Jihočeská univerzita v Českých Budějovicích

Přírodovědecká fakulta

Pokročilá analýza zranitelnosti bezkontaktních transakcí

Bakalářská práce

Jakub Škornička

Vedoucí práce: Ing. Rudolf Vohnout, Ph.D.

České Budějovice 2016

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

ZADÁVACÍ PROTOKOL BAKALÁŘSKÉ PRÁCE

Student: Jakub ŠKORNIČKA
(jméno, příjmení, tituly)

Obor – zaměření studia: Aplikovaná Informatika – Design web aplikací

Katedra: Ústav aplikované informatiky

Školitel: Rudolf Vohnout, Ing., Ph.D.
(jméno, příjmení, tituly, u externího š. název a adresa pracoviště, telefon, fax, e-mail)

Garant z PřF:
.....
(jméno, příjmení, tituly, katedra – jen v případě externího školitele)

Školitel – specialista, konzultant: Jan Doubek, MBA, 603 800 446, Husitská 73/76 Krupka
(jméno, příjmení, tituly, u externího š. název a adresa pracoviště, telefon, fax, e-mail)

Téma bakalářské práce:

Pokročilá analýza zranitelnosti bezkontaktních transakcí

Cíle práce:

Hlavní cíl:

- Otestovat bezpečnost přenosu informací prováděných na krátkou vzdálenost s využitím technologii NFC.

Popis práce:

Práce si klade za cíl analyzovat všechny bezpečnostní aspekty bezkontaktních transakcí, které jsou v poslední době v ČR velmi populární.

Základní doporučená literatura :

GOMZIN Slava: *Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions 1st Edition*. Wiley; 1 edition (February 17, 2014). 312 stran. ISBN: 978-1118810118

Bibliografické údaje

Škornička Jakub, 2016: Pokročilá analýza zranitelnosti bezkontaktních transakcí. [Advanced analysis of the vulnerability of contactless transactions. Bc. Thesis, in Czech.] – 48 p. Faculty of Science, University of South Bohemia, České Budějovice, Czech Republic.

Anotace

Tato bakalářská práce se zabývá testováním bezpečnosti bezkontaktních transakcí a následným vyhodnocení získaných výsledků. Další náplní práce je zhodnocení, srovnání a prozkoumání dnes již známých útoků, včetně možnosti zabezpečení a prevencí před nimi.

In english

This bachelor thesis is dealing with testing of security of contactless transfer, including evaluation of acquired results. Another part of this thesis is evaluation, comparison and examination of attacks that are already well known today, including ways to secure against them and their prevention.

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích, dne 14.prosince 2016

Podpis: _____

Poděkování

Rád bych poděkoval panu Ing. Rudolfu Vohnoutovi, Ph.D. za ochotu, trpělivost a odborné konzultace při vedení mé bakalářské práce. Mé díky taktéž patří panu Ing. Petru Břehovskému za odborné konzultace a trpělivost. Dále bych rád zmínil Radioklub Písek a jejich maximální vstřícnost a pomoc při spolupráci především na praktické části mé práce. Neposlední díky náleží mé rodině, přátelům a kamarádům za podporu a pevné nervy.

Obsah

1. Úvod

V současné době si můžeme povšimnout pozvolného nárůstu technologií i v běžném životě. V tomto ohledu začíná být bezkontaktní technologie nepostradatelnou součástí života většiny z nás, a to hlavně díky úspoře financí a zvýšení komfortu, které s sebou tato technologie přináší. Využívat se začíná především pro platební účely z důvodu možnosti platby tímto bezkontaktním přenosem téměř kdekoliv (od obchodů až po automaty na kávu). Mimo jiné můžeme tento trend zvyšování používání bezkontaktní technologie vypozorovat i na bankovním trhu.

Technologie zodpovědné za možnost využívání bezkontaktního světa jsou založeny na RFID a NFC technologii. Jen hrstka lidí tuší, jak často využívají právě RFID technologii. Tato technologie slouží v podstatě k přenosu a ukládání dat pomocí elektromagnetických vln, a je využita například u dálkových ovladačů, ale i u zabezpečení aut. Další, dnes již hojně rozšířená technologie, je NFC (Near Field Communication), která vychází z již zmíněné technologie RFID. Stručně lze NFC definovat jako technologii umožňující bezdrátovou komunikaci mezi dvěma zařízeními na velmi krátkou vzdálenost.

Hlavní, a tím i nejvíce rozšířenou rizikovou oblastí, je využití těchto technologií v oblasti plateb. Jelikož se klienti v průběhu let stávají náročnějšími, jsou banky nuceny neustále vyvíjet technologie modernější, což způsobuje vznik nových a nových rizik, ať už z důvodu toho, že se potencionální útočníci snaží udržet krok, tak i díky lidské neopatrnosti a neznalosti.

Proto je třeba si položit otázku ohledně bezpečnosti těchto technologií. Cíl mé práce spočívá v prozkoumání zabezpečení této technologie především z praktické stránky. Přece jen, jak již bylo zmíněno, je to dnes a denně využívaná technologie milionem lidí, což ji předurčuje k tomu, být diskutovatelným odvětvím v budoucnosti.

1.1. Motivace

Ověřit vlastnosti, díky kterým je bezkontaktní technologie jednou z nejrozšířenějších technologií na světě. Tato práce vychází z nastudování v praxi tolik rozšířené technologie, což je také vysoce přínosné pro budoucí uplatnění na trhu práce.

Popularita bezkontaktních transakcí neustále stoupá. Hlavně z důvodů úspory financí a času se dá jistě říct, že tento trend bude růst čím dál rychleji. Přeci jen se bezkontaktní platební karty začaly u nás nabízet již v červnu roku 2011 a dnes tuto technologii nevyužívá jen hrstka z nás. Platit bezkontaktně lze dnes téměř všude – například i v Městské hromadné dopravě. Takto rostoucí tendence je obrovskou motivací pro zájem o tuto oblast.

Otestovat bezpečnost těchto transakcí je opravdu důležité. Z důvodu rozšíření této technologie totiž stoupá i riziko zneužití citlivých informací poskytovaných bezkontaktně. Výsledky mého testování by mohly mít vliv na všední životy spousty lidí. Většina z nich si není vědoma rizik spojených s použitím této poměrně nové technologie, popřípadě je ignorují. Avšak pouze do té doby, než se sami stanou obětí.

1.2. Cíle

a) Hlavní cíl

- Otestovat bezpečnost přenosu informací na krátkou vzdálenost pomocí NFC => Fyzicky nasimulovat reálné útoky, které je eventuální útočník schopen zneužít.

b) Dílčí cíle

- Rozebrat jednotlivá rizika bezkontaktního světa => Prozkoumat dnes již známé hrozby, seznámit se s nimi a nahlédnout do potencionálních chyb této technologie.

- Prozkoumat principy zabezpečení technologií využitých při bezkontaktních transakcích => Prozkoumat bezpečnostní prvky použitých v těchto technologiích. Seznámit se s obranou a prevencí na tyto útoky.

- Shrnout výsledky získané při testování bezpečnosti přenosu => Sepsat jednotlivé kroky při simulaci útoků a na základě úspěchu vyvodit závěr ohledně problematiky s bezkontaktní technologií.

1.3. Struktura

Tato práce se zabývá detailním rozborem technologií využívajících bezkontaktní transakce.

Při samotném testování je kladen velký důraz na bezpečnost přenosu informací prováděných na krátkou vzdálenost za pomocí NFC technologie.

Úvodní kapitola stručně uvádí čtenáře do problematiky a předkládá motivaci autora ke zvolení tohoto tématu. Také rekapituluje cíle této práce.

Druhá kapitola je teoretická. Jsou zde popsány bezkontaktní technologie, jejich vývoj a důvod masivního využití. Není zde samozřejmě vynechaná ani stručná legislativa, historie a představení pojmů.

Třetí kapitola popisuje řešení problematiky z pohledu metodiky vývoje, seznámení s jednotlivými útoky, ale i současný stav problematiky. Také popisuje požadavky na vývoj a představení silných i slabých stránek této technologie. Nechybí rozbor jednotlivého zabezpečení a ochrany včetně principů a důvodu jeho zavedení.

Čtvrtá kapitola je implementační. Jejím obsahem je rozbor testovaných subjektů, popis simulace jednotlivých kritických momentů a získání jakýchkoliv zneužitelných informací. Kapitola je zakončena porovnáním mnou zkoušených bezpečnostních složek.

Poslední kapitolou je závěr. V závěru jsou v bodech shrnuty a zhodnoceny splněné cíle mé práce. Pod touto kapitolou je náhled do budoucnosti ochrany a celkového vývoje bezkontaktních transakcí.

2. Bezkontaktní technologie

2.1.Metodika vývoje

Bezkontaktní technologii můžeme rozdělit do 3 kategorií: optickou (světlo), rádiovou a sonickou (zvuk). Tato technologie je nedílnou součástí výrobních procesů. Vzdálenost mezi jednotlivými body se může pohybovat od několika centimetrů (NFC) až po milióny kilometrů (družice). Za oficiálního vynálezce bezdrátové technologie můžeme považovat pana Nikola Teslu, avšak první, kdo přenesl signál na delší vzdálenost (přes 1,8km) byl pan Guglielmo Marconi. Pokud půjdeme hluboko do minulosti, některé zdroje uvádějí jako jeden z prvních způsobů bezkontaktní technologie dokonce kouřové signály starých indiánů.

2.2.RFID technologie

RFID technologie je moderní způsob identifikace jednotlivých objektů za pomoci radiofrekvenčních vln. RFID (rádio-frekvenční identifikace) čipy

dokáží poskytovat a ukládat informace v reálném čase. RFID čipy se dají rozdělit do dvou kategorií, na pasivní a aktivní. Pasivní fungují na principu chvilkového nabití kondenzátoru z elektromagnetických impulzů, vysílaných z blízkého vysílače či čtečky, a následného vyslání informace zpět do čtečky. Aktivní se liší v tom, že v sobě obsahují zdroj, tudíž jsou nákladnější a dnes jsou pomalu nahrazovány technologií NFC. Díky nízkým nákladům na čip je RFID dnes hojně využíván v nejrůznějších odvětvích, kde je důležitým faktorem rychlé a přesné zpracování informace a okamžitý přenos dat, která jsou dále zpracovávána. Dnes se s RFID nejčastěji setkáme v obchodech, v průmyslu a dokonce i u identifikování zvířat.
První čip byl vytvořen roku 1973 v USA a první patent na něj získal o 10 let později Charles Walton. Po roce 1980 se začal masově využívat a to především do bezkontaktních vstupních karet.

2.3.NFC techn ologie

Jedná se o bezkontaktní komunikaci mezi dvěma zařízeními na poměrně krátkou vzdálenost (v jednotkách centimetrů). NFC používají 3 základní rychlosti přenosu dat – 106 kbps, 212 kbps a 424 kbps. NFC (Near Field Communication) je nástupce RFID čipu a má toho s ním mnoho společného. Momentálně je tato technologie stále více žádaná hlavně z pohledu finančního, ale i z hlediska mobilních telefonů. V průběhu několika let ovlivní nárůst této technologie kompletně celý svět bezkontaktních plateb. Momentálně nejvíce využívaná je především na bezkontaktní platby, reklamu a kontrolu přístupu. Obrovská výhoda spočívá v tom, že na veškerou komunikaci pomocí NFC stačí pouze mobilní telefon podporující NFC technologii. Díky tomu se o toho odvětví zajímají nejen banky, ale i výrobci mobilních telefonů. NFC technologie je primárně navržena pro mobilní telefony, ale dnes se čip dá ukrýt například do prstýnku, hodinek nebo jako nejčastější provedení tzn. NFC tag.

Mezi hlavní důvody rozšíření technologie NFC určitě patří nenáročnost použití (stačí pouze dotyk), všestrannost (technologii lze použít v mnohých

odvětvích) a bezpečnost (nutnost spojení pouze na krátkou vzdálenost izoluje některé útoky na rozdíl od RFID).

2.3.1 Historie NFC

NFC technologie se začala vyvíjet roku 2002 spoluprací firem Sony a Philips jako bezpečná náhrada RFID čipu, který byl snadný terč pro odposlech. Také se již od začátku očekávalo jeho možné využití v mobilních telefonech.

V roce 2004 společnosti Sony, Philips a Nokia založili asociaci NFC Forum, která sdružuje společnosti zajímající se o NFC (dnes čítá přes 170 členů). Tato nezisková organizace vytváří standarty, podporuje rozvoj produktů podporující NFC a také propaguje NFC mezi veřejnost.

2.3.2 Normy

V roce 2003 byla NFC technologie schválena jako norma ISO/IEC. Necelý rok poté byla odsouhlasena také jako norma ECMA. Standardy ISO/IEC 18092 a ECMA-340 specifikují schémata modulace, kódování, přenosové rychlosti, formáty rámců radiofrekvenčního rozhraní, inicializační schémata, transportní protokol a metody výměny dat. NFC vychází z technologie RFID, tudíž je s nim zpětně kompatibilní díky tomu, že RFID zahrnuje normu ISO/EIC 14443, která je součástí normy ISO/EIC 18092.

2.3.3 Princip NFC technologie

Samotná komunikace probíhá na základě elektromagnetického pole, které zařízení vytváří ve svém okolí. Jakmile se v tomto pásmu objeví prvek fungující na stejné frekvenci, začnou komunikovat. Na rozdíl od RFID mohou NFC komunikovat oboustranně. NFC vychází z technologie RFID, tudíž je s ním zpětně kompatibilní. NFC technologie funguje jako Half-Duplex, což se dá

vysvětlit tak, že zařízení není schopné současně vysílat i přijímat data. NFC se stejně jako RFID dělí na aktivní a pasivní.
Přenos pomocí NFC může probíhat 3 režimy:

- Reader/writer
- Peer-to-peer
- Card emulation

Režim reader/writer

Tento režim se využívá pro čtení/zápis NFC tagů. Není zde vyžadováno vysoké zabezpečení (výjimku tvoří např. platební karty, kde je celý přenos zašifrován). NFC tag je v tomto případě napájen elektromagnetickým polem a maximální přenosová rychlost je zde 106 kbps.

Režim peer-to-peer

Umožňuje obousměrnou komunikaci mezi dvěma zařízeními. Obě zařízení musí být v aktivním režimu. Maximální přenosová rychlost je 424 kbps.

Režim Card emulation

Režim umožňuje, aby se aktivní NFC zařízení chovalo jako pasivní čip. Názorným příkladem můžeme uvést mobilní telefon, který se bude chovat jako forma autentizačního prvku nebo jako sms jízdenka.

2.3.4 Využití

Jak již bylo řečeno, NFC technologie nachází největší uplatnění při platebních transakcích. Není to však zdaleka jediné její využití. Dnes je již běžně využita celou řadou dopravců. Mezi prvními dopravci jsou Německé dráhy a služba „Touch and Travel“. Princip této služby je takový, že si uživatel

nainstaluje aplikaci, po nastoupení přiloží telefon k terminálu a při výstupu toto zopakuje. Tím se odešle zpráva o celkové cestě a vypočítá se cena.

Další rozšířené využití NFC našlo v identifikaci. Díky tomu nám může NFC nahradit celý svazek klíčů. Zajímavé využití je například při odemykání auta. S tímto trendem přišel na trh jako první Hyundai a prohlásil: „S touto technologií je Hyundai schopný využít všechny funkce dnešních smartphonů a přirozeně je integrovat do každodenního řízení auta. Díky neustálému vývoji technologií v autě si budou NFC čipy schopny zapamatovat například polohy sedadla a vnějších zrcátek, což nabídne zákazníkům pohodlné a individuální prostředí pro řízení.“ [1]

NFC aplikace dále můžeme propůjčit časově omezený klíč komukoliv a odkudkoliv. Představte si situaci, při které potřebujeme něco někomu zanechat, ale on není doma. Díky této technologii jsme schopni na dálku povolit například otevření kufru po dobu 5 minut.

NFC nám také slouží k usnadnění komunikace a navázání spojení. Pokud potřebujeme například použít headset, stačí nám pouze přiložit sluchátka k telefonu a již posloucháme. Dalším příkladem může být spolupráce telefonu s promítačem, kde opět stačí pouze přiložit telefon s čipem pro jednoduché zobrazení obrazu z telefonu do promítačky. Dnes se také hojně využívá pro nastavení budíku. Jednoduše si nalepíme NFC tag na noční stolek, pak už stačí pouze položit k němu telefon.

A v neposlední řadě NFC využívá dnes ve velké míře marketing. Jelikož se cena tagů neustále snižuje, tak se momentálně s NFC čipem setkáme například ve formě vizitek nebo ve věrnostních kartách či kuponech.

2.3.5 NFC Tag

NFC tag si lze představit jako velmi malou paměťovou kartu. Samotný tag obsahuje NFC čip a anténu. Anténa se nám stará o přenos energie a dat, kdežto čip řídí celou komunikaci a obsahuje paměť. Jelikož je kapacita značně omezena (cca 40-8000 bajtů), tak se dnes převážně využívají v osobních dokladech, vizitkách, vstupních kartách nebo jízdenkách.

Výhodou tohoto provedení je, že není potřeba nabíjení. Podobně jako RFID v sobě obsahuje kondenzátor, který se nám při přiblížení například mobilního telefonu pomocí elektromagnetické indukce sám nabije a odešle v sobě uložené informace. Nejčastěji se s NFC čipem můžeme setkat v podobě nálepky o rozměrech nepřesahující kostičku čokolády. Dnes je také velmi oblíbené provedení například v prstenu či hodinkách. Nyní je i možnost speciálních ochranných prvků, které nám dokáží komunikaci odstínit.

Je zřejmé, že na tagy budou klienti klást nejrůznější požadavky, ať už z pohledu kapacity nebo rychlosti přenosu dat, tak i velikosti a odolnosti. Odolnost je velmi důležitá, jelikož se spousta tagů ukládá do venkovních prostor. Z tohoto důvodu se klade velký důraz na odolnost vůči vlhkosti, mrazu, teplu a dokonce i vandalismu. Většina tagů se dříve nesměla umisťovat na kovový materiál kvůli možnosti rušení antény. I to je dnes již vyřešeno pomocí magnetické folie. Každý tag by měl být také patřičně označen například logem N-Mark nebo logem NFC fóra. Také proto NFC forum rozdělilo tagy do 4 kategorií:

	Typ 1	Typ 2	Typ 3	Typ 4
Norma	ISO IEC 14443 A	ISO IEC 14443 A	JIS X 6319-4	ISO IEC 14443 A/B
Produkty	Topaz	NXP MifareUltralight NXP NTAG203	Sony Felica	NXP DESFire NXP SmartMX-JCOP
Výrobce	Broadcom	NXP	Sony	Více výrobců
Kapacita	96 bytů	48 bytů/144 bytů	4 KB, 9 KB	4KB / 32KB
Rychlost přenosu	106 kbps	106 kbps	212 kbps 424 kbps	106kbps, 212 kbps, 424 kbps
Cena	nízká	nízká	vysoká	střední/vysoká

Tabulka 1 -Typy NFC tagů

2.4.NFC Data Exchange Format (NDEF)

NFC Data Exchange Format (dále už jen jako NDEF) zabaluje přenášená data mezi dvěma NFC zařízeními. Utváří jednotný formát, který podporují všechny NFC zařízení. Každý NDEF záznam obsahuje typ záznamu, unikátní ID, délku a data. Existují 4 základní typy NDEF zpráv: jednoduchý textový záznam, chytrý obrázek, jednotný identifikátor zdroje a podpis.

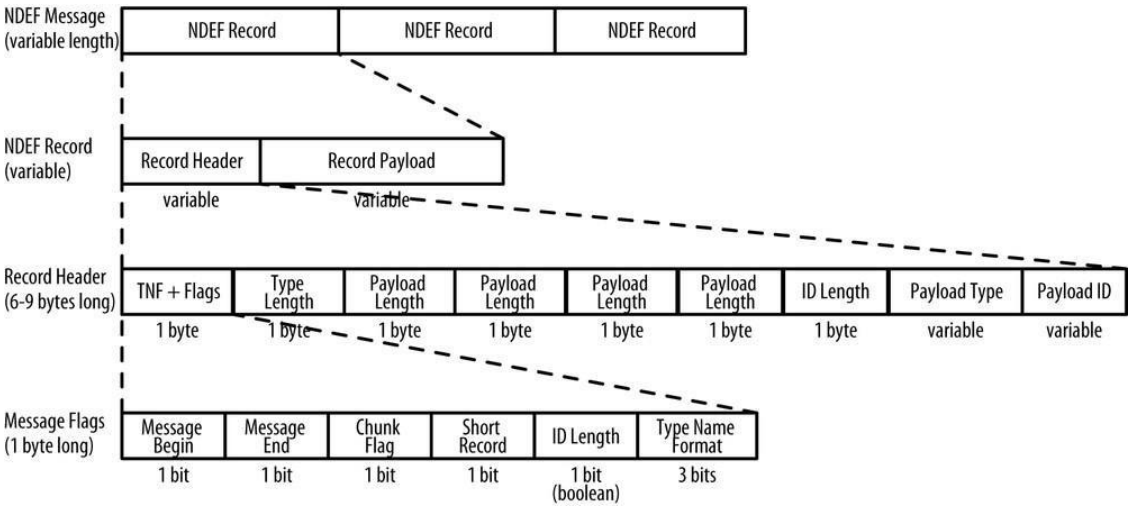
a) Jednoduchý textový záznam (Simple text record) – Tento typ obsahuje textový řetězec. Takovéto zprávy neobsahují informace pro cílové zařízení, jak se zprávou naložit.

b) Chytrý obrázek (smart poster) – Tento typ je nejčastěji využíván v oblasti marketingu. Je zde obsažen reálný obrázek, u kterého může být přiložen text či URI adresa.

c) Jednotný identifikátor zdroje (Uniform Resource Identifier – URI) – Jak už název napovídá, tak zde je uložen odkaz na webovou stránku. NDEF záznam by měl být schopný společně se zprávou tohoto typu předat i informace pro aplikaci, jak s takovou zprávou naložit (nejčastěji spuštění webového prohlížeče).

d) Podpis (Signature) – Zde jsou ukryta důvěrné informace o původu dat.

Každý NDEF záznam tvoří hlavička (zde je obsažen typ, délka atd…) a data (tzv. payload). Viz obrázek.



Obrázek 1 - Struktura NDEF, zdroj: IGOE TOM, Beginning NFC, str. 50

3. Bezpečnost a ochrana

3.1.Bezkontaktní platby

Bezkontaktní platba je metoda, která umožňuje platbu nejčastěji pomocí standartní debetní nebo kreditní karty, mobilním telefonem nebo jinak upraveným zařízení. Při samotném placení odpadá nutnost vložení karty do terminálu. Kartu pouze přiložíme na terminál a po pár sekundách dojde ke spárování. Po provedení tohoto úkonu jen počkáme na přijmutí/odmítnutí platby a odejdeme. Díky této metodě není vyžadován PIN do částky 500 Kč. Při placení vyšší částky než již zmiňovaných 500 Kč, lze také platit bezkontaktně, ale již je požadována identifikace pomocí PINu.

V roce 2006 představili společnosti MasterCard a VISA nové bezkontaktní čipové karty MasterCard PayPass a VISA payWave. PayPass a payWave jsou vzájemně hardwarově kompatibilní.

3.1.1 Bezkontaktní karta

Dnes je součástí většiny platebních karet tzv. dual-interface čip, jinými slovy čip, který umožňuje platit jak kontaktně, tak i bezkontaktně.

V ČR se bezkontaktní karty objevili začátkem roku 2011. Přišla s nimi Česká spořitelna. Zájem o ně stoupl tak rychle, že během jednoho roku tuto možnost poskytovala většina bank.

3.1.2 Bezkontaktní nálepka

Bezkontaktní nálepka neboli „sticker“ je vlastně malá platební karta. Díky své velikosti a technologii NFC je též hojně využívána. Nálepka funguje na

principu platební karty, lze s ní tedy platit na stejných terminálech. Díky NFC je tento způsob relativně nový. U nás se první nálepka dala pořídit až v roce 2013.

Obrázek 2- Bezkontaktní nálepka

3.1.3 Mobilní telefon

Možnost placení mobilním telefonem je díky NFC technologii dnes velmi rozsáhlá z důvodu pohodlnosti, především proto, že je dnes mobilní telefon nedílnou součástí snad každého z nás. Stačí mít mobilní telefon podporující NFC a připojení k internetu. Dnes je již možné nahrát všechny platební karty nezávisle na sebe.

3.1.4 MasterCard PayPass

Tato technologie nám umožňuje platit hlavně malé částky bez nutnosti vkládání PINu a vkládání karty do terminálu. Postup je následující: pokud je prodejce vybaven terminálem podporující danou službu, zákazník pouze přiloží kartu na vyznačené místo, počká pár sekund a po obdržení účtenky od obchodníka může odejít.

3.1.5 VISA PayWave

VISA PayWave je konkurenční produkt k MasterCard PayPass. Dalo by se říci, že VISA pouze obměnila dosud používanou technologii. Fungují na stejném principu a pro obě služby lze použít stejný terminál, je však třeba mít správný software.

Obrázek 3- Ukázka loga výše zmíněných operací.

3.2.Zabezpečení bezkontaktních plateb

Sama metoda MasterCard PayPass má zabezpečení několik. Mezi ty nejdůležitější určitě patří složitá šifrovací technologie, která poskytuje vysokou ochranu od nežádoucího nákupu. Další aspekt je výhoda neustálého kontaktu zákazníka s kartou. Také jí nemusí dávat do samotného terminálu a tím ulehčit případnému útočníkovi okopírovat kartu. A jako další aspekt ochrany je nutnost přiložení karty opravdu blízko ke čtečce, tudíž je opět ztížená možnost zneužití.

Karta má také hned několik bezpečnostních limitů. Pokud je použita několikrát po sobě k zaplacení, je vyžádáno zadaní PINu bez ohledu na zadanou částku. To slouží k zabránění zneužití odcizené karty. Tento limit nastavuje banka podle množství, hodnoty nebo náhodného prvku.

Bezpečnostní limity jako takové dělíme do 3 kategorii

a) Soft limit pro online terminály – Na kartě je nastaven limit pro počet transakcí i částku pro online terminály, kde se po překročení tohoto limitu další transakce zamítne.
b) Soft limit pro offline terminály – Na kartě je nastaven limit pro počet transakcí i částku pro offline terminály, kde po překročení tohoto limitu je další transakce zamítnuta.
c) Hard limit – Na kartě je nastaven obecný počet transakcí. Po překročení limitu další transakce zamítne.

3.3.Secure element

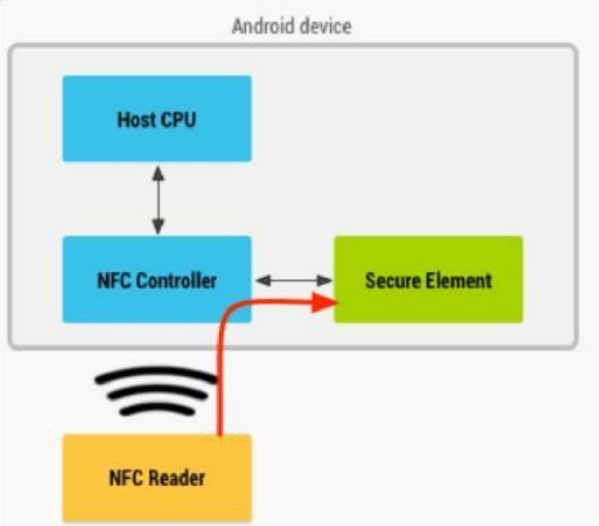
Spousta zařízení je vybaveno NFC čipem, ne vždy však i secure elementem. Secure element je nezávislý čip, který je mezi NFC čipem a infrastrukturou telefonu. Je to kombinace softwaru, hardwaru a protokolů. Slouží jako zabezpečené uložiště dat a ukládají se zde například platební údaje, věrnostní karty nebo MHD jízdenky. Veškerá důležitá data jsou ukládána šifrovaně a třízena do jakýchsi složek (aby nedocházelo například ke zjištění platebních údajů při použití NFC jízdenky). Secure element existuje ve 3 formách:

a) Sim karta (UICC) – Nejčastější řešení. Je nahrazena SIM kartou novou, která v sobě obsahuje secure element. Velká nevýhoda spočívá v tom, že SIM kartu vydává operátor a ten i řídí přístup do secure elementu. Výhoda této formy spočívá přenositelnosti (možnost přenést na jiný telefon bez nutnosti opětovného nahrání).

b) Integrovaný secure element přímo v telefonu – Již není možno čip se secure elementem vyjmout, tudíž zde není možnost přenositelnosti (každý další uživatel si musí element nastavit podle svých představ). Při této formě se k secure elementu může dostat každý.

c) Externí secure element – Nejméně používaný způsob. Výhodou je velká kapacita a přenositelnost. Využívá se zde například paměťových karet (microSD).

Unikátnost secure elementu spočívá v tom, že i když je telefon vybitý do takové míry, že nelze zapnout, tak máme stále dost energie na to, aby byl NFC čip i secure element stále použitelný.



Obrázek 4- Ukázka Secure elementu u Android zařízení [2]

3.4.Hrozby bezkontaktních transakcí

NFC sice funguje pouze na malou vzdálenost, což nám odbourává několik typů hrozeb, avšak samotná technologie není nijak zabezpečená. Je nutné, aby se proti zneužití bránil jak samotný klient, tak i výrobce NFC. Základních útoků existuje více typů.

3.4.1 Odposlech

Jelikož je NFC bezdrátová technologie není nečekané, že jednou z největších hrozeb je odposlech. K odposlechnutí signálu potřebuje útočník 3 věci: anténu, zesilovač a dekódovací zařízení. Jelikož musí být zařízení blízko vysílače, má útočník omezený rozsah pro zachycení signálu. Samotný odposlech můžeme rozdělit na dva typy. První je útok na pasivní NFC zařízení. Tento útok je ztížen, jelikož je třeba být opravdu blízko, aby se zařízení nabilo. Tento způsob dle některých zdrojů funguje do vzdálenosti okolo jednoho metru. Druhý typ je na aktivní NFC zařízení, které je díky vlastnímu napájení schopno vyslat signál dle některých zdrojů až do deseti metrů. Je možné se bránit tzv. navázání zabezpečeného kanálu, kde jsou informace zašifrovány a následně je lze dekódovat pouze autorizovaným přístrojem.

Proti samotnému odposlechu nemá NFC žádnou obranu. Jediná možnost je vytvoření šifrované komunikace.

3.4.2 Modifikace dat

Stejně jako u RFID může snadno docházet k narušení komunikace. Stačí, aby zařízení běželo na stejném kmitočtu (13,56 MHz) s vyšším výkonem a rušilo posloupnost přenášených bitů. To způsobí náhodnou modifikaci dat na straně příjemce. Momentálně neexistuje způsob, jak se rušení efektivně bránit. Jediným způsobem je neustálá kontrola elektromagnetického pole ve svém okolí, což je bohužel náročné. Dále existuje tzv. úmyslná modifikace. Tento útok spočívá v podstrčení údajů příjemci tak, aby se mu jevili jako validní. Tento typ je mnohem náročnější. Útočník musí změnit jednotlivé bity v přesný okamžik a ještě za použití vyššího vysílacího výkonu, aby mohl bity vůbec změnit.

Chránit se proti modifikaci dat lze hned několika způsoby. První způsob je lepší hloubka amplitudové modulace. Další možnost je neustálá kontrola radiofrekvenčního pole, kdy vždy před odesláním informací si zařízení zkontroluje pole kolem sebe. Pokud by došlo k narušení, zařízení okamžitě uzavírá komunikaci. Poslední způsob je opět využití šifrování při komunikaci.

3.4.3 Data insertion

Tento útok spočívá ve vkládání škodlivého kódu uprostřed komunikace. V podstatě se jedná opět o složitější proces, kde musí útočník v přesný okamžik odeslat kód dříve než zařízení, se kterým čtecí zařízení komunikuje. Pokud by se datové toky překryli, čtecí zařízení je vyhodnotí jako chybné a zahodí je.

Zásadní opatření je zde snížení doby potřebné pro odpověď. Díky tomu nestihne útočník vložit data včas, zařízení detekuje útok a ukončí komunikaci. Další možnost je monitorování pole kolem sebe, pokud zařízení zjistí, že někdo

jiný posílá data, opět uzavře komunikaci. A poslední způsob je opět šifrovaná komunikace.

3.4.4 Přerušení komunikace

Tento útok je založen na časovači. Pokud máme v NFC čipu citlivé informace a k nim nastavený časovač, tak zařízení vždy po nějakém časovém intervalu bez odpovědi sepne a vyžaduje další autentizaci. Pokud ovšem zařízení neukončí komunikační kanál, může útočník navázat tam, kde zařízení skončilo bez nutnosti autentizace.

Zde stačí zmenšit časovač, aby se útočník nestihl zapojit do komunikace včas. Další možností je lepší algoritmus pro ukončování nebo občasné ověření uživatele. Poslední způsob se týká opět šifrované komunikace.

3.4.5 Replay Attack

V tomto případě útočníkovy stačí zachytit jen začínající komunikace, uložit si ji a používat jí dále. Pro názornost uvedu příklad. Útočník zachytí přenos NFC čipu jako jízdenku na MHD, uloží si informaci a dále se vydává za majitele jízdenky. Tohoto se dá zneužít i u platební karty, pokud odposlechne navázání spojení, může jí v budoucnu přehrát znovu.

Na tento útok je nejlepší způsob zabezpečení pořadová čísla, časová razítka či čítač transakcí, který se inkrementuje při každém navázání spojení.

3.4.6 Odcizení

Proti tomuto „útoku“ neexistuje žádný způsob zabezpečení kromě prevence. Jediné zabezpečení existuje ve formě PINu nebo odemknutí obrazovky. Samotné NFC aplikace by měli mít možnost zabezpečovací/autentizační metody v sobě (například náhodné vyžádání hesla).

U tohoto typu útoku je nejlepší zabezpečení dodržení tzv. bezpečnostní politiky. Konkrétně používaní aplikací se šifrovacími algoritmy, spolu se silnými hesly. Dále je zde samozřejmostí existence PINu a kódu pro odemknutí obrazovky. Jinými slovy, čím více zabezpečení bude použito, tím je větší šance na neúspěch útočníka.

3.4.7 Phishing

Útočník nahraje na tag odkaz na falešnou stránku, která na první pohled vypadá podobně té hledané. Pak už stačí pouze tag umístit na místo, které se jeví pro uživatele jako věrohodné. Jedná se o velmi levný a jednoduchý útok. I když se zdá tento útok jako velmi primitivní, tak je hojně a úspěšně využíván po celém světě.

Jako první příklad uvedu systém veřejné dopravy ve Vídni. Zde je možnost koupit elektronickou jízdenku pomocí SMS. Aby uživatel nemusel SMS zprávu psát ručně, je na každé zastávce umístěn NFC tag, kde po přiložení pouze potvrdíte odeslání SMS a čekáte na odpověď. Útok spočíval v tom, že útočník zde přidal pouze jeden NFC tag upraven tak, aby stržené peníze přišli na útočníkovo konto. Útok byl fascinující v tom, že vedle tohoto podvrhnutého tagu byl ten skutečný, a když uživateli nepřišla potvrzující SMS, tak jednoduše vyzkoušel druhý funkční tag a první měl za nefunkční (díky tomu trvalo déle, než byl útok odhalen).

Oficiální NFC tagy by měly být označeny oficiálním logem, avšak toto nám nevylučuje možnost zfalšování oficiálních tagů. Další možnost obrany je důkladné poučení uživatelů.

3.4.8 Denial of service

Takzvané odmítnutí služby slouží k „pošpinění“ služby nebo poskytovatele. Podobně jako u phishingu opět útočník nahraje nežádoucí příkazy na NFC tag a

přelepí ním originální NFC tag. Na modifikovaný tag může například útočník nahrát příkaz na restartování telefonu nebo několikanásobné vypsání chybového hlášení, což má za následek výrazné zpomalení zařízení a tím i ztrátu sympatií ze strany uživatele.

Proti tomuto typu útoku se lze bránit pomocí deaktivace reader/writer režimu. Dále také jako u předchozího útoku, označením oficiálním logem.

3.5.Bezpečnost pro uživatele

Kritickým situacím lze předejít pomocí dodržování určitých pravidel a obezřetností. Zde se hlavně myslí bezpečné zacházení při práci s platebními kartami a jinými prostředky sloužící k placení. Taková hlavní pravidla jsou shrnuta pod „Desatero pro držitele platebních karet“, které je v příloze č. 1. Pokud dojde ke zneužití platebního prostředku, vlastník je povinen neprodleně uplatnit reklamaci podle zákona č. 284/2009 Sb. o platebním styku.

Jako další možnost obrany proti potencionálním útokům je například obal/kryt. Tento kryt ruší elektromagnetické pole, a proto nelze z daného zařízení nic získat. Míru dosažených informací nám samozřejmě určuje kvalita daného krytu. Nejběžnější s čím se setkáme, je ve své podstatě několik vrstev hliníkové folie slisované k sobě. Osobně jsem měl možnost vyzkoušet, jak kryt na bezkontaktní platební kartu, tak i obal na telefon a oboje splnilo svůj účel. Našel jsem i různé srovnávací testy, kde ukazovali, jak je možné získat cenné informace i přes tento druh zabezpečení.

3.5.1 Zabezpečený kanál

Je to zajisté nejúčinnější forma zabezpečení komunikace mezi NFC zařízeními proti téměř všem známým útokům. Při tvorbě zabezpečeného kanálu je nejprve použit standartní protokol sloužící k výměně klíčů (nejčastěji Diffieho-Hellmanova výměna klíčů). Uživatel nejprve pomocí vytvořeného tajného klíče zašifruje symetrický klíč a odešle ho k druhému uživateli, který

následně pomocí tajného klíče dešifruje data. Po získání symetrického klíče z obdržených dat může dále šifrovat komunikaci. Pro vytvoření symetrického klíče se používá nejčastěji algoritmus „standard pokročilého šifrování“ (Advanced Encryption Standard).

4. Metodika

Pro začátek bylo provedeno důkladné seznámení s technologii a uvedení do problematiky jako takové (včetně příkladů). Následovalo postupně shrnutí těchto poznatků do práce. Čímž bylo dosaženo prvního z cílů mé bakalářské práce.

První krokem pro provedení mé bakalářské práce byla analýza HW na trhu, po dostatečném zhodnocení možností výběru zařízení byla zakoupena NFC čtečka ACR122U, které mi byla zapůjčena pro seznámení se s technologií. Dále bylo pro experimentální účely nutné zakoupení několika NFC a RFID čipů. Dalším nutným krokem před samotným provedením experimentu byl nutný výběr operačního systému. Nejprve byl zvolen jako operační systém Windows 7, bohužel se však neprokázal jako ideální z důvodů nesplnění nároků pro cíle práce. Po bližším prostudování a konzultaci s panem Ing. Břehovským byl zvolen pro použití operační systém Kali Linux který v sobě obsahoval spoustu předpřipraveného softwaru a byl tak pro účely dostačující.

Dalším krokem bylo třeba vymezit si útoky, kterými se bude experiment věnovat. Konkrétně jsme se zabývali klonováním čipů Man-in-Middle attack, dále jsme zjišťovali co nejvíce informací o daném čipu a zjistili/otestovali jejich případně zneužití útočníkem. Mimo cíle bakalářské práce byl implementován úspěšně navíc útok Denial of Service.

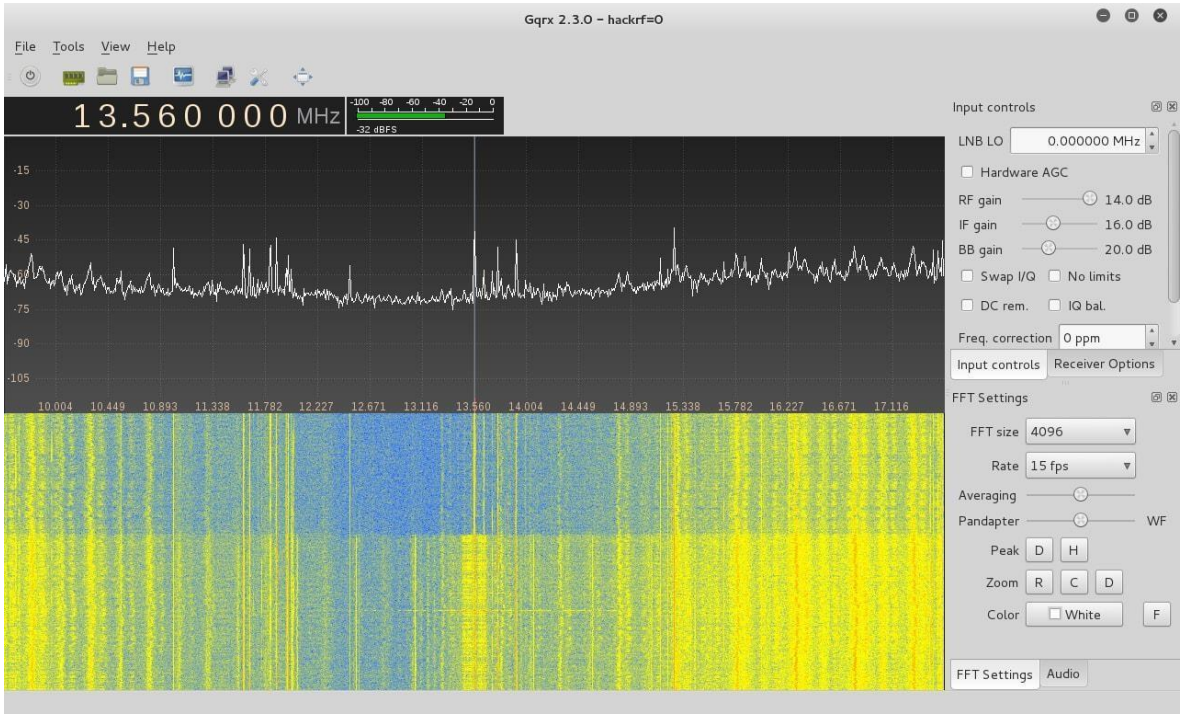
Dalším cílem bakalářské práce bylo dokázat snadné zneužití bezkontaktních technologií potencionálním útočníkem, poukázat na toto riziko a zdůraznit neznalost veřejnosti ohledně této problematiky.

5. Implementační část

Cílem implementační části bylo prozkoumat, vyzkoušet bezpečnost na bezkontaktních technologiích nasimulováním některých útoků. Pro uskutečnění experimentu bylo potřeba sehnat příslušné vybavení. Konkrétně čtečku karek, vysílací a přijímající zařízení. Byl udělen průzkum dostupných čtecích zařízení a následně byla zvolena NFC čtečka ACR122U (dále pouze „bílá čtečka“), která splňovala požadavky jak z pohledu rychlosti komunikace, tak i podporovanou frekvencí. Následně bylo pro pokus poskytnuto i čtecí/vysílací zařízení a to konkrétně HackRF One from Great Scott Gadgets, které dokáže pracovat se signálem v rozmezí 1 MHz až 6 GHz.

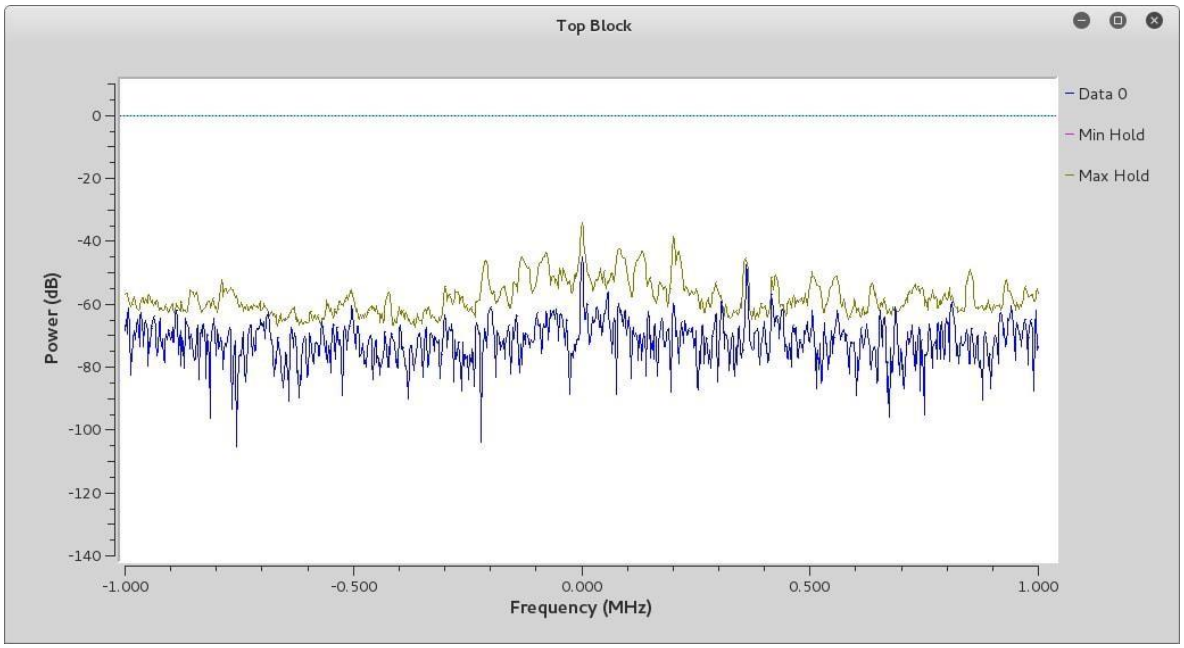
Další důležitou volbou byl výběr kvalitního softwaru, který se dokáže se zařízením spárovat a zároveň bude obsahovat potřebné funkce. První volbou byl operační systém Windows, který se však neprokázal vhodným. S ohledem na nefunkčnost operačního systému Windows byl zvolen operační systém Kali Linux. I tento operační systém měl ze začátku problém se spárováním se zařízením HackRF One, který byl však po bližším prozkoumání odstraněn.

První zvolený software byl Gqrx verze 2.3.0, ve kterém byli přizpůsobeny podmínky pro experiment. Díky němuž se podařilo zachytit viditelně signál i s možností zvukové stopy. Signál byl převeden do formátu RAW. Program poskytnul i zvukovou stopu, která nebyla dál využita. Výsledek experimentu je znázorněn na obrázku 5. Z obrázku je vidět rozdíl mezi odposlechem NFC čtečky a následné vzdálení od zařízení. Horní tmavá polovina grafu znázorňuje na ose x frekvenci (Hz) a na ose y sílu signálu (dB). Spodní barevná část grafu zachycuje časovou osu.



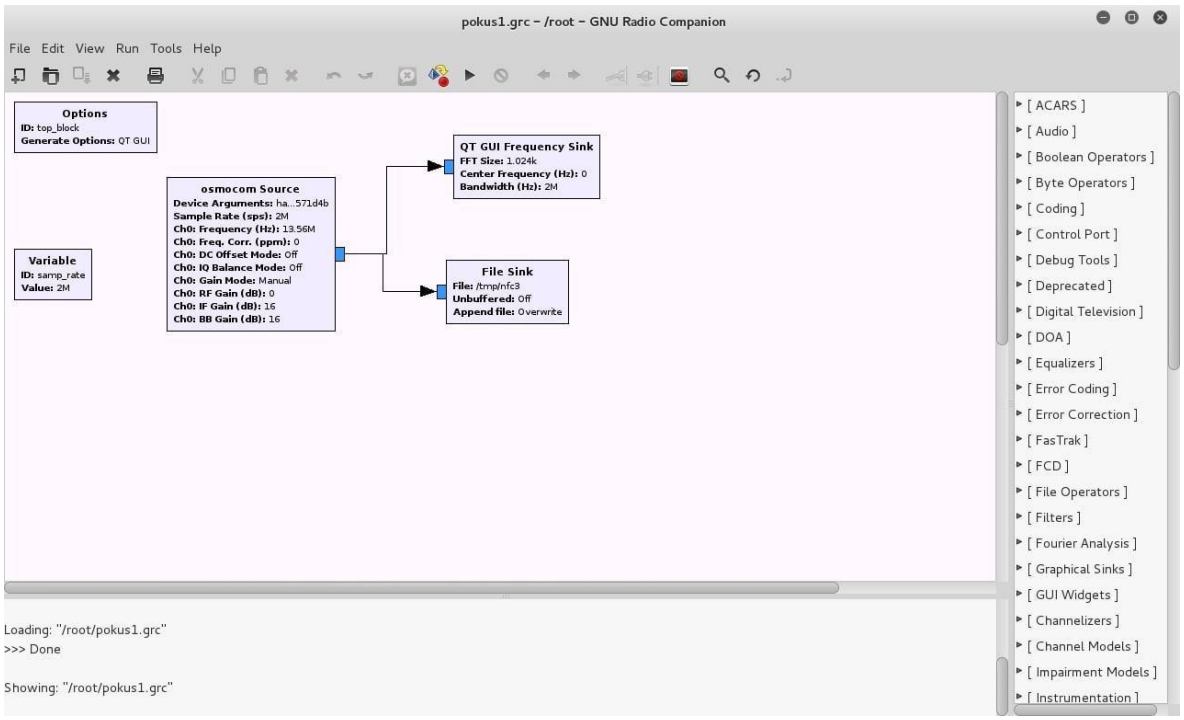
Obrázek 5- GQRX schéma

Další ze softwarových programů pro experiment byl využit GNU Radio Companion verze 3.7.5. Tento program byl uživatelsky náročnější, obsahuje spousty funkcí a možností pro bezkontaktní technologie. I s tímto programem se podařilo odchytit signál do souboru. Pro využití signálu dále v experimentu bylo nutné zachytit aktivní část signálu. Na obrázku 6 je vidět nažloutlý graf, který znázorňuje maximální hranici (jinými slovy, zde je signál, pokud zrovna čteme čip) a modrý graf je kolísající momentální signál.



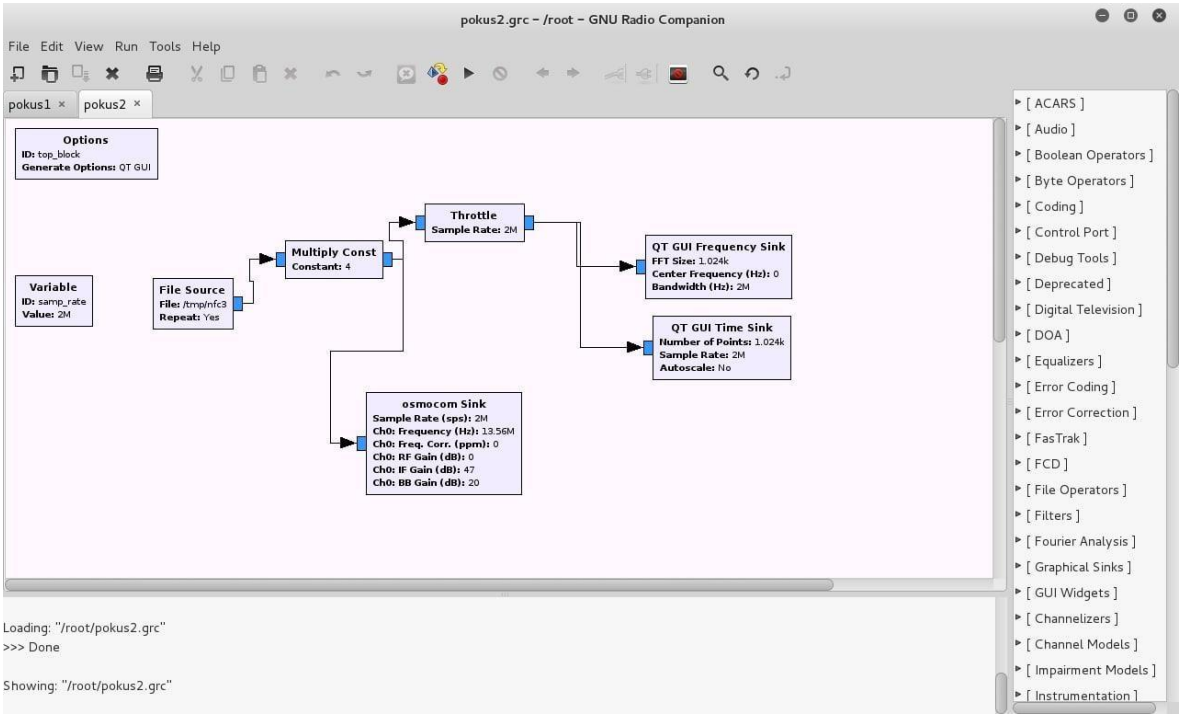
Obrázek 6- GNU radio schéma signálu

Přesné nastavení programu je patrné z obrázku 7. Konkrétně se zde nastavila frekvence, rozsah, počet bodů, zesílení a umístění pro uložení souboru.



Obrázek 7- Schéma zachycení/uložení signálu

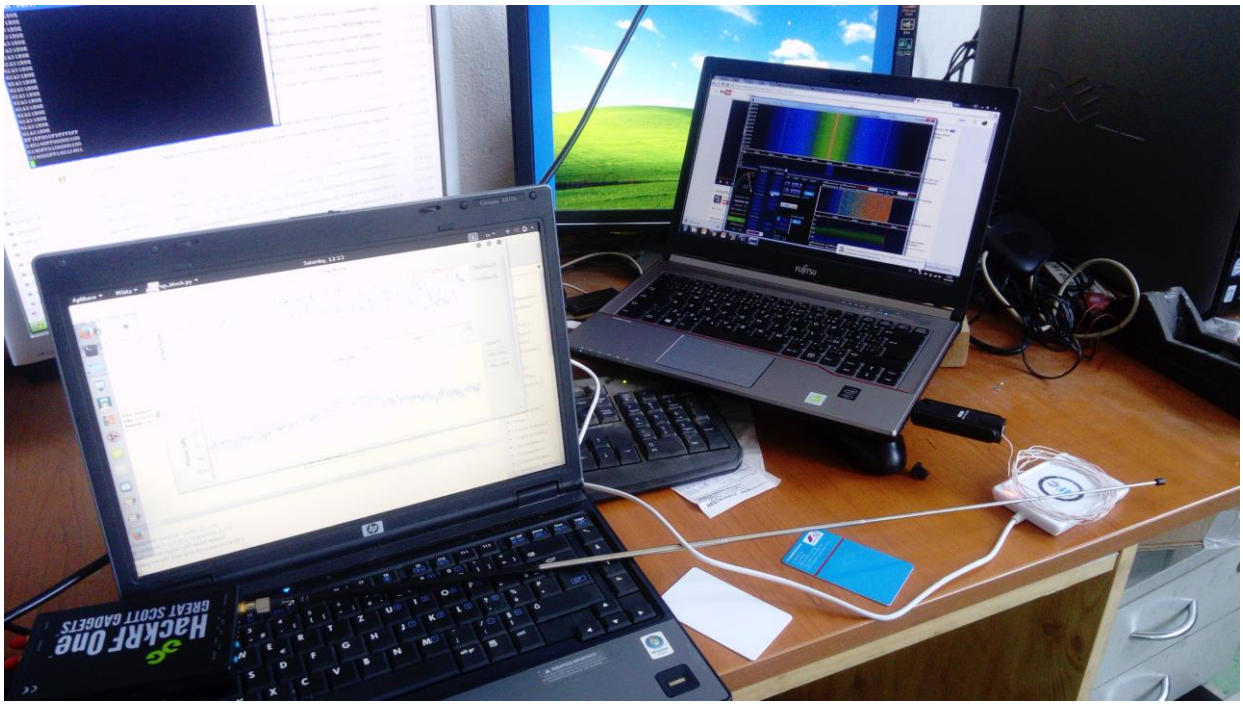
Dalším důležitým krokem bylo odeslání uloženého signálu, ke kterému byl použit GNU Radio Companion. Tento krok představoval komplikaci v experimentu, jelikož se nedařil signál odeslat v takové podobě, aby se dal zachytit. Problém zde nastal také z důvodu zesílení signálu, který byl prováděn metodou „pokus omyl“. Nakonec byla použila metoda Multiply Const, která násobí/zesiluje vyslaný signál. Největší komplikací je zde oddělení signálu, jelikož NFC čtečka vysílá neustále svůj signál, potřebný pro „nabití“ a spárování s RFID/NFC čipem. Schéma odesílání signálu je zachyceno na obrázku 8.



Obrázek 8- Odeslání signálu

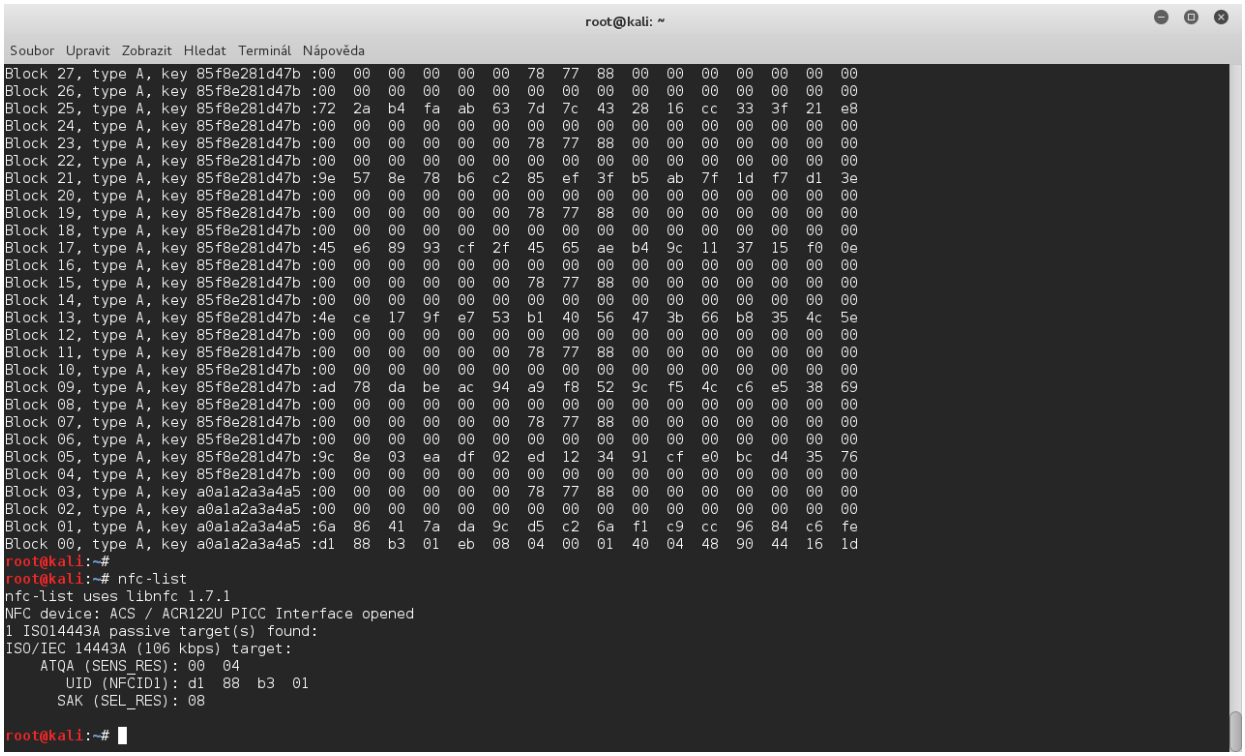
Přes usilovnou snahu se v experimentu opakovaně nedařilo zachytit vysílaný signál čtečkou. Po konzultaci s vedoucím bakalářské práce jsme se rozhodli kontaktovat kroužek Radioamatérství v Domu dětí a mládeže v Českých Budějovicích, kteří bohužel s touto technologií neměli zkušenosti. Dále byl kontaktován Radioklub Písek s kterým jsem dále přínosně spolupracoval na experimentální části.

Experiment tedy pokračoval prvním simulovaným útokem, který se povedl náhodně při snaze o zachycení signálu čtečkou. Jako první se díky výše zmiňovanému schématu z obrázku 8 v GNU Radio Companion podařilo nasimulovat Denial of Service. Z důvodu vysílání rozsahu celého signálu nemohl být signál zachycen žádnou čtečkou. Pro účel experimentu bylo zapůjčeno několik čtecích zařízení a mezi tím i jedna ruská čtečka. Díky této čtečce se jednoduše snímalo UID všech čipů. V tomto útoku plnila čtečka funkci pouze kontrolní, konkrétně tedy byla ujištěním funkčnosti, bezproblémovosti a kontroly přítomnosti signálu. Prvním krokem bylo připojeno bílé čtečky k PC a potvrzení přijímaného signálu na frekvenci 13,56 MHz. Poté bylo k notebooku připojeno HackRF One a anténa byla položena přes bílou čtečku. Nakonec byla položena karta přes antény. Celé popisované schéma útoku je znázorněno na obrázku 9. Bílá čtečka přijímala signál z karty pouze do chvíle kdy bylo schéma aktivní a zařízení HackRF One vysílalo. Díky již uvedenému faktu, že byl vysílán celý rozsah signálu bylo bílé čtečce znemožněno cokoliv přečíst z karty.



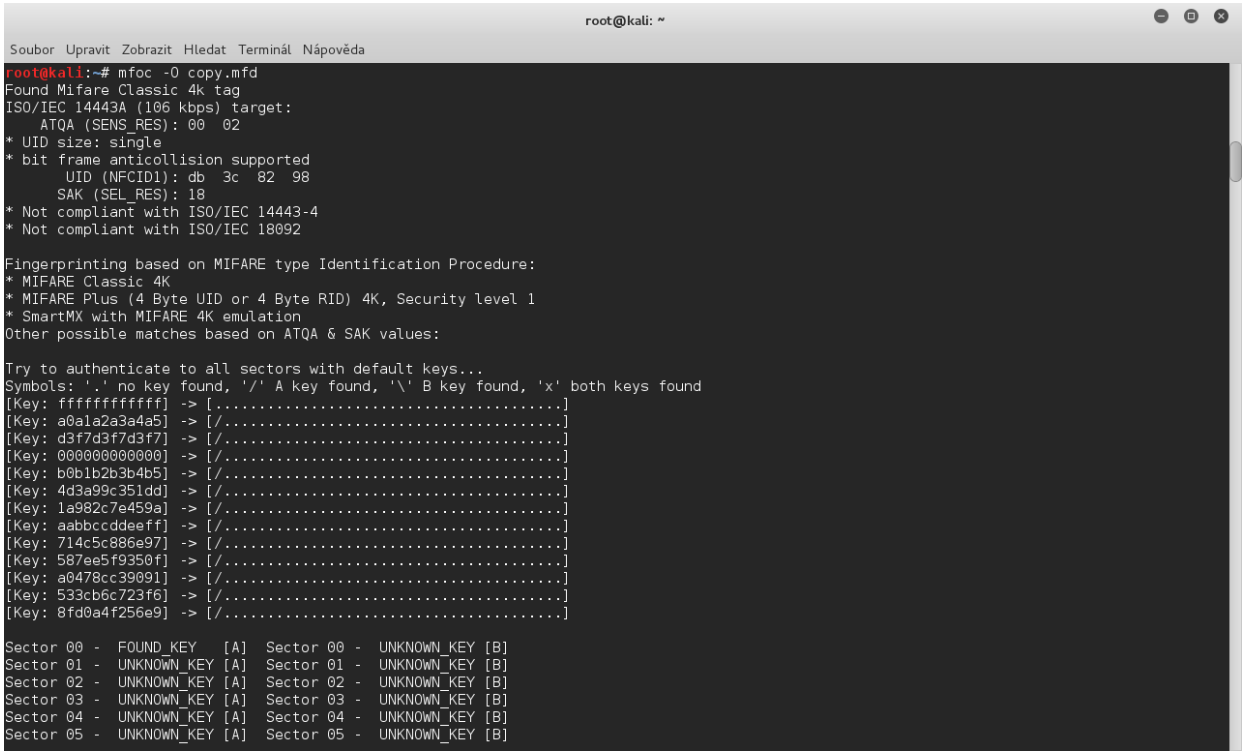
Obrázek 9- Foto při útoku Denial of Servvice

Dalším zajímavým aspektem experimentální části byla možnost průzkumu veškerých možných zjistitelných informací o čipu. První zachycená informace obsahovala ATQA, UID, SAK a typ daného čipu pomocí příkazu „nfc-list“ viz obrázek 10.

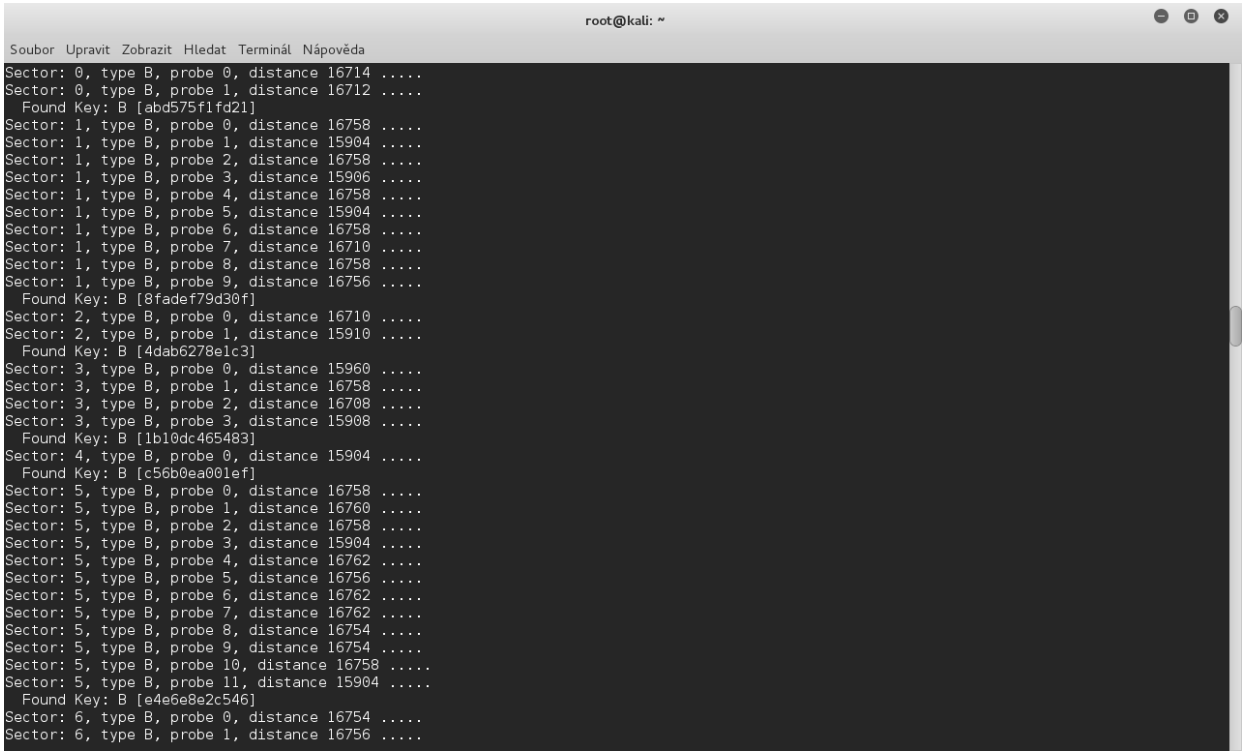


Obrázek 10- Ukázka základních informací o čipu

V další fázi experimentu se podařilo zjistit komunikační klíče A i B a tudíž jsme byli schopni data překopírovat na jinou kartu. V rané části experimentu jsme neměli přístup k čipům se pozměnitelným UID, a proto jsme byli schopni změnit pouze 63 ze 64 sektorů. Byl k tomu použit příkaz „mfoc -0 nazev_souboru.mfd“, jenž uložil klíče i s daty do souboru. Toto bylo třeba provést i s prázdným čipem a následně příkaz „nfc-mfclassic w a nazev_souboru.mfd prazdny_cip.mfd“ nám přepsal tento soubor prázdého čipu tím souborem z karty, kterou klonujeme. Toto bylo zajímavé hlavně z důvodu získání a možné úpravy některých dat na čipu. Nevýhoda spočívá v dlouhém hledání klíče u některých karet (u jednoho případu trvání něco málo přes hodinu času) viz obrázek 11. Průběh dohledávání klíčů je znázorněn v obrázku 12.

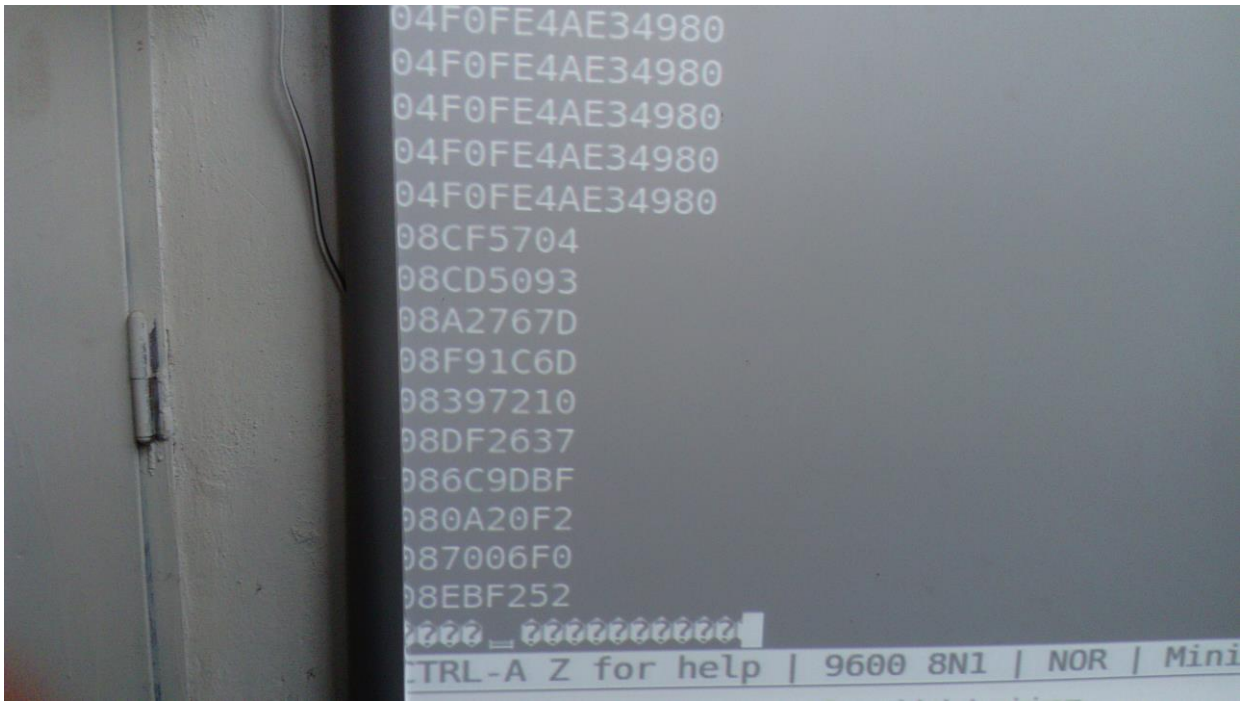


Obrázek 11- Vypsání, které klíče jsme zjistily, a které je třeba dohledat



Obrázek 12- Dohledávání klíčů

V dalším bodě experimentu jsme se snažili o ruční změnu UID, která nebyla úspěšná, jak je viditelné na obrázku 13.



Obrázek 13- Foto z interaktivní tabule při pokusu změny UID

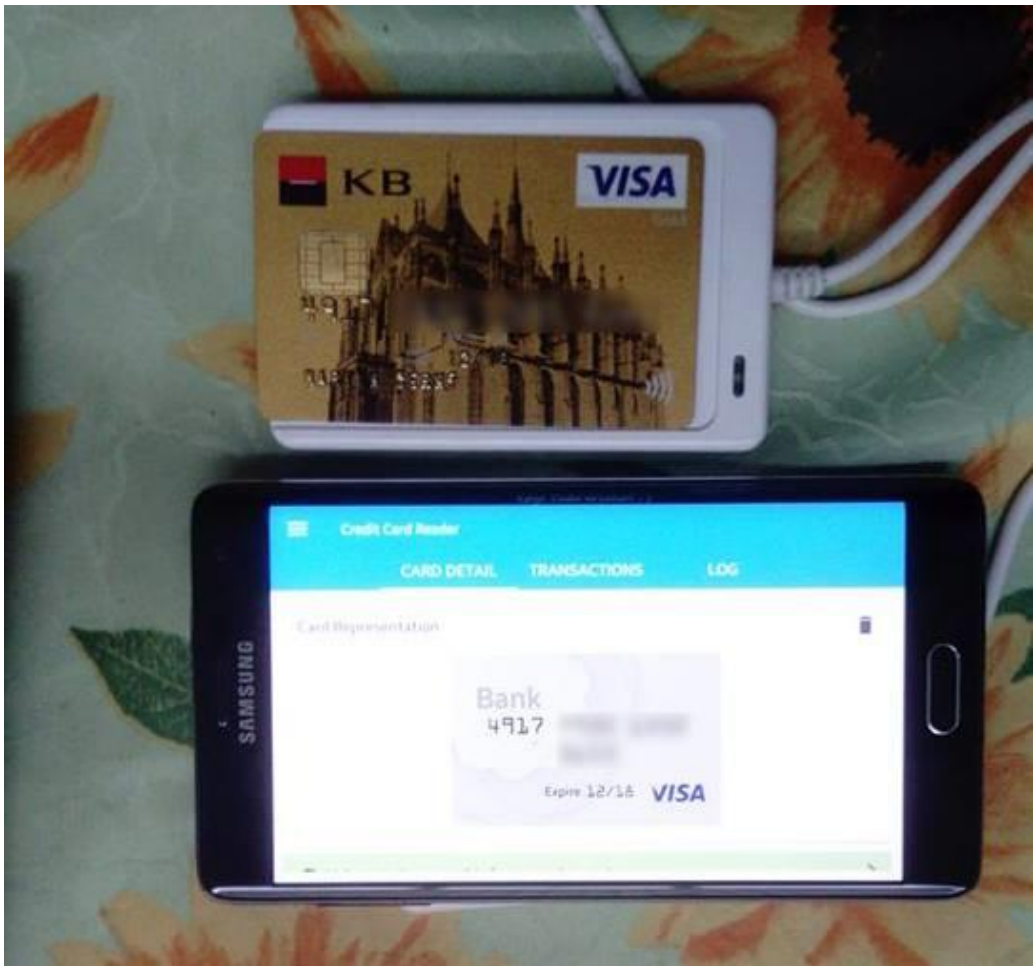
Dalším typem simulovaného útoku byl Relay attack (Man in Middle) s použitím dvou bílých čteček propojených skrz notebook s nainstalovaným operačním systémem Kali Linux. Schéma přípravy zařízení je na obrázku 14. Přes prvotní problém se synchronizací obou čteček, došlo k úspěšnému přečtení čipu. Použit byl software obsažený přímo v operačním systému. Na první bílou čtečku byla položena karta, na druhou bílou čtečku byl umístěn telefon s podporou NFC. Do terminálového okna (obrázek 15), byl zadán příkaz „nfc-relay-picc“. Na mobilním telefonu došlo k načtení karty včetně historie transakcí viz obrázek 16.

Obrázek 14- Příprava útoku Man-in-Middle

```
root@kali: ~
Soubor  Upravit  Zobrazit  Hledat  Terminál  Nápověda
    ATQA (SENS_RES): 00  02
       UID (NFCID3): 08  3c  82  98
      SAK (SEL_RES): 18
                ATS: 75  33  92  03
NFC emulator device: ACS / ACR122U PICC Interface opened
nfc-relay-picc: ERROR: Initialization of NFC emulator failed
root@kali:~# nfc-relay-picc
nfc-relay-picc uses libnfc 1.7.1
NFC reader device: ACS / ACR122U PICC Interface opened
Found tag:
ISO/IEC 14443A (106 kbps) target:
    ATQA (SENS_RES): 00  02
       UID (NFCID1): db  3c  82  98
      SAK (SEL_RES): 18
Hint: tag <---> initiator (relay) <---> target (relay) <---> original reader

We will emulate:
ISO/IEC 14443A (106 kbps) target:
    ATQA (SENS_RES): 00  02
       UID (NFCID3): 08  3c  82  98
      SAK (SEL_RES): 18
                ATS: 75  33  92  03
NFC emulator device: ACS / ACR122U PICC Interface opened
```

Obrázek 15- Terminál při Man-in-Middle

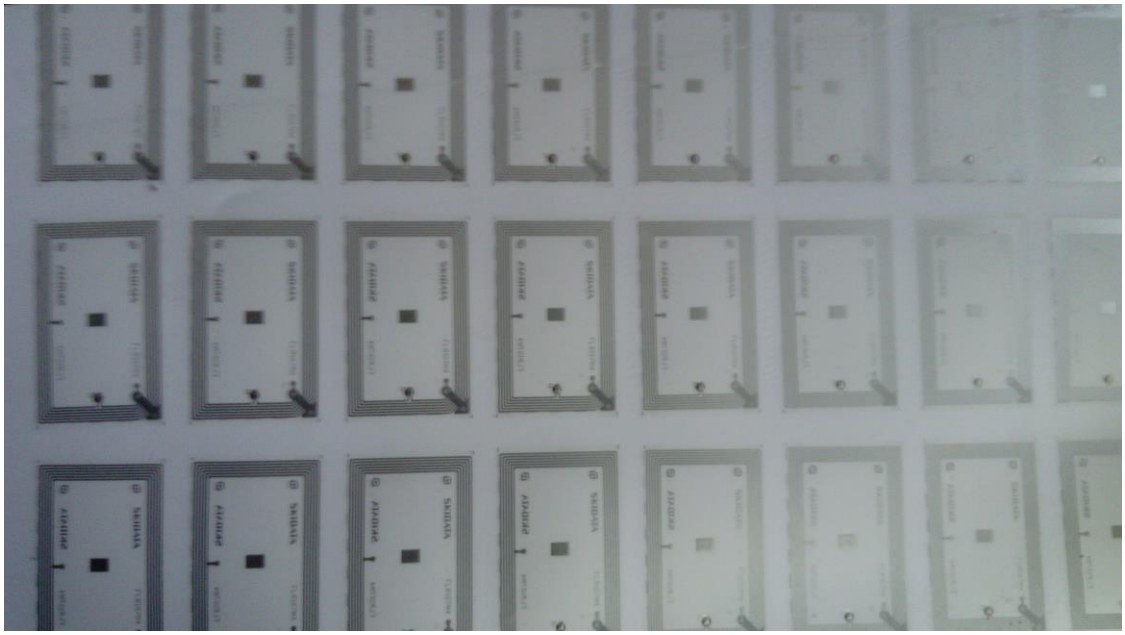


Obrázek 16- Úspěšný výsledek u Man-in-Middle

Pozitivní výsledky experimentální části zapříčinili další výzkum. Pro experimentální část byli dodatečně pořízeny karty s přepisovatelným UID sektorem. Teoreticky jsme tedy byli schopni kartu naklonovat kompletně. Pro tyto účely bylo nutné obstarat čip stejného typu. Po bližší prozkoumání dokumentace jsme došli k příkazu, který dokázal přenést i UID sektor. Konkrétně „nfc-mfclassic W a nase_karta.dmp prazdna_karta.dmp“. Z počátku byl přenos neúspěšný, po kontrole veškerého materiálu a nastavení bylo zjištěno, že jediná chyba byla v citlivosti kódu ohledně velkých a malých písmen. Po dokončení přepisu i nultého sektoru byl přepis úspěšný i se vstupní kartou sportovního střediska. Klonování karet bylo různě časově náročné. U některých kusů to trvalo řádově v sekundách. U složitějších byla časová náročnost v řádu desítek minut.

K experimentům nebyli využívány pouze mifare a platebními kartami, ale také jsme měli k dispozici například pasy či čipy používané pro identifikaci zvířat o frekvenci 125 kHz (konkrétně dobytka) viz obrázek 17. Také jsme si mohli vyzkoušet takzvanou

„klonovačku čipů“ (obrázek 18) z Číny, což je také velmi zajímavá a uživatelsky velmi jednoduchá věc.



Obrázek 17- Plato čipů pro dobytek

Obrázek 18- „Klonovačka“ čipů

6. Diskuze a otevřené otázky

Určitě je daleko více možností, jak experimentovat s bezkontaktní technologií. Já si vybral NFC/RFID. Hlavně z důvodů postupnému rozšíření nejen v platebním odvětví. Často se uvádí, že útočníci přišli s něčím novým a přitom úplně prostým. Vydal jsem se cestou simulování těchto útoků, také díky své zvědavosti a konkrétně útok Man-in-Middle mě opravdu zaujal. Bohužel jsem nezkoušel tento útok přes síť, respektive na větší vzdálenost. Další bod pro budoucí zkoumaní, je útok Denial of Service na větší vzdálenost. Respektive rušení služby z několika metrové (nebo dokonce i větší) vzdálenosti. Pro mě, ale nejzajímavější útok je Replay attack, který se mi nepodařilo nasimulovat. Bohužel mi není vědomo, jak tento útok zrealizovat, a to ani za pomoci kolegů. Upřímně si ani nejsem jistý, zda by se vůbec dal v platební sféře zneužít. Za zmínění stojí zajímavost, že jsem se dočetl o několika úspěšných pokusech, jak tento útok použít na odemykání aut, takže i tento útok si zaslouží bližší prozkoumání v budoucnu.

Pro čtenáře bych se na závěr zmínil, že je stále co v tomto odvětví zkoumat a s čím experimentovat. Teď nemám na mysli pouze NFC/RFID. Ještě dodám, že v reálném ozkoušení v praxi je přece jen problém s ohledem na zákon, což je velká škoda, avšak je to pochopitelné.

7. Závěr

Po prozkoumání a experimentování s čipy jsem došel k závěru, že celá oblast bezkontaktního světa není zdaleka tak bezpečná, jak si široká veřejnost myslí. Jak je vidět, ke zneužití platební karty či čehokoliv jiného stačí útočníkovi pouhá chvilka. Je třeba brát toto riziko v úvahu a dobře se proti němu chránit. Je pravda, že se stále snaží tuto oblast zabezpečit víc a víc, ale s tím drží krok i potencionální útočníci. Celá tato problematika je velmi zajímavá a jelikož je tato technologie poměrně nová, tak stále ještě není důkladně prozkoumána.

Osobně mě také zaujalo, jak málo například banky informují klienty ohledně bezpečnosti bezkontaktních karet. Když jsem toto probíral s lidmi ve svém okolí, většina lidí ani nevěřila, že je zneužití vcelku jednoduchá věc. Žalostná je dále věc, že ani zaměstnanci poboček některých bank, kde jste takřka donuceni si vzít bezkontaktní platební kartu, nic o bezpečnosti nevědí. Nejvíce překvapen jsem byl faktem, že své klienty o možnosti zabezpečením a možnosti hrozeb s bezkontaktními kartami spojeným neinformují. Takže závěrem bych chtěl zdůraznit, že je opravdu třeba nenechat se ovlivnit marketingem či veřejným míněním, ale vždy být obezřetní a dodržovat jednoduchá pravidla v celé oblasti bezkontaktních technologii.

Slovník pojmů

FeliCa (Felicity card) - čip kompatibilní s formátem ISO14443 od SONY

IEC (International electrotechnical commission) - nezisková nevládní organizace s mezinárodní působností, zaměřující se na normy pro elektrické, elektronické a jiné související technologie

ISO (International organization for standardization) - největší světový vývojář a vydavatel mezinárodních norem

NFC (Near field communication) - bezdrátová komunikační technologie

N-Mark – univerzální symbol pro NFC

NXP (Next experience) - společnost pro výrobu a vývoj polovodičů

PIN (Personal indentification number) - identifikátor pro autorizaci

RFID (Radio frequency identification) - technologie využívaná pro bezkontaktní identifikaci pomocí elektromagnetických vln

SIM (Subscriber identity module) - identifikační karta pro identifikaci v mobilní síti

UICC (Universal integrated circuit card) - nová generace SIM

NDEF (NFC data exchange format) - formát pro ukládání dat do NFC tagů a komunikaci pomocí peer-to-peer protokolu

8. Seznam použité literatury

GOMZIN Slava: Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions 1st Edition. Wiley; 1 edition (February 17, 2014). 312 stran. ISBN: 978-1118810118

ROLAND Michael: Security Issues in Mobile NFC Devices (T-Labs Series in Telecommunication Services) 2015th Edition. Springer; 2015 edition (February 12, 2015). 185 stran. ISBN: 978-3319154879

FINKENZELLER, K.RFID Handbuch, 3rd edition, Munich /Vienna, Carl HanserVerlag, 2002, ISBN 3446220712

FINKENZELLER, K.RFID Handbook: Fundamentals and Applications in ContactlessSmart Cards and Identification, 2nd edition, NewYork, John Wiley & Sons, 2003.

RANKL, W., EFFING, W.Smart Card Handbook, 3rd edition, New York, John Wiley & Sons, 2003.

Rankl, W. – Effing, W. Smart Card Handbook, John Wiley & Sons, 2000. ISBN 0471988758

MIFARE DESFire, Contactless Multiapplication IC with DES and 3DES Security, MF3 IC D40, Philips Semiconductors, Eindhoven 2004.

Záhlava, Vít,. Návrh a konstrukce desek plošných spojů / Vyd. 1. Praha : Česká technika - nakladatelství ČVUT, 2005. 75 ISBN 80-01-03351-1.

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.

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

Mitrokotsa, A.; R.Rieback, M.; Tanenbaum, A. S.: Classifying RFID attacks and defenses. Information Systems Frontiers , roËnÌk 12, November 2010: s. 491{505, ISSN 1387-3326.

[1] *Hyundai a NFC: v roce 2015 nechte klíče od auta doma* [online]. [cit. 2016-11-13]. Dostupné z: https://nearfield.cz/clanky/hyundai-a-nfc-v-roce-2015-nechte-klice-od-auta-doma-90

[2] ISIS Mobile Wallet / Google Wallet / iPhone Mobile Payment. *EverydayNFC* [online]. [cit. 2016-11-13]. Dostupné z: http://everydaynfc.com/?tag=secure-element

9. Obrázky

10. Přílohy

DESATERO PRO DRŽITELE PLATEBNÍCH KARET

1.KARTA JE VÍC NEŽ HOTOVOST. K platební kartě se chovejte stejně jako k penězům. Buďte na ni opatrní a noste ji odděleně od dokladů. Platební kartu podepište ihned při převzetí do podpisového proužku. Po skončení platnosti se řiďte pokyny své banky. Neodevzdanou neplatnou kartu znehodnoťte.

2. JAKO OKO V HLAVĚ. Stále si kartu hlídejte a při provádění transakcí ji nespouštějte z očí. Platební kartu nikomu nepůjčujte ani nedávejte do zástavy. Pravidelně kontrolujte, že stále víte, kde kartu máte, i když ji nepoužíváte každý den.

3. PIN JE KLÍČ K VAŠEMU ÚČTU. PIN uchovejte v naprosté tajnosti. PIN si nikam nezaznamenávejte! Za žádných okolností jej nesdělujte jiné osobě, bance ani policii či jiným orgánům.

4. DŮVĚRYHODNOST. Platební kartu používejte pouze na důvěryhodných obchodních místech (včetně internetových) a důvěryhodných zařízeních. Nemáte-li k obchodníkovi důvěru, použijte k platbě raději hotovost.

5. ZADÁVÁNÍ PINu. PIN zadávejte vždy diskrétně. Dbejte na to, aby ho nemohl nikdo odpozorovat. Při zadávání PIN u bankomatu nebo terminálu zakryjte klávesnici tělem a volnou rukou i shora a zabraňte jeho odezření nebo snímání kamerou.

6. PLATBA KARTOU. Po skončení transakce zkontrolujte, zda vám byla vrácena skutečně vaše platební karta. Uschovejte si potvrzení o kartové transakci. Obchodník je oprávněn ověřit si vaši totožnost, proto s ním spolupracujte.

7. POZOR NA DOKUMENTY. Zbavujte se opatrně všech dokumentů, které obsahují celé číslo vaší karty. Před vyhozením je roztrhejte nebo rozdrťte.

8. NEODKLÁDEJTE KONTROLU. Pečlivě kontrolujte výpisy kartových transakcí z banky nebo kartové společnosti vůči prodejním a výplatním dokladům. Pokud zjistíte neobvyklou transakci, kontaktujte ihned vydavatele karty.

9. ZTRÁTA KARTY. Při ztrátě nebo odcizení platební karty jednejte rychle a kartu ihned zablokujte u vydavatele, poté v případě krádeže kontaktujte policii. K zablokování použijte telefonní číslo určené vydavatelem. Telefonní čísla určená pro blokaci karet dle jednotlivých vydavatelů naleznete také na našich stránkách v sekci "BLOKACE KARET".

10. INFORMUJTE SE. Některé vydavatelské banky poskytují k platebním kartám další doplňkové služby a produkty sloužící ke zvýšení bezpečnosti nebo zmírnění následků případného zneužití karty.

Hodnocení participující organizace Radioklubu Písek na přípravě bakalářské práce.

Škornička Jakub nás požádal o spolupráci při tvorbě své bakalářské práce. Zajímala ho oblast radiové komunikace mezi čtečkou čipových karet a samotnou čipovou kartou. Jelikož byl vybaven jak teoreticky, tak prakticky začalo nás téma také zajímat jako možnost rozšířit své znalosti o moderní a denně používané radiové technologie.

Práci v Radioklubu jsme pojali jako přednáškové turné s několika přednáškami a vždy s praktickým předvedením diskutované problematiky.

V prvním kole jsme se společně seznámili s teoretickým pozadím radiové komunikace mezi čtečkou a kartou. Diskutovali jsme typy a vlastnosti jednotlivých norem a dohodli jsme se, že další téma bude již věnováno výhradně Mifare a NFC. V praktické části jsme použili technický prostředek Hack RF a zaujala nás Jakubova znalost softwarového řešení Gnuradio, které nás již delší dobu zajímá.

V druhém kole jsme po teoretické diskusi použili softwarové nástroje pro načtení karet a diskutovali o možných útocích a jejich praktických dopadech.

V dalších několika meetincích jsme jednotlivé útoky procházeli, testovali a snažili se v našem kolektivu dojít k nějakému smysluplnému útoku, který by mohl znamenat praktické ohrožení.

V závěru se nám několik útoků podařilo za Kubova vedení dokončit a našemu kolektivu předvést. Jejich praktické dopady Kuba popsal ve své práci, kterou nám v závěrečném meetingu představil.

Pro Radioklub Písek jsou taková setkání velmi obohacující. Máme možnost se potkat s technologiemi, které běžně nezasahují do Radioamatérského světa. Nicméně používají stejné principy a základy.

Je také velmi zajímavé se setkat s mladými lidmi a pokusit se je svým přístupem k technice a technologiím ovlivnit a otevřít jim přirozeným způsobem i další obzory jako je radioamatérství a technické sporty obecně.

Práci Škornička Jakub vypracoval samostatně, Radioklub Písek byl jen ukazatelem slepých cest a nadšeným testerem prováděných útoků. Technologie a postupy, které byly používány, byly v Radioklubu Písek známé pouze povrchně a tak jejich detailní nasazení a zkoumání bylo přínosem pro obě strany.

Na závěr bych ještě rád vyzdvihl Kubovu ochotu cestovat za námi do Písku. Doufáme, že tím tato spolupráce s Kubou nekončí.

Za Radioklub Písek hodnocení vypracoval Ing. Martin Černý, vedoucí operátor kolektivní stanice OK1KPI, za aktivního přispění členů, hostů a vedení Radioklubu.