2 Útoky na komunikační vrstvu

3.2.1 Klonovaní tagu

Klonování je vytvoření logické kopie tagu, která je pro čtečku na úrovni protokolu neodlišitelná od originálního tagu. Na nižší úrovni už obvykle rozlišitelné bývají - např. díky tolerancím elektronických součástek tagů jsou mezi nimi drobné rozdíly ve spotřebě nebo rychlosti odezvy. Tyto parametry ale běžné čtečky nerozlišují. Dále se může kopie od originálu lišit např. rozměry nebo vzhledem, to už je však úplně mimo rozpoznávací možnosti čtečky. Pro většinu případů stačí útočníkovi v kopii tagu podporovat pouze přečtení identifikace nebo dat, k jiným operacím dochází poměrně zřídka. Protože obyčejný tag vždy vysílá stejnou informaci, postačí pouze napodobit rádiový signál jím vysílaný. Klonování tagu je nebezpečné zejména v aplikacích, kde je jednoznačná identifikace objektu klíčová, tedy v přístupových systémech apod.

Protiopatření: Klonování lze omezit použitím autentizačních protokolů výzva - odpověď (ISO 9798), mechanismů proti útoku hrubou silou a asymetrické kryptografie. Tu však nelze u běžných tagů z důvodu omezení výpočetních prostředků použít, pro tyto tagy lze použít symetrickou kryptografii s autentizací PINem. Dalším a velmi zajímavým řešením pro levné tagy, které příliš nezvyšuje jejich cenu, je použití fyzicky neklonovatelné funkce (PUF - Physical Unclonable Function). Ta je implementována při výrobě hardwarově, pro každý tag je unikátní, nelze její chování dopředu předpovědět nebo jej naprogramovat. Využívá odlišné zpoždění při šíření signálu v křemíkovém čipu různými cestami, které jsou sestaveny multiplexery v závislosti na vstupu. Vstupem funkce je výzva čtečky a výstupem odpověď. Odpověď na určitou výzvu je v okamžiku přidání tagu do systému uložena do databáze a na začátku jakékoliv další komunikace je tag autentizován na základě shody odpovědi tagu a předpokládané odpovědi, uložené v databázi. [7] Jiným řešením, vhodným zejména pro přístupové systémy, je detekce průniku (IDS - Intrusion Detection System) založená na vzorech chování držitelů přístupových tagů. Porovnávají se obvyklé vzory chování držitele tagu a pokud dojde k podezřelé odchylce, je generováno varování. Tento systém však není stoprocentně spolehlivý. [21] Poměrně jednoduchým opatřením je korelace informací s databází. Přístupový systém neakceptuje žádost o vstup do budovy, pokud již daná osoba v budově je nebo není akceptován cestovní pas na českých hranicích, pokud byl před několika minutami použit v Japonsku. Toto opatření však vyžaduje vyšší výkon backend systému, který musí prohledávat historii transakcí a aplikovat na ni pravidla.

3.2.2 Podvržení informace - Spoofing

Jedná se o variantu klonování, tag zde však není fyzicky naklonován. Pomocí speciálního zařízení je tag pouze emulován. Tomu musí předcházet získání dat z originálního tagu, např. odposlechem legitimní komunikace. Je tak nutná znalost komunikačního protokolu a případných autentizačních klíčů. Tak mohou být podvrženy přístupové nebo platební systémy, čtečky cestovních pasů apod.

Protiopatření: Podvržení informace lze zabránit použitím autentizačních protokolů, sekundární autentizací (heslo, PIN, biometrická vlastnost) nebo pseudonymizací[1].

3.2.3 Imitace čtečky

Pokud neexistuje žádná autentizace čtečky, je možné pomocí jakékoliv čtečky podporující daný standard získat nebo modifikovat data v tagu. Pokud je nějaký autentizační mechanismus přítomen a kryptografické klíče jsou uloženy přímo ve čtečce, je možné je získat její krádeží.

Protiopatření: Použitím autentizačních protokolů a bezpečným uložením klíčů.

3.2.4 Úmyslná kolize

Tento útok má za cíl obejití antikolizních mechanismů. Útočník se chová jako jeden nebo více tagů, které současně odpovídají na dotaz čtečky, dojde tedy ke kolizi. Systém nemůže standardně pracovat, jedná se o variantu DoS útoku.

[1] Pseudonymizace je zavedení náhradního identifikátoru, který lze se skutečným identifikátorem spojit pomocí speciální procedury nebo bezpečně uložené převodní tabulky.

3.2.5 Odposlechnutí dat - Eavesdropping

Protože je mezi čtečkou a tagem použit úzkopásmový rádiový přenos a médium je sdílené a veřejné, je snadné komunikaci mezi nimi odposlechnout a případně dále použít pro útok podvržení informace, přehrávání nebo sledování (pokud útočník dokáže dekódovat data na úrovni aplikační vrstvy). Snazší je odposlech downlink kanálu nežli uplink kanálu, protože čtečka vysílá silnější signál. Možné vzdálenosti odposlechu jsou v případě indukční vazby (frekvenční pásma LF a HF) u downlinku až několik desítek metrů, u uplinku až 5ti násobek nominálního dosahu tagu. V případě backscatter vazby lze odposlouchávat do vzdálenosti 100 až 200 metrů, při použití směrové antény dokonce do 500 až 1000 metrů. Postačuje tedy, aby byl útočníkův přijímač dostatečně blízko (samozřejmě v závislosti na velikosti antény), naladěn na správnou frekvenci a nastaven na modulaci používanou RFID systémem. Více o odposlechu v kapitole 5 na straně 30.

Protiopatření: Zabránit odposlechu lze šifrováním komunikace, přidáním šumu nebo použitím složitější modulace signálu. Vhodné je také zvážit uložení citlivých dat do databáze a do tagů ukládat pouze unikátní ID. Tento přístup není vhodný pro jednodušší a menší systémy a mobilní aplikace, pro většinu ostatních systémů nabízí celou řadu výhod [15]:

- nižší cena - postačí levné tagy s malou pamětí
- je možný přístup k datům a jejich změna bez přítomnosti tagu
- snadnější migrace dat při změně systému
- jednodušší interoperabilita mezi systémy
- snadné úprava struktury dat
- možnost uložit neporovnatelně více dat
- jednodušší zajištění bezpečnosti - propracovanější řízení přístupu, data se nepřenášejí rádiovým rozhraním

3.3 Útoky na aplikační vrstvu

3.3.1 Přečtení informací z tagu (skimming)

Běžné tagy nemají funkce řízení přístupu, útočník může pomocí vlastní čtečky přečíst informace z RFID tagu. Pokud například tag obsahuje informaci o ceně jím označeného objektu, může si útočník vytipovat cenné objekty ke krádeži.

Protiopatření: Obranou je uložení citlivých dat do databáze, kde je lze lépe zabezpečit, a v tagu ponechat pouze identifikační data. Díky tomu postačí tagy s menší pamětí a tedy s příznivější cenou. I pokud tag obsahuje řízení přístupu, lze data z něj přečíst např. útokem postranními kanály.

3.3.2 Modifikace dat v tagu

V případě tagu s pamětí typu *Write-Many* může útočník modifikovat nebo smazat informace v něm uložené. K tomu lze například použít nástroj *RF Dump* [12], který podporuje mnoho standardů a slouží k bezpečnostnímu auditu RFID tagů. Nebezpečnost tohoto útoku závisí na konkrétní aplikaci, např. v případě medicínské aplikace bude jistě velmi vysoká.

Protiopatření: Zabránění neautorizované modifikaci obsahu tagu lze jednoduše použitím read-only tagů (samozřejmě pokud to konkrétní použití dovoluje). V době, kdy není tag používán lze přístupu k němu zabránit jeho odstíněním (např. odstíněná peněženka pro ochranu přístupových karet) nebo použitím „blokovacího“ tagu. Ten simuluje velké množství virtuálních tagů a tím zamaskuje existenci tagu skutečného.

3.3.3 Útoky na backend/middleware

V tomto případě systém místo požadovaných dat obdrží systémové příkazy. Může se jednat o variantu známého útoku SQL injection, který je však i v RFID systému možný, jelikož SQL databáze se v nich běžně používají. Podobným způsobem by bylo možné napadnout i samotný řídící software, například využitím chyby přetečení bufferu. Ačkoliv se zdá, že z důvodu omezené paměťové kapacity tagů není tento útok reálně proveditelný, opak je pravdou. V některých standardech existují příkazy pro opakované načtení bloku dat z tagu, v jiných stačí použít tag nebo jeho emulátor s vyšší paměťovou kapacitou, než s jakou autor middleware počítal. Pokud systém zapisuje data z databáze na jiné tagy, může pomocí nich šířit virus dále. Také mohou být systému podstrčena data jiného formát, než jaký očekává (např. textový řetězec místo čísla)

Protiopatření: Backend systém by měl být naprogramován tak, aby byl imunní vůči buffer overflow útoku. Předejít takovému útoku lze také začleněním filtrovací funkce (nejlépe již do middleware), která rozpozná SQL nebo systémový příkaz v datové oblasti požadavku, zablokuje jej a tím zabrání jeho načtení provedení. Také by mělo být kontrolováno, zda formát dat odpovídá předpokládanému formátu.

3.3.4 Desynchronizace

K desynchronizaci dojde, pokud stav objektů skutečného světa neodpovídá stavu jejich obrazů v databázi. Tento útok je proveden eliminací zápisu dat do tagu. Příkladem je zabránění aktualizace dat v tagu, k tomu však může dojít i náhodnou ztrátou konektivity mezi čtečkou a middleware.

Protiopatření: Částečně lze tento útok ztížit zpětným přečtením aktualizované hodnoty, i to však může útočník nasimulovat.

3.4 Vícevrstvé útoky

3.4.1 Skrytý kanál

Při útoku skrytým kanálem může útočník zneužít tagy využitím volného paměťového místa pro přenos dat ze systému. Tento útok je obtížně odhalitelný, obvykle se na něj přijde až při změně systému, která ovlivní strukturu dat v tagu.

Protiopatření: Jak již bylo řečeno, není lehké útok skrytým kanálem odhalit a ještě těžší je mu předejít. Řešením může být periodické mazání nepoužité paměti, které však vyžaduje přítomnost tagů. Toto opatření může útočník obejít také pozměněním programového kódu operace pro mazání dat tak, aby např. místo nul do paměti zapisovala přenášená data.

3.4.2 Odmítnutí služby - DoS

Tento útok může být proveden různými způsoby: zarušením rádiového pásma, úmyslnou kolizí (tzv. blocking tag), použitím příkazu KILL nebo LOCK, fyzickou destrukcí tagů, napadením čtečky/middleware/databáze (viz „Útoky na backend/middleware“) nebo komunikačních kanálů mezi nimi atd.

Protiopatření: Možnost útoku zarušením rádiového pásma nebo generováním „virtuálních“ tagů je možné minimalizovat odstíněním prostoru, ve kterém dochází ke čtení tagů. To je však účinné pouze v případě, kdy je útok veden z okolí. Ne však v případě, kdy bude blocking tag/rušička umístěn u legitimního tagu např. na zboží. Na úrovni middleware je možné provádět filtrování pouze těch požadavků které je nutné dále zpracovat. K předejití zahlcení požadavky by měl být backend systém pokud možno výkonově naddimenzován oproti předpokládané zátěži. Je také vhodné výkonově náročné (ale časově méně kritické) akce řadit do fronty a odtud je podle dostupného výkonu systému postupně odebírat a vykonávat.

3.4.3 Analýza komunikace

Analýza komunikace na jakékoliv vrstvě, ať už šifrované nebo nešifrované, může pomoci útočníkovi získat cenné informace. Útočník může v analýze postupovat od nižší komunikační vrstvy k vyšší. Úspěšnost útoku stoupá s objemem zachycené komunikace.

Protiopatření: Opatření proti útokům odmítnutí služby a analýzy komunikace jsou ještě ve stádiu vývoje z důvodu omezených výpočetních zdrojů RFID tagů. Pro ztížení útoků využívajících odposlech komunikace lze také použít omezení všesměrového vysílání čtečky úmyslným odstíněním nebo snížení jejího vysílacího výkonu.

3.4.4 Útoky na kryptografické funkce

Pomocí útoku hrubou silou, postranními kanály či pomocí reverzního inženýrství může pokročilý útočník získat šifrovaná data v tagu nebo se úspěšně autentizovat do systému. Nejsložitější je útok postranními kanály, útočník musí podrobně znát hardwarovou architekturu, na které je daný algoritmus naimplementován a vlastnit potřebné vybavení. Při časové analýze je využívána závislost délky provádění jednotlivých kroků algoritmu na tajném klíči, při odběrové analýze (elektromagnetického pole) je měřen odběr proudu tagu v závislosti na právě prováděné operaci.

Protiopatření: Útokům na kryptografické funkce lze zamezit použitím silných algoritmů s dostatečně dlouhými tajnými klíči. Ztížit útok postranními kanály lze snížením elektromagnetického vyzařování, zvýšením složitosti obvodu tagu a zavedením nadbytečných instrukcí nebo náhodných časových zpoždění mezi instrukcemi (a tím nejen těžším pochopením činnosti obvodu útočníkem, ale také zvětšením rozměrů a především ceny tagu).

3.4.5 Přehrávání - Replay

Při legitimní komunikaci je útočníkem zachycena odpověď tagu a později znovu vyslána čtečce při jejím dotazu na tag. Tak je možno například simulovat větší množství podobných objektů nebo způsobit vyčerpání výpočetních prostředků systému a tím zabránit načtení dalších platných tagů. Jako obranu obsahují některé tagy čítač dotazů, který při překročení předem nastavené maximální hodnoty zablokuje tag.

Protiopatření: Replay útokům lze čelit pomocí použití časových razítek, hesel na jedno použití a šifrovaným protokolům výzva-odpověď se sekvenčními nebo pseudonáhodnými čísly či časovou synchronizací. Tu však nelze použít u pasivních tagů, které nemohou mít vnitřní hodiny kvůli neexistenci vlastního zdroje napájení.

3.4.6 Sledování - Tracking

Sledování není útokem na systém, ale na soukromí uživatelů. Konkrétního uživatele lze vysledovat podle unikátního ID tagu (např. přístupové karty) nebo podle kombinace několika neunikátních údajů z tagů (např. seznam položek v nákupním košíku).

Kapitola 4

Zabezpečení RFID

Tato kapitola popisuje aktuální stav a používané metody pro zabezpečení technologie RFID a to jak samotných standardů, tak i řešení průmyslových výrobců, která jsou na těchto standardech postavena.

4.1 Bezpečnostní metody

V této části si představíme technické metody pro zvýšení bezpečnosti technologie RFID, které jsou běžně implementovány ve v současnosti používaných standardech. Kromě nich existuje spousta netechnických metod, které jsou sice pro reálné aplikace velmi důležité, ale mimo záběr této práce. Pokud se i s těmito chce čtenář seznámit, nalezne je v [19].

4.1.1 Autentizace a integrita dat

Autentizace heslem

Slouží k omezení neautorizované manipulace s daty v tagu. Operace chráněná heslem proběhne, jen pokud je příkaz k jejímu provedení doplněn platným heslem. Mezi takto zabezpečené operace patří čtení, zápis, funkce KILL a LOCK. Při využití autentizace heslem je nutná kvalitní správa hesel zahrnující jejich náhodné generování, bezpečný přenos do tagu (nejlépe v dobře fyzicky zabezpečeném prostředí, kde je eliminována možnost odposlechu na minimum - heslo je totiž posíláno v čitelné formě) a bezpečné uložení hesla do databáze. Není doporučeno používat stejné heslo pro více tagů, aby se omezil dopad jeho odhalení útočníkem. Záznam každého tagu v databázi může obsahovat nahédně vygenerované heslo, spárované s UID tagu. Další možností je generování při každém použití (on-demand) např. pomocí hashe hodnoty, která vznikne sloučením UID tagu a globálního hesla. Pak stačí uchovávat v tajnosti pouze globální heslo. Samozřejmostí je použití dostatečně odolného hashovacího algoritmu. Pokud je to možné, je vhodné heslo pravidelně měnit. V případě některých pasivních tagů lze heslo získat pomocí odběrové analýzy. Krátká nebo slabá hesla mohou snadno podlehnout útoku hrubou silou.

Keyed-Hash Message Authentication Code (HMAC)

Slouží k jednostranné nebo oboustranné autentizaci a zajištění integrity přenášených zpráv. HMAC používá čtečkou a tagem sdílený klíč a libovolný hashovací algoritmus (doporučena je některá vyšší verze SHA). Oproti autentizaci heslem poskytuje silnější zabezpečení (neposílá nezabezpečená hesla přes rádiové rozhraní), autentizaci tagu a zajištění integrity

zpráv. Také však vyžaduje výkonnější tagy.

Autentizace tagu probíhá následovně:

1. Čtečka pošle tagu náhodnou výzvu.
2. Tag vypočte HMAC pomocí klíče a výzvy čtečky a odešle ji zpět čtečce.
3. Čtečka vypočítá HMAC a porovná jej s odpovědí tagu. V případě shody je tag autentizován.

Oboustranná autentizace probíhá stejným způsobem vzájemně, tj. tag generuje náhodnou výzvu pro čtečku a poté ověřuje správnost její odpovědi. Integrita zprávy je ověřována výpočtem HMAC pomocí klíče a obsahu zprávy. Při jejím přenosu je posílána jak samotná zpráva, tak i její HMAC. Toto zabezpečení je založeno na utajení sdíleného klíče. Může být tedy prolomeno, pokud má útočník fyzický přístup k tagu, ze kterého získá tajný klíč.

Digitální podpis

Použití asymetrické kryptografie, tzv. „autentizované RFID“. Čtečka podepisuje ID tagu, časová razítka a veškeré operace s tagem a podpisy ukládá do tagu. Zároveň je veden záznam o akcích s jejich podpisy. Tak lze později ověřit platnost dat.

Postup je následující:

1. Tag má neměnné ID, které bylo nastaveno při jeho výrobě.
2. Čtečka vygeneruje veřejný a soukromý klíč a obdrží odpovídající certifikát.
3. Čtečka vypočte hash ID tagu a případných dalších dat operace, zašifruje jej svým soukromým klíčem a tím získá digitální podpis operace. Ten uloží do tagu.
4. Jiná čtečka přečte z čipu digitální podpis, dešifruje jej veřejným klíčem první čtečky, vypočítá stejný hash zprávy a porovná jej s hashem z tagu. Pokud se shodují, je zaručena autentičnost předchozí operace.

Tato metoda je bezpečnější než HMAC, na tag nejsou kromě dostatečné paměti pro podpisy kladeny žádné speciální požadavky, nejsou v něm uložena žádná tajemství, pouze ve čtečce je uložen její tajný soukromý klíč a jeden nebo více certifikátů - vhodné pro mobilní čtečky bez konektivity k síti. Také je zvýšena bezpečnost systémů, sdílených více organizacemi (sdílí mezi sebou pouze veřejné klíče čteček). Systém vyžaduje čtečky s podporou digitálního podpisu a také správu klíčů (Public Key Infrastructure - PKI). Požadavky na paměť tagu jsou v případě algoritmu RSA 1024 resp. 2048 bitů na jeden podpis, v případě algoritmů na bázi eliptických křivek jsou podpisy odpovídající síly jako RSA 162 resp. 224 bitů dlouhé.

4.1.2 Zabezpečení rádiového rozhraní

Cover-Coding

Metoda pro jednoduché šifrování downlink kanálu pomocí operace XOR. Postup je následující:

1. Čtečka pošle tagu žádost o klíč.
2. Tag vygeneruje klíč (16bitové pseudonáhodné číslo) a pošle jej čtečce.
3. Čtečka zašifruje zprávu použitím operace XOR zprávy a klíče a zašifrovanou zprávu odešle tagu.
4. Tag zprávu opět pomocí operace XOR s klíčem dešifruje.

Snižuje riziko zaslání neautorizovaného příkazu tagu, např. KILL nebo WRITE. Je vhodná pro použití v aplikacích s pasivními tagy, kde je vysílací výkon čtečky mnohem větší než vysílací výkon tagu a předpokládá se, že útočník bude ve větší vzdálenosti od tagu než čtečka. Pokud však útočník zachytí přenos klíče na uplink kanálu, dokáže dešifrovat veškerou komunikaci. Důležitá je také kvalita generátoru pseudonáhodných čísel v tagu.

Šifrování přenášených dat

Používá se v případech, kde je technika Cover-Coding nedostatečná (útočník dokáže odposlechnout komunikaci na uplink kanálu). Data jsou šifrována před jejich odesláním přes rádiové rozhraní. Tag může sloužit pouze pro uložení šifrovaných dat, kdy nemá schopnost je sám dešifrovat (běžné pasivní tagy) nebo může obsahovat dešifrovací obvod, což ovšem vede ke složitějším a nákladnějším tagům s větší spotřebou a zpožděním. Tento způsob tedy není vhodný pro systémy s vysokými požadavky na rychlost komunikace s tagy.

Omezení šíření signálu

Elektromagnetické stínění Stínění slouží k omezení šíření radiofrekvenčního signálu mimo vyhrazený prostor pomocí vodivé bariéry (Faradayova klec). Redukuje možnost odposlechu komunikace útočníkem. Kromě trvalého stínění v průmyslu lze využít také stínění po dobu nepoužívání tagu (elektronického pasy, přístupové karty apod.) v podobě obalů z hliníkové fólie.

Snížení vysílacího výkonu Snížením vysílacího výkonu čtečky lze omezit dosah komunikace a tím i možnost jejího nežádoucího odposlechu. Výkon však lze snížit maximálně na hodnotu, která zaručí spolehlivou a bezproblémovou funkci systému.

Manuální aktivace tagu

Tag je vybaven přepínačem pro jeho aktivaci a deaktivaci, uživatel tak má kontrolu nad jeho aktivitou a snižuje se možnost útoku na tag. Toto řešení se používá u přístupových a platebních systémů. Jeho nevýhodou je nutnost seznámení uživatele s touto funkcí (kde, kdy a po jakou dobu má být tag aktivní). Nelze jej použít v aplikacích typu elektronického mýtného, kde není přípustné, aby musel uživatel během jízdy jakkoliv manipulovat s tagem.

4.1.3 Zabezpečení dat v tagu

Řízení přístupu k paměti tagu - LOCK

Některé tagy mají funkci pro ochranu paměti pomocí hesla. Heslo je při přenosu zabezpečeno proti odposlechu pomocí cover coding techniky. Existují dočasné (LOCK) nebo

stálé (PERMALOCK) zámky. Dále se rozlišuje ochrana proti zápisu nebo proti čtení i zápisu. Existuje také LOCK POINTER, což je adresa místa v paměti s platnými daty. Oblast paměti s nižšími adresami, než je LOCK POINTER jsou chráněny proti zápisu. Efektivita tohoto řešení závisí na délce hesel a jejich správě. Díky ochraně hesla pouze technikou cover coding je nutné zabránit odposlechu dat, která vysílá tag.

Šifrování dat

Ukládání dat do paměti tagu v šifrované podobě je totožné s případem z „šifrování přenášených dat“ v předchozí části, kdy jsou data do tagu přenesena již zašifrována a tag je nedešifruje, ale uloží do paměti zašifrované. Jsou tak zároveň chráněna proti přečtení útočníkem, který má přístup k tagu.

Deaktivace tagu - KILL

Zaslání příkazu KILL tagu jej definitivně deaktivuje. To je užitečné v případě, kdy se nepředpokládá, že by tag byl ještě použit a jeho další případné neautorizované použití je nežádoucí. Tuto operaci podporuje pouze standard EPCglobal a je chráněna heslem, konkrétně verze standardu EPCglobal Class-1 Generation-2 používá 32bitové heslo, rozdílné od hesla funkce LOCK. Heslo je při přenosu zabezpečeno proti odposlechu pomocí cover coding techniky. Primárně zde slouží pro ochranu soukromí zákazníků. Existují různé přístupy pro implementaci tohoto příkazu. Jeden z nich pouze deaktivuje anténu tagu, ten je však stále funkční, jen je omezen jeho dosah například na několik centimetrů. Tím je zachována funkčnost, která může být ještě potřebná. Například po zaplacení zboží se tag deaktivuje, ale později z něj lze přečíst data pro případ reklamace apod. Na druhou stranu je existence této funkce dalším možným slabým místem, které může být zneužito útočníkem. To hrozí zejména v případě použití krátkých nebo slabých hesel nebo v případě sdílení totožného hesla více tagy. Nebezpečí odhalení hesla také stoupá s dobou, po kterou je heslo neměnné. Data z tagu nejsou samotnou operací KILL smazána, jsou tedy i po jeho deaktivaci uložena v paměti a ohrožena útoky pokročilých útočníků.

4.2 Přehled standardů

V této sekci je uveden přehled zabezpečení nejrozšířenějších standardů RFID systémů.

4.2.1 ISO 11784/11785

Použití: Identifikace zvířat
Pásmo: LF
Velikost paměti: 64bitové ID
Důvěrnost: Žádná.
Integrita: CRC kontrola.

4.2.2 ISO/IEC 14443

Použití: Přístupové karty, jízdenky apod.
Pásmo: HF
Velikost paměti: 32, 56 nebo 80bitové ID

Důvěrnost: Žádná.
Integrita: CRC kontrola.

4.2.3 ISO/IEC 15693

Použití: Přístupové karty s větším dosahem (1m)
Pásmo: HF
Velikost paměti: 64bitové ID a až 8 kB Read/Write paměti
Důvěrnost: Žádná ochrana čtení, žádné šifrování nebo autentizace.
Integrita: Permanentní LOCK, CRC kontrola.

4.2.4 ISO 18000-3

Použití: Evidence zboží a zavazadel
Pásmo: HF
Velikost paměti: 64bitové ID a Read/Write paměť dat
Důvěrnost: Čtení chráněné 48bitovým heslem (Mode 2)
Integrita: Permanentní LOCK, CRC kontrola. V případě Mode 2 navíc zápis chráněný 48bitovým heslem a LOCK pointer, zamykající nevyužitou paměť.

4.2.5 EPCglobal Class-1 Generation-2 (ISO/IEC 18000-6C)

Použití: Zásobování
Pásmo: UHF
Velikost paměti: až 496bitové ID, WORM a Read-Write paměť pro data
Důvěrnost: Cover-Coding (šifrování downlink kanálu), adresace tagů čtečkou pomocí 16bitových náhodných čísel.
Integrita: Části paměti lze uzamknout proti zápisu nebo trvale uzamknout, CRC kontrola.

4.3 Řešení na trhu

V této sekci jsou stručně představena v praxi nyní nejčastěji používaná řešení různých výrobců, některé jejich parametry a použité zabezpečovací mechanismy.

4.3.1 MIFARE

MIFARE je velmi rozšířená implementace standardu ISO/IEC 14443-A pro bezkontaktní chytré karty (smart cards) od společnosti NXP Seminductors (Philips). Bylo prodáno přes 3,5 miliardy integrovaných obvodů a 40 milionů čteček. Používá se v mnoha aplikacích jako jsou přístupové systémy, elektronické mýtné, parkovací karty, dopravní karty, letenky, vstupenky, dárkové karty a mnoho dalších. Dosah komunikace je kolem 10cm. Technologie MIFARE zahrnuje několik produktů[29]:

MIFARE Classic

1 nebo 4 kB EEPROM
7bajtové unikátní sériové číslo
16 nebo 40 bezpečně oddělených sektorů pro použití více aplikací

Životnost dat 10 let

Oboustranná three-pass autentizace dle ISO/IEC DIS 9798-2
Proprietární proudová šifra CRYPTO1 pro zabezpečení všech příkazů (přenosu dat) a autentizaci, byla však již prolomena pomocí reverzního inženýrství [23]
Každý sektor je chráněn dvěma jedinečnými klíči pro nastavení oprávnění ke čtení/zápisu.

MIFARE Ultralight

Odlehčená verze MIFARE Classic pro použití jako vstupenky, krátkodobé jízdenky apod.
512bitová EEPROM, 32bitová WORM oblast, 384 bitů uživatelské Read/Write paměti
Životnost dat 5 let

Read-Only LOCK pro jednotlivé stránky paměti
Kontrola integrity pomocí 16bitového CRC
Žádné šifrování ani autentizace

MIFARE DESFire EV1

Pražská karta OpenCard je od dubna 2008 vydávána v této variantě [20].
2, 4 nebo 8 KB EEPROM
Až 28 aplikací a 32 souborů/aplikaci
7bajtové unikátní sériové číslo
Přenos dat až 848 kbit/s
Automatická záloha dat

Oboustranná three-pass autentizace
CRC na fyzické vrstvě pro kontrolu integrity
DES/3DES nebo AES šifrování přenášených dat
Common Criteria certifikace EAL4+

MIFARE Plus

Paměťová struktura kompatibilní s MIFARE Classic
2 nebo 4 KB EEPROM
7bajtové unikátní sériové číslo
Přenos dat až 848 kbit/s
Životnost dat 10 let

Řízení přístupu k paměti
Common Criteria certifikace EAL4+
CRYPTO1 nebo AES (128bitové) pro autentizaci a šifrování dat

4.3.2 iCLASS

Jedná se o řešení od firmy HID [3] pro přístupové systémy, postavené na ISO/IEC 14443-B a ISO 15693.

256 Bajtů, 2 kB nebo 4 kB paměti
Až 16 aplikací na kartě
Životnost dat 10 let

Ochrana přístupu k paměti dvěma 64bitovými Read/Write hesly pro každý aplikační sektor paměti
Vzájemná autentizace

Existuje zde několik úrovní bezpečnosti, přičemž u nejnižších (Standard Security a High Security - iCLASS Elite) je pro šifrování přenosu dat a autentizaci použit proprietární šifrovací algoritmus nebo DES a šifrovací klíče jsou nastaveny výrobcem (dokonce stejné pro všechny systémy na úrovni Standard Security) a zákazník je nemůže změnit. Až nejvyšší úroveň (High Security - iCLASS Field Programmer) umožňuje použít pro šifrování 3DES a zákaznickou správu klíčů. [30]

4.3.3 LEGIC

Řešení přístupových a platebních systémů švýcarské firmy LEGIC Identsystems Ltd, založené na standardech ISO 14443 a ISO 15693 a vlastním proprietárním řešení *LEGIC RF*. Nabízí několik stupňů zabezpečení podle použití, výběr z šifer DES, 3DES, AES-128 a AES-256, vzájemnou autentizaci, autentizaci zpráv, uživatelsky definované Read/Write hesla, end-to-end šifrování a Common Criteria certifikaci EAL4+ a EAL5+.

256, 1024 nebo 2048 bajtů paměti
Až 127 aplikací na jedné kartě
Paměť není rozdělena na pevné sektory, může tak být využita bezezbytku.

Kapitola 5

Odposlech komunikace a čtení tagu na větší vzdálenosti

Největší výhoda technologie RFID, kterou je možnost bezdrátového přenosu dat, je zároveň potencionální bezpečnostní dírou. I když je často použito šifrování komunikace a útočník nedokáže získat pro něj čitelná data na úrovni aplikační vrstvy, přesto pro něj někdy může být užitečná již pouhá informace o přítomnosti RFID tagu či přítomnosti tagu s daným UID. S vysokou pravděpodobností z ní vyplývá i přítomnost objektu, který je s tagem vázán, a který může být například cílem krádeže apod. Deklarovaná komunikační vzdálenost je poměrně malá (zejména při použití pasivních tagů), což se na první pohled jeví jako bezpečné. Například u přístupových systémů se nepředpokládá nepozorovaná přítomnost odposlouchávacího zařízení ve vzdálenosti v řádech několika centimetrů od legitimní čtečky. Prakticky lze ovšem číst tagy nebo odposlouchávat jejich komunikaci se čtečkou na mnohem větší vzdálenosti. Toho se dosahuje zejména zlepšením příjmových vlastností antén, jejich zvětšením nebo použitím kvalitních zesilovačů signálu. Dále se používá postprocessing signálu, umožňující získat užitečná data z poměrně hodně zašuměného signálu pomocí algoritmů na odstranění šumu. Pokud není při analýze bezpečnostních rizik konkrétního RFID systému vzata do úvahy možnost odposlechu na podstatně delší vzdálenosti než je deklarovaný operační dosah a není zváženo použití jiné technologie nebo nejsou přijata případná protiopatření ve formě odstínění nebo snížení vysílacího výkonu čteček apod., může se jednat o vážný bezpečnostní problém.

V této kapitole bude představena teorie a výsledky tzv. skimming a eavesdropping útoků na RFID systémy dle standardů ISO 14443A/B[1] a ISO 15693[2] pracujících na frekvenci 13,56 MHz. Ty používají indukční vazbu a mají malou deklarovanou operační vzdálenost (10 cm, resp. 100cm), proto je u nich riziko falešného pocitu bezpečí nejvyšší. Útok na ně je také pro útočníka často nejvýhodnější, neboť se používají v aplikacích, pro které je bezpečnost dat kriticky důležitá (přístupové systémy, platební karty, elektronické pasy, elektronické jízdenky atd.) a jejich kompromitace tedy přináší nejvyšší zisk.

5.1 ISO 14443A - přenos dat

Downlink kanál je přenášen na frekvenci nosné $f_n = 13,56MHz$ pomocí amplitudové modulace (ASK) s modulačním indexem 100%. Data jsou kódována modifikovaným Millerovým kódem a přenášena rychlostí 106 kbit/s. Uplink kanál je přenášen také pomocí ASK modulace (modulační index 8-12%) vlivem změny impedance obvodu tagu na subnosné o frekvenci

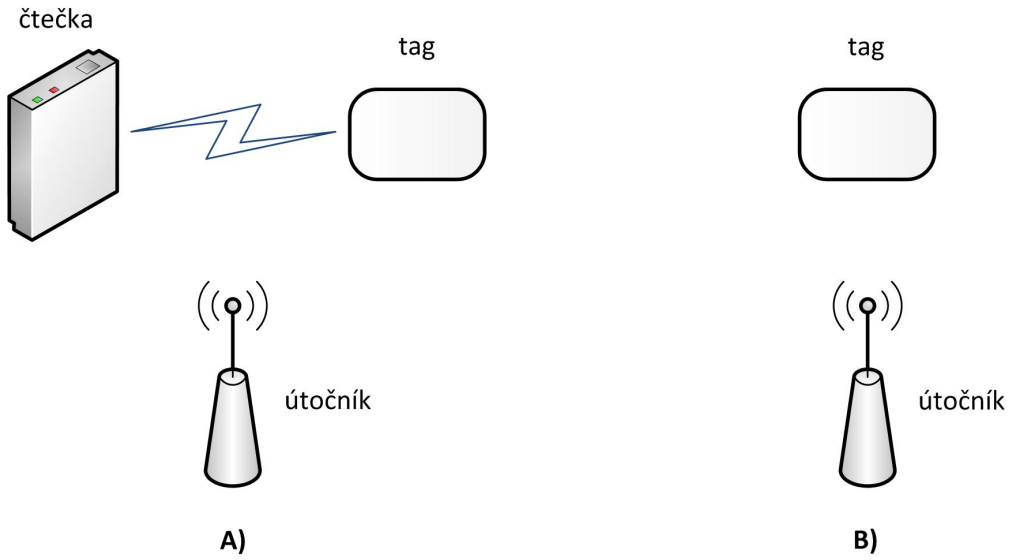
$f_s = 847kHz$ s kódováním Manchester na komunikační rychlosti 106 kbit/s. Tato subnosná vytváří dvě pásma o šířce 424 kHz o středních frekvencích 12,712 MHz ($f_c - f_s$) a 14,408 MHz ($f_c + f_s$).

5.2 ISO 14443B - přenos dat

Downlink kanál je kódován pomocí NRZ (Non-Return-to-Zero) kódování, využívá amplitudovou modulaci s modulačním indexem 10% a přenáší data rychlostí 106 kbit/s. Uplink kanál je modulován pomocí BPSK s modulačním indexem 8-14% a kódován NRZ kódem. Subnosná na 847 kHz vytváří kanál šířky 212 kHz.

5.3 ISO 15693 - přenos dat

Downlink kanál přenáší data kódovaná kódem PPM (Pulse Position Modulation) „1 ze 4“ rychlostí 26,48 kbit/s nebo kódem „1 ze 256“ rychlostí 1,65 kbit/s. Používá ASK modulaci s modulačním indexem 10 nebo 100 %. Uplink kanál kóduje data pomocí kódu Manchester a přenáší je rychlostmi 6,62 kbit/s nebo 26,48 kbit/s při použití jedné subnosné na 423,75 kHz, resp. rychlostmi 6,67 kbit/s nebo 26,69 kbit/s při použití i druhé subnosné na 484,28 kHz.



Obrázek 5.1: Eavesdropping (A) a skimming (B)

5.4 Odposlech komunikace (eavesdropping)

Cílem tohoto útoku je odposlech probíhající komunikace mezi tagem a legitimní čtečkou. Protože tag je již napájen polem legitimní čtečky, může být vzdálenost útočníka od tagu větší. Problémem je nutnost odposlechu v čase komunikace tagu se čtečkou, např. v okamžiku, kdy osoba přiblíží přístupovou kartu ke čtečce u vchodu. Zároveň to ale může být jediný moment, kdy je tag dostupný - pokud je uchováván v obalu, který odstiňuje rádiové vlny.

Podle toho, jakou informaci lze při odposlechu získat, rozlišujeme tři vzdálenosti [14]:

- Vzdálenost, při které útočník detekuje komunikaci na downlink kanálu (čtečka vysílá data), nemůže však spolehlivě získat přenášená data. Získá pouze informaci o tom, že probíhá komunikace mezi čtečkou a tagem.
- Vzdálenost, při které útočník dokáže získat přenášená data na downlink kanálu.
- Vzdálenost, při které útočník dokáže získat přenášená data na uplink kanálu (tag vysílá data).

Pro úspěšný odposlech dat je nutné je odposlechnout bez chyby přenosu. Díky povaze bezdrátového šíření signálu je pravděpodobný výskyt takovéto chyby vlivem rušení, útlumu či odrazů signálu. Standard ISO 14443A navíc nepoužívá žádné mechanismy umožňující korekci chyb přenosu dat. Spolehlivost příjmu posloupnosti bitů je dána délkou této posloupnosti a hodnotou BER (Bit Error Rate), která vyjadřuje procento chybně přenesených bitů a která je závislá na použité modulaci signálu a poměru užitečného signálu a šumu (SNR, Signal-to-Noise Ratio). Čím větší datový rámec chceme přijmout, tím větší je pravděpodobnost, že dojde během jeho přenosu k chybě. Tato pravděpodobnost (FER, Frame Error Rate) je pro n-bitový rámec dána vzorcem

$$1 - FER = (1 - BER)^n$$

Například pokud je BER = 1%, pak pravděpodobnost bezchybného příjmu 4 bajtového rámce (délka UID karet Mifare Classic) je ucházejících 72,5%. V případě rámce dlouhého 16 bajtů je to však pouze 27,6%. Standard ISO 14443A však umožňuje přenášet až 256 bajtové rámce. Pro 50 % pravděpodobnost, že takto dlouhý rámec správně přijmeme, je nutná BER = 0,034 %. Vidíme tedy, že útok na systém používající pouze UID tagu, je technicky jednodušší než v případě systému, který z paměti tagu čte větší množství dat. Orientační příklad potřebných hodnot SNR pro dodržení BER v závislosti na použité demodulaci[1] jsou v tabulce 5.1. Tyto hodnoty platí, pokud není použito další zpracování signálu za účelem jeho pročištění od šumu z okolního prostředí. Pokud je použito, mohou být hodnoty SNR nižší, a přesto se podaří kvalitně zrekonstruovat data. Pro zvýšení BER se také používá synchronní detekce signálu.

demodulace / BER	0,1%	0,01%
koherentní	9,8 dB	11,4 dB
nekoherentní	12,8 dB	14,4 dB

Tabulka 5.1: Minimální hodnoty SNR pro požadované BER a danou metodu demodulace

Na frekvenci 13,56 MHz jsou v průmyslovém/kancelářském a obytném prostředí jakožto místu nejčastějších útoků na tyto systémy dominantním zdrojem šumu především různé přístroje. Tato frekvence totiž spadá do ISM (Industrial, Scientific and Medical applications) pásma 13,553 - 13,567 MHz, které používají zejména průmyslové aplikace pro dielektrický ohřev různých materiálů jako je keramika, textil, papír, dřevo nebo plast za účelem jejich vysušení či vytvrzení [17]. Také je v prostředí tohoto typu vyšší výskyt RFID čteček (např. přístupový systém v kancelářské budově), které zpravidla pracují na stejné

[1] Koherentní demodulace je hardwarově složitější, pro demodulaci signálu využívá synchronizaci s jeho fází.

frekvenci. Hladina šumu je průměrně 45,4 dB v průmyslovém prostředí, 41,1 dB v obytném prostředí a 26 dB v prostředí pouze s galaktickým šumem[2]. Protože hladina šumu klesá se vzrůstající frekvencí, je pro odposlech uplink kanálu lépe využít pásma subnosné o středové frekvenci 14,408 MHz, avšak rozdíl oproti hladině šumu pásma o nižší frekvenci subnosné není příliš markantní. Pro minimalizaci šumu se používají vstupní filtry, propouštějící pouze žádanou frekvenci a potlačující zbytek frekvenčního pásma.

Na sílu přijímaného signálu má také vliv vzájemná poloha vysílací a přijímací antény (cívky). Radiální magnetické pole je do vzdálenosti $\lambda/2\pi$ (hranice tzv. „near field“) dvakrát silnější než tangenciální pole. Nad touto hranicí se ovšem rychlost poklesu síly radiálního pole zvětšuje a při vzdálenosti větší než 8,3 m (platí pro frekvenci 13,56 MHz) je tangenciální pole silnější než pole radiální. Tato vzdálenost je závislá pouze na frekvenci. Odposlech je tedy do vzdálenosti menší než 8,3 m spolehlivější (vazba je silnější), pokud je anténa odposlouchávacího zařízení v axiálním uspořádání s anténou čtečky. Ve vzdálenosti větší než 8,3 m je odposlech spolehlivější, pokud jsou antény v planárním uspořádání (viz Obr.5.2).

Ve standardu ISO 14443 je definována intenzita nemodulovaného magnetického pole antény čtečky v rozmezí od 1,5 do 7,5 A/m (rms). Tuto hodnotu nesmí překročit, jinak hrozí zničení tagu. Naopak nízká intenzita nedokáže naindukovat dostatečné napětí v přijímacím obvodu tagu, který v důsledku toho nebude mít dostatek energie pro svůj provoz. Ve stejném rozmezí intenzity magnetického pole musí operovat také tag. V případě standardu ISO 15693 je tento rozsah 150 mA/m až 5A/m (rms).

Tabulka 5.2 zobrazuje maximální teoretické vzdálenosti, na které lze odposlechnout RFID komunikaci na downlink kanálu v různých prostředích s různými průměrnými hodnotami RF šumu. Ve výpočtech byla použita modelová čtečka A s poloměrem antény 3 cm a maximální intenzitou magnetického pole v místě antény čtečky 1,5 A/m (rms) a čtečka B s poloměrem antény 7,5 cm a maximální intenzitou magnetického pole 7,5 A/m (rms). Tabulka 5.3 zobrazuje totéž pro uplink kanál a intenzitu magnetického pole v místě antény tagu 1,5 A/m a 4,5 A/m (rms). Jak je vidět, maximální vzdálenosti jsou v případě vyšší intenzity magnetického pole paradoxně kratší. To je způsobeno tím, že se vzrůstající intenzitou magnetického pole klesá impedance obvodu tagu. V důsledku toho klesá jeho schopnost ovlivňovat amplitudu signálu čtečky. Vzdálenosti byly vypočteny při použití nekoherentní demodulace a s ohledem na okolní šum, avšak s ideálními podmínkami šíření signálu ve volném prostoru bez překážek a odrazů. Při použití koherentní demodulace se vzdálenosti teoreticky zvětší o cca 40% v případě downlink kanálu a o cca 15% v případě uplink kanálu.[32]

	Průmyslové	**Obytné**	**Galaktický šum**
čtečka A	7,9/7,2 m	12,8/10,5 m	76,3/63,4 m
čtečka B	0,6/0,5 km	1,0/0,9 km	6,0/5,0 km

Tabulka 5.2: Maximální teoretické vzdálenosti pro odposlech downlink kanálu při nekoherentní demodulaci. Vzdálenosti jsou uváděny pro BER = 0,1% / BER = 0,01%

Reálná maximální vzdálenost pro odposlech RFID systémů pracujících na této frekvenci závisí na mnoha faktorech:

- vysílacím výkonu čtečky, resp. síle modulace signálu čtečkou a tagem
- síle vzájemné vazby čtečky a tagu, závislé na jejich vzdálenosti a orientaci v prostoru

[2]Hladiny šumu jsou vztaženy k termálnímu šumu při teplotě 288 K.

	Průmyslové	**Obytné**	**Galaktický šum**
H_t **= 1,5 A/m (rms)**	2,8/2,6 m	3,4/3,2 m	7,2/6,6 m
H_t **= 4,5 A/m (rms)**	2,0/1,8 m	2,4/2,2 m	4,7/4,4 m

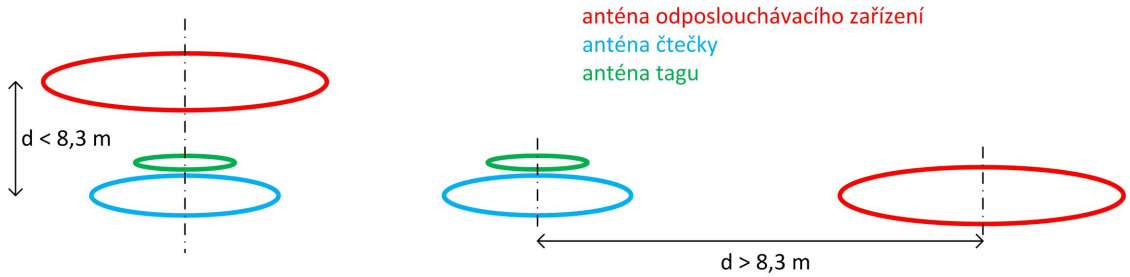
Tabulka 5.3: Maximální teoretické vzdálenosti pro odposlech uplink kanálu při nekoherentní demodulaci. Vzdálenosti jsou uváděny pro BER = 0,1% / BER = 0,01%

- vlastnostech antény odposlouchávacího systému
- útlumu signálu v odposlouchávacím systému
- vnitřního šumu odposlouchávacího systému (především zesilovače)
- RF šumu pocházejícího z jiných zdrojů v prostředí
- vodivých předmětech v prostředí, které ovlivňují magnetické pole

Typicky je maximální vzdálenost odposlechu dat z uplink kanálu kratší než vzdálenost pro odposlech downlink kanálu, to je i případ ISO 14443A. V případě ISO 14443B je naopak vzdálenost odposlechu uplink kanálu cca o metr větší než u downlink kanálu[13].Tyto rozdíly jsou způsobeny odlišným způsobem modulace a také rozdílem ve vysílacím výkonu tagu oproti výkonu čtečky (cca o 60dB slabší signál na frekvenci 13,56 MHz a vazební vzdálenosti čtečka-tag 10 cm). Útočníka však obvykle zajímají právě data čtená z tagu na uplink kanálu, jelikož downlink kanál obsahuje často pouze instrukce pro tag. Z tohoto důvodu se jeví snazší odposlech komunikace dle standardu ISO 14443B.

V [25] se autorům podařilo odposlechnout data vyslaná 7 různými tagy typu A pracujícími na frekvenci 13,56 MHz až na vzdálenost 15 m. Údajně přitom nepoužili žádná drahá zařízení a tohoto výsledku nebylo dosaženo v odstíněné laboratoři, ale v prostředí s běžným rádiovým šumem a s použitím „malých“ antén. Vzdálenost odposlechu silně závisela na konkrétním tagu (pro některé byla „pouze“ 8 m). Vysvětlením pro takové výsledky může být minimální SNR pouhých 6 dB, které autorům mělo stačit pro spolehlivé dekódování dat (zřejmě z důvodu kvalitního zpracování signálu) a také možná přítomnost kovových předmětů v prostředí, kde pokus probíhal. Může se jednat o kabely, kovové výztuhy stropu a zdí nebo kovové trubky. Ty mohou sloužit jako antény snižující útlum signálu vlivem zvětšující se vzdálenosti. Podrobnosti o tomto pokusu se nalézají v dokumentu [24], který však není veřejně dostupný a neuspěl jsem ani u autorů s žádostí o jeho zaslání.

Výsledky pokusů v [13] se pro tag dle ISO 14443A (Mifare Classic) blíží výše uvedeným teoretickým vzdálenostem pro průmyslové prostředí: 5 m (resp. 10 m při jiném nastavení antény - [14]) pro downlink a průměrně 2,5 m pro uplink kanál, naměřeno v prostoru s vícero RFID čtečkami přístupového systému a v blízkosti laboratoří se zdroji RF šumu. Charakter tohoto prostředí odpovídá zařazení do kategorie průmyslových/kancelářských prostor, podle naměřených vzdáleností se tedy přibližně shoduje se studií [32] i co se týče hodnot okolního šumu. Ačkoliv má ISO 15693 podstatně větší dosah, vzdálenosti odposlechu jsou srovnatelné s ISO 14443A. To proto, že většího dosahu není dosaženo vyšším vysílacím výkonem čtečky, ale schopností pracovat i s nízkou intenzitou magnetického pole. Při pokusech byl použit komerční RF receiver, aktivní feritová anténa pro magnetická pole a zpracování signálu pomocí FIR (Finite Impulse Response) filtru a korelace. Autor také vyzkoušel levný (za v přepočtu méně než cca 1500 Kč) RF receiver s anténou o průměru 10 cm a podařilo se mu s ním odposlechnout oba kanály na vzdálenost 60 cm, což může být v mnoha případech dostačující.



Obrázek 5.2: Optimální uspořádání odposlouchávací antény od čtečky podle jejich vzájemné vzdálenosti (platí pro frekvenci 13,56 MHz)

5.4.1 Aktivní odposlech

Při pasivním odposlechu je komunikace mezi tagem a čtečkou zachytávána na nosné frekvenci. Naproti tomu při aktivním odposlechu útočník vysílá nemodulovaný signál na frekvenci odlišné od nosné frekvence legitimních prvků. Pokud je tato frekvence blízko legitimní frekvence, je také ovlivňována změnami impedance tagu na uplink kanálu. Příjmem legitimní frekvence i frekvence vysílané útočníkem a jejich sečtením lze komunikaci zachytávat spolehlivěji než při pasivním odposlechu. V [4] se autorům použitím aktivního odposlechu v laboratorních podmínkách (odstíněná komora) podařilo zdvojnásobit maximální vzdálenost oproti pasivnímu odposlechu uplink kanálu komunikace s tagem dle UHF standardu EPC Gen2 (pracujícím na frekvenci v rozmezí 860 MHz - 960 MHz). Tuto metodu lze použít i v případě skimming útoku (viz dále).

5.5 Čtení tagu na větší vzdálenosti (skimming)

Skimming je útok, při kterém jsou neoprávněně přečtena data z tagu bez vědomí jeho vlastníka. Útočník tedy může vyslat tagu libovolný příkaz a číst/editovat data na něm uložená. Pro útočníka je důležité zvětšení vzdálenosti, na kterou je schopen s tagem spolehlivě komunikovat, aby nevzbudil podezření vlastníka tagu. To však v určitých situacích nemusí být nutné (např. útočník se posadí vedle osoby s tagem v hromadném dopravním prostředku apod.). Oproti eavesdropping útoku je zde nutnost kromě příjmu dat z tagu jej také napájet. Výhodou tohoto útoku oproti eavesdroppingu je možnost opakovat dotaz a tím také opakovaně získat odpověď tagu, díky čemuž lze eliminovat chyby přenosu.

Rozlišujeme dvě vzdálenosti, na které je možné provést útok:

- Vzdálenost, na kterou útočník dokáže polem čtečky napájet tag a zaslat mu příkaz (např. přepsaní místa v paměti tagu pro DOS útok).
- Vzdálenost, na kterou útočník dokáže napájet tag, zaslat mu příkaz a přijmout odpověď (typicky přečtení informace z tagu).

Pro útočníka však může být nutnost napájet tag také výhodou, neboť může pro jeho napájení použít magnetické pole o vyšší intenzitě, než jakou poskytují standardní čtečky. Toho využil autor v [13], kde použil čtečku s jednou anténou pro napájení tagu a komunikaci s ním a jednu anténu pro odposlech. Tím se vlastně přiblížil k eavesdropping útoku. Napájecí anténa může být menší, což je pro reálný útok praktičtější, hlavní výhodou ale je, že lze pro každý účel použít anténu s vhodnými vlastnostmi. Při velikosti napájecí antény cca

15x21 cm a její vzdálenosti 15cm od tagu Mifare Classic (ISO 14443A) a s pomocí 1W zesilovače se mu podařilo dekódovat odpověď tagu na vzdálenost 2m. Se 4W zesilovačem a větší anténou 30 x 42 cm však pouze na vzdálenost 27 cm. To si autor vysvětluje stejným způsobem jako v případě výsledků odposlechu v tabulce 5.3, tedy omezenými možnostmi obvodu tagu ovlivňovat amplitudu nosné.

Kapitola 6

Útok na Mifare Classic

Bezpečnost tagu Mifare Classic stojí dle principu „security by obscurity“ na utajení proprietárního symetrického šifrovacího algoritmu Crypto1, který pro tyto tagy vyvinul jejich výrobce, společnost NXP Seminductors (dříve PHILIPS). Pomocí reverzního inženýrství byl však algoritmus odhalen [23] a dalšími analýzami byly objeveny chyby v návrhu algoritmu i v jeho implementaci. Poté bylo nalezeno několik typů útoků, které těchto chyb zneužívají. Pro praktickou realizaci jsem si vybral útok, který dokáže pomocí běžné RFID čtečky a opakování pokusů o autentizaci získat klíče ke všem sektorům paměti tagu. Umožňuje tedy bez předchozí znalosti klíče přečíst a editovat veškerý obsah paměti tagu[6][35].

6.1 Popis Mifare Classic

Mifare Classic[28][26] jsou čipy pro bezdrátové čipové karty dle standardu ISO/IEC 14443-A, pracující na frekvenci 13,56 MHz. Jsou velmi rozšířeny a používány například jako identifikační karty v nejrůznějších přístupových systémech, jako elektronické jízdenky nebo věrnostní karty.

Operační frekvence	13,56 MHz
Rychlost přenosu dat	106 kbit/s
Dosah	do 10 cm (dle geometrie antény a nastavení čtečky)
Velikost EEPROM	1kB / 4kB
Životnost dat	10 let

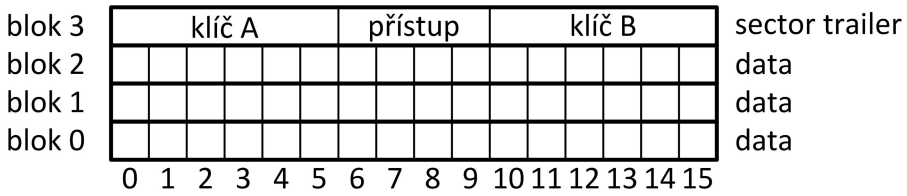
Tabulka 6.1: Parametry čipu Mifare Classic

6.1.1 Organizace paměti

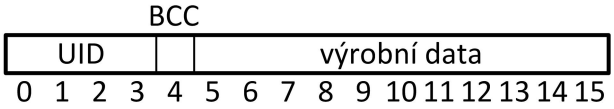
EEPROM paměť tagu je rozčleněna na sektory, které se skládají z 16bajtových bloků. V prvním bloku prvního sektoru (tzv. Manufacturer Block) je uloženo 4bajtové UID[1] a další výrobní data. Ta jsou zapsána při výrobě čipu a jsou uzamčena pouze pro čtení. Poslední blok každého sektoru (tzv. Sector Trailer) obsahuje klíče A a B a definici oprávnění pro přístup k blokům v tomto sektoru. Pokud postačuje jeden klíč, může být paměť vyhrazená pro klíč B použita pro uložení dat. Díky organizaci paměti na sektory se samostatnými

[1] resp. NUID (non-unique ID), problematika popsána v [27]

klíči a definicemi přístupových oprávnění je možné jeden tag použít pro vícero na sobě nezávislých aplikací různých provozovatelů.



Obrázek 6.1: Struktura 4blokového paměťového sektoru



Obrázek 6.2: Struktura manufacturer bloku

Verze	Kapacita paměti	Organizace
1K	1024 B	16 sektorů po 4 blocích
4K	4096 B	32 sektorů po 4 blocích a 8 sektorů po 16 blocích

Tabulka 6.2: Kapacita a organizace paměti

6.1.2 3-průchodová autentizace

Jakmile se tag ocitne tak blízko čtečky, aby energie elektromagnetického pole byla schopná jej napájet, vyšle své UID. Tím započne antikolizní fáze, kdy si čtečka vybere, se kterým tagem bude komunikovat, pokud bylo současně vysíláno více UID. Je použit deterministický antikolizní algoritmus (viz 2.7)Po výběru konkrétního tagu začne vzájemná 3průchodová autentizace:

1. Čtečka vyšle požadavek na autentizaci, který obsahuje číslo sektoru a informaci, zda bude použit klíč A nebo B.
2. Tag zašle náhodné číslo (tag nonce, n_T).
3. Čtečka vypočte z tag nonce a UID tagu odpověď a_R, vygeneruje náhodný reader nonce n_R a spolu s vypočtenou odpovědí a_R je zašle tagu. Od tohoto kroku je již komunikace šifrována.
4. Tag ověří, zda odpověď čtečky souhlasí s jím vypočtenou hodnotou a vypočte odpověď a_T na reader nonce a odešle ji čtečce.
5. Čtečka zkontroluje správnost odpovědi tagu.

Tím jsou obě strany vzájemně autentizovány na základě společného tajemství (sdíleného klíče A nebo B).

6.1.3 Paměťové operace

Pokud je čtečka úspěšně autentizována pro daný sektor, může (za předpokladu, že operace je povolena prostřednictvím přístupových oprávnění v Sector Traileru) v paměťovém prostoru sektoru provádět následující operace:

- **Read** - přečte jeden blok
- **Write** - zapíše jeden blok
- **Increment** - inkrementuje obsah bloku a výsledek uloží do interního registru
- **Decrement** - dekrementuje obsah bloku a výsledek uloží do interního registru
- **Transfer** - zapíše obsah interního registru do bloku
- **Restore** - uloží do interního registru obsah bloku

Operace Read a Write lze provést nad bloky typu *read/write* a *value* i nad *Sector Trailerem*, ostatní operace pouze nad blokem typu *value*.

6.2 Crypto1

Crypto1 je symetrická proudová šifra se 48bitovým klíčem. Algoritmus byl výrobcem úspěšně utajován, avšak v roce 2008 byl pomocí reverzního inženýrství odhalen[23] a ukázalo se, že délka klíče není jedinou slabinou algoritmu[9]. Implementace šifry je opravdu miniaturní, zabírá pouze cca 400 hradel (pro porovnání: implementace algoritmu AES zabírá cca 3400 hradel). Šifru tvoří spojení 48bitového posuvného registru se zpětnou vazbou (LFSR) a filtrovací funkce f [10]. Zpětná vazba posuvného registru je definována jako

$$\begin{aligned} L(x_0 x_1 \dots x_{47}) =& x_0 \oplus x_5 \oplus x_9 \oplus x_{10} \oplus x_{12} \oplus x_{14} \oplus x_{15} \oplus x_{17} \oplus x_{19} \oplus x_{24} \oplus x_{25} \oplus x_{27} \oplus x_{29} \\ & \oplus x_{35} \oplus x_{39} \oplus x_{41} \oplus x_{42} \oplus x_{43} \end{aligned}$$

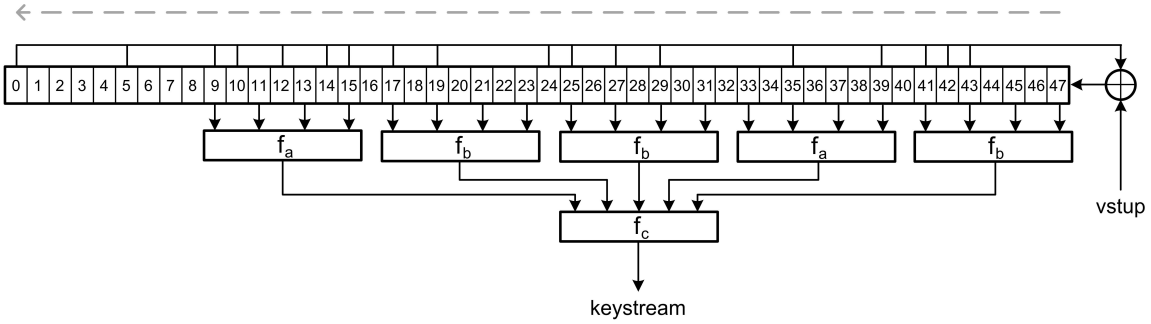
kde $\oplus$ značí funkci XOR.

S každým taktem hodinového signálu je obsah posuvného registru posunut o jeden bit doleva a nejpravější bit je vygenerován dle zpětnovazební funkce L. Vstupem dvoustupňové filtrovací funkce f 6.2 jsou liché bity 9, 11 ... 47 posuvného registru, na jejím výstupu je jeden bit keystreamu proudové šifry.

$$\begin{aligned} f(x_0 x_1 \dots x_{47}) :=& f_c(f_a(x_9, x_{11}, x_{13}, x_{15}), f_b(x_{17}, x_{19}, x_{21}, x_{23}), f_b(x_{25}, x_{27}, x_{29}, x_{31}), \\ & f_a(x_{33}, x_{35}, x_{37}, x_{39}), f_b(x_{41}, x_{43}, x_{45}, x_{47})) \end{aligned}$$

kde

$$\begin{aligned} fa(y0, y1, y2, y3) :=& ((y0 \vee y1) \oplus (y0 \wedge y3)) \oplus (y2 \wedge ((y0 \oplus y1) \vee y3)) \\ fb(y0, y1, y2, y3) :=& ((y0 \wedge y1) \vee y2) \oplus ((y0 \oplus y1) \wedge (y2 \vee y3)) \\ fc(y0, y1, y2, y3, y4) :=& (y0 \vee ((y1 \vee y4) \wedge (y3 \oplus y4))) \oplus ((y0 \oplus (y1 \wedge y3)) \wedge ((y2 \oplus y3) \\ & \vee (y1 \wedge y4))) \end{aligned}$$



Obrázek 6.3: Šifra Crypto1, skládající se z 48bitového LFSR a filtrovací funkce f

6.2.1 Generátor pseudonáhodných čísel

Generátor je tvořen 16bitovým posuvným registrem se zpětnovazební funkcí

$$L_{16}(x_0 x_1 \dots x_{15}) := x_0 \oplus x_2 \oplus x_3 \oplus x_5$$

Obsah registru má na počátku funkce (jakmile začne být tag napájen polem čtečky a čip je inicializován) konstantní hodnotu a s každým taktem hodinového signálu o frekvenci 106kHz je jeho obsah posunut. Ačkoliv je generátor pouze 16bitový, slouží ke generování 32bitového n_T.

6.2.2 Inicializace šifry

Inicializace šifry probíhá během vzájemné autentizace tagu a čtečky. Označme bity klíče jako k_i a stav LFSR šifry jako a_i v čase i.

- LFSR je inicializován příslušným 48b klíčem sektoru $\quad a_i := k_i \; \forall i \in [0, 47]$
- poté je do LFSR načteno $n_T \oplus UID \quad a_{i+48} := L(a_i, \dots, a_{i+47}) \oplus n_{Ti} \oplus UID_i \; \forall i \in [0, 31]$
- nakonec je načteno $n_R \quad a_{i+80} := L(a_{i+32}, \dots, a_{i+79}) \oplus n_{Ri} \; \forall i \in [0, 31]$

Při inicializaci šifry je sjednocen stav šifry ve čtečce i tagu. Výstup LFSR šifry přes filtrovací funkci f produkuje keystream $b_i := f(a_i, a_{i+1} \dots a_{i+47}) \; \forall i \; \in \mathbb{N}$ v čase i. Tím jsou pomocí funkce XOR šifrována přenášená data. Jak již bylo zmíněno, při inicializaci šifry (resp. autentizaci čtečky a karty) začíná šifrování dat. Ta jsou šifrována částmi keystreamu, označovanými jako $ks1$ až $ks3$:
$\{n_R\} = n_R \oplus ks1$
$\{a_R\} = a_R \oplus ks2$
$\{a_T\} = a_T \oplus ks3$

tyto pojmenované části keystreamu odpovídají následujícím bitům:
$ks1 := b_{32} \dots b_{63}$
$ks2 := b_{64} \dots b_{95}$
$ks3 := b_{96} \dots b_{127}$

6.3 Slabá místa

V této sekci budou popsána slabá místa objevená jak v samotném návrhu šifry Crypto1, tak i v její implementaci v čipech Mifare Classic.

6.3.1 Generátor pseudonáhodných čísel

Registr LFSR, který slouží pro generování náhodného 32bitového n_T, je pouze 16bitový, což má za následek velmi nízkou míru entropie n_T. Protože je LFSR taktován hodinovým signálem o frekvenci 106 kHz, je stejný n_T vygenerován každých 618 ms. Obsah registru je navíc po resetu vždy inicializován na konstantní hodnotu.

6.3.2 Šifra Crypto1

Výstupní bity LFSR

Jak již bylo řečeno, jako výstup LFSR jsou použity pouze liché bity č. 9 až 47. Bity LFSR můžeme použitím techniky „rozděl a panuj“ rozdělit na liché a sudé. Pokud se nejprve zaměříme pouze na liché bity, je v jednom kroku vygenerován jeden bit keystreamu (proudu bitů na výstupu šifry) pomocí 20 bitů 9, 11...47. V dalším kroku je vygenerován následující bit keystreamu, který nás ale nyní nezajímá, protože je vypočten ze sudých bitů LFSR. V následujícím kroku je vygenerován další bit keystremu pomocí bitů 11, 13...47 z předchozího „lichého“ kroku a nového 47. bitu, který byl vygenerován zpětnovazební funkcí v předchozím „sudém“ kroku. Pokud známe dva bity keystreamu, které byly vygenerovány lichými bity LFSR, můžeme omezit možné hodnoty těchto 21 bitů na ty, které aplikací filtrovací funkce generují právě tyto dva známé bity keystreamu. Obdobně pro sudé bity.

Další slabinou je fakt, že jako výstup LFSR není použit nejlevější (nultý) bit. Díky tomu lze provést zpětný běh LFSR. Pokud známe jeho obsah v jednom časovém okamžiku, lze postupně dopočítat všechny předchozí stavy LFSR až do výchozího stavu, kdy je jeho obsahem klíč sektoru, vůči němuž se čtečka autentizuje. Předpokládejme, že známe stav LFSR v okamžiku, kdy byla právě vsunuta hodnota n_R. Vrátíme stav LFSR doprava o jeden krok zpět, nejlevější bit nastavíme na libovolnou hodnotu r. Protože je v tomto stavu na výstupu filtrovací funkce bit keystreamu $ks1_{31}$ (n_R je šifrováno částí keystreamu $ks1$), který sloužil k zašifrování posledního bitu n_R, vypočteme poslední bit n_R jako $\{n_R\} \oplus ks1_{31}$. Pomocí zpětnovazební funkce dopočteme správnou hodnotu r. Pokud toto zopakujeme ještě 63krát, bude obsahem LFSR tajný klíč sektoru.

Pravděpodobnostní odchylka

V [6] bylo objeveno slabé místo ve vazbě mezi proudem šifry a obsahem LFSR, na základě jehož je generován. Konkrétně se jedná o keystream $ks1$ a náhodný nonce čtečky n_R. Pravděpodobnost, že $ks1$ je generován nezávisle na posledních 3 bitech n_R, je 0,75. Navíc Courtois zjistil, že pokud v konkrétním případě předchozí platí, pak rozdíl ve stavu šifry kdykoliv během výpočtu $ks2$ a $ks3$ je lineární funkcí, která závisí na rozdílech v posledním bajtu n_R.

6.3.3 Komunikační protokol

Dle standardu ISO 14443-A, z něhož Mifare Classic vychází, je každý přenášený bajt následován paritním bitem. Mifare Classic přenáší šifrovaná data, ovšem paritní bit je vypočten z nezašifrovaných dat, čímž dohází k úniku informace o nich. Navíc je bit keystreamu, jímž je šifrován paritní bit, použit také k zašifrování prvního bitu z následujícího šifrovaného bajtu. Neplatí tedy pravidlo, že je každý bit keystreamu použit pouze jednou.

Dalším slabým místem komunikačního protokolu je únik informace o správnosti parity přijatého páru n_R,a_R. Pokud všech 8 paritních bitů dešifrované zprávy souhlasí, avšak

odpověď a_R není korektní, tag odpoví 4bitovým chybovým kódem o hodnotě 0x5. Ten je navíc také zašifrován, což umožňuje díky známému plaintextu získat část keystreamu. Šifrován je pomocí $ks3$, protože je zasílán místo odpovědi a_T.

6.4 Popis útoku

Implementoval jsem „card-only“ útok z [6], který vyžaduje, aby tag odpovídal na autentizační výzvu stejným n_T. Ačkoliv je perioda mezi obnovením napájení tagu a vysláním autentizační výzvy teoreticky konstantní a tedy bychom měli od tagu obdržet pokaždé stejné n_T, ve skutečnosti se její délka mění kvůli přerušení procesoru, obsluze USB řadiče apod. Konstantnost n_T tedy nelze při použití PC plně dodržet. Lepší situace je při použití specializovaného hardwaru (např. Proxmark[37] na bázi FPGA). Postup útoku je následující:

1. **Výběr „konstantního“ tag nonce**
   Provedeme 2000 pokusů o autentizaci vůči tagu. Před každým pokusem vypneme a zapneme elektromagnetické pole čtečky, abychom restartovali tag, a před vysláním požadavku na autorizaci vyčkáme po dobu konstantního zpoždění (tzv. „drop field + constant delay“ metoda). To by nám mělo zajistit co nejkonstantnější n_T. Jako zprávu n_R, a_R používáme náhodné hodnoty včetně náhodné parity. Pokud tag odpoví 4bitovou chybou NACK, do seznamu uložíme získané n_T (pokud ještě není v seznamu) nebo inkrementujeme čítač jeho výskytů. Kromě n_T uložíme i n_R, a_R a paritní bajt. Poté vybereme n_T s nejvyšší hodnotou čítače výskytů.

2. **Kombinace n_R**
   Poté ponecháme konstantních prvních 29 bitů odpovídající hodnoty $\{n_R\}$, celé $\{a_R\}$ a první 3 bity paritního bajtu. Opakujeme pokusy o autentizaci, a pokud je přijaté n_T shodné s naším vybraným, postupně zkoušíme pro každou z osmi kombinací $\{n_R\}$(3 proměnné bity) správnou kombinaci paritních bitů, při které tag odpoví 4bitovým NACK. Uložíme si všech 8 kombinací $\{n_R\}$ a k nim příslušející paritu, $\{a_R\}$ a jednotlivé zašifrované odpovědi NACK. Z těch získáme části keystreamu pomocí operace XOR s hodnotou 0x5.

3. **Redukce stavů LFSR**
   S pravděpodobností 0,75 jsme se mohli trefit do případu, kdy je keystream konstantní pro všech 8 odpovědí, lišících se posledními třemi bity n_R. V tom případě dokážeme odhadnout rozdíly mezi stavy LFSR pro těchto 8 případů. Díky znovupoužití 21 výstupních bitů LFSR po dvou krocích, které generují bity keystreamu $ks3_0$ a $ks3_2$, máme 2^{21} možných kombinací pro tyto bity. Pro každou z 8 odpovědí NACK ověříme shodnost těchto bitů pro každou kombinaci, čímž redukujeme počet kombinací na 21 bitech na 2^5. Analogicky provedeme pro dalších 21 bitů LFSR, které generují bity keystreamu $ks3_1$ a $ks3_3$. Získali jsme 2^{10} kombinací pro 42 bitů stavu LFSR. Doplněním všech kombinací pro zbývajících 6 bitů získáme 2^{16} kombinací obsahu LFSR.

4. **Zpětný běh LFSR**
   Nyní můžeme využít slabiny šifry, umožňující provést zpětný běh LFSR. Ten provedeme pro každou kombinaci, čímž získáme 2^{16} kandidátních klíčů. Provedením šifry a kontrolou shodnosti parity pro všech 8 kombinací n_R získáme tajný klíč.

6.5 Implementace útoku

Pro implementaci útoku jsem zvolil jazyk C pro jeho nízkou úroveň abstrakce, která jej činí vhodným pro práci s hardware. Pro komunikaci se čtečkou je použita knihovna *libnfc*. RFID čtečku *ACS ACR122U* jsem zvolil kvůli kompatibilitě s knihovnou a její cenové dostupnosti. Disponuje rozhraním USB a kromě tagů dle standardů ISO 14443-A/B podporuje také technologii NFC. Jako cíl útoku posloužila univerzitní identifikační karta. Původně měly být použity čisté karty kompatibilní s Mifare 1K (model Mango TK S50), ty ovšem nevrací odpověď NACK, tudíž jsou vůči tomuto útoku odolné. Kroky útoku 3 a 4 jsou realizovány knihovnou *Crapto1*, která implementuje „common prefix“ útok z [6], zejména následujícími funkcemi:

- `lfsr_common_prefix` - redukuje kombinace obsahu LFSR dle keystremu (krok 3)
- `lfsr_rollback_word` - provede zpětný běh LFSR od hodnoty $n_T \oplus UID$ (krok 4)

Aplikace se spouští z příkazové řádky s následujícími parametry:
`-s` s možnými hodnotami 1 (pro fázi sběru dat opakovanými pokusy o autentizaci) a 2 (pro fázi zjištění klíče z nasbíraných dat). Bez tohoto parametru jsou provedeny obě fáze
`-b` s povinnou hodnotou, kterou je číslo bloku, ke kterému se chceme autentizovat (platné pouze pro fázi 1)
`-k` s povinnou hodnotou A nebo B, označující klíč sektoru
`-a` s povinnou hodnotou pro počet pokusů o autentizaci ve fázi výběru „konstantního“ n_T (pokud není parametr použit, je výchozí hodnota 2000 pokusů)
`-f` s povinným názvem souboru, ze kterého mají byt přečtena data (lze použít pouze s fází 2)
`-v` zapíná podrobnější výpisy

Např. pro získání tajného klíče A pro přístup k bloku 4 (obě fáze): `attack -b4 -kA`

Na konci první fáze jsou získaná data uložena do binárního souboru s názvem ve formátu „UIDtagu_cisloSektoru_klicA/B_tagNonce.mfa“. Na konci druhé fáze je v případě úspěchu na standartní výstup vypsán získaný klíč, v opačném případě informace o neúspěchu.

Pro funkčnost aplikace na platformě Windows je požadováno následující:

- čtečka kompatibilní se standardem ISO 14443-A a s knihovnou libusb
- nainstalovaná knihovna libusb
- nainstalovaný ovladač čtečky

6.5.1 Časová náročnost útoku

Reálná časová složitost útoku je ovlivněna úspěšností udržet konstantní čas zpoždění mezi obnovením pole čtečky a vysláním autentizačního dotazu. Při praktických pokusech (se zpožděním 40 ms po vypnutí a 20 ms po zapnutí pole čtečky) byla časová náročnost následující:
Fáze výběru „konstantního“ n_T s počtem 2000 dotazů trvá 385 sekund, tedy cca 6,5 minuty. Fáze iterování možných hodnot 3 bitů $\{n_R\}$ a 5 bitů parity trvá průměrně 92 sekund

Obrázek 6.4: RFID/NFC čtečka ACS ACR122U (www.acs.com.hk) a univerzitní identifikační karta

(pokud pro každou z 8 hodnot parity předpokládáme odpověď NACK v 16. dotazu). Pokud uvažujeme ideální stav, kdy je odpovědí na každý dotaz totéž n_T, pak je doba trvání druhé fáze při výše uvedených zpožděních 23 sekund. Nejčastěji se vyskytující n_T se však reálně podařilo získat průměrně v 25% dotazů. Úspěšnost se snižuje se zvyšujícím se zatížením počítače jinými aplikacemi, které generují přerušení procesoru a tím snižují konstantnost vyslání příkazu do čtečky přes sběrnici USB. Je proto doporučeno spouštět pouze tuto aplikaci. Výpočet klíče ze získaných hodnot trvá méně než sekundu. Kompletní útok trvá v drtivé většině případů od 7,5 do 10,5 minuty, průměrně 8 minut. Z mých testů vyplývá, že útok je úspěšný (klíč je zjištěn) v 60% pokusů o útok, ve 13% případů se nepodaří klíč zjistit (vygenerovaný $ks1$ je závislý na posledních 3 bitech n_R) a ve 27% případů se nepodaří vybrat „konstantní“ $\{n_T\}$, protože tag neodpověděl alespoň dvěma NACK odpověďmi se stejným $\{n_T\}$.

V [35] se autorovi podařilo provést celý útok za necelých 5 minut. Důvodem bylo jen 1000 pokusů o autentizaci pro výběr „konstantního“ $\{n_T\}$. I přes prakticky stejnou úspěšnost udržení konstantního časování (30%) se mi nepodařilo při testech s tímto počtem pokusů docílit požadované spolehlivosti útoku z důvodu nízkého počtu získaných odpovědí NACK.

Kapitola 7

Technologie NFC

Technologie NFC (Near Field Communication) se v dnešní době rozšiřuje a přibývá aplikací, které jsou na ní založeny. Jedná se o rozšíření technologie RFID, má s ní tedy hodně společných vlastností. Oproti ní se však kromě pouhé identifikace zaměřuje i na obecný přenos dat. Je také pro běžného uživatele dostupnější a snazší pro použití, protože je implementována v některých mobilních telefonech. Uživatelé si tedy nemusí pořizovat další předmět, veškeré hardwarové vybavení již mají a stále nosí u sebe. V této kapitole bude stručně představena a budou popsána její specifika, i co se bezpečnosti týče.

7.1 Popis

NFC byla vyvinuta společnostmi Philips a Sony v roce 2002. Slouží pro bezdrátovou komunikaci zařízení na velmi krátkou vzdálenost. Je popsána ve standardech ISO 18092/ECMA-340(NFCIP-1) a ISO 21481/ECMA-352(NFCIP-2), které vychází ze standardů ISO 14443, ISO 15693 a JIS X 6319. Proto je kompatibilní s technologiemi Mifare a FeliCa, které jsou na těchto standardech postaveny. Komunikace je poloduplexní a mohou se jí účastnit pouze dvě zařízení v jeden okamžik. Fyzikálně je založená na indukční vazbě mezi zařízeními.[5] Komunikujícími prvky v NFC jsou:

- *NFC čtečka*
- *NFC tag* = pasivní RFID tag
- *Mobilní telefon s podporou NFC* schopný pracovat v módu čtečky nebo v módu emulace tagu

Komunikace pomocí NFC je v mobilních telefonech často používána pro inicializaci spojení jinou technologií, která umožňuje vyšší rychlost nebo větší vzdálenost přenosu (např. Bluetooth nebo WiFi).

7.2 Módy komunikace a aplikace

Zařízeními, která se účastní komunikace, je *initiator* iniciující spojení a řídící komunikaci (NFC čtečka nebo mobilní telefon vybavený NFC) a *target*, který odpovídá na požadavky (NFC tag nebo mobilní telefon). NFC definuje dva komunikační módy:

Operační frekvence	13,56 MHz
Rychlost přenosu dat	106/212/424 kbit/s
Dosah	až 20 cm (se standardními anténami)
Topologie	Point-to-Point
Doba ustavení spojení	do 0,1 s

Tabulka 7.1: Některé parametry technologie NFC
[1]

- *Aktivní* - obě zařízení generují RF pole, jehož prostřednictvím přenáší data. To je případ komunikace čtečky a mobilního telefonu nebo dvou mobilních telefonů.
- *Pasivní* - RF pole generuje pouze initiator a target zařízení jej využívá pro komunikaci. To je případ spojení čtečky a tagu nebo mobilního telefonu a tagu.

Podle toho, s jakým zařízením komunikuje NFC mobilní telefon, jsou rozlišovány tři operační módy. Každý z nich přitom používá jiné standardy a komunikační protokoly a jsou na něm založeny rozdílné aplikace.

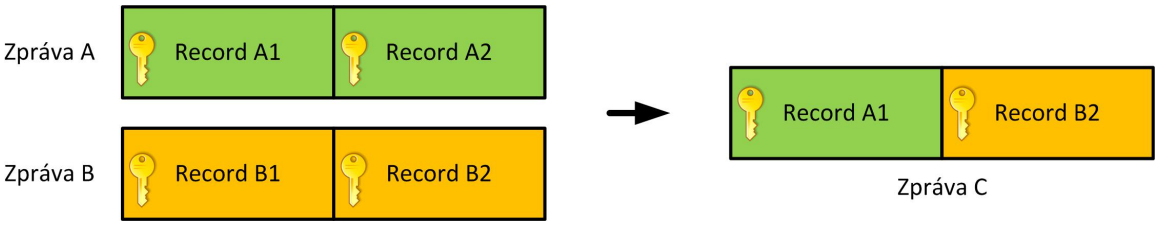
- *Reader/Writer mód* - mobilní telefon iniciuje spojení s pasivním NFC tagem, ze kterého může číst nebo na něj zapisovat data. Chová se tedy jako NFC čtečka. Výhodou je snadnost použití pro uživatele. Tento mód se používá například pro tzv. „chytré plakáty“[2].
- *Peer-to-Peer mód* - dva mobilní telefony spolu komunikují za účelem přenosu obecných dat, typicky fotografií, videí, digitálních vizitek apod. Na spojové vrstvě používá protokol LLCP, umožňující spojově i bezspojově orientovaný přenos dat.
- *Mód emulace tagu* - v tomto módu se pro NFC čtečku chová mobilní telefon jako tag. NFC obvod v mobilním telefonu slouží pouze pro poskytnutí komunikačního rozhraní, samotná emulace tagu se odehrává v tzv. Secure Elementu - viz 7.4.2. Nahradí tedy různé platební, věrnostní a přístupové karty nebo elektronické vstupenky a jízdenky.

Dalšími aplikacemi založenými na technologii NFC mohou být medicínské aplikace (např. identifikace pacienta a uložení informací o předepsaných lécích a alergiích do náramku s NFC tagem nebo stažení informací z kardiostimulátoru), zábavní aplikace (různé hry založené na hledání a načítání NFC tagů), aplikace sociálních sítí (např. načtením tagu na zakoupeném CD mobilní telefon publikuje zprávu na sociální síti), výukové aplikace (např. zobrazení internetové stránky s fakty na displeji mobilního telefonu po načtení tagu na historicky významném místě), navigační aplikace (např. zjištění polohy nejbližšího bankomatu z tagu na veřejném místě) a mnoho dalších. Některé aplikace spadají do kategorie tzv. „internetu věcí“ (Internet of Things), kde má fyzický objekt svůj virtuální obraz na internetu.

[2] Chytrý plakát (Smart Poster) je plakát doplněný o NFC tag. Je využíván např. k reklamním účelům i poskytování různých služeb založených na NFC.

7.3 Přenos dat - formát NDEF

Pro přenos dat lze kromě formátů používaných standardy ISO 14443, ISO 15693 a JIS X 6319 používat binární formát NDEF, vytvořený asociací NFC Forum[3]. Ten pro přenos dat používá NDEF zprávy (NDEF message), které se skládají z jednoho či více záznamů (NDEF record). Každý záznam obsahuje kromě samotných dat (2^{32} B, tedy cca 4 GB) také hlavičku s jejich velikostí, identifikátorem jejich typu (některý z MIME typů, URI, elektronický podpis aj.), příznaky fragmentace zprávy do více záznamů, začátku a konce zprávy atd. Na bezpečnost použití elektronického podpisu NDEF zpráv pro zajištění jejich autenticity a integrity se zaměřili autoři v [34]. Ti upozorňují na možné bezpečnostní problémy, které vyplývají z toho, že formát NDEF umožňuje podepisovat každý záznam zvlášť pomocí typu „Signature Record Type“ a navíc každý záznam zprávy může být podepsán jiným podpisem. To umožňuje útočníkovi z několika záznamů (např. textu, který se zobrazí uživateli a URL, která bude otevřena v prohlížeči) podepsaných subjektem nebo subjekty, kterým oběť útoku důvěřuje, a které pochází z různých zpráv, složit jednu zprávu. Ta bude složená z důvěryhodných záznamů, ale bude mít zcela jiný význam. Podobně lze skládat podepsané a nepodepsané záznamy.



Obrázek 7.1: Složení podvržené NDEF zprávy C ze dvou NDEF záznamů, pocházejících ze dvou odlišných legitimních zpráv A a B

Takový útok může být zneužit např. při použití služby pro bezhotovostní platbu za zboží z automatu. Existují služby, kdy je na automatu připevněn NFC tag, jehož přečtením se odešle z uživatelova mobilního telefonu SMS s identifikátorem automatu. Po přijetí SMS zprávy systém vydá uživateli předem vybrané zboží. Pokud však útočník tag vymění nebo změní jeho obsah, aby zobrazoval na displeji identifikátor dotyčného automatu, ale odeslal SMS s identifikátorem jiného automatu, je odblokován jiný automat. U toho čeká útočník a získává zboží za peníze oběti. Útočník (např. konkurenční provozovatel služeb) také může složit podvodnou zprávu ze dvou logicky nesouvisejících zpráv, jejich spojení nedává smysl - např. jedné pro zobrazení textu „Zakoupení jízdenky z místa A do místa B“ na displeji a druhé s URL vedoucí na zpravodajský portál. Pokud budou obě tyto zprávy podepsány, uživatel bude přesvědčen, že obsah pochází od vlastníka podpisu a nebude mu již nadále věřit a využívat jeho služby. Pro zabránění takovému typu útoku je nutné důvěřovat pouze takovým NDEF zprávám, které jsou podepsány jako celek a je zajištěna jejich integrita. Obecně je také nutné zajistit bezpečné doručení řetězce certifikátů do zařízení před ověřením podpisu zprávy. Pokud totiž zařízení ani samotná zpráva daný certifikát neobsahuje, může jej získat z části zprávy, která obsahuje URL certifikátu. Tím se ale otevírá další možnost pro podstrčení škodlivého obsahu.

[3]NFC Forum je asociace více jak 170 společností z řad výrobců, vývojářů, finančních a ostatních institucí, která se od roku 2004 zabývá standardizací a rozšiřováním technologie NFC. Více na www.nfc-forum.org

7.4 Bezpečnost

Díky tomu, že je technologie NFC postavena na standardech RFID pro identifikační karty, jsou jejich bezpečnostní rizika velmi podobná. Cílem útoku může být jak celý systém, tak pouze kterákoliv jeho komponenta (tag, čtečka, mobilní telefon nebo backend). NFC je však zacílena na užití širokou veřejností, proto je více provázána s technologiemi, které jsou rozšířené a laickým uživatelům známé (telefonní hovory, SMS, hlavně však internetové a mobilní aplikace). To sebou přináší větší potenciál pro nové útoky, které buď v „holém" RFID neexistují nebo jsou použitelné v mizivém procentu RFID systémů, tudíž na ně útočníci necílí. Právě rozšířenost těchto technologií a to, že je útočníci znají a používají pro jiné útoky, jim otevírá nové možnosti.

Mobilní telefon v Reader/Writer módu po přiblížení k NFC tagu z něj přečte data, obsahující akci, kterou má vykonat a obsah (doplňující data). Akcí může být:

- spuštení aplikace
- odeslání/uložení/editace SMS
- vytočení/uložení/zobrazení telefonního čísla
- uložení jiných dat (např. hypertextového odkazu)
- připojení k WiFi síti nebo jinému zařízení skrze Bluetooth

Doplňujícími daty jsou podle konkrétní akce tedy:

- data předávaná aplikaci (např. poloha)
- text SMS a telefonní číslo příjemce
- telefonní číslo
- adresa URL
- heslo pro navázání WiFi/Bluetooth spojení

Z uvedeného vidíme, že možnosti zneužití aplikací založených na NFC jsou široké. To je způsobeno především možnostmi komunikace mobilního telefonu více kanály, z nichž některé jsou placené. Útoky, které tyto kanály používají, mohou tedy způsobit uživateli přímou finanční škodu (a útočníkovi zisk). Takový útok může mít podobu výměny nebo editace obsahu stávajícího tagu. Ten poté zasílá mobilnímu telefonu oběti podvržená telefonní čísla pro hovory nebo SMS zpoplatněné vyšším tarifem (prémiová čísla), URL s webovou stránkou, která je kopií legitimní stránky a slouží k získání údajů od uživatele (phishing) či vede na škodlivý kód, útočící na operační systém či aplikace v mobilním telefonu. Také může obsahovat pozměněná data o finanční transakci s číslem bankovního účtu útočníka apod.

Díky tomu, že některé NFC tagy jsou umístěné na veřejných prostranstvích, jsou pro útočníka snadno dostupné, což mu velmi zjednodušuje útok. Pro ochranu před změnou obsahu tagu je potřeba zabezpečit jeho autenticitu a integritu. To je možné zajistit prostřednictvím digitálního podpisu dat uložených v tagu. To ovšem nezabrání kopírování nebo výměně jednotlivých tagů. Útok typu DoS (Denial of Service) je možný fyzickou destrukcí tagu nebo použitím silného RF pole. Fyzické destrukci lze zabránit použitím odolného krytu, ovšem např. v případě chytrých plakátů, které mají být levné, je to kontraproduktivní.

7.4.1 NFC-SEC

NFC-SEC (ECMA 385 - NFCIP-1 Security Services and Protocol) a NFC-SEC-01 (ECMA 386) jsou standardy definující zabezpečení spojové vrstvy nad NFCIP-1 při použití Peer-to-Peer spojení mezi dvěma NFC zařízeními. Není tak nutné používat jiné metody zabezpečení přenosu na aplikační úrovni. Definuje dvě služby:

- *Shared Secret Service (SSE)* - poskytuje sdílené tajemství (klíč) pro použití zabezpečení dat na aplikační úrovni.
- *Secure Channel Service (SCH)* - poskytuje zabezpečený kanál pro přenos dat.

Pro ustavení sdíleného klíče slouží protokol Diffie-Hellman s použitím 192b eliptických křivek. Šifrování dat a jejich integritu zajišťuje algoritmus AES v módu CTR a délkou klíče 128b. Tento mechanismus neposkytuje obranu proti Man-in-the-middle útoku, protože neexistuje možnost autentizace komunikujících prvků.

7.4.2 Secure Element (SE)

Pokud je mobilní telefon v módu emulace tagu, je potřeba mít aplikace a data emulovaného tagu spouštěná a uložená v bezpečném prostředí, do něhož nebudou mít přístup jiné aplikace mobilního telefonu. K tomuto účelu slouží kombinace hardwaru a softwaru označovaná jako Secure Element. Ten může mít různou podobu. Nejčastější je integrovaný SE čip v mobilním telefonu. Dalšími možnostmi je vyjímatelná paměťová karta (Secure Memory Card), jejíž výhodou je velký paměťový prostor umožňující použití velkého množství aplikací nebo SE jako součást SIM karty. Aplikace v tomto typu SE může spravovat operátor mobilní sítě přes technologii Over-the-Air (OTA), díky které má nad obsahem SE absolutní kontrolu. Velké naděje jsou vkládány do Trusted Mobile Base (TMB), což je izolovaná výpočetní oblast procesoru mobilního telefonu. Toto řešení je z hlediska bezpečnosti velmi perspektivní z důvodu velmi výkonných procesorů v dnešních mobilních telefonech. Ty umožní použití bezpečnějších (a výkonově náročnějších) algoritmů. Všechna tato provedení SE jsou z hlediska bezpečnosti na úrovni smart karet.

Kapitola 8

Elektronické pasy

Jednou z aplikací technologie RFID, kterou používá obrovské procento populace, jsou elektronické pasy. Ty jsou také nazývány biometrickými pasy, neboť jsou na nich mimo jiných dat uložena i biometrická data. Elektronický pas vypadá na první pohled stejně jako klasický pas formátu knížky, je ale navíc vybaven RFID čipem a strojově čitelnou zónou (MRZ - Machine Readable Zone). Ta je složena z 88 znaků informací, které jsou vytištěny OCR (Optical Character Recognition) fontem. Zařízení pro čtení pasů kombinuje RFID čtečku a optický snímač pro nasnímání MRZ. Specifikaci elektronického pasu popisuje dokument ICAO[1] 9303[16]. Dle tohoto dokumentu musí RFID čip komunikovat dle standardu ISO 14443A/B a jeho operační systém musí splňovat standard ISO 7816-4. Na čipu musí být povinně uložena kopie dat, která jsou v MRZ (vydávající stát, jméno držitele, číslo pasu, národnost, datum narození, pohlaví, datum platnosti aj.), standardizovaná fotografie obličeje a data pro ověření integrity obsahu čipu (elektronický podpis). Volitelně obsahuje další data jako je adresa, místo narození, telefon, povolání, datum vydání, informace o dalších osobách atd. a také biometrická data o otisku prstu a duhovce.

8.1 Bezpečnostní mechanismy

Jedinou povinnou bezpečnostní metodou je tzv. *pasivní autentizace*. Ta má podobu vydávající autoritou digitálně podepsaného hashe datového obsahu čipu, čímž je zajištěna pouze integrita a autenticita dat uložených na čipu. Další metody jsou dle ICAO 9303 volitelné. *Aktivní autentizace* zajišťuje autenticitu čipu, tedy to, že nebyl naklonován. V čipu je uložen čitelný a vydávající autoritou podepsaný veřejný klíč a z vnějšku nečitelný soukromý klíč. Tento pár je unikátní pro každý čip. Při vzájemné autentizaci čtečky a čipu je ověřeno, zda čip obsahuje odpovídající pár klíčů. Ochranu před eavesdropping a skimming útoky zajišťuje řízení přístupu. *Základní řízení přístupu (Basic Access Control)* využívá data přečtená z MRZ k vygenerování dvou 3DES klíčů: klíče pro autentizaci a zajištění integrity zprávy (MAC) a klíče pro šifrování přenášených dat. Pro přečtení dat je tedy potřeba otevřít pas. *Rozšířené řízení přístupu (Extended Access Control)* pomocí mezinárodní PKI ověřuje, zda je čtečka autorizována ke čtení dat, obzvláště těch biometrických.

Pro hashovací funkci může být dle ICAO 9303 použita některá z variant algoritmu SHA (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512). Pro asymetrickou kryptografii se používají algoritmy RSA, DSA a ECDSA. Dokument obsahuje i doporučené hodnoty velikosti modulů a základních bodů.

[1] International Civil Aviation Organization - http://www.icao.int/

8.2 Hrozby

8.2.1 Únik dat

Použití základního řízení přístupu je z hlediska zajištění důvěrnosti dat nedostatečné. Data v MRZ, která jsou použita pro vygenerování klíče, totiž mohou nabývat pouze omezených hodnot (např. den a měsíc narození), některá lze částečně odhadnout, např. rok narození ale i číslo pasu. To je vlastně sériové číslo, které je navíc vydáváno dle číslovacího plánu. Nevýhodou je tedy nízká míra entropie těchto dat (cca 52 bitů), díky které je tato metoda náchylná vůči brute-force útoku. Z tohoto důvodu je vhodné použití rozšířeného řízení přístupu, případně přechovávání pasu v kovovém obalu pro obranu proti neoprávněnému čtení.

Samozřejmě je nutné udržet v tajnosti soukromé klíče ať již samotných autorit vydávajících pasy, tak i soukromé klíče, které jsou ukládány na čipy a využívány při aktivní autentizaci. Pokud je použito základní řízení přístupu, klíče vygenerované během čtení MRZ by neměly být nikde trvale ukládány, aby se předešlo jejich zneužití při možné kompromitaci systému. Je také potřeba zajistit revokaci pasů pro případ ztráty či úniku citlivých dat. Stejně tak je potřeba zabránit zneužití čtecího zařízení v případě jeho odcizení, např. vydáváním časově omezených certifikátů.

8.2.2 Sledování pasu

Čipy v biometrických pasech komunikují dle standardu ISO 14443. Ten definuje i antikolizní proceduru, využívající UID čipu. To je možno odposlechnout či přečíst bez jakékoliv autentizace a na jeho základě sledovat pohyb určité osoby. Řešením je použití náhodného UID při každé aktivaci čipu. Je však potřeba zajistit, aby se vygenerované UID příliš často neopakovalo.[18]

Závěr

Práce vysvětluje princip funkce technologie RFID, její vlastnosti, výhody, nevýhody a možnosti použití. Popisuje útoky, které mohou být vedené na RFID systémy a opatření, která vedou k minimalizaci rizik či úplnému zamezení provedení útoků. Shrnuje její současné bezpečnostní možnosti v běžně používaných řešeních.

Čtenář byl také seznámen s možnostmi odposlechu komunikace mezi čtečkou a tagem a s komunikací s tagem na větší vzdálenosti. Prakticky dosažitelné vzdálenosti, na které lze takovéto útoky provést, jsou mnohem větší než deklarované operační vzdálenosti, na které jsou schopny komunikovat standardně vyráběné prvky RFID systémů. Útočník s přístupem k technice špičkových parametrů a při použití účinného postprocessingu signálu je schopen odposlechnout komunikaci dle standardu ISO 14443 na vzdálenost cca 15 m a přečíst obsah tagu na cca 2 m. Při použití aktivního odposlechu lze vzdálenosti teoreticky ještě zdvojnásobit. Reálná vzdálenost se liší případ od případu dle parametrů prvků RFID systému, okolních podmínek a vybavení útočníka. V porovnání se standardní operační vzdáleností 10 cm jsou tyto hodnoty více než varovné. Při návrhu RFID systémů by tento možný problém neměl být brán na lehkou váhu.

V rámci práce byl implementován útok na bezpečnost RFID karet Mifare Classic. Jeho cílem je získání autentizačního klíče pro přístup k datům, která jsou uložena v paměti karty. Celý útok trvá průměrně 8 minut a vyžaduje umístění karty oběti v dosahu standardní RFID čtečky útočníka, tedy cca do 10 cm. Tento útok však může být zkombinován s popsaným skimming útokem a je tedy možné ho realizovat i na vzdálenost okolo 2 m. Takový útok může tedy být proveden, aniž by o tom oběť měla tušení. Jistě totiž není pro útočníka velký problém zdržovat se po dobu 8 minut v této vzdálenosti od oběti (přesněji její karty, pokud ji má např. v zavazadle).

Řešením je použití takové technologie karet, která používá nejen dostatečně bezpečné algoritmy pro autentizaci a šifrování dat, ale kde jsou tyto algoritmy a komunikační protokoly také správně implementovány (tedy bez jakýchkoliv slabých míst).

Náchylné k útoku jsou také systémy (např. přístupové), které pro identifikaci tagu používají pouze jeho UID. To může být útočníkem pomocí eavesdropping či skimming útoku přečteno a vytvořen klon tagu, neboť stačí, aby na výzvu čtečky pouze odpověděl správným UID. Obranou je čtení identifikátoru z paměti tagu, která je dostupná až po oboustranné autentizaci. Samozřejmě musí být použit mechanismus autentizace, při kterém nejsou přenášena tajemství v otevřené podobě, tedy např. HMAC nebo asymetrická kryptografie. Pokud není změna technologie karet možná, je vhodné, aby byly karty chráněny alespoň před možností skimmingu. To lze provést např. pomocí hliníkových obalů na karty, které zabrání průniku signálu ke kartě v čase, kdy není používána.

Biometrické pasy na bázi RFID jsou v případě použití doporučených bezpečnostních mechanismů a důkladného zabezpečení systémů pro jejich vydávání a čtení a za předpokladu, že nebude kompromitována vydávající PKI autorita v současné době dostatečně bezpečné.

Při použití technologie RFID je tedy nutné komplexně zvážit všechny bezpečnostní aspekty a možné hrozby, kterých v reálném systému rozhodně není málo. To je bohužel daň za snadnost a rychlost použití, které tato technologie přináší.

Literatura

[1] ISO/IEC 14443 Identification cards - Contactless integrated circuit cards - Proximity cards.

[2] ISO/IEC 15693 : Vicinity cards.

[3] HID Global. http://www.hidglobal.com, 2012 [cit. 2012-01-09].

[4] Chai, Q.; Gong, G.; Engels, D. W.: How to develop clairaudience - active eavesdropping in passive RFID systems. In *WOWMOM'12*, IEEE Computer Society, 2012, s. 1–6.

[5] Coskun, V.; Ozdenizci, B.; Ok, K.: A Survey on Near Field Communication (NFC) Technology. *Wireless Personal Communications*, 2012: s. 1–36, ISSN 0929-6212.

[6] Courtois, N. T.: The dark side of security by obscurity and cloning MiFare classic rail and building passes anywhere, anytime. http://eprint.iacr.org/2009/137.pdf, 2009 [cit. 2013-04-27].

[7] Devadas, S.; Suh, E.; Paral, S.; aj.: Design and Implementation of PUF-Based 'Unclonable' RFID ICs for Anti-Counterfeiting and Security Applications. In *2008 IEEE International Conference on RFID*, 2008, ISBN 978-1-4244-1711-7.

[8] Finkenzeller, K.: *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*. Wiley, 2003, ISBN 0-470-84402-7.

[9] Garcia, F. D.; de Koning Gans, G.; Muijers, R.: Dismantling Mifare Classic. In *13th European Symposium on Research in Computer Security*, 2008 [cit. 2013-04-27], s. 97–114.

[10] Garcia, F. D.; Rossum, P. v.; Verdult, R.; aj.: Wirelessly Pickpocketing a Mifare Classic Card. In *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, 2009, ISBN 978-0-7695-3633-0, s. 3–15.

[11] Glover, B.; Bhatt, H.: *RFID Essentials*. O'Reilly, 2006, ISBN 978-0-59-600944-1.

[12] Grunwald, L.: RF-DUMP. http://www.rfdump.org, 2008-01-27 [cit. 2012-01-07].

[13] Hancke, G. P.: Practical eavesdropping and skimming attacks on high-frequency RFID tokens. *J. Comput. Secur.*, 2011: s. 259–288, ISSN 0926-227X.

[14] Hancke, G. P.; Centre, S. C.: Eavesdropping Attacks on High-Frequency RFID Tokens. 2008.

[15] Henrici, D.: *RFID Security and Privacy: Concepts, Protocols, and Architectures*. Springer, 2008, ISBN 978-3-540-79075-4.

[16] International Civil Aviation Organization: Machine Readable Travel Documents. http://www.icao.int/publications/pages/publication.aspx?docnum=9303, 2005-2008 [cit. 2013-04-27].

[17] International Telecommunication Union: Report ITU-R SM.2180 - Impact of industrial, scientific and medical (ISM) equipment on radiocommunication services. 2010 [cit. 2013-04-27].

[18] Juels, A.; Molnar, D.; Wagner, D.: Security and Privacy Issues in E-passports. In *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, 2005, s. 74–88.

[19] Karygiannis, T.; Eydt, B.; Barber, G.; aj.: *Guidelines for Securing Radio Frequency Identification (RFID) Systems*. National Institute of Standards and Technology, 2007.

[20] Magistrát hl. m. Prahy: OpenCard. http://opencard.praha.eu, 2010 [cit. 2012-01-09].

[21] Mirowski, L.; Hartnett, J.: Deckard: A System to Detect Change of RFID Ownership. *International Journal of Computer Science and Network Security*, ročník 7, July 2007: s. 89–99, ISSN 1738-7906.

[22] Mitrokotsa, A.; R.Rieback, M.; Tanenbaum, A. S.: Classifying RFID attacks and defenses. *Information Systems Frontiers*, ročník 12, November 2010: s. 491–505, ISSN 1387-3326.

[23] Nohl, K.; Evans, D.; Starbug, S.; aj.: Reverse-engineering a cryptographic RFID tag. In *SS'08 Proceedings of the 17th conference on Security symposium*, 2008.

[24] Novotny, D.; Guerrieri, J.: HF RFID Eavesdropping and Jamming Tests. In *Report Number 818-7-71*, Electromagnetics Division, Electronics and Electrical Engineering Laboratory, National Institute of Standards and Technology, 2006.

[25] Novotny, D.; Guerrieri, J.; Francis, M.; aj.: HF RFID electromagnetic emissions and performance. In *Electromagnetic Compatibility, 2008. EMC 2008. IEEE International Symposium on*, 2008, s. 1 –7.

[26] NXP Semiconductors: MIFARE Classic 4K datasheet. http://www.nxp.com/documents/data_sheet/MF1S703x.pdf, 2010 [cit. 2013-04-26].

[27] NXP Semiconductors: MIFARE and handling of UIDs. http://www.nxp.com/documents/application_note/AN10927.pdf, 2011 [cit. 2013-01-14].

[28] NXP Semiconductors: MIFARE Classic 1K datasheet. http://www.nxp.com/documents/data_sheet/MF1S50YYX.pdf, 2011 [cit. 2013-04-26].

[29] NXP Seminductors: MIFARE. http://www.mifare.net, 2012 [cit. 2012-01-09].

[30] OpenPCD.org: HID iCLASS security demystified. http://www.openpcd.org/HID_iClass_demystified, 2011 [cit. 2012-01-09].

[31] Paret, D.: *RFID and Contactless Smart Card Applications*. Wiley, 2005, ISBN 0-470-01195-5.

[32] Pfeiffer, F.; Finkenzeller, K.; Biebl, E.: Theoretical Limits of ISO/IEC 14443 type A RFID Eavesdropping Attacks. In *Smart Objects, Systems and Technologies (SmartSysTech), Proceedings of 2012 European Conference on*, 2012, s. 1–9.

[33] Rankl, W.; Effing, W.: *Smart Card Handbook*. Wiley, 2003, ISBN 0-470-85668-8.

[34] Roland, M.; Langer, J.; Scharinger, J.: Security Vulnerabilities of the NDEF Signature Record Type. In *Near Field Communication (NFC), 2011 3rd International Workshop on*, 2011, s. 65–70.

[35] Tan, W. H.: Practical Attacks on the MIFARE Classic. http://www.doc.ic.ac.uk/~mgv98/MIFARE_files/report.pdf, 2009 [cit. 2013-04-27].

[36] Thornton, F.; Haines, B.; M.Das, A.; aj.: *RFID Security*. Syngress Publishing, 2006, ISBN 1-59749-047-4.

[37] Verdult, R.; de Koning Gans, G.: PROXMARK webpage. http://www.proxmark.org/, 2011 [cit. 2013-04-27].

[38] Vojáček, A.: Více i méně běžné RFID frekvence a jejich vliv na komunikaci. http://automatizace.hw.cz/vice-i-mene-bezne-rfid-frekvence-jejich-vliv-na-komunikaci, 2008-01-27 [cit. 2012-01-01].

[39] Zhen-hua Ding; Jin-tao Li; Bo Feng: A Taxonomy Model of RFID Security Threats. In *11th IEEE International Conference on Communication Technology Proceedings*, 2008, ISBN 978-1-4244-2251-7.

Příloha A

Obsah CD

Na přiloženém CD jsou umístěny zdrojové soubory aplikace a potřebných knihoven spolu s textem této práce ve formátu PDF.