VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

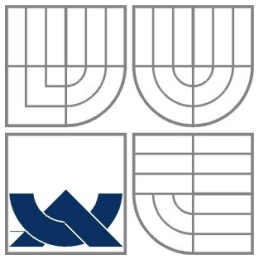
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

BEZPEČNOST RFID

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE — RADIM HANAČÍK
AUTHOR

BRNO 2011



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

Fakulta elektrotechniky a komunikačních technologií
Ústav telekomunikací
Faculty of Electrical Engineering and Communication
Department of Telecommunications

BEZPEČNOST RFID

RFID SECURITY

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE — RADIM HANAČÍK
AUTHOR

VEDOUCÍ PRÁCE — Ing. ZDENĚK MARTINÁSEK
SUPERVISOR

BRNO 2011

ANOTACE

Tahle práce se zabývá popisem teorie rádio frekvenční identifikace, zejména zabezpečením komunikace. Seznamuje s rozdělením komunikačních zařízení jednak podle čipů karet a jednak podle frekvencí, na kterých zařízení komunikují. Práce je zaměřena na bezkontaktní karty, postavené na čipu MiFare classic. Je zde popis návrhu a realizace emulátoru, který slouží pro demonstraci výrobních nedostatků zmíněných karet a možnost vytvoření její kopií. Zjistilo se, že karty s Mifare Classic disponují velkými nedostatky již z výroby a je snadné vytvořit si jejich duplikát.

Klíčová slova: RFID, emulátor, bezpečnost, transpondér, čárový kód

ABSTRACT

The thesis describes the theory of radio frequency identification and is focused on the security of communication. Smart cards are divided by type of chip and operating frequencies. The thesis is focused on contactless cards based on the Mifare Classic and on a description and construction of the emulator, which is able to demonstrate the production defects. We can make a copy of the card using the emulator. Laboratory task was designed and implemented demonstrating the communication between cards.

Keywords: RFID, emulator, security, transponder, barcode

Bibliografická citace práce:

HANAČÍK, R. Bezpečnost RFID. Bakalářská práce. Brno: Ústav telekomunikací FEKT VUT v Brně, 2011, 36 stran.

Prohlašuji, že svoji semestrální práci na téma Bezpečnost RFID jsem vypracoval samostatně pod vedením vedoucího semestrální práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené semestrální práce dále prohlašuji, že v souvislosti s vytvořením této práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

……

OBSAH

SEZNAM OBRÁZKŮ 7
SEZNAM SYMBOLŮ A ZKRATEK 8
ÚVOD 9
1 RFID 10
1.1 TAGY 10
1.2 IDENTIFIKACE RFID TAGŮ 11
1.3 DOSAH SIGNÁLU A POUŽITÉ FREKVENCE 11
1.4 ROZDĚLENÍ TAGŮ DLE TŘÍD 12
1.5 ČÁROVÉ KÓDY A RFID 12
1.6 SNÍMAČE 13
1.7 VYUŽITÍ 14
1.8 BEZPEČNOST RFID 16
2 ČIPOVÉ KARTY 18
2.1 HISTORIE VZNIKU 18
2.2 KARTY MIFARE 22
2.3 ÚTOKY NA RFID TECHNOLOGII 23
3 KONSTRUKCE EMULÁTORU 27
3.1 POPIS ZAŘÍZENÍ 27
3.2 OŽIVENÍ 29
4 NÁVRH LABORATORNÍ ÚLOHY 31
ZÁVĚR 36
5 POUŽITÁ LITERATURA 37

SEZNAM OBRÁZKŮ

obr.: 1-1 Ukázka pasivního čipu 11
obr.: 1-2 Čárový kód 13
obr.: 2-1 SIM karta 18
obr.: 2-2 Kontaktní karta, platební karta 20
obr.: 2-3 Bezkontaktní smart karta 21
tab.: 2.2-1 Typ přístupu v závislosti na indexu konfigurace....23
obr.: 3-1 Schéma obvodu navržené v programu Eagle 27
obr.: 3-2 Obrázek neosazeného (nahoře) a osazeného (dole) emulátoru na desce plošného spoje....28

SEZNAM SYMBOLŮ A ZKRATEK

C…. kapacita kondenzátoru, jednotkou je F (Farad) (1.1)

$f_{RES...}$ rezonanční frekvence, jednotkou je Hz (Herz) (1.1)

L…. indukčnost cívky, jednotkou je H (Henry) (1.1)

R…. odpor, jeho velikost se značí v Ω (ohm) (1.2)

Π…. Ludolfovo číslo, přibližná hodnota je 3,14159 (1.2)

ÚVOD

Dlouhou řadu let je sváděn boj mezi výrobci, kteří vymýšlí nové zabezpečovací řešení, a útočníky, jež se snaží prolamovat ochrany různých zařízení. Je to nekonečný koloběh neustálých soubojů, ve kterých se obě strany neustále střetávají a získávají nové znalosti a zkušenosti. Jelikož neexistuje absolutní bezpečnost, mohou útočníci tuto bezpečnost narušit, pokud mají dostatek času a finančních prostředků.

Čipové karty spadají do skupiny nejmladších a nejchytřejších identifikačních karet. Jsou velice flexibilní. Ve svém tradičním těle, které je vyrobeno z PVC nebo ABS, mají vložený čip obsahující mikroprocesor, na který se ukládají všechna potřebná data. Čipová karta je jedním z nejbezpečnějších médií, kam lze v současnosti uložit data. Mikroprocesor bývá umístěn pouze v jediném čipu, čím se zajistí vyšší odolnost čipových karet proti možným útokům.

Čipové karty nás dnes a denně obklopují na každém kroku a mají velmi různé využití. Svojí velkou univerzálností nacházejí uplatnění v mnoha různých oblastech, jako jsou platební a identifikační systémy, dále také zdravotnictví, předplacené karty pro parkování a dopravu, řízení přístupů do budov a systémů, placených televizí či mobilních telefonů nebo telefonních karet. Zde všude jsou převážně využívány čipové karty, které se šíří celým světem s vysokým nasazením.

Cílem práce je bližší seznámení s technologií RFID,čipovými kartami, jejich bezpečností a realizace laboratorní úlohy, která demonstruje použití emulátoru. Teoretická část popisuje teorii rádio frekvenční identifikace, rozdělení čipových karet a známé metody útoků. Praktická část měření se věnuje návrhu a konstrukci emulátoru.

1 RFID

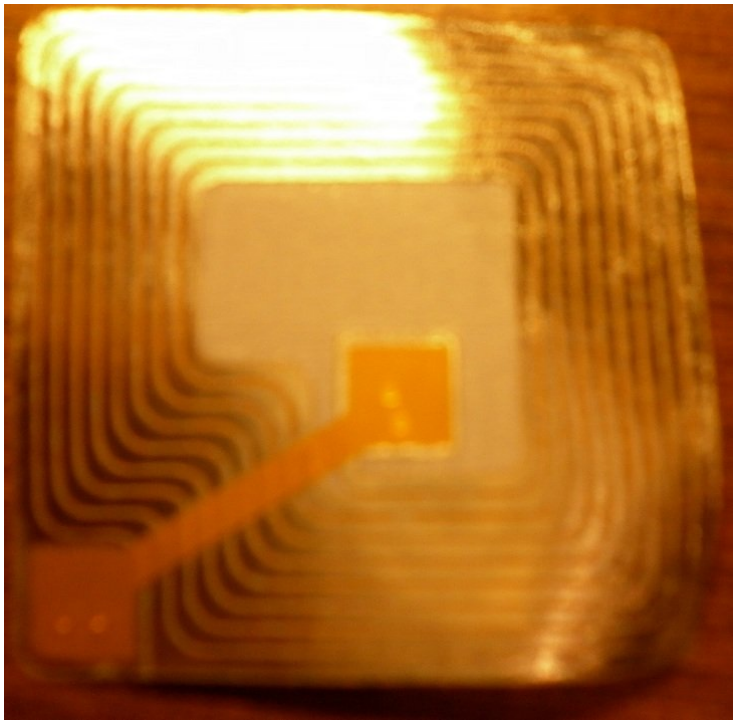
RFID (Radio Frequency Identification) - radiofrekvenční systém identifikace je moderní technologie identifikace objektů pomocí radiofrekvenčních vln. Tento systém lze úspěšně nasadit v mnoha odvětvích a oblastech, kde je kladen důraz na co nejrychlejší a přesné zpracování informací a okamžitý přenos těchto načtených dat k následnému zpracování. To následně vede ke zvýšení přesnosti, rychlosti a efektivnosti obchodních, skladových, logistických a výrobních procesů. Informace jsou v elektronické podobě ukládány do malých čipů-tagů, ze kterých je lze následně načítat a opakovaně přepisovat pomocí rádiových vln, toto zpracování se však neděje po jednotlivých čteních jako u v současnosti používaných čárových kódů, ale hromadně. Současná čtecí zařízení dokážou najednou načíst až několik set tagů za minutu. Technologie RFID je v současné době považována za přímého nástupce čárových kódů, z hlediska budoucího vývoje se však nepředpokládá úplné nahrazení čárových kódů, budou oblasti trhu kde budou dominovat RFID technologie, případně kombinace RFID značení s čárovým kódem. Již dnes se využívají tiskárny, které dokáží potisknout RFID tag informacemi s čárovým kódem. Takové tiskárny při potisku zároveň zapisují informace do tagu a dokonce pokud je RFID tag poškozen, toto zjistí a tag označí. S myšlenkou na vznik bezdrátové technologie zpracování informací přišla před lety největší maloobchodní firma WalMart, která před několika desetiletími stála u zrodu čárového kódu. Základem byla myšlenka vyvinout takovou technologii, která dokáže objekt identifikovat na větší vzdálenost, bez přímé viditelnosti tak, aby v reálném čase bylo možno zpracovat více objektů současně. V současné době se technologie RFID velice rozvíjí a dochází k nasazení v mnoha dalších oblastech trhu, největší uplatnění nachází v logistice, výrobě, sledování objektů - logistických jednotek (zboží, palet, kontejnerů), sledování majetku, sledování zavazadel na letištích a evidence osob. Podobně jako u čárových kódů se informace zaznamenávají na nosič dat - tzv. RFID tag , který je připevněn na sledované objekty, tag obsahuje malý čip s anténou a pamětí. RFID tagy jsou základem systému pro ukládání a přenos informací pomocí elektromagnetických vln. Může je hromadně přečíst a zaznamenat příslušné čtecí zařízení, které může být pevné nebo mobilní. Pomocí vln vyzářených z čtecího zařízení dojde k nabití chipu a následně se informace uložená v chipu bezdrátově přenese zpět do čtecího zařízení (každý tag obsahuje tzv. EPC kód - electronic product code, jedná se o jednoznačné sériové číslo tagu). Každá implementace RFID technologie obsahuje tagy pro označení objektů, čtecí zařízení a tzv. middleware (řídící systém, který zajišťuje hromadné zpracování všech načtených tagů v dosahu čtecích zařízení a přenesení zpracovaných dat do návazného informačního či řídícího systému).

1.1 Tagy

Čipy můžeme rozdělit podle toho, jakým způsobem mezi sebou komunikují, nebo podle použité paměti.

Pasivní čipy

Již z názvu lze vydedukovat, že tyhle čipy nemají žádný vlastní zdroj energie. Proto nemůžou vysílat jakýkoli signál směrem k přijímači. Vysílač (přijímač, za rovnocenný název můžeme použít slovo čtečka) periodicky vysílá puls do svého okolí. Jestliže se v jeho okolí bude nacházet jakýkoli pasivní čip, tak dojde k nabití jeho napájecího kondenzátoru a ten posléze odešle svou odpověď zpět čtečce. Jedno z nejvýznamnějších využití je jako nástupce čárového kódu. Obrázek takového čipu je na obr.: 1-1.



obr.: 1-1Ukázka pasivního čipu

Aktivní čipy

Je mnohem méně používán. Zejména díky složitosti návrhu a ceně výroby. Musí mít implementovaný zdroj napájení, nejčastěji baterii. Díky tomu jsou právě proto schopny samy vysílat. Hlavní výhoda je možnost použití jako lokalizace osob, zvířat nebo případně věcí (automobilů,…). Životnost takového čipu, respektive baterie se uvádí na maximálně 5 let. Nicméně právě kvůli použití baterie, je omezena jejich odolnost, především díky počasí.

Semiaktivní čipy

Pasivní čip s baterií, která je tam pouze pro účel většího dosahu signálu.

1.2 Identifikace RFID tagů

Každý čip má své EPC (electronic product kode), 96 bitové unikátní číslo. Přiděluje se výrobcům v řadách a lze jím rozpoznat na 268 milionů výrobců, hlouběji jej můžeme členit na 16 milionů výrobků a ještě podrobněji na 68 miliard sériových čísel. Což se zdá alespoň prozatím docela zbytečné, proto nám dostačuje 64 bitové unikátní číslo, protože výroba tohoto čipu je levnější. Opačně je možnost rozšířit až na 128b. Některé čipy mohou mít kromě svého jedinečného čísla ještě dodatečnou paměť, kam lze ukládat i jiné další informace. Paměť může být různých typů: RAM, ROM, EEPROM nebo FLASH. Pokud výrobce daného čipu dodržuje standard EPC, lze získat informace o čipu pomocí služby ONS (object name service).[3]

1.3 Dosah signálu a použité frekvence

Čipy vyrábí s různou frekvencí nosného signálu a ta je závislá na maximálním možném dosahu vysílaného pulsu (signálu).

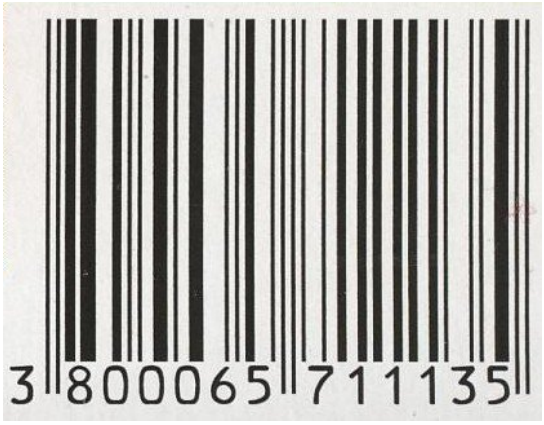
- Tagy, které vysílají na nízkých frekvencích- LF (125 a 135kHz) mají dosah pouze do ½ metru a rychlost komunikace není nikterak uchvacující. Ovšem výhodou je použití ke čtení přes kapaliny, omezeně přes kov. Fungují i ve vlhkém prostředí.
- Tagy s vysoko frekvenčním přenosem- HF (13.56MHz) poskytují vyšší komunikační rychlost, běžný dosah se pohybuje okolo 1m, avšak jejich funkčnost, respektive dosah, přes kapalné a pevné prostředí je znatelně omezen. HF tagy se nejlevněji vyrábí, protože jsou již nejvíce rozšířeny.
- Tagy s ultravysokofrekvenčním rozsahem – UHF, 865-869MHz pro Evropu a Afriku, 902-928MHz Amerika, Kanada a Mexiko, 950-956MHz pro Japonsko a Asii. Dosah se pohybuje okolo hodnoty 3m. Jejich rychlost komunikace je označována za velkou. Použití nachází při snímání dat, kde se čipy rychle pohybují, např. mýtné brány na dálnicích. Neumožňují čtení přes kapaliny a přes kovové předměty velmi omezeně. Další nevýhodou je použití nestejných frekvencí v různých světadílech.
- Tagy s mikrovlnou frekvencí- MW (2.45 a 5.8GHz) komunikační rychlost až 2Mb/s, dosah signálu až 10m. Bohužel jsou nejsložitější, tudíž i cena je vysoká. Jsou vysoce náchylné už jen na blízkost kapalin a kovů.

1.4 Rozdělení tagů dle tříd

- Class0: pouze pro čtení, programováno ve výrobě, 64 nebo 96bit, čtení 1000tagů/sec
- Class1: zápis jednou/zápis mnohokrát, programováno při použití, 64 nebo 96bit, čtení 200tagů/sec
- Class0+ : čtení/zápis, programováno kdykoliv, 256bit, čtení 1000tagů/sec
- Gen2: čtení/zápis, programováno kdykoliv, 256 bit, čtená 1600tagů/sec

1.5 Čárové kódy a RFID

Čárové kódy viz obr.: 1-2 fungují na trhu již několik let. Ani do budoucna se nepočítá s tím, že by jej tagy RFID měly nahradit. Můžeme říct, že technologie RFID umožňuje zapsat/získat více informací do/o daném zboží, avšak mnohem více pravděpodobné je určité sloučení čárových kódů právě s tagy RFID. S touhle metodou se již dnes lze setkat. Jako největší plus, pro zavedení RFID namísto čárových kódů, považujeme možnost bezkontaktní kontroly, díky které jsme schopni registrovat stovky, až tisíce kusů výrobků ve zlomku krátkého časového intervalu, namísto vyskládání každého kusu na běžící pás, manipulaci prodavačky a zpětného naložení do nákupního koše či tašek. Místo toho by stačilo projet košem plným nakoupeného zboží okolím snímače a zbývalo by pouze zaplatit. Obdobným způsobem by se tím zjednodušila práce např. lidem, kteří pracují ve skladech. Dostačovalo by jim pouhé procházení mezi regály se snímačem



obr.: 1-2Čárový kód

v ruce a tím by získali data a informace o veškerém zboží, které mají k dispozici. Další výhodou by byla přesná konkretizace každého výrobku. Nezjistili bychom pouze, o jaký typ zboží se jedná, ale měli bychom k dispozici informace třeba přímo o výrobním čísle daného výrobku nebo o jeho manipulaci od vyskladnění z výrobny, aj. Do budoucna se počítá, že budeme moci zapsat do jednoho tagu a tisíc různých informací. Základním problémem, proč se tahle technika doposud tak znatelně nerozšířila, je cena čipu. Ta ani v blízké době nebude na takové úrovni, jako jsou dnes už dobře zaběhnuté čárové kódy. Avšak díky tomu, že o právě zmiňované RFID tagy se zájem čím dál více zvětšuje, dá se očekávat, že právě proto, jeho ceny budou směřovat postupně dolů, až je časem začnou využívat i drobní obchodníci, díky zmiňovaným možnostem dohledu a kontroly nad zbožím ve skladu, v obchodě. Bohužel snad každá nová, nastupující technika má i určité nevýhody. V případě RFID je to bezpečnost. Té se budeme věnovat dále, o něco hlouběji a podrobněji. Příklad čárového kódu je vidět na obrázku výše.[7]

1.6 Snímače

Snímače neboli čtečky RFID jsou zařízení, která dokážou zachytit vysílání aktivního nebo pasivního tagu. Čtečka nemusí pouze informace zachycovat, ale může je také do tagu zapisovat. Čtečka používá pro vysílání a přijímání signálu anténu, která může být vestavěná nebo externí.

Základním požadavkem na čtečku je schopnost zpracovat obrovské množství dat. Čtečky musí poznat již jednou přečtené tagy a detekovat (ignorovat) odrazy signálů tagů od pevných překážek (např. kovu) a musí zvládnout současně načíst velký počet tagů. S tím souvisí schopnost paralelně načítat tagy v relativně krátkém časovém intervalu. Čtečka přistavená vedle palety se zbožím by měla být schopna přečíst celý obsah palety.

Čtečky jsou stacionární nebo mobilní. Na mobilní čtečky jsou kladeny větší požadavky, např. odolnost proti pádům, extrémním teplotám, prašnosti nebo vlhku. Tyto čtečky většinou komunikují bezdrátově prostřednictvím WiFi nebo Bluetooth, za jejichž použití se aktuálně snímané hodnoty v reálném čase přenášejí do centrální databáze. Stacionární čtečky se uplatní tam, kde není třeba „chodit za tagy“, ale tagy (např. na zboží opatřené tagy na paletě) procházejí okolo čtečky, např. v podobě čtecí brány. Při výběru vhodné stacionární čtečky je třeba zohlednit, zda bude čtečka instalována venku nebo uvnitř budovy. Čtečky a tagy musí pracovat na stejné frekvenci.

K počítači lze čtečku kromě bezdrátové sítě připojit zpravidla i prostřednictvím rozhraní USB nebo RS-232 (sériový port).

Při výběru čtečky je třeba nejprve zodpovědět tyto otázky:

- kde se vyskytují tagy, které je třeba číst,
- jaké množství tagů současně je očekáváno,
- budou se tagy při čtení pohybovat, a pokud ano, jakou rychlostí,
- je třeba redundantní data odhalovat již ve čtečce, nebo až v systému?

Někdy je třeba číst jen tagy, které se vyskytují na určitém místě, např. projíždějí na pásovém dopravníku. Jindy je nutné číst všechny tagy v daném prostoru. Podle toho se vybere vhodný počet antén se správnou směrovou charakteristikou.

Čtečky lze rozlišit podle množství tagů, které jsou schopny současně zpracovat. Mobilní čtečky zpravidla nejsou schopny současně zpracovat velké množství tagů současně, naproti tomu stacionární čtečky v rámech to dokážou.

Tagy se někdy mohou pohybovat vysokou rychlostí (např. jedoucí auta na dálnici při výběru mýtného – v tomto případě může jít o rychlosti převyšující 100 km/h), nebo se tagy pohybují vzhledem ke čtečce pomalu (např. výrobky na výrobním pásu).

Pro filtrování redundantních dat lze využít jeden ze dvou postupů: jednoduché čtecí zařízení bude pouze snímat tagy a získaná data bude posílat dále ke zpracování na server, nebo lze použít propracovanější čtecí zařízení, které bude umožňovat identifikaci již jednou přečtených dat, tzn. očekává se od něj určitá analýza vstupních dat. Na server se potom posílají pouze prověřená data.

Vezmou-li se v úvahu všechny již zmíněné body při výběru čtečky, ukáže se, že jednoduché čtečky jsou použitelné, jestliže:

- bude přítomna obsluha čtečky, např. operátor, který bude činit určitá rozhodnutí za čtečku (např. – filtrování redundantních dat),
- tagy budou v drtivé většině v jednom směru čtení a na jednom místě,
- počet tagů snímaných současně bude relativně malý, a jestliže se budou tagy pohybovat, tak pomalu.

Budou-li tyto předpoklady splněny, lze použít jednoduché čtečky s jednoduchou anténou. Jednoduché čtečky s několika anténami mohou vyřešit problém s umístěním tagu, problém s počtem současně snímaných tagů či problém s vyšší rychlostí pohybu snímaného tagu.[9]

1.7 Využití

Technika RFID nachází využití v mnoha oblastech lidské činnosti.

Zdravotnictví

Hlavním důvodem zavádění RFID do nemocničních zařízení je prevence chyb zdravotnického personálu. Každý pacient při příjmu dostane plastový náramek, ve kterém je tag RFID s pamětí, do kterého se uloží základní údaje o pacientovi. Dalšími informacemi ukládanými do paměti čipu v tagu může být kompletní chorobopis. Chorobopis se aktualizuje podle stavu pacienta, mohou se do něj zapisovat podané léky, podstoupené zákroky a další informace o pacientově stavu. Sníží se i riziko chyb, které by mohly vznikat při přepisování informací o pacientovi do centrální databáze. V čipu může být uložena i krevní skupina pacienta. Krevní konzervy jsou také opatřeny čipy, tudíž nemůže dojít k záměně a použití jiné krevní konzervy.

Hlídání pohybu zboží

Nejjednodušší využití RFID ve kterém se uplatí dokonce **jednobitové** RFID identifikátory. Na vstupu do skladu/obchodu stačí umístit čtečku, stejně tak jako na výstupu. A pak už jenom stačí hlídat, zda něco s RFID neprochází. V praxi můžete podobné systémy najít v mnoha obchodech.

Docházkové systémy

RFID systémy se velmi často uplatňují ve firmách – umožňují nejenom evidovat docházku, ale také slouží jako „elektronické klíče“. Osobní „magnetické“ karty vybavené identifikací pracovníka se ve spojení s docházkovým systémem snadno postarají o oprávnění vstupu do určitých míst a stejně tak dokáží evidovat příchody a odchody. Proč si například nepředstavit vysokoškolský index vybavený RFID čipem?

Stravovací systémy a předplatní systémy

Propojení osobních „magnetických“ karet s účetním systémem jídelny (nebo třeba plaveckého bazénu či fitness centra) je ideální. Osobní „magnetická“ karta je prakticky nezničitelná (pro plavecký bazén může být navíc vyhotovena jako náramek z plastu) a perfektně poslouží. Informační systém poskytovatele služby potom eviduje stav účtu návštěvníka (a umožňuje mu například „dobíjet“ kartu potřebnými peněžitými částkami). Protože odpadá nutnost kontaktu identifikátoru (s kartou například stačí projít dveřmi vybavenými anténou), odpadají i fronty a zbytečné zdržování. RFID vybavené „magnetické“ karty pak mohou sloužiti jako parkovací či tankovací karty. Stejně dobře poslouží pro výběr elektronického mýtného. A od těchto využití je již jenom krok k elektronické peněžence.

Plně elektronické pokladny v obchodech

Jakkoliv je použití čárového kódu na zboží obrovským ulehčením (pro zákazníka i pokladní), může jít RFID ještě dál. V ideálním případě zjistí pokladní kompletní obsah nákupního košíku najednou a bez jeho vyložení. Pokud si dobře všímáte času a úsilí nutného na odbavení jednoho nákupního košíku u pokladny v současnosti, musí vám být více než jasné, jak by se celý postup zjednodušil.

Skladová či výrobní evidence

Podobně jako u pokladny (v podstatě výstup ze skladu) je možné RFID nasadit pro skladovou evidenci. Naskladnění kompletní palety či kontejneru je potom také otázkou několik minut (stačí načíst všechny identifikátory). Stejně tak je možné například automaticky evidovat části vyráběného zboží. Díky RFID mohou existovat regály v obchodech, které samy upozorní na nedostatek určitého zboží. Stačí, aby regál byl vybaven snímačem a propojen s počítačem.

Sledování pohybu zboží či strojů

Stroje (automobily, čistící či transportní stroje) vybavené RFID identifikátory mohou být nepřetržitě sledovány. Přijímače umístěné v podlaze to zajistí snadno a automaticky. Zpětně, za předpokladu ovladatelnosti strojů bezdrátově, je možné stroje řídit.

Identifikace jako taková

RFID se může používat pro označování zvířat (obdoba psích známek), poštovních zásilek, leteckých zásilek či čehokoliv dalšího u čeho je potřeba rychlé a jednoznačné identifikace. RFID naleznete i v imobilizérech – klíče od automobilu vybavené RFID spárované s elektronikou

automobilu. S identifikační schopností RFID čipů se ovšem může počítat i pro využití místo osobních dokladů. Představa označkování člověka RFID čipem je sice poněkud divoká, ale pouze budoucnost ukáže jak hodně.

Identifikovat lze (a je potřeba) ale řadu dalších věcí. Praktické využití RFID může být například v knihovnách či video/dvd půjčovnách.

Inteligentní lednička

Proč nevybavit ledničku RFID čtečkou? Vaše lednička by potom „věděla“ co obsahuje. Dokázala vám říct, zda vaše mléko není zrovna ve stavu nepoživatelném. A případně i poradit, co vlastně můžete uvařit k večeři.[1]

1.8 Bezpečnost RFID

Nová technika s sebou vždy přináší otázky spojené s bezpečností. Vzhledem k tomu, že s RFID se opravdu počítá v budoucnosti ve velkém měřítku, tak je třeba se zamyslet nad její neužitelností o to více. Jedním z nejzávažnějších témat v souvislosti s RFID je otázka ochrany soukromí. Čipy jsou aktivní i potom, co se zboží stane majetkem osoby, která si takové zboží s čipem pořídila. Přestože výrobci tvrdí, že umí čipy deaktivovat, je otázka, zda to prodejci skutečně budou dodržovat. Do ruky se jim totiž dostává naprosto bezkonkurenční marketingový nástroj: dokážou sledovat, co který člověk nakupuje, a následně mířit cílenou reklamu na danou osobu. Například pan X si půjde do obchodu koupit boty. V botách bude standardní pasivní tag RFID. Pan X tyto boty zaplatí platební kartou. Platební karta je ovšem na jméno, tudíž již při placení může obchodník zaznamenat, že tyto boty nekoupil pan X, ale konkrétní osoba, a to pan Adam Smith. Je tedy jasně asociováno jeho jméno s čipem, který má v nových botách. Obchod mu čip nedeaktivoval, protože informace využívá dále. Pan Adam Smith začal boty nosit a jednoho dne opět zavítá do obchodu, kde boty koupil. Ovšem nyní se pohybuje např. v drogerii. Budou-li zde šikovně rozmístěny čtečky tagů, není problém zjistit, kde přesně se pan Smith nachází – na takový výpočet stačí obyčejné trigonometrické funkce. Obchodník má nyní naprosto detailní informace, u kterých regálů se pan Smith zastavuje. Po zaplacení lze zaznamenat informace o obsahu jeho nákupního košíku a uložit je do informačního systému. Ze získaných údajů lze sestavit nákupní profil zákazníka a dále informace využít k marketingovým účelům.

Druhým bezpečnostním problémem je bezkontaktní čtení tagu RFID. Nikdo nepostřehne, že byla načtena data z čipu. Budou-li v něm uloženy biometrické údaje, které budou součástí např. určité identifikační karty, lze i z dálky až deseti metrů tyto údaje načíst. Technické údaje uvádějí dosah v řádů centimetrů, ale pokusy s mobilními čtečkami dokázaly, že někdy lze údaj přečíst z mnohem větší vzdálenosti. Již dnes se na trhu objevují peněženky, které rádiový signál odstíní, ale někdy je prostě nutné z ní identifikační kartu vyjmout.

Další problém spojený s RFID je nezabezpečená komunikace mezi čipem a čtečkou. Pro snížení pořizovacích nákladů na tagy je komunikace čtečky a čipu založena na prostém systému dotaz-odpověď. Objevily se již čipy s šifrováním. Čtečka vyšle signál, čip odpovědí signalizuje svou přítomnost a dohodnou si způsob šifrování. Dále je již veškerá komunikace šifrovaná. Při šifrování se používá buď symetrický šifrovací klíč, nebo metoda asymetrické kryptografie. Ovšem všechny tyto „nadstandardy“ zvyšují spotřebu energie a rychlost zpracování a rovněž i složitost jednotlivých čipů, což zvyšuje jejich cenu.

Je třeba zmínit i možnost hackerských útoků na systémy RFID. Tyto útoky využívají slabiny v systémech, kde je technika RFID používána. Dosud se počítalo pouze s tím, že čtečka přečte čip a zanese data do systému. Nikdo ovšem nepředpokládal, že se od „infikovaného“ čipu může nakazit celý systém. Tento systém představil Bruno Crispo a jeho kolegové na univerzitě v Amsterdamu [2]. Pracuje tak, že nakažený čip využije slabá místa softwaru, který ovládá čtečku, a následně virus zanese z čipu do systému. Potom je možné, aby se virem nakazily i další čtené čipy. Stačí, aby útočník koupil v supermarketu kečup s tagem RFID, ten doma nahradil svým tagem, do kterého naprogramoval virus, a šel znovu do stejného supermarketu tag načíst. Tak může způsobit až totální destrukci celého informačního systému daného supermarketu.

Ovšem je nutné podotknout, že na legislativních změnách se celosvětově pracuje od prvního upozornění na možné zneužití RFID pro marketingové účely. Proto je patrný velký důraz na ochranu osobních údajů, aby uvedená situace nemohla nastat. Marketingové firmy se pod hrozbou velkých pokut neodváží takto nabyté informace zneužít, protože by to pro ně mělo likvidační charakter. Taktéž zmíněný scénář proniknutí do informačního systému (IS) supermarketu je možný pouze za předpokladu, že supermarket bude využívat „hloupé“ čtečky a samotný vstup do IS nebude kontrolován s ohledem na možnost hackerských útoků, což je v dnešní době zabezpečených IS velmi nepravděpodobné. Proto není třeba se RFID bát, pouze je nutné brát ohled na možnosti RFID v celé její šíři.

2 ČIPOVÉ KARTY

Čipová karta, též můžeme použít název smart karta neboli anglicky smart card. Integrovaný obvod umístěný nejčastěji v plastovém pouzdře. Obvykle se jedná o obdélníkový tvar, standardizovaného rozměru 85.60 x 53.98 mm [6], tedy má stejnou velikost jako např. řidičský průkaz či průkaz zdravotního pojištění. Dobře známým příkladem jsou kreditní karty. Druhou, velmi rozšířenou podobou je takzvaná SIM karta, příklad je uveden níže na obr.: 2-1: (jako anglická zkratka pro subscriber identity module), která je určena pro identifikaci účastníka v mobilní síti. Té je normována velikost na 25 x 15mm. Oba dva zástupci smart karet mají danou tloušťku, ta činí 0.76mm. Každá čipová karta má vevnitř implementován integrovaný obvod, ve kterém je mikropočítač s koprocesorem, dále musí mít paměť (ať už RAM, ROM nebo EEPROM) a určitý software, uložený v paměti. Předností pro využití smart karet tkví v tom, že umožňují nejen ukládání dat, ale i zpracování informací, jejž si vymění čtečka s pamětí.[4]

obr.: 2-1SIM karta

2.1 Historie vzniku

Vynález čipové karty by se dal ohodnotit jako jeden z nejvýznamnějších v elektrotechnice za 20té století.

Princip čipů si nechalo patentovat hned několik na sobě nezávislých odborníků z celého světa. Ovšem za průkopníka je považován francouzský novinář Roland Moreno. Ten založil v roce 1972 v Paříži společnost Societé International pour l´Innovation – známou též jako "Innovatron". V roce 1974 vynalezl prsten. Jím se mohlo platit v určitých obchodech, které disponovaly k tomu určeným snímačem. Zmíněný prsten bylo možno „nabít“ hotovostí na pobočkách bank a placení jím bylo relativně bezpečné.

Bohužel bankám se taková podoba tohoto vynálezu nezamlouvala. Nejzajímavější výhoda právě pro banky tkvěla v tom, že by takový systém placení mohl vyřešit problém s nepovolenými debety klientů na běžných účtech způsobených šeky, které tehdy byly hlavním prostředkem k disponování s účtem. Tehdy ředitel technického vývoje v bance Crédit Industrie et Commercial, Jeana-Claude Repolte, doporučil pro použití takového systému právě formát kreditní karty.

Při tehdejší velikosti mikroprocesorů se však jejich umístění do tenkého plastu platební karty, zdálo jako neřešitelné, a podařilo se zvládnout až ve spolupráci s francouzskou společností CII-Honywell Bull. Následně v březnu 1975 vyrobeno prvních sedm kusů karet s mikročipem a také první zařízení, které umožňovalo jejich příjem.

V roce 1976 koupil Bull od Morenovy firmy licence na čipové karty a založil specializovanou dceřinou společnost Bull CP8, orientovanou výhradně na tyto technologie.

Zlomovým se stal rok 1984, kdy si kosorcium francouzských bank objednalo více jak 12 milionů čipových karet. Již následující rok zahájily podobné projekty i banky v dalších zemích a v současnosti je tato technologie v bankovním sektoru již více méně standardem.

Čipové karty nenašly ovšem uplatnění jen u bank, ale jsou stále populárnější i v jiných oblastech, jako je zdravotnictví (karta pacienta s uloženými údaji), doprava, stravování, školství, aj. Zde může sloužit nejen jako identifikátor a nosič věrnostních bodů, ale je i prostředkem pro

vybudování vlastních platebních řešení, kontrola přístupu (ať už ve zmiňovaném školství či nejrůznějších firmách).[11]

Typy karet

Smart karty se dají rozdělit do několika kategorií:

1. Typ čipu
2. Způsob čtení informací
3. Využitelnost

1. Existují dva druhy čipů, kterými může karta disponovat, nazýváme je:
   - paměťové karty- čip je paměťové zařízení, které umožňuje pouze uložení dat. Tyhle karty jdou zabezpečit PIN kódem (osobní identifikační číslo),
   - mikroprocesorové karty- v jejich pamětech je uložen zabezpečovací software pro přístup k datům. Operace, jenž na kartě probíhají, jsou výpočetně mnohem náročnější, proto využívají svůj mikroprocesor, ten je spojený ještě s koprocesorem. Z toho důvodu je vyžadována nutnost operační i pevné paměti. [10]
2. Dalším členěním je způsob komunikace neboli získávání informací z karty
   - Kontaktní- na plastovém obalu je kontaktní oblast. Jeho velikost a tvar je standardizována. Karty mohou mít různé kontaktní čipy. Úplně jednoduché, které jsou v podstatě paměťovým médiem s pamětí desítky a stovky bytů bez operačního systému až po současné „inteligentní“ (smart) čipy s vlastním operačním systémem, pamětí desítek kilobytů a vlastními kryptografickými koprocesory. Mezi takové čipy patří i SIM karta, která ovšem nedosahuje takových parametrů jako nejlepší čipové karty (např. od společnosti SafeNetInc). Přístup k těmto kartám je chráněn heslem (PIN), který zná vlastník karty. Jedná se tedy o dvou faktorovou bezpečnost: něco, co máte (Vaše čipová karta) a něco, co znáte (Vaše heslo–PIN). Nikdo se nemůže dostat k Vašim důvěrným informacím, aniž by měl Vaši kartu a současně znal heslo. Nejlepší čipové karty podporují PKI, elektronickou autorizaci dat (elektronický podpis) a šifrování (symetrické i asymetrické). Tyto čipové karty jsou schopny ve svém koprocesoru generovat šifrovací klíčové páry a provádět s nimi veškeré požadované operace, a tak privátní klíč nikdy neopustí tuto kartu a není možné jej odchytit (odposlechnout) cestou po síti či v PC. Dostatečně velká paměť EEPROM umožňuje ukládání digitálních certifikátů, využívaných pro autentizaci uživatele do PC, sítě, VPN a k aplikacím, šifrování komunikace a elektronický podpis pošty, dokumentů i webových formulářů. Čím je paměť větší, tím více certifikátů i dalších informací (hesla, atd.) se na kartu vejde. Toto je důležité hlavně při nasazení v infrastruktuře veřejných klíčů, kdy se na kartě mohou nechat uložené i certifikáty po době platnosti, a tak zajistit, že si bez problémů přečtete i staré zašifrované dokumenty. Vaše digitální certifikáty jsou v mnohem větším bezpečí na čipové kartě než na harddisku Vašeho počítače nebo na disketě. Lze jich samozřejmě využít i jako elektronickou peněženku nebo pro věrnostní programy. Nejnovější čipové karty (JavaCard) lze použít jako platební kartu dle standardu EMV (rezidentně uložený aplet VISA) nebo na kartu uložit vlastní Java aplety. Pro komunikaci s čipovou kartou je potřeba kontaktní čtečka čipových karet a speciální software [13].

Ukázka takové karty je vidět na obr.: 2-2, jedná se velmi často o platební karty bank.

obr.: 2-2Kontaktní karta, platební karta

- Bezkontaktní- jsou v dnešní době nejvíce perspektivním typem. Využívají technologii rádio frekvenční identifikace (RFID). Smart karta obsahuje vestavěnou indukční anténu a čip s integrovaným obvodem. Pro lepší mechanickou ochranu je čip s integrovaným obvodem umístěn do malého bloku, který se připojuje ke koncům antény. Vestavěný integrovaný obvod se skládá ze dvou dílů – bezkontaktního rádio frekvenčního rozhraní a mikro řadiče. Obvod RF rozhraní je připojený do výstupu antény smart karty a používá střídavé elektromagnetické pole emitované snímačem pro získání napájecí energie pro smart kartu a pro výměnu dat mezi kartou a snímačem. Bezkontaktní smart karta funguje ve vzdálenosti od 10 cm do 1 m v závislosti od pracovní frekvence snímačů a nepotřebuje přesné centrování, což zaručuje její stabilní práci, pohodlí při využití a vysokou přenosovou schopnost. Čip většinou obsahuje pouze sériové číslo karty, které slouží pro autentizaci majitele. Lepší čipy mohou obsahovat i další údaje, které ovšem nepřesahují řádově desítky bytů. Čipy jsou v podstatě dvojího druhu – údaj (obvykle sériové číslo) lze na kartě pouze přečíst nebo údaje na kartě lze nejenom přečíst, ale další i zapsat. S těmito kartami se používá další zařízení: čtečky karet (karty je nutné přiblížit ke čtečce), turnikety, závory atd. Pro zvýšení zabezpečení se používají i čtečky, kde je potřeba zadat heslo (PIN) [12]. Příkladem je karta studenta VUT obr.: 2-3, tahle zároveň může být použita i jako platební karta, proto se na kartě můžeme spatřit kontaktní pole.

obr.: 2-3Bezkontaktní smart karta

- Další možností, jak získat informace z karty je tzv. dvojité rozhraní. Není to nic jiného, než spojení kontaktní a bezkontaktní karty. Tedy na takové smart kartě se nachází jak kontaktní pole, tak je v jejím těle anténa. Tím pádem umí komunikovat s více druhy snímačů. Ten generuje elektromagnetické záření určité frekvence. Při vkládání karty do vysílacího pole snímače, elektromagnetické záření zapojí čip karty přes vestavěnou anténu do karty a RF rozhrání. V okamžiku, kdy karta dostane potřebné množství energie pro vykonání práce, přepošle do snímače svoje identifikační číslo pomocí elektromagnetických impulsů dané frekvence.

3. Pohodlí, spolehlivost a multifunkčnost smart karet způsobuje široké spektrum jejich využití. Smart karty nacházejí uplatnění v mnoha oblastech činností člověka:

   - telefony – platební karty pro telefonní automat, GSM-karty v mobilních telefonech,
   - doprava – jízdenky,
   - zdravotnictví – zdravotní karta, karta pojištění,
   - zákaznická karta – věrnostní program (slevy a bonusy), atd.

Je třeba podotknout, že obzvlášť vážnou oblasti využití smart karet jsou jejich aplikace, citlivé k bezpečnosti nebo přímo zajišťující informační bezpečnost. K takovým aplikacím patří:

- finance – použití při různých bankovních operacích, např. platba za zboží a služby, kreditní debetní karty, karty pro připsání stipendia, mezd a důchodů atd.,
- městské dopravě a metro – jízdenky,
- uschová důvěrných dat (včetně kryptografických dat a jiné identifikační informace),
- zajištění identifikační bezpečnosti – identifikace uživatelů počítačových sítí a systémů, kontrola přístupu do chráněných prostor a docházky atd.

Výhody smart karet:

- smart karta obsahuje paměť, která ji umožňuje uchovat docela velký objem informace potřebné pro práci,
- smart karta má spolehlivý systém zabezpečení, obsahuje vestavěný systém ochrany proti neoprávněnému kopírování dat a jejích falšování,
- smart karta je docela odolná. Její životnost se liší v závislosti na způsobu využití a v průměru se pohybuje od 3 do 10 let.[10]

Bezpečnost smart karet

Z hlediska bezpečnosti představují špičku PKI (Public Key Infrastructure - Infrastruktura veřejného klíče) čipové karty. Tyto čipové karty jsou schopny ve svém koprocesoru generovat šifrovací klíčové páry a provádět s nimi veškeré požadované operace, a tak privátní klíč nikdy neopustí tuto kartu a není možné jej odchytit (odposlechnout) cestou po síti nebo v PC. Dostatečně velká paměť EEPROM umožňuje ukládání digitálních certifikátů, využívaných pro autentizaci uživatele do PC, sítě a k aplikacím; šifrování komunikace a elektronický podpis pošty, dokumentů i webových formulářů. Čím je paměť větší, tím více certifikátů i dalších informací (hesla, atd.) se na kartu vejde. Toto je důležité hlavně při nasazení v infrastruktuře veřejných klíčů (PKI), kdy se na kartě mohou nechat uložené i certifikáty po době platnosti, a tak zajistit, že si bez problémů přečtete i staré zašifrované dokumenty.

Čipové karty poskytují dvou-faktorovou bezpečnost: něco, co máte (čipová karta) a něco, co znáte (heslo - PIN). Nikdo se nemůže dostat k Vašim důvěryhodným informacím, aniž by měl Vaši kartu a současně znal heslo. Vaše digitální certifikáty jsou mnohem lépe chráněné na PKI čipové kartě než na harddisku Vašeho počítače, na disketě nebo na obyčejné paměťové čipové kartě (telefonická karta apod.).

Čipové karty navíc umožňují rozšíření o další bezpečnostní prvky, jako jsou magnetické proužky, bezkontaktní čipy, natištěné informace (fotografie, jméno, identifikační číslo, čárový kód, apod.), a tak jedinou čipovou kartou můžete vyřešit bezpečnost Vašeho informačního systému, objektovou bezpečnost, docházkový systém a mnoho dalších.

2.2 Karty MiFare

Karty typu MIFARE jsou dnes velice dobře známým příkladem tzv. „chytrých“ karet. Tahle karta byla vyvinuta společností NXP Semiconductors. Ty se díky své nízké ceně rozšířily do celého světa (odhaduje se na několik stovek milionů kusů v oběhu). Jejich základní komunikační rozhraní je kompatibilní se standardem ISO 14443-A. Nad tímto rozhraním se nenachází rozhraní ISO 7816, nýbrž proprietárního aplikačního protokolu MIFARE, který si společně s algoritmem CRYPTO1 firma Philips dobře hlídá.

V praxi se můžeme setkat s kartami o kapacitě 1kB nebo 4kB. Dostupná paměť se dělí do bloků po 16B a tyto bloky se dále sdružují do tzv. sektorů. Na rozdíl od čistě paměťových karet řídí MIFARE přístup k paměťovým blokům na základě prokázání znalosti příslušného kryptografického klíče. Zda je použita varianta tříprůchodné autentizace dle ISO 9798-2, při níž se dohodnou klíče pro šifrování komunikace mezi kartou a terminálem. Primární autentizací klič má sice jen 48b a hlavní kryptografický algoritmus s názvem CRYPTO1 je neveřejný. [8]

Volné datové bloky je možné využít buď pro ukládání libovolných 16B řetězců, nebo jako čítače nějakých jednotek. To, jaké operace jsou s blokem povoleny, popisuje v rámci jeho sektoru

speciální blok označovaný jako zavaděč sektoru. V případě 1kB karty tvoří sektor celkem 4 paměťové bloky. V zavaděči mohou být uloženy až dva 48b klíče, označované A a B. Dále je zde pole příznaků, které pro každý datový blok sektoru zvlášť předepisuje jedno z osmi možných řízení přístupu. Tabulka klíčů je přiložena pod textem v **Error! Reference source not found.**.

tab.: 2.2-1 Typ přístupu v závislosti na indexu konfigurace

index konfigurace	typ přístupu			
	read	write	increment	decrement
0	klíč A/B	klíč A/B	klíč A/B	klíč A/B
1	klíč A/B	nelze	nelze	nelze
2	klíč A/B	klíč B	nelze	nelze
3	klíč A/B	klíč B	klíč B	klíč A/B
4	klíč A/B	nelze	nelze	klíč A/B
5	klíč B	klíč B	nelze	nelze
6	klíč B	nelze	nelze	nelze
7	nelze	nelze	nelze	nelze

Blok 0 sektoru 0 má speciální význam, neboť obsahuje pevné údaje výrobce, kde je mimo jiné i 4B sériové číslo karty. Ostatní datové bloky jsou již návrhářům aplikací plně k dispozici. Kapacitu karty je přitom vhodné rozdělit po sektorech, protože každý sektor definuje pro řízení přístupu ke svým blokům své vlastní klíče A a B a tím jednotlivé aplikace kryptograficky rozděluje. [18] Příkladem karty s MiFare čipem je již dříve zmiňovaná VUT studentská karta, **Error! Reference source not found.**.

2.3 Útoky na RFID technologii

Čip MiFare může být terčem útoku

Dva vědci, Němec Henryk Plotz a Američan Karsten Nohl, demonstrovali způsob prolomení šifrování běžně používaného RFID čipu MiFare Classic. Tento čip je používán v milionech zařízeních po celém světě, například v čipových dopravních průkazech nebo v přístupových kartách do budov. Bezpečnost systému byla považována za dostatečnou vzhledem k oblastem, kde se MiFare nasazuje. Prolomení ochranné šifry Crypto1 bylo sice pokládáno za možné, ale příliš nákladné. Při demonstraci ovšem postačilo obyčejné PC a několik minut. Použitou metodou bylo reverzní inženýrství, v tomto případě ovšem s použitím mikroskopu a čtečky RFID kódů OpenPCD. Hack byl proveden na základě analýzy hardwarového uspořádání jednotlivých vrstev asi milimetr tlustého čipu, která byla provedena programem běžícím v rámci Matlabu. Celkem zde bylo asi 10 000 bloků zhruba odpovídajících například jednotlivým logickým hradlům. Hackerům se podařilo v rámci analýzy identifikovat oblasti vztahující se k šifře. [2]

Získání přístupových klíčů

Každá RFID čtečka, která přistupuje k jednotlivým blokům, musí mít nastavený správný přístupový klíč. Samotný klíč zabezpečí, že čtečka má k danému sektoru povolený přesně definovaný přístup (čtení, zápis, inkrementace, dekrementace).

Pomocí RFID čtečky s přednastaveným klíčem

V případě, že je k dispozici dostupná veřejná RFID čtečka (terminál) s přednastaveným klíčem, je možné získat klíč odposlechem a prolomením záchytené komunikace mezi samotnou

kartou a čtečkou. To se dá realizovat na testovacích kartách pomocí speciálního zařízení Proxmark III s příslušnou vysokofrekvenční anténou. Zachycení původní komunikaci („challenge-response authentication“) stačí úplně k prolomení klíče k sektoru, ke kterému se daná čtečka autentifikovala. Tento útok umožňuje získat klíče jen k sektorům, ke kterým přistupuje legitimní RFID čtečka, ne ke všem. Na vytvoření funkčního klonu je ale nevyhnutné získat všechny klíče ke všem sektorům karty.

Získání klíčů „offline“ útokem na samotnou kartu

Mifare Classic karty obsahují množství různých bezpečnostních zranitelností, které umožňují realizovat kompletní „offline“ útok bez potřeby legitimní RFID čtečky s přednastavenými klíči. Na demonstraci závažnosti zranitelností Mifare Classic karet byl vytvořen a veřejně publikován „offline nested“ útok, pomocí kterého je možné jen útokem na samotnou kartu (bez potřeby legitimní RFID čtečky) získat všechny klíče pro všechny sektory karty. Jediná podmínka na to, aby bylo možné útok úspěšně realizovat a získat všechny klíče je, aby samotná karta obsahovala minimálně jeden sektor šifrovaný „default“ klíčem anebo tento klíč byl dopředu známý. V případě, že by dané karty neobsahovali žádný sektor šifrovaný „default“ klíčem, stále je možné získat potřebný jeden klíč odposlechem komunikace mezi legitimní RFID čtečkou a samotnou kartou (viz. předešlá sekce) a potom realizovat „offline nested“ útok a získat všechny klíče. Nicolas T. Courtois navrhoval vlastní multi-diferenciální útok, kdy by bylo možné aspoň jeden klíč získat i bez prolomení komunikace karty s legitimní RFID čtečkou – též jde o „offline“ útok. Implementace tohoto útoku ale zatím nebyla zveřejněna. Tento útok umožňuje získat všechny klíče ke všem sektorům, což stačí na úplnou kontrolu nad kartou (možnost ji kompletně načíst, modifikovat, či naklonovat).

Zneužití čipových karet

Znalost uvedených klíčů získaných buď odposlechem a prolomením komunikace mezi kartou a legitimní RFID čtečkou anebo „offline nested“ útokem umožňuje realizovat nad kartou následující druhy útoků:

- možnost danou kartu kompletně načíst (v případě fyzické blízkosti cestujících ve veřejných dopravních prostředcích je možné získat kompletní kopii čipové karty libovolného cestujícího, to znamená všechny informace o něm uložených na kartě včetně jejich křestního jména, bydliště, studentského čísla, ...),
- možnost modifikovat libovolný sektor na kartě (kromě nultého „read-only“sektoru) a teda upravit případný kredit na kartě, jméno vlastníka, nebo jiné citlivé informace,
- možnost vytvořit 99.6% klonu karty (kromě nultého bloku v nultém sektoru),
- možnost vytvořit 100% klonu karty (včetně nultého bloku v nultém sektoru) kompletní emulací všech sektorů pomocí zařízení Proxmark III.

Náklady na případné zneužití

V případě, že útočník disponuje znalostí přístupových klíčů, náklady na popisované zneužití jsou velmi nízké – potenciální útočník může použít libovolně lacinou RFID čtečku (dá se sehnat bez problémů do 1000kč), čisté čipové Mifare Classic karty (trhová cena začíná na 25kč/kus) a veřejně dostupný software použitelný na modifikaci nebo klonování čipových karet.

Náklady na získání klíčů pomocí zachycení komunikace mezi RFID čtečkou a čipovou kartou jsou vyšší – aktuální cena zařízení Proxmark III se pohybuje od zhruba 7000kč.

Je nevyhnutné podotknout, že náklady na případné zneužití potenciálním útočníkům budou vždy klesat (nikdy ne růst) díky neustálému zveřejňování novějších a lepších nástrojů jako i snižování ceny RFID hardwaru. Proto pravděpodobnost potenciálního zneužití bude s časem jen narůstat.

Jak zabezpečit

Nejlepším způsobem, jak karty MiFare classic zabezpečit je, vyměnit ty dosavadní za nové karty s jiným čipem. Ovšem z důvodu jejich celosvětové užívanosti nelze s tímhle razantním krokem počítat. Proto se spíš rozmáhá kompromis mezi kvalitou zabezpečení (ani ta nejlepší možnost zabezpečení není nepřekonatelná) a jednoduchostí útoku.

Identitu každého uživatele karty se proto doporučuje spojit s „read only“ unikátním identifikátorem karty (UID), což představuje sériové číslo karty, které je zatím nemodifikovatelné.

Aby toto svázání bylo účinné, je nutné při samotné kontrole ověřovat, či dané UID je v systému už zanesené a teda systém danou kartu pozná nebo jde o naklonovanou kartu (tzv.„whitelisting“). Další možnost je samotné UID karty použít při vytváření digitálního podpisu karty a následně ho ověřovat při každé kontrole karty.

Vzhledem k tomu, že pomocí Proxmark III je možné kompletně celou kartu odemulovat a je jen otázka času, kdy budou na trhu nelicencované klony Mifare Classic s modifikovatelným nultým sektorem, silně se doporučuje uvedené karty nepoužívat a nahradit je bezpečnějšími.

Je třeba podotknout, že svázání identity uživatele s UID sériovým číslem jeho karty zabrání jen případným laciným klonům, neznemožní ale útočníkovi modifikaci karty (například se záměrem obnovit původní kredit, teda původní kopii karty).

Digitální podpisy pomocí asymetrické kryptografie výrazně znemožňují modifikovat obsah čipové karty. Bohužel to ale neznamená, že karta je dokonale chráněná - v případě, že daná karta obsahuje „kredit“ v jakékoli formě, útočník dokáže při nabitém stavu získat její kompletní kopii (tzv. „snapshot“ vrácení platného digitálního podpisu), kartu použít a opětovně uvedenou kopii obnovit. V praxi to znamená, že i navzdory útočníkově neznalosti daného digitálního podpisu, útočník dokáže ovlivnit kredit podle vlastní vůle a teda použití jakýchkoli digitálních podpisů se stává neúčinné. Jediné řešení, které může trvat několik dní, je uvedené správné odhalení centrální kontrolou (jestli bude sedět stav kreditu cestujícího na kartě a v centrálním systému) a zablokovat UID příslušné vyklonované karty na všech koncových RFID čtečkách, to může byť velmi pracné. V tomto případě je ale nevyhnutné, aby jednotlivé čtečky ověřovali, či karta s daným UID je platná nebo ne, případně používali UID karty při vytváření digitálního podpisu.

I přes to, že identita cestujícího bude totožná s UID karty a bude použit digitální podpis obsahu karty, stále hrozí reálné riziko zneužití karty – t.j. útočník dokáže opětovně získat původní kredit karty obnovením kopie karty, která byla vytvořená při plném kreditu.

Toto riziko může být částečně eliminované centrální kontrolou, pokud ale uvedená kontrola není „online“, teda okamžitá, stále je prostor pro útočníka na potenciální zneužití. Nedoporučuje se používat algoritmy na vytváření digitálního podpisu, ani hashe, na které se objevili už kolize (MD5, SHA1), ale bezpečné (Blowfish, SHA-2). Vzhledem na kapacitní možnosti karty, v případě asymetrického šifrování doporučuje se použít algoritmy, které používají kratší klíče.

„Decrement counter“ představuje řešení, které kombinuje výhody předešlých dvou řešení a současně implementuje na kartě speciální „počítadlo“, jejíž hodnotu je možné jen načíst a dekrementovat (to je zabezpečené pomocí speciálních oprávnění klíčů A/B, které žádné jiné operace nad uvedeným počítadlem neumožňují). Současně je na kartě zabezpečené, že uvedené oprávnění klíčů A/B je nemožné upravovat. Počítadlo je při vydání karty nastavené na maximální hodnotu (0xffffffff), při každé autorizované operaci (dobití, platba, změna kreditu) je dekrementované. Celý obsah karty je digitálně podepsaný (pomocí klíče, kterým disponuje pouze vydavatel karty), při digitálním podpisu se ale též uplatňuje UID karty (znemožňuje jednoduché vyklonování) a „decrement counter“ (znemožňuje vytvoření kopie karty a její znovu obnovení, protože není je možné obnovit původní hodnotu počítadla).

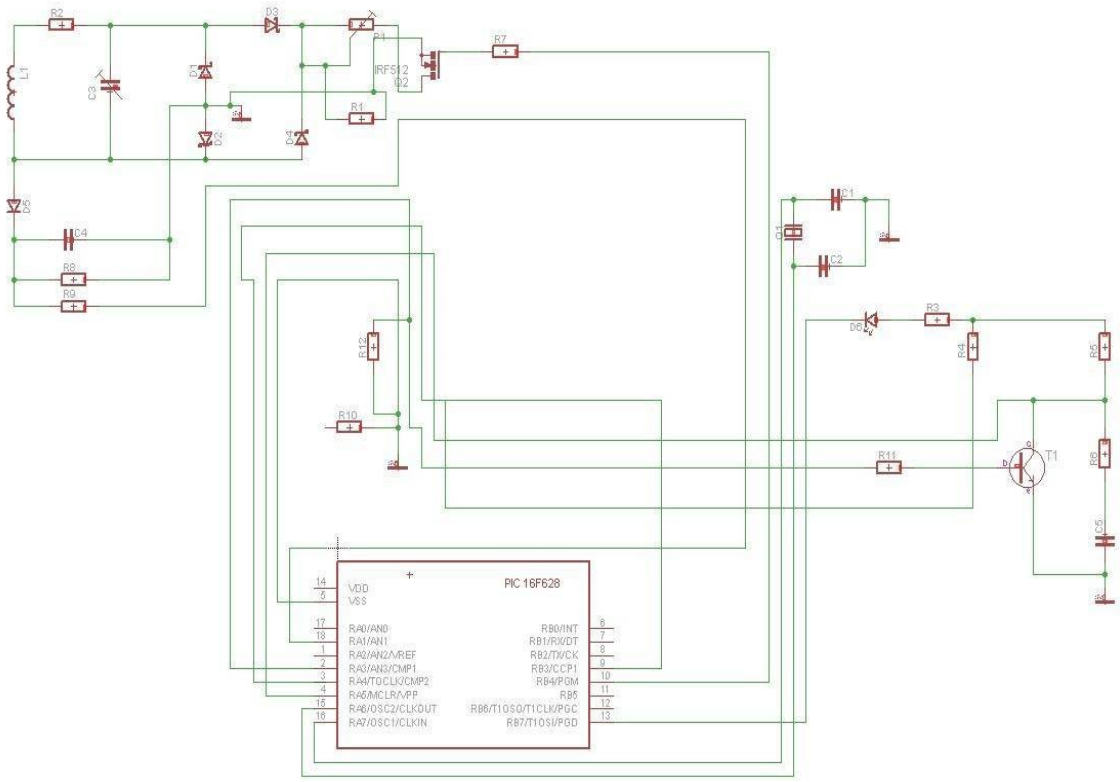
Navzdory tomu, že uvedené řešení chrání kartu proti neautorizované modifikaci či klonování, toto řešení je ale neúčinné vůči:

- kompletnímu prolomení klíčů a načítání celé karty (a citlivých informací, jako křestní jméno, bydliště, či rodné číslo),
- proti 100% emulované kartě pomocí zařízení Proxmark III,
- proti dalším implementačním chybám Mifare Classic, které se můžou objevit v budoucnosti a budou umožňovat obnovení původní hodnoty počítadla.

3 KONSTRUKCE EMULÁTORU

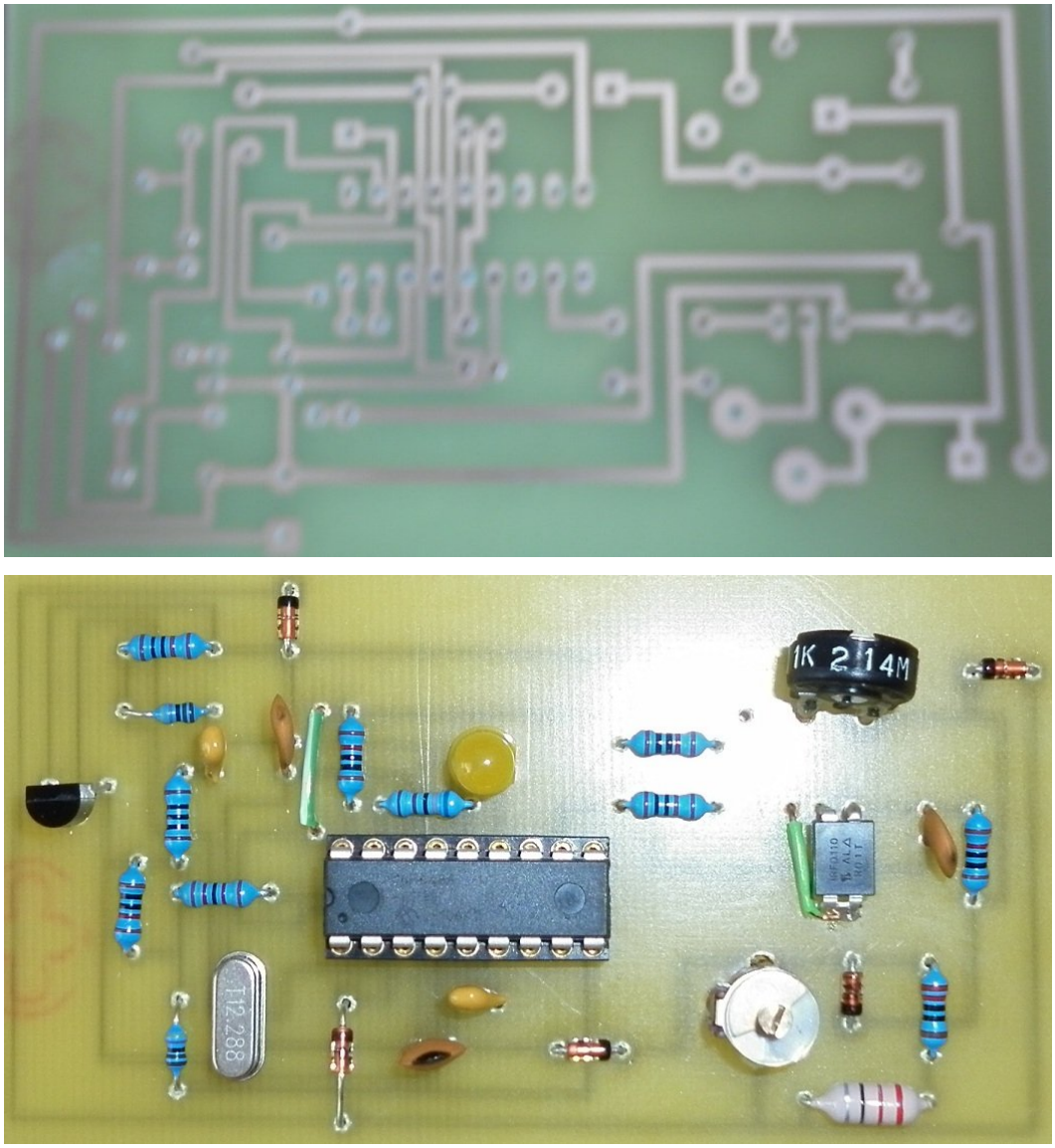
3.1 Popis zařízení

V obvodu je použito kromě řadiče PIC co nejméně dalších součástek, jedná se tedy o tzv. PicNic. Obrázek neosazeného a hotového obvodu je zde obr.: 3-2 a obrázek návrhu v programu Eagle je na obr.: 3-1. Tahle verze zapojení je určena především pro experimenty



obr.: 3-1Schéma obvodu navržené v programu Eagle

s útoky na čipy MiFare. Při návrhu se počítalo s podporu standardu ISO 14443A. Jestliže se ještě trochu upraví schéma a přepíše zdrojový kód programu, budou se moci aplikovat i standardy ISO 14443B a ISO 15693. K obvodu lze připojit sériový programátor, aniž by se musel demontovat řadič. Tudíž modifikace kódu nejsou nijak složité. Byl zvolen procesor PIC16F648A. Kdyby byla potřeba zajistit větší paměť pro procesor, nebude těžké vyhledat jiný, alternativní, který bude nabízet minimálně stejné periferie.



obr.: 3-2Obrázek neosazeného (nahoře) a osazeného (dole) emulátoru na desce plošného spoje

Vlastní magnetická anténa zapojení se skládá z indukčnosti, sériového rezistoru a ladícího kondenzátoru. U takovýchto druhů antén vždy jejich funkčnost závisí na tom, jak se její naladění zrovna „podaří“. Z hlediska elektromagnetického pole je vhodné cívku antény konstruovat jako několik závitů v rovině kolem plochy zhruba odpovídající běžné čipové kartě. Z hlediska obvodového nás zajímá, hlavně její indukčnost. Tu musíme udržet v řádu nejvýše desítek μH, aby bylo možné nastavit příslušnou rezonanční kapacitu na ladícím kondenzátoru. Pro odhad můžeme vyjit z Thompsonova vzorce:

$$f_{RES} = \frac{1}{2}\sqrt{LC}\ ,(1.1)$$

kde f_{RES} je rezonanční frekvence, L indukčnost cívky antény a C kapacita jejího kondenzátoru.

S indukčností úzce souvisí ještě činitel jakosti antény, který ovlivňuje šířku pásma. V tomto případě je potřeba alespoň 1,7MHz. Podle toho se zvolí hodnota rezistoru antény. Vyjde se ze vztahu:

$$R \triangleright 3{,}4 \cdot 10^6 \cdot \pi \cdot L \quad ,(1.2)$$

kde R je odpor rezistoru a π Ludolfovo číslo.

Zároveň se jeho hodnota zvolí co nejmenší, aby se zbytečně netlumila anténa. Za anténou se nachází diodový AM detektor, k němuž je přes odpor šetřící přepěťové ochrany PICu připojen vstup vnitřního komparátoru RA1. Výstup je dále vnitřně veden na vstup čítače TMR0, ten je použit k převodu modifikovaného Millerova kódu na nemodifikovaný. Z jeho LSB si následně data odebírají čtecí smyčky procedury MillerDecoder. Propojení s RB3 slouží k řízení záchytného registru pro další vnitřní časovač- TMR1, který je využit k synchronizaci rámců odpovědi podle poslední hrany signálu (norma ISO 14443-3A). Dále je k anténě připojen modulátor tvořený Graetzovým můstkem, se zátěží ovládanou tranzistorem MOSFET s indukovaným kanálem N. Zmíněné technologické použití je žádoucí, protože spínací vlastnosti klasického bipolárního tranzistoru, řízeného asymetrickým vstupním napětím se ukázaly být nedostatečné pro frekvenci pomocné nosné 847,5kHz. Prahové napětí tranzistoru určuje minimální provozní napětí celého přípravku. Použitý typ vyhovuje napětí od 4,5V. Jestliže by byla potřeba mít nižší napětí, musel by se použít jiný tranzistor s nižším minimálním napětím. Modulační zátěž má převážně odporový charakter. Velikost lze regulovat zapojeným trimrem. Pro ladící účely a odposlech terminálu se v zapojení počítá s připojením sériového rozhraní. Nesmí se zapomenout na nutnost úpravy napěťové úrovně podle zvoleného připojeného zařízení. Samozřejmě může být použita bezdrátová technologie, jakou je např. bluetooth. Ta totiž hodně usnadní použití v terénu. Pro snazší ovládání je obvod automatického resetu doplněn při změně úrovně řídícího signálu DTR, který využívá mj. vnitřní komparátor s řízenou inverzí výstupu. Taktování procesoru je odvozeno od frekvence zvoleného krystalu. [17]

3.2 Oživení

Trimr R13 nastavíme na hodnotu přibližně 100Ω. Po přivedení napájení (4,5-6V) a nastavení DTR na hodnotu „H“ přiblížíme anténu ke čtečce, která generuje pouze základní nosnou (to se dá ověřit pomocí magnetické sondy). Následně nastavíme anténní laditelný kondenzátor tak, aby na výstupu detektoru AM (C1, R2) bylo maximální možné stejnosměrné napětí. Nyní je anténa naladěna. Tou se ještě dá zahýbat v poli, z důvodu zjištění hraničních vzdáleností. Dostatečnou sílu signálu zobrazuje rozsvěcováním LED dioda, která je připojena přes ochranný rezistor na RB7 (pokud se nachází v poli- svítí pokud ne, LED dioda je zhasnutá). V téhle fázi se může vyzkoušet příkaz výběru (select). Jestliže vše funguje tak jak má (správně), tak PicNic odpoví číslem, které čtečka předá. V opačném případě zkusíme měnit vzdálenost antény vůči čtečce v hodnotě max +-1cm. Pokud tohle nepomůže, což by ve většině případů mělo, musí se provést hlubší diagnostika. Nejprve je vhodné nastavit DTR=L a vyzkoušet, zda přípravek dekóduje a po sériové lince vysílá správně příkazy čtečky. Pokud tomu tak není, může být na vině příliš velká jakost antény, případně chyba v zapojení detektoru a komparátoru. Proměřením obvodu součástky po součástce vyloučíme či upravíme odpor antény. Pokud nyní dekodér pracuje správně, nastavíme DTR = H a zjistíme, jaké hodnoty máme na modulátoru. V tomto případě je vhodné vyvést ladící vývod přímo ze čtečky. Celý přípravek je konstruován zejména pro čipy rodiny MiFare, bude vhodné orientovat se na čtečku v tomto prostředí obvyklým komunikačním čipem MF RC531 či nověji pinově i instrukčně zpětně kompatibilnímu CL RC632. Dokumentace je bohužel neveřejná, avšak při troše snahy ji lze na internetu sehnat. Konkrétně potřebujeme vyvést piny AUX, MFOUT a zem AVSS. Kromě toho, že čip je snadno přístupný, je zásadní výhodou, že programové rozhraní čtečky transparentně zpřístupňuje všechny registry RC531.

Možnost jejich zápisu/čtení nabízí dokonce i menu demonstrační aplikace, která je součástí vývojového kitu. Nastavením registru 0x3A na hodnotu 0x04 přivedeme na vývod AUX demodulovanou základní nosnou, čili analogový signál pomocné nosné od PicNicu, jak ho vidí čtečka (fáze I, hodnota 0x05 je pro fázi Q). Dále nastavíme registr 0x26 na hodnotu 0x04 čímž na pinu MFOUT získáme obraz pomocné nosné po jejím reformování a digitalizaci. Porovnáním průběhů obou signálů snadno odhalíme chyby a nastavení našeho modulátoru. Průběh na AUX ukazuje, zda čtečka vůbec PicNic „slyší“ zatímco MFOUT ukazuje, zda mu také „rozumí“. Kromě nízké úrovně signálu působí potíže i přebuzení. Při přebuzení obvykle pomůže oddálení antén, někdy je nutné sáhnout k zatlumení zvýšením hodnoty R13. Je vhodné myslet i na malou šířku pásma antény, která se při příjmu dat nemusela projevit, pak pomůže zvýšení odporu antény. [17]

4 NÁVRH LABORATORNÍ ÚLOHY

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ	Předmět BDAK	
	Ročník 2	Studijní skupina B-TLI
Číslo úlohy X	Název úlohy **Demonstrace útoku na RFID**	

Zadání

1. Seznamte se s obsluhou přístrojů, v případě jakýchkoli nejasností si projděte přiložené návody (nachází se na pracovišti) nebo kontaktujte vyučujícího.
2. Před samotným měřením si pročtěte úvod.
3. Demonstrujte zranitelnost aplikace založené na UID.
4. Výsledky měření zpracujte do protokolu.

Úvod

Radio Frequency Identification, bezdrátová identifikace na rádiové frekvenci pomocí paměťových čipů = tagů. V dnešní době mohutně rozvíjející se možnost identifikace zboží, převážně pomocí čárových kódů. Technologii lze používat v široké škále odvětví, kde je zapotřebí rychlost a přesnost zpracovávaných informací. Každý tag (též nosič dat či transpordér) se skládá z čipu, antény a případně baterie a ke své funkci nepotřebuje přímou viditelnost se snímačem. Dále, každý čip má své identifikační číslo, to může být za určitých podmínek jedinečné a je stálé po celou dobu životnosti tagu.

Čipy můžeme rozdělit podle toho, jakým způsobem mezi sebou komunikují, nebo podle použité paměti. **Pasivní**- tím, že je přiložíme do pole čtečky se nabije napájecí kondenzátor a karta odešle svou identifikaci. **Aktivní**- mají vlastní zdroj energie, sami vysílají, životnost max 5let, omezená odolnost

Identifikace tagů: Každý čip má své EPC (electronic product kode), 96 bitové unikátní číslo. Některé čipy mohou mít kromě svého jedinečného čísla ještě dodatečnou paměť, kam lze ukládat i jiné další informace.

Čipy se vyrábí s různou frekvencí nosné, ta je závislá na maximálním dosahu vysílaného pulsu a zároveň s tím souvisí odolnost vůči rušivým odrazům. Na výběr jsou pásma LF, HF, UHF a MW. S vyšší frekvencí stoupá dosah, komunikační rychlost, klesá odolnost.

RFID jakožto nástupce čárového kódu umožňuje zapsat/získat více informací do/o daném zboží. Bezkontaktní kontrola, díky které jsme schopni registrovat stovky, až tisíce kusů výrobků ve zlomku krátkého časového intervalu, namísto vyskládání každého kusu na běžící pás. Místo toho by stačilo projet košem plným nakoupeného zboží okolím snímače a zbývalo by pouze

zaplatit. Obdobného zjednodušení by docílili i skladníci ve firmách. Další výhodou by byla přesná konkretizace každého výrobku. Nezjistili bychom pouze typ zboží, ale měli bychom k dispozici informace třeba o výrobním čísle výrobku nebo o jeho manipulaci od vyskladnění z výrobny, aj. Do budoucna se počítá, že budeme moci zapsat do jednoho tagu až tisíc informací. Základním problémem je cena čipu. Ta ani v blízké době nepřiblíží ceně čárového kódu.

Snímač neboli čtečka RFID je zařízení, které dokáže vysílat/přijímat data od tagů. Čtečka musí být schopna zpracovat paralelně velké množství požadavků. Musí být přes nějaké rozhraní spojena s databází výrobků a zboží, vhodné je použití nějaké bezdrátové technologie (Wi-Fi, Bluetooth).

Příklad čtečky karet

Jestliže byla zmíněna čtečka, je potřeba mít i nějaké čtené zařízení, tedy **čipovou kartu**. Integrovaný obvod umístěný nejčastěji v plastovém pouzdře. Každá čipová karta má vevnitř implementován integrovaný obvod, ve kterém je mikropočítač s koprocesorem, dále musí mít paměť (ať už RAM, ROM nebo EEPROM) a určitý software, uložený v paměti. Předností pro využití smart karet tkví v tom, že umožňují nejen ukládání dat, ale i zpracování informací, jejž si vymění čtečka s pamětí.

Bezkontaktní karta

Hlavním nedostatkem celé technologie je **zabezpečení** jednak přístupových operací a jednak přenosu dat.

Prvním problémem může být (ne)úmyslné deaktivování čipu při koupi zboží. Do ruky se jim totiž dostává naprosto bezkonkurenční marketingový nástroj: dokážou sledovat, co který člověk nakupuje, a následně mířit cílenou reklamu na danou osobu.

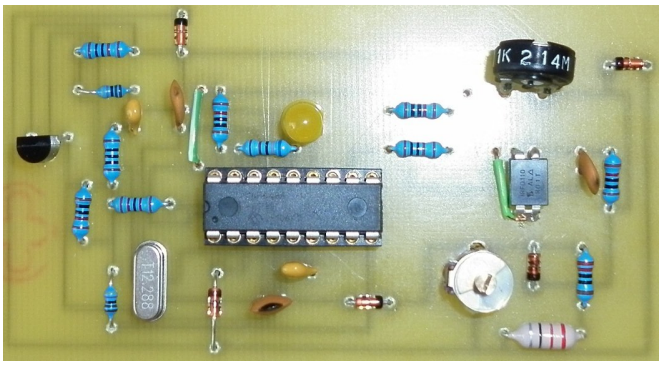
Další problém spojený s RFID je nezabezpečená komunikace mezi čipem a čtečkou. Pro snížení pořizovacích nákladů na tagy je komunikace čtečky a čipu založena na prostém systému dotaz-odpověď. Objevily se již čipy s šifrováním. Čtečka vyšle signál, čip odpovědí signalizuje svou přítomnost a dohodnou si způsob šifrování. Dále je již veškerá komunikace šifrovaná. Ovšem

tyto „nadstandardy“ zvyšují spotřebu energie a rychlost zpracování a rovněž i složitost jednotlivých čipů, což zvyšuje jejich cenu.

Je třeba zmínit i možnost hackerských útoků na systémy RFID. Tyto útoky využívají slabiny v systémech, kde je technika RFID používána. Dosud se počítalo pouze s tím, že čtečka přečte čip a zanese data do systému. Nikdo ovšem nepředpokládal, že se od „infikovaného“ čipu může nakazit celý systém. Pracuje tak, že nakažený čip využije slabá místa softwaru, který ovládá čtečku, a následně virus zanese z čipu do systému. Potom je možné, aby se virem nakazily i další čtené čipy. Stačí, aby útočník koupil v supermarketu kečup s tagem RFID, ten doma nahradil svým tagem, do kterého naprogramoval virus, a šel znovu do stejného supermarketu tag načíst.

Bezpečnost karet: špičku představují PKI (Public Key Infrastructure - Infrastruktura veřejného klíče) čipové karty. Tyto čipové karty jsou schopny ve svém koprocesoru generovat šifrovací klíčové páry a provádět s nimi veškeré požadované operace, a tak privátní klíč nikdy neopustí tuto kartu a není možné jej odchytit (odposlechnout) cestou po síti nebo v PC. Čipové karty poskytují dvou-faktorovou bezpečnost: něco, co máte (čipová karta) a něco, co znáte (heslo - PIN). Nikdo se nemůže dostat k Vašim důvěryhodným informacím, aniž by měl Vaši kartu a současně znal heslo. Vaše digitální certifikáty jsou mnohem lépe chráněné na PKI čipové kartě než na harddisku Vašeho počítače, na disketě nebo na obyčejné paměťové čipové kartě (telefonická karta apod.). Čipové karty navíc umožňují rozšíření o další bezpečnostní prvky, jako jsou magnetické proužky, bezkontaktní čipy, natištěné informace (fotografie, jméno, identifikační číslo, čárový kód, apod.).

Získání přístupových klíčů: každá RFID čtečka, která přistupuje k jednotlivým blokům, musí mít nastavený správný přístupový klíč. Samotný klíč zabezpečí, že čtečka má k danému sektoru povolený přesně definovaný přístup (čtení, zápis, inkrementace, dekrementace).



Jednoduché zařízení, pomocí kterého lze vytvořit duplikát karty

Pomocí RFID čtečky s přednastaveným klíčem

Pokud je k dispozici dostupná veřejná RFID čtečka (terminál) s přednastaveným klíčem, je možné získat klíč odposlechem a prolomením zachycené komunikace mezi samotnou kartou a čtečkou. Na vytvoření klonu je ale nevyhnutné získat všechny klíče ke všem sektorům karty.

Získání klíčů „offline“ útokem na samotnou kartu

Mifare Classic karty obsahují množství různých bezpečnostních zranitelností, které umožňují realizovat kompletní „offline“ útok bez potřeby legitimní RFID čtečky s přednastavenými klíči. Na demonstraci závažnosti zranitelností Mifare Classic karet byl vytvořen a veřejně publikován „offline nested“ útok, pomocí kterého je možné jen útokem na samotnou kartu (bez potřeby legitimní RFID čtečky) získat všechny klíče pro všechny sektory karty. Jediná podmínka na to,

aby bylo možné útok úspěšně realizovat a získat všechny klíče je, aby samotná karta obsahovala minimálně jeden sektor šifrovaný „default“ klíčem anebo tento klíč byl dopředu známý.

Zneužití čipových karet: Znalost klíčů získaných buď odposlechem a prolomením komunikace mezi kartou a legitimní RFID čtečkou anebo „offline nested“ útokem umožňuje realizovat nad kartou následující druhy útoků:

- možnost danou kartu kompletně načíst (v případě fyzické blízkosti cestujících ve veřejných dopravních prostředcích je možné získat kompletní kopii čipové karty libovolného cestujícího, to znamená všechny informace o něm uložených na kartě.
- možnost modifikovat libovolný sektor na kartě (kromě nultého „read-only“sektoru.
- možnost vytvořit klonu karty

Jak zabezpečit: nejlepším způsobem, jak karty MiFare classic zabezpečit je, vyměnit ty dosavadní za nové karty s jiným čipem. Ovšem z důvodu jejich celosvětové užívanosti nelze s tímhle razantním krokem počítat. Proto se spíš rozmáhá kompromis mezi kvalitou zabezpečení (ani ta nejlepší možnost zabezpečení není nepřekonatelná) a jednoduchostí útoku. Identitu každého uživatele karty se proto doporučuje spojit s „read only“ unikátním identifikátorem karty (UID), což představuje sériové číslo karty, které je zatím nemodifikovatelné. Aby toto svázání bylo účinné, je nutné při samotné kontrole ověřovat, či dané UID je v systému už zanesené a teda systém danou kartu pozná nebo jde o naklonovanou kartu. Další možnost je samotné UID karty použít při vytváření digitálního podpisu karty a ověřovat ho při každé kontrole karty. Je třeba podotknout, že svázání identity uživatele s UID sériovým číslem jeho karty zabrání jen případným laciným klonům, neznemožní ale útočníkovi modifikaci. Digitální podpisy pomocí asymetrické kryptografie výrazně znemožňují modifikovat obsah čipové karty. Bohužel to ale neznamená, že karta je dokonale chráněná - v případě, že daná karta obsahuje „kredit“ v jakékoli formě, útočník dokáže při nabitém stavu získat její kompletní kopii, kartu použít a opětovně uvedenou kopii obnovit.

Pracovní postup

1. Zapněte počítač a přihlaste se jako uživatel *bdak*, heslo je *bdak*.
2. Zkontrolujte správnost zapojení úlohy (všechny konektory jsou připojené, studenti během měření nic nnemění), pokud tomu tak není, zavolejte vyučujícího.
3. Pokud jste doposud neučinili, přečtěte si úvod, ten slouží k seznámení technologie RFID a k pochopení smyslu celé laboratorní úlohy.
4. Spusťte program Fake UID, zástupce najdete na ploše.
5. Zapněte ostatní přístroje na pracovišti, pokud jste tak doposud neučinili. Nyní by měl být na osciloskopu zobrazen harmonický signál o frekvenci 13.56MHz. Pokud mají osy zvolené nevhodné měřítko, zmáčkněte na osciloskopu AUTOSCALE.
6. Vezměte kartu označenou VZOR a přibližte ji ke čtečce. Pokud je karta v dostatečně silném poli, na emulátoru se rozsvítí LED dioda. Přípravek je nyní v režimu odposlechu, takže načtený průběh je zobrazen na osciloskopu a periodicky se opakuje.
7. Zmáčkněte *stop* tlačítko na osciloskopu, změňte nastavení os, abyste viděli 1 periodu vysílaných dat. Data jsou zároveň odeslána do počítače. Paměť karty se člení do 16B

bloků a ty dále do sektorů. Blok 0 sektoru 0 má speciální význam, obsahuje pevné údaje výrobce, mimo jiní 4B sériové číslo karty, které nás pro výrobu duplikátu zajímá (přístup je chráněn pouze pomocí UID). Ostatní datové bloky jsou volně k dispozici. Jelikož karta vysílá data ne moc silně, mohl by být problém načíst data správně. Na (ne)štěstí ono sériové číslo vystupuje zároveň jako identifikátor karty během tzv. antikorozní procedury, která je povinná a s níž si terminál z mnoha možných čipů v dosahu vybírá, s kým chce komunikovat. Podle ISO 14443-A jej musí minimálně jednou (silně) zopakovat. Tím jsme bez problémů získali odposlechem bezchybně rozpoznatelné námi požadované UID, můžete se přesvědčit na zobrazovaném průběhu. Samotné UID je zobrazeno v okně programu na počítači.

8. Nahraďte kartu v poli přípravku za druhou, označenou DUPLIKÁT.
9. Nyní v programu přepněte na zápis dat do duplikátu. Obslužný program přepnul zařízení do módu emulátor, tedy vysílá data do paměti karty. Jakmile kartu z pole vyjmete, dojde zpět k přepnutí do režimu odposlechu.
10. Protože vzorová karta měla udělený přístup do laboratoře, vezměte duplikovanou kartu, přiložte ji ke čtečce u dveří a pokud se vám uvolní zámek k jejímu otevření, máte vytvořenou kopii přístupové karty.
11. Na konci měření duplikovanou kartu znovu vložte do pole emulátoru a pomocí obslužného prográmku jí vymažte paměť.

    Jak jste si jistě všimli, nepotřebujete znát význam jednotlivých bitů, abychom byli schopni vytvořit kopii karty, vystačíme s tím, že víme, co se přenáší v příslušných blocích. Pokud je přístup založen na „jen UID“ není problém s volně dostupným softwarem i schématem pro výrobu emulátoru vytvořit tento zajímavý nástroj, jehož meze využití záleží čistě na uživateli.

ZÁVĚR

V bakalářské práci byla nastudována teorie o problematice RFID technologie, rozdělení podle druhu čipů a dále podle frekvence, na které komunikují. Dále teorie o smart kartách a bezpečnosti při komunikaci bezkontaktní karty se snímačem v oblasti rádiových frekvencí. Byly popsány oblasti využitelnosti čipových karet založených na RFID a porovnání s čárovými kódy. Z doporučené literatury bylo použito schéma k výrobě emulátoru. Během praktické části byl vypracován návrh v programu Eagle, rozvržení na DPS a jeho osazení. Při konstrukci se vyskytl problém, který se po důkladnější analýze podařilo odstranit. Funkční emulátor je určen pro studenty druhých ročníků, navštěvujících laboratoře předmětu datové komunikace (BDAK). Posledním cílem, který se podařilo splnit, bylo vytvoření laboratorní úlohy, která pomocí emulátoru demonstruje útok na bezkontaktní kartu a vytvoří její duplikát. Předností emulátoru PicNic je, že zpřístupňuje praktické experimenty s emulací čipů RFID v pásmu KV co nejširší komunitě zájemců. Komerčně dostupné emulátory jsou několikánásobně finančně náročnější, než PicNic, který je možno vyrobit řádově za stovky korun.

5 POUŽITÁ LITERATURA

[1] DOČEKAL, Daniel. *Http://www.pooh.cz* [online]. 29.9.2004 [cit. 2010-11-25]. RFID aneb Svět ve kterém víte všechno o všech a všem. Dostupné z WWW: <http://www.pooh.cz/pooh/a.asp?a=2010731>.

[2] HOUSER, Pavel. *Http://securityworld.cz* [online]. 20.3.2008 [cit. 2010-11-16]. RFID čip MiFare může být terčem útoku. Dostupné z WWW: <http://securityworld.cz/securityworld/rfid-cip-mifare-muze-byt-tercem-utoku-725>.

[3] *Http://cs.wikipedia.org* [online]. 6.11.2010 [cit. 2010-12-6]. RFID. Dostupné z WWW: <http://cs.wikipedia.org/wiki/RFID>.

[4] *Http://cs.wikipedia.org* [online]. 23.11.2010 [cit. 2010-12-10]. SIM karta. Dostupné z WWW: http://cs.wikipedia.org/wiki/SIM_karta.

[5] *Http://cs.wikipedia.org* [online]. 2010-10-21 [cit. 2010-12-2]. Čipová karta. Dostupné z WWW: http://cs.wikipedia.org/wiki/%C4%8Cipov%C3%A1_karta.

[6] *Http://en.wikipedia.org* [online]. listopad 2010 [cit. 2010-12-01]. Smart card. Dostupné z WWW: http://en.wikipedia.org/wiki/Smart_card.

[7] *Http://www.itbiz.cz* [online]. 11.12.2007 [cit. 2010-12-4]. Mýty a pověry o bezpečnosti technologie RFID. Dostupné z WWW: http://www.itbiz.cz/rfid-bezpecnost.

[8] *Http://www.nethemba.com* [online]. 25.10.2009 [cit. 2010-12-06]. Bezpečnostná analýza zraniteľností slovenských a českých čipových RFID kariet založených na technológii Mifare Classic. Dostupné z WWW: http://www.nethemba.com/mifare-classic-zranitelnosti.pdf.

[9] *Http://www.odbornecasopisy.cz* [online]. červenec 2009 [cit. 2010-12-5]. RFID z pohledu bezpečnosti. Dostupné z WWW: <http://www.odbornecasopisy.cz/index.php?id_document=39331>.

[10] *Http://www.pvccard.cz* [online]. 2010 [cit. 2010-12-09]. Smart karty. Dostupné z WWW: http://www.pvccard.cz/smart-karty/.

[11] *Http://www.smartcard.cz* [online]. 2010 [cit. 2010-12-02]. Čipové karty. Dostupné z WWW: http://www.smartcard.cz/cards.html.

[12] *Http://www.tsoft.cz* [online]. 2010 [cit. 2010-12-04]. Bezkontaktníkarty. Dostupné z WWW: <http://www.tsoft.cz/sites/default/files/download/Bezntaktni_karty_0.pdf>.

[13] *Http://www.tsoft.cz* [online]. 2009 [cit. 2010-12-5]. Kontaktníkarty. Dostupné z WWW: <http://www.tsoft.cz/sites/default/files/download/Kontaktni_karty_0.pdf>.

[14] *Http://www.tsoft.cz* [online]. 2010 [cit. 2010-12-04]. Smart karty - čipové karty. Dostupné z WWW: <http://www.tsoft.cz/smart-karty-cipove-karty>

[15] PŘIBYL, Tomáš. *Http://www.ictsecurity.cz* [online]. 2010 [cit. 2010-12-10]. RFID z hlediska bezpečnosti. Dostupné z WWW: http://www.ictsecurity.cz/sk/09/01-eps+ezs-/-dohledove-systemy-pco-ip-kamery/rfid-z-hlediska-bezpecnosti.html.

[16] ROSA, Tomáš; KLÍMA, Vlastimil . *Http://crypto.hyperlink.cz* [online]. leden 2008 [cit. 2010-11-26]. Bezpečněji s MIFARE. Dostupné z WWW: http://crypto.hyperlink.cz/files/ST_2008_01_x_x.pdf.

[17] ROSA, Tomáš; KLÍMA, Vlastimil. *Http://crypto.hyperlink.cz* [online]. leden 2009 [cit. 2010-10-25]. PicNic pro RFID-KV. Dostupné z WWW: <http://crypto.hyperlink.cz/files/ST_2009_01_12_13.pdf>.

[18] ROSA, Tomáš; KLÍMA, Vlastimil. *Http://crypto.hyperlink.cz* [online]. únor 2007 [cit. 2010-12-07]. Bezkontaktní karty MIFARE. Dostupné z WWW: <http://crypto.hyperlink.cz/files/ST_2007_02_x_x.pdf>