Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

Bakalářská práce

2017

Pavel Brániš

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

Analýza bezpečnostních rizik technologie NFC

Bakalářská práce

Pavel Brániš

Školitel: Ing. Petr Břehovský

České Budějovice 2017

Bibliografické údaje

Brániš P. 2017: Analýza bezpečnostních rizik technologie NFC [NFC Security Risk Analysis. Bc. Thesis in Czech] – 51p., Faculty of Science, University of South Bohemia, České Budějovice, Czech Republic.

Anotace

Tato bakalářská práce se zabývá analýzou bezpečnostních rizik technologie NFC. V teoretické části obsahuje popis technologie NFC od jejího principu až po její dnešní využití. Dále také známé hrozby a útoky na NFC včetně možností zabezpečení komunikace proti nim. Praktická část obsahuje popis použitých komponent a aplikací. Jádrem práce jsou testovací scénáře možných hrozeb a jejich výsledky po jejich zkušební realizaci.

Klíčová slova

NFC, Android, Arduino, Adafruit, PN532

Annotation

This bachelor thesis deals with analysis of security risks of NFC technology. The theoretical part contains a description of the NFC technology from its principle to its present use. Furthermore known threats and attacks on NFC, including the options to secure communications against them. The practical part contains a description of used components and applications. The core of the thesis are test scenarios of possible threats and their results after their trial implementation.

Key words

NFC, Android, Arduino, Adafruit, PN532

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 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 ..... podpis autora .....

Poděkování

Rád bych poděkoval panu Ing. Petru Břehovskému za rady a konečné korekce a za čas věnovaný vedení této práce. Také děkuji rodině za podporu při studiu.

Obsah

1. Úvod

V dnešním světě moderních technologií se již na každém kroku setkáváme s chytrými mobilními telefony, které jsou každodenní součástí životů svých majitelů. Chytré telefony se tedy staly určitou cestou, jak dostat technologie mezi širokou veřejnost. Bohužel však právě běžní uživatelé často nevěnují pozornost všem aspektům zabezpečení svých mobilních zařízení.

Pro možné útočníky se tedy stávají jedním z možných cílů pro získání osobních a dalších citlivých dat. Hledají proto všechny možné cesty, jak se k nim dostat. Jednou z těchto možností je napadnutí telefonu přes dnes velice často rozšířené bezdrátové sítě.

Speciálním případem jedné ze sítí je NFC, která se využívá pro velice citlivou komunikaci, která vyžaduje vysoký stupeň zabezpečení. Ať už se jedná o bezkontaktní platební transakce, nebo i způsoby autentizace, stala se dnes NFC jedním z vektorů, který mohou útočníci zneužít pro získání přístupu k citlivým datům uloženým v paměti mobilního telefonu vybaveného NFC modulem.

Avšak NFC není využito pouze v mobilních telefonech, jeho funkce je velice těsně svázána i technologií RFID, která se dá považovat za jakéhosi předchůdce NFC. Obě technologie jsou na určité úrovni kompatibilní. Ať už ve formě bezkontaktních platebních/přístupových karet nebo elektronických jízdenek pro hromadnou dopravu NFC zasahuje hlavně do oblastí, kde se pracuje s osobními a jinými velice důležitými daty.

2. Cíle práce

- Popsat možnosti narušení bezpečnosti NFC
- Popsat způsoby zabezpečení NFC
- Teoretická část: základní informace o technologii NFC, jejím vzniku a použití
- Popis mobilních aplikací pro práci a testování bezpečnosti NFC
- Popis programovatelného hardwaru pro práci a testování bezpečnosti NFC
- Návrh testovacích scénářů pro otestování zranitelnosti technologie NFC
- Testování zranitelnosti

3. Metodika použitá při tvorbě bakalářské práce

Samotnému zpracování teoretické a praktické části bude předcházet analýza dané problematiky. Jedná se o pojmy NFC, RFID, bezpečnost NFC/RFID/Android tedy komunikace NFC, zabezpečení, útoky, implementace technologie a aplikace pro Android.

Teoretická část je rozdělena na dvě části. První se zabývá představením technologie NFC, jejím vznikem, specifikací, uplatněním a použitím v dnešní době. Druhá část se zaměřuje na bezpečnost NFC, kde jsou rozebrány možnosti zabezpečení komunikace, známé hrozby a popsána jejich teoretická i praktická zneužitelnost včetně možných doporučení, jak se proti těmto teoretickým hrozbám chránit.

Začátek praktické části obsahuje průzkum dnešních technologií používajících NFC a testování bezpečnosti, včetně popisu aplikací pro mobilní telefony s operačním systémem Android.

Dále v praktické části je proveden návrh testů bezpečnosti NFC technologie, které je možné provést za pomocí aplikací pro Android a zakoupeného hardwaru. Testy vycházejí z předchozí rešeršní činnosti.

Samotné testování bylo provedeno na vývojové desce Arduinu UNO s Adafruit PN532 NFC Shieldem, na které byly odzkoušeny programy pro testování. Testování proběhlo také za pomoci mobilního telefonu vybaveného NFC a vybranými aplikacemi. Dále bylo při testování k dispozici několik druhů čipových karet použitých při testování.

V závěrečné diskuzi jsou shrnuty výsledky testů a závěrečné posouzení jejich vypovídací hodnoty a míra přínosu cílené informace o zabezpečení technologie NFC.

Slovník použitých zkratek

NFC – Near Field Communication

RFID – Radio Frequency Identification

NXP – Next Experience, NXP Semiconductors, dříve Phillips Semiconductors

ECMA – European Computer Manufacturers Association

NDEF – NFC Data Exchange Format

LLCP – Logical Link Control Protocot

SNEP – Simple NDEF Exchange Protocol

HCE – Host Control Emulation

URL – Uniform Recource Locator

UICC – Universal Integrated circuit card

SIM – Subscriber Identity Module

RSA – RSA šifra

AES – Advanced Encryption Standard

3DES – Triple DES (Data Encryption Standart)

DoS – Denial of Service

PIN – Personal Identification Number

UID – Unique Indentification Number

OTP – One Time Programmable

ISO – International Organization for Standardization

IEC – Internacional Electrotechnical Commission

JIS – Japanese Industrial Standard

GSM – Globální **S**ystém pro **M**obilní komunikaci

FeliCa – Felicity Card

Seznam pojmů

N-Mark – globální symbol pro NFC technologie

DEF CON – jeden z největším hacker shromáždení, který se každý rok pořádá v Las Vegas v Nevadě

NinjaCon – NinjaCon (dříve známý jako PlumberCon) je každoroční hackerská konference zaměřená na výzkumníky v oblasti bezpečnosti konající se v Rakousku.

4. Near Field Communication

Kapitola se zabývá technologií NFC jejím vznikem, specifikací a uplatněním jejích implementací v dnešní době.

4.1. Definice NFC

NFC je bezdrátová technologie, která umožňuje zařízení shromažďovat a interpretovat data z jiného zařízení nebo NFC tagu umístěného ve velmi malé vzdálenosti.

4.1.1. Vznik NFC

NFC je bezdrátová technologie pro komunikaci na krátké vzdálenosti. Byla vyvinuta společnostmi NXP Semiconductors (dříve Philips Semiconductors) a Sony. NFC je rozšířením technologie RFID a pracuje na jedné z jejích frekvencí, které podporuje, a to 13,56 MHz. Dále ji můžeme považovat za pokrok v proprietárních smartcard protokolech firem Sony a Phillips, proto může být viděna jako další logický krok ve vývoji bezkontaktních technologií u bezkontaktních jízdenek či platebních aplikací.

V roce 2003 byla NFC technologie schválena jako ISO/EIC 18092 standard, který byl již dříve uznán jako ECMA standart. O její standardizaci se dnes stará nezisková organizace NFC fórum, kterou založili v roce 2004 firmy Nokia, Philips a Sony.

NFC fórum je neziskové sdružení vývojářů, výrobců a finančních institucí. Dnes jsou členy tohoto sdružení nejen podniky na výrobu mobilních telefonů, ale také nadnárodní společnosti jako Microsoft Corporation, Visa Inc., MasterCard Worldwide. V roce 2008 měla již přes 150 členů [8].

Obrázek 1 - N - Mark oficiální symbol pro Near field communication

Dva roky od svého založení NFC fórum uveřejnilo svou první specifikaci pro NFC tagy, která měla vzbudit v zainteresovaných skupinách zájem o tvorbu vlastních produktů. Dalším krokem v roce 2006 bylo vydání prvního mobilního telefonu, Nokia 6131, s podporou NFC společností Nokia.

4.1.2. Technologie NFC

Near field Communication je bezdrátová bezkontaktní technologie a jejím konceptem je poskytnout snadnou metodu, jak zprostředkovat propojení mezi zařízeními na krátkou vzdálenost bez nutnosti zabezpečovacích a konfiguračních procedur, jak je tomu u jiných komunikačních technologií [8].

Propojení dvou zařízení probíhá na krátkou vzdálenost několika centimetrů, teoreticky až do 20 cm, ale dosah spojení záleží na řadě faktorů, které ho ovlivňují. NFC pracuje na rádiové frekvenci 13,56 MHz, tedy na jedné ze standardizovaných frekvencí technologie RFID (Radio-frequency identification), ze které NFC vychází a je jejím rozšířením.

Tato frekvence je globálně dostupným a neregulovaným pásem. Tím pádem nejsou zapotřebí žádné licence pro operování v pásmu této frekvence. Přenos dat v rádiovém poli může být kódován Manchester kódováním, nebo Millerovým kódováním.

Technologie je založená na modelu „iniciátor“ a „cíl“, kde iniciátor generuje malé elektromagnetické pole, které napájí cíl, takže cíl nepotřebuje samostatný zdroj napájení. Tento způsob komunikace se nazývá pasivní a je použit pro čtení a zapisování RFID tagů na frekvenci 13,56 MHz odpovídajících standartu ISO14443A.

Aktivní komunikace je možná v případě, že jsou obě dvě zařízení samostatně napájená a každé si nezávisle vytvoří vlastní elektromagnetické pole a poté jedno zaujme funkci iniciátora, druhé cíle a naopak [1].

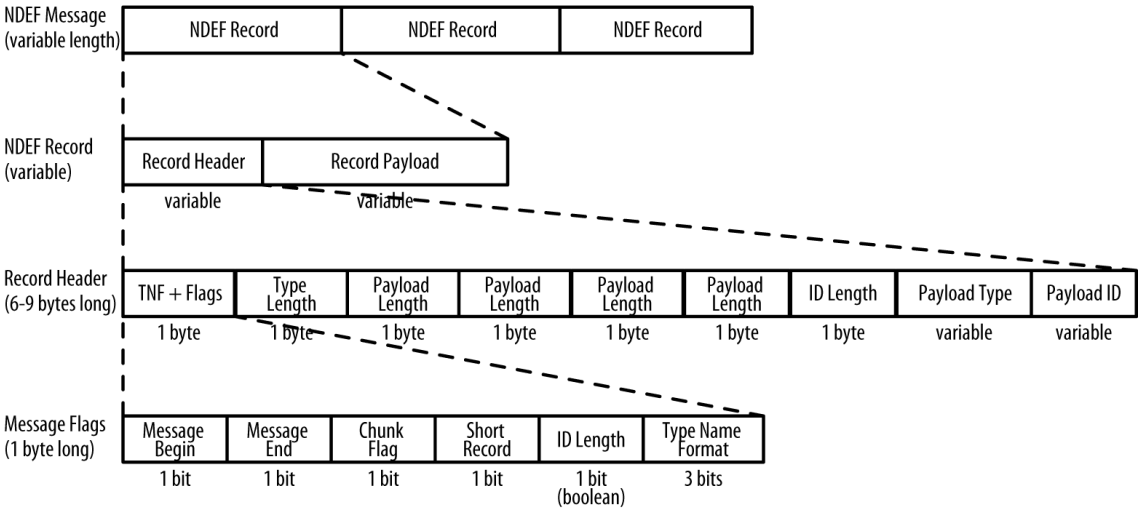
Rychlost přenosu dat se pohybuje v hodnotách 106, 212 a 424 kbps, počáteční rychlost přenosu dat nastavují až samostatné aplikace, které jí mohou později měnit v závislostech na prostředí, v němž probíhá komunikace, a na základě jiných požadavků.

4.1.3. NDEF

NFC Data Exchange Format je standardizovaný binární formát pro ukládání dat na NFC tagy a výměnu informací mezi NFC zařízeními v „peer – to – peer“ módu komunikace pro

zařízení, která dodržují specifikace NFC Fóra [1]. Formát se skládá z NDEF zpráv a NDEF záznamů.

NDEF zapouzdřuje aplikační data a metainformace. Samotná data jsou zabalena do NDEF záznamů. NDEF odstiňuje data od paměťového média a komunikačního kanálu, takže aplikační vrstva NFC zařízení je schopna pracovat s NDEF zprávami a nemusí se zabývat rozdílnými druhy NFC tagů a režimy přenosu. Více NDEF záznamů se sdružuje do NDEF zprávy.



Obrázek 2 - Struktura NDEF zprávy

4.1.3.1. NDEF záznam

Každý NDEF záznam obsahuje "náklad" dat a metadata nutná k správné interpretaci nákladu. Náklad z anglického „payload" je zamýšlená zpráva bez hlaviček a metadat, je to nejdůležitější část celého záznamu, protože je to zpráva uživatele, kterou odesílá. V hlavičce každého NDEF záznamu je obsažen datový typ nákladu, který záznam obsahuje [2].

4.1.3.2. NDEF zpráva

Každá NDEF zpráva může obsahovat více NDEF záznamů jdoucích za sebou. První záznam obsahuje příznak MB, začátek zprávy, a poslední obsahuje ME, konec zprávy. Minimální délkou zprávy je jeden záznam, to je docíleno vložením obou příznaků do jednoho záznamu.

4.1.4. Režimy přenosu

4.1.4.1. Reader/Writer

Režim Reader/Writer (čtení/zápis), nebo také pasivní komunikace probíhá mezi dvěma NFC zařízeními, kde se jedno z nich ujímá role iniciátoru komunikace, tedy ten, který se pokouší

informace přečíst, nebo zapsat. Druhé zařízení se v této chvíli komunikace nachází v roli cíle a pomocí ovlivňování elektromagnetických cívek se na cíli, v podobě transpondéru, začne hromadit energie. Po dosažení dostatečné hladiny odešle anténa transpondéru odpověď zpět druhému zařízení, tedy iniciátoru. V roli cíle komunikace neboli transpondéru se ve většině případů nachází tag odpovídající standartu NFC fóra, se kterým bude moci druhé zařízení navázat kontakt, ale také RFID tagy a bezkontaktní platební karty založené na stejných standardech, ISO/IEC 14443 a FeliCa (JIS X 6319–4) [1]. Ne všechna NFC zařízení jsou kompatibilní se všemi druhů tagů/transpondérů.

4.1.4.2. Peer – to – Peer

Peer – to – Peer režim komunikace neboli aktivní režim komunikace, je velice podobný režimu P2P z počítačových sítí, který je založený na protokolech TCP/IP. Pro NFC je definován ve standartu NFCIP-1(Near field communication – Interface and Protocol, ECMA – 340) a dále pomocí protokolů LLCP a SNEP. Komunikace v Peer – to – Peer režimu je příhodná pro výměnu dat mezi dvěma NFC zařízeními, například mobilními telefony, kde v rámci výměny dat můžeme sdílet kontakty či textové zprávy. U telefonů s operačním systému Android je tato metoda komunikace implementována pod názvem Android Beam nebo u telefonů od společnosti Samsung SBeam.

Stejně jako u režimu Reader/Writer se zde objevují u zařízení role iniciátoru a cíle komunikace. Obě zařízení jsou napájena a střídají se v rolích iniciátoru a cíle. První zařízení zahajuje začátek komunikace, druhé poslouchá a poté naopak. Děje se to díky zapínání (vysílání) a vypínání (poslouchání) magnetického pole obou zařízení.

4.1.4.3. Card Emulation

Card Emulation je třetí režim komunikace v rámci NFC. Při používání Card Emulation se mobilní telefon, nebo jiné proprietární NFC zařízení, začne chovat jako bezkontaktní čipová nebo platební karta. Takto emulovaná karta je poté kompatibilní se všemi zařízeními schopnými pracovat na standardech ISO/IEC 14443 Typ A, ISO/IEC 14443 Typ B a JIS X 6319-4 (FeliCa od Sony) [1]. Komunikace po emulaci karty funguje velice podobně jako v režimu Reader/Writer, kdy čtecí zařízení je iniciátorem komunikace a NFC zařízení s emulovanou kartou zastává roli cíle.

Konkrétně se o emulaci karty stará Secure element, tedy čip uvnitř NFC zařízení, většinou mobilního telefonu, kde se ukládají citlivá data. Emulace karty není nutně řešena pouze

hardwarově, ale může být provedena procesorem hlavní aplikace zařízení, tato metoda se nazývá HCE (Host-based card emulation).

4.2. Dnešní využití technologie NFC

Díky velké míře implementace technologie NFC do mobilních telefonů v dnešní době se s NFC během života setká velké množství jejich majitelů/uživatelů. Dnes se však NFC neobjevuje jen v mobilních telefonech a bezkontaktních platbách.

4.2.1. Bezkontaktní platby

Nejvíce viditelným uplatněním NFC se stala oblast bezkontaktních plateb, která umožňuje za pomoci mobilního telefonu se zabudovaným NFC modulem provést platbu z bankovního účtu. Existuje několik aplikací od různých společností využívajících NFC pro bezkontaktní platby, jako pár příkladů lze uvést Google Wallet, Apple Pay, Samsung Pay a Android Pay. Dále se také bezkontaktní platby pomocí NFC uplatňují u dobíjecích jízdenek pro městkou hromadnou dopravu.

4.2.2. Autentizace

NFC se dá využít pro rychlou autentizaci nebo předání autentizačních údajů a síťových nastavení ostatním uživatelům. Pro příklad lze uvést přeposlání údajů pro připojení k Wi-Fi síti bez nutnosti jejich vyplňování nebo navazování spojení dvou mobilních telefonů pro Bluetooth přenos bez nutnosti potvrzování. Díky krátkému dosahu NFC je spojení navázáno se zařízením, které se nachází v poli druhého zařízení. Tímto se velice zrychluje proces párování zařízení.

Další využití se týká spíše technologie RFID karet, které jsou využívány jako studentské karty nebo hotelové karty. Tato možnost je uvedena z důvodu kompatibility často používaných karet se standarty NFC.

4.2.3. Mobilní telefony

Mobilní telefony s NFC modulem mají dnes velice velkou škálu využití, a to i například díky funkci Beam Everything, s níž je možné přes NFC komunikaci sdílet téměř cokoliv, jako kontaktní údaje, nebo jakákoliv jiná data obsažená ve fyzické paměti mobilního telefonu i ve formě obrázků. Je však nutno pamatovat na to, že se NFC rychlostí nevyrovná jiným bezdrátovým technologiím podporovaným chytrými telefony.

Dále je možné telefony konfigurovat, spouštět jejich aplikace či komunikovat s automobilem též vybaveným NFC. Uživatel musí mít nainstalované aplikace pro práci s NFC, aby mohl

provádět určité úkony, avšak u některých modelů telefonů není povolena úplná podpora NFC například uživatel bude moci pracovat pouze s některými typy NFC tagů.

V poslední době se také začínají objevovat tzv. NFC Wearables, doplňky oděvů obsahující NFC moduly (např. náramky, brýle, prsteny atd.), které je uživatel schopen konfigurovat mobilním telefonem přes aplikace tomu určené.

4.2.4. Hry

I herní průmysl se začal zajímat o NFC technologii a objevují se herní předměty obsahují NFC čipy. Jako příklady lze uvést Skylanders od společnosti Activision, Amiibo od společnosti Nintendo nebo Disney Infinity od společnosti Disney. Aplikace NFC do her jinými způsoby lze najít například u společností Facebook a Rovio, kde je využito propojení dvou mobilních telefonů.

4.2.5. Služby pro společnosti

V dnešní době lze najít využití NFC pro účely reklamy v podobě tzv. „smart posters“. Jedná se o plakáty s integrovanými NFC tagy, které mohou obsahovat odkazy na webové stránky, slevové kupóny nebo jiné dodatečné informace. Podobně řešené jsou i elektronické vizitky v podobě NFC tagu s odkazy na určený web nebo textovým dokumentem obsahujícím požadované údaje. Dalším využitím jsou docházkové systémy s čipovými kartami, znovu se jedná spíše o technologii RFID, ale karty jsou kompatibilní se standarty NFC a jejich čtení bude probíhat pomocí mobilního telefonu vybaveného NFC modulem.

4.2.6. Ostatní

Ostatní využití NFC jsou zde popsány spíše z důvodu budoucího využití pro technologie jako je například zdravotnictví, kde se již experimentuje s nápady na použití elektronických karet pacientů nebo podkožních čipů. Je vidět, že NFC technologie má široké spektrum využití a do budoucna se jistě bude objevovat častěji v dalších oblastech moderních technologií, které se stále častěji stávají součástí životů běžných uživatelů.

4.3. Typy NFC tagů

NFC Fórum vytvořilo 4 standarty typů NFC tagů z důvodu společné spolupráce poskytovatelů NFC tagů a výrobců NFC zařízení a sdílení zkušeností v zájmu dosáhnutí konzistentní uživatelské spokojenosti [7]. Tagy typů 1 a 2 se značně liší od tagů 3 a 4, jak už velikostí kapacity paměti, uspořádáním, nebo také tím, že tagy typů 1 a 2 jsou určeny pro uživatele, kteří si jejich obsah nakonfigurují sami pomocí běžně dostupných prostředků jako je mobilní telefon. Oproti tomu tagy typů 3 a 4 jsou již předkonfigurovány výrobcem a na jejich změnu je zapotřebí vlastnit speciální nástroje na přepisování tagů tohoto typu. Díky tomu je předpokládaný přesah jejich aplikací spíše omezený [8].

NFC Forum [7] a Radio Electronics [8] uvadí následující typy tagů:

- **Tag typu 1** je založen na ISO/IEC 14443 A. Tagy jsou schopny operací, jako je čtení a zápis, dají se nakonfigurovat jako tagy pouze pro čtení. Paměť dosahuje velikosti 96 bajtů až 2 kbajty. Komunikace s tagem typu 1 je založena na technologii NFC – A. Komunikací je myšleno, s jakými typy NFC zařízení bude možno komunikovat podle standartu NFC Fóra. Tagy typu 1 jsou svou velikostí paměti dostačující pro uložení URL nebo malého množství dat. Rychlost komunikace dosahuje hodnot 106 kbit/s, Díky své jednoduchosti a nízké ceně je vhodný pro mnoho NFC aplikací. Kompatibilní produkt je Innovision Topaz.
- **Tag typu 2** je stejně jako předchozí typ založen na ISO/IEC 14443, je schopen vykonávat čtení, zápis a také se dá konfigurovat jako tag pouze pro čtení. Paměť tagů typu 2 dosahuje velikostí 48 bajtů až 2 kbajty. Komunikace s tagem typu 2 je také založen na technologii NFC–A. Rychlost komunikace je stejná jako u tagu typu 1, 106 kbit/s. Na rozdíl od tagu typu 1 obsahuje anti-kolizní mechanismus, který je součástí všech dalších typů tagů. Kompatibilní produkty jsou NXP Mifare Ultralight a NXP Mifare Ultralight C.
- **Tag typu 3** je založen na japonském průmyslovém standartu JIS X 6319-4, který je také známý jako FeliCa od společnosti Sony. Tagy jsou již z výroby předkonfigurovány, aby bylo možné je číst byli přepisovatelné nebo pouze na čtení. Velikost paměti u tagů typu 3 se liší, ale teoretický limit je až 1MBajt. Komunikace je založena na technologii NFC-F, která je kompatibilní s japonským standardem JIS X 6319-4. Rychlost komunikace je 212 kbit/s. Tag typu 3 se využívá pro

komplexnější aplikace než tagy typu 1 a 2 tím pádem je jeho cena vyšší. Kompatibilní produkt je Sony Felica.

- **Tag typu 4** je plně kompatibilní se standardem ISO/IEC 14443. Tagy jsou předkonfigurovány, aby mohli být čteny, byli přepisovatelné nebo pouze na čtení. Paměť tagů typu 4 dosahuje velikosti, až 32 KB. Komunikační rozhraní je v souladu s typem A, nebo typem B. Komunikace typu 4 je založena na ISO Data Exchance Protocol, který je plně kompatibilní se standardem ISO/IEC 14443 a je vybudován na technologiích NFC-A a NFC-B. Rychlost komunikace tag typu 4 se pohybuje mezi 106 až 424 kbit/s. Kompatibilní produkty jsou NXP DESFire a NXP SmartMX – JCOP.
- **Tag typu 5** nejnovější specifikace tagu od NFC Fóra z roku 2015. Tag je kompatibilní se standartem ISO/IEC 15693. Jedním z jeho úkolů je implementace NFC-V technologie do specifikací NFC fóra.

5. Bezpečnost NFC

Kapitola se zabývá prvky ochrany NFC i různými hrozbami pro NFC. NFC je sama o sobě považována za bezpečný způsob komunikace díky svému krátkému dosahu, i přesto se objevují různé možnosti, jak NFC zneužít.

5.1 Bezpečnostní prvky technologie NFC

NFC je standardně považováno za poměrně bezpečnou komunikaci, bezpečnější než RFID, ze které NFC vychází, pouhé zkrácení dosahu signálu vysílání a přijímaní však není dostatečné pro zabezpečení. Bezkontaktní platby pomocí mobilních telefonů nebo jiné aplikace operují s citlivými daty a na základě toho vyžadují vyšší stupeň zabezpečení.

5.1.1. Secure element

Secure element je založen na čipových kartách a v důsledku toho poskytuje stejnou funkcionalitu a ochranu. Pro softwarovou emulaci karet poskytuje secure element bezpečné úložiště a zabezpečené prostředí s hardwarovou podporu pro kryptografické operace. Dokáže ukládat kryptografické klíče takovým způsobem, že je není možné přečíst vně secure elementu. Tím pádem zastává funkci bezpečnostního zařízení, jež nelze duplikovat, může provádět dešifrování a digitální podpisy na základě těchto klíčů. Podobně jako veřejné klíče mohou být ukládány takovým způsobem, aby je mohli aktualizovat pouze autorizovaní účastníci, a proto může secure element fungovat jako nemodifikovatelné bezpečnostní zařízení pro šifrování a ověření digitálních podpisů.

Secure element lze díky svým atributům použít jako bezpečnostní zařízení pro identifikaci, autentizaci a bezpečnost zpráv. Dále se používá v digitálních peněženkách pro uložení platebních karet. Data a aplikace obsažená v secure elementu jsou spravována přes síť mobilního telefonu, jinak nazvané „over-the-air“ management.

SABELLA [3] uvádí následující implementace Secure elementu:

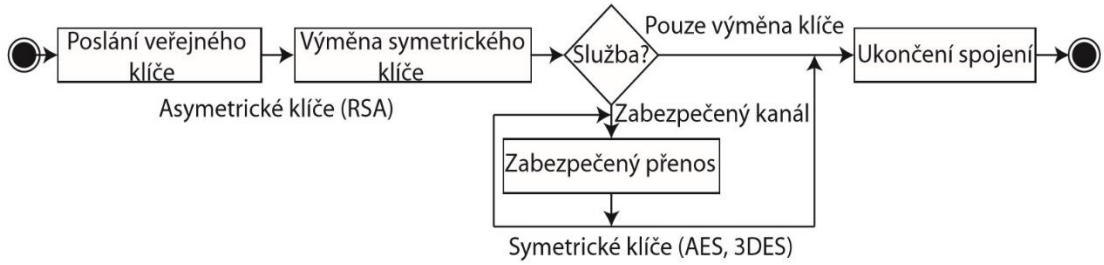
Vestavěný security element je prvkem mobilního telefonu od jeho výroby. Jeho hlavní výhodou, že není potřeba dokupovat další speciální zařízení, aby bylo dosaženo bezpečnostních. Díky tomu, že je secure element pevně napájen na základní desku telefonu nebo je součástí NFC kontroléru, není možné jej snadno vyjmout a vložit do jiného zařízení. Obvykle bývá spravován svým výrobcem, nebo příslušným operátorem mobilní sítě.

Další možností je použití zabezpečení založené na SIM kartách, které se nazývá Universal Intergrated Circuit Card neboli UICC, a je povinný pro standarty GSM a LTE. Pomocí něj získáme nejjednodušší možnost pro podporu Secure Elementu u jakéhokoliv chytrého telefonu. Tím pádem jí však někdo může potencionálně snadno odcizit a použít kartu v jiném zařízení.

Třetí možností je použití SD paměťové karty, která obsahuje NFC čip, nebo se dokáže propojit s NFC kontrolérem obsaženým v mobilním telefonu. Tento způsob je již zastaralý, jeho hlavním účelem bylo umožnit majitelům starších telefonů provádět bezkontaktní platby. Dnešní chytré telefony už mívají nativně zabudovaný Secure element od výrobce díky dnešní rozsáhlé podpoře NFC.

5.1.2. Secure channel

Vytvoření zabezpečeného kanálu mezi NFC zařízeními je nejlepší způsob, jak ochránit komunikaci proti odposlechu a dalším útokům zaměřujícím se na modifikaci dat. Při vytváření zabezpečeného kanálu je nejprve použit protokol pro výměnu klíčů, například Diffie-Helmann založený na RSA nebo Eliptické křivky k vytvoření sdíleného tajemství mezi dvěma zařízeními. Sdílené tajemství pak může být použito k odvození symetrického klíče jako 3DES nebo AES, který je použit pro zabezpečený kanál, který poskytuje důvěrnost, integritu a autenticitu přenášených dat [9].



Obrázek 3 - Základní kroky pro vytvoření zabezpečeného kanálu

Zmiňovaný způsob je považován za standartní šifrovací mechanismus, ale je možné se od něj odchýlit a implementovat mechanismus specifického klíče. Ten teoreticky také poskytuje dostatečnou bezpečnost, ale nevyžaduje použití asymetrické kryptografie, a proto výrazně redukuje výpočetní nároky. Dosud tento mechanismus nebyl standardizován ISO normou. Tento mechanismus funguje na principu synchronizace mezi dvěma zařízeními, ale podmínkou je, že jedno ze zařízení musí být aktivní, aby mohlo inicializovat proces

synchronizace. Zařízení komunikují ve stejný čas a pracují se stejnými bity amplitudami radiofrekvenčního signálu. Bezpečnost tohoto mechanismu závisí na kvalitě dosažené synchronizace mezi zařízeními a na vzdálenosti potencionálního útočníka [12].

5.2. Možnosti zneužití NFC

NFC technologie se vyznačuje svým velice krátkým dosahem, který se pohybuje pouze v rozmezí několika centimetrů, i přestože je tento atribut považován za bezpečnostní aspekt, objevují se různé možnosti zneužití NFC.

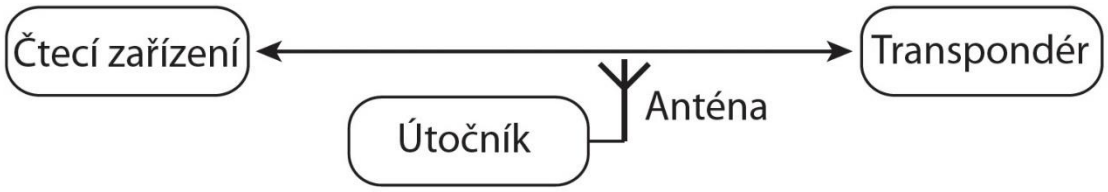
Technologie NFC má standardně nezabezpečenou komunikaci. O její zabezpečení se poté starají až samy komunikující strany na vyšších vrstvách, nebo je možné použít další přídavné algoritmy pro zabezpečení průběhu komunikace samotné.

Díky své poměrné jednoduchosti se NFC technologie v posledních letech velice prosadila, ale také je díky ní zranitelná v oblasti možných odposlechů komunikace a tím pádem i k modifikaci dat během ní [4].

5.2.1. Eavesdropping – Odposlech

NFC je technologie bezdrátové komunikace, a proto vyvstává otázka, zda se dá komunikace mezi dvěma NFC zařízeními odposlouchávat. NFC komunikace se sama o sobě nešifruje a díky tomu je její odposlech možný pomocí antény, zesilovače a dekódovacího zařízení [4].

Možnosti úspěšného odposlechu záleží na velkém množství proměnných, zejména v jakém režimu je komunikace prováděna, zda v aktivním či pasivním. Odposlech komunikace v pasivním módu je velice složitý z toho důvodu, že tagu je energie dodávaná čtecím zařízením a odpověď je odesílána s relativně nízkým ziskem na krátkou vzdálenost. Během komunikace v aktivním režimu je situace pro odposlech příznivější, protože obě zařízení disponují vlastním napájením a obě jsou schopná vytvářet vlastní rádiové pole.



Obrázek 4 - Schéma odposlechu

Nutná vzdálenost útočníka pro úspěšný odposlech se nedá naprosto přesně určit. Tento parametr záleží na několika velice důležitých faktorech [1], mezi které můžeme zařadit charakteristiky odesílacího zařízení nebo útočníkovi antény, kvalitu útočníkova

přijímače/dekodéru, lokaci, ve které bude odposlech prováděn, nebo množství energii poslané NFC zařízením.

Při zohlednění všech těchto faktorů může být odposlech teoreticky proveden při aktivním režimu na vzdálenost do 10 metrů a při pasivním na vzdálenost do 1 metru.

Úspěšný odposlech není definován jako odposlechnutí celé probíhající komunikace, ale pouze její dostatečně velké části, aby z ní útočník získal takové množství informací, které jsou dostačující pro zjištění obsahu.

Zabezpečení komunikace mezi zařízeními proti odposlechu je možné pouze použitím zabezpečeného kanálu, který bude šifrovat danou probíhající komunikaci, protože NFC technologie sama neobsahuje žádný implementovaný mechanismus pro šifrování komunikace.

5.2.2. Data Corruption – Poškození dat

Poškození dat neboli Data Corruption je jednou z možností, jak narušit NFC komunikaci. Může to být provedeno tím, že útočník začne vysílat signál na správné frekvenci ve správný čas a zamezí tím čtecímu zařízení porozumět komunikaci se zamýšleným zařízením. Správný čas vysílání se dá vypočítat za předpokladu, že útočník má znalosti o použitém modulačním schématu a kódování. Útok není příliš složitý, protože útočník nepotřebuje dešifrovat zprávy zašifrované v komunikaci, ale neumožňuje útočníkovi manipulovat s odesílanými daty, a to znamená, že je jednou z forem DoS (Denial of Service) útoku [1, 7].

Moderní zařízení vybavené NFC se dokážou těmto útokům bránit kontrolou rádiového pole ve svém okolí, které si vytváří, a díky tomu může detekovat útok. Energie nutná k přerušení komunikace je mnohem větší než množství energie, které je potřeba k detekci NFC zařízení. Na základě tohoto tvrzení je možné každý tento útok detekovat, ale ne mu zcela zabránit [1, 4].

5.2.3. Data Modification – Modifikace dat

Během modifikace dat se případný útočník snaží upravit obsah komunikace, aby se jevil zařízení, které data přijímá, jako naprosto validní. Tento typ útoku je mnohem složitější, něž pouhé narušení komunikace. Pokud chce útočník úspěšně provést tento typ útoku, musí mít velké znalosti o použitém kódování a hloubce modulace, protože na nich proveditelnost útoku velmi záleží, následné dekódování signálu se liší podle kódování a modulace.

Změna přenášených dat probíhá modifikací jednotlivých bitů radiofrekvenčního signálu ve velice krátkém časovém intervalu. Útočník k tomu musí znovu použít větší vysílací výkon, než je výkon komunikujících zařízení, aby byl schopen zasáhnou do komunikace a změnit její jednotlivé bity [1, 4, 8].

Ochránit NFC komunikaci proti modifikaci dat je možné při použití lepšího kódování a větší hloubce amplitudové modulace, jako například použitím Millerova kódování. U tohoto typu kódování lze měnit pouze některé bity naproti tomu u kódování typu Manchester lze měnit všechny bity. Tím lze snížit riziko úspěšné modifikace dat během komunikace.

Dále lze jako u předchozího útoku za účelem poškození dat průběžně kontrolovat radiofrekvenčního pole při odesílání dat a při zjištění narušení, zastavit přenos dat a uzavřít komunikaci. Další možností, jak se bránit proti podobným útokům, je využití zabezpečeného kanálu pro komunikaci [1, 4, 8].

5.2.4. Data Insertion – Vkládání dat

Vkládání dat do komunikace mezi NFC zařízeními je útočníkem proveditelné pouze v případě, že NFC transpondér potřebuje pro odpověď čtecímu zařízení dlouhou dobu. V takové chvíli je možné, aby útočník odeslal svoji alternativní zprávu čtecímu zařízení dříve než NFC transpondér. Zpráva se poté bude zdát jako validní a čtecí zařízení zprávu přijme.

Tento útok velice závisí na rychlosti, jakou je útočník schopen odpovědět a na době jakou bude muset čtecí zařízení čekat na odpověď od transpondéru. Pokud se útočníkova zpráva bude překrývat se zprávou od transpondéru, data se poškodí a čtecí zařízení je obě vyhodnotí jako chybné [1, 4].

Existuje několik opatření, která mohou zabránit útočníkovi úspěšně provést tento útok. První takové opatření spočívá ve zkrácení doby nutné pro odpověď čtecímu zařízení, aby útočník nestačil vložit svá data do komunikace a byla přijata pouze originální data od správného transpondéru.

Dalším opatřením je monitorování elektromagnetických vln v okolí transpondéru a při detekci narušení odstoupení od komunikace. Posledním opatřením pro zabránění útoku je použití zabezpečeného kanálu pro komunikaci [1,4].

5.2.5. Man in the Middle attack – Útok ze středu

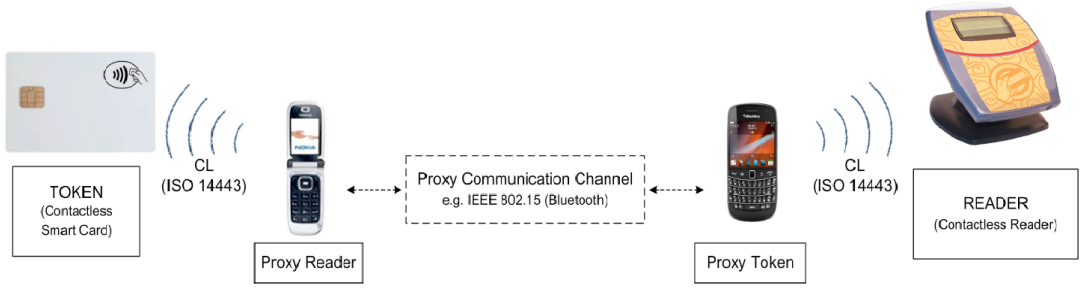
Man – in – the – middle útok je za pomoci technologie NFC prakticky neproveditelné uskutečnit v reálných podmínkách, ale pouze za velice nepravděpodobných předpokladů by jej bylo možné teoreticky provést. V obou režimech přenosu, ať už pasivním režimu Reader/Writer nebo i aktivním Peer-to-peer režimu komunikace, vždy jedna strana zaznamená narušení komunikace a je ji schopna poté přerušit a zabránit útočníkovi dál pokračovat v útoku [1].

I když je Man – in – the – middle útok proveditelný pouze teoreticky za nereálných podmínek existují doporučení i proti tomuto útoku, mezi která patří používání prioritně pasivní režim komunikace a sledování radiofrekvenčního pole okolo zařízení iniciátorem komunikace z důvodu detekce narušení komunikace potencionálním útočníkem [1, 8].

V odborné literatuře se Man – in – the – Middle útok často zaměňuje nebo dokonce slučuje s Relay Attack – Přepojovaným útokem. Avšak v prvním zmíněném případě útočník zasahuje do již započaté komunikace mezi dvěma stranami a během Přepojovaného útoku je právě útočník iniciátorem komunikace mezi ním a obětí.

5.2.6. Relay Attack – Přepojovaný útok

Pro úspěšné provedení přepojovaného útoku, tedy útoku podobného man – in – the – middle útoku, útočník potřebuje dvě zařízení, kdy jedno působí jako token a druhé jako čtecí zařízení. Tato zařízení jsou připojena přes vhodný komunikační kanál, aby bylo možné přenést informace na delší vzdálenost například Bluetooth nebo Wi-Fi. Proxy-čtecí zařízení se používá pro komunikaci se skutečným tokenem, zatímco proxy-token je umístěn v blízkosti skutečného čtecího zařízení. Jakékoli informace přenášené čtecím zařízením jsou přijaté proxy-tokenem a přenášeny na proxy-čtecí zařízení, který přenese informace do tokenu. Token předpokládá, že s ním komunikuje skutečné čtecí zařízení a standartním způsobem odpovídá zpět. Odpověď tokenu je potom převedena zpět na proxy-token, který předá informace skutečnému čtecímu zařízení. Záměr útočníka je zajistit, aby skutečné čtecí zařízení nebylo schopno rozlišit mezi skutečným tokenem a proxy-tokenem. Jestliže uspěje, skutečné čtecí zařízení předpokládá, že token a jeho pravý majitel jsou v jeho těsné blízkosti a poskytne tak přístup útočníkovi [5].



Obrázek 5 - Přepojovaný útok za pomocí dvou mobilních telefonů

Proveditelnost daného útoku závisí zcela na tom, že jedno ze zařízení bude pasivní a druhé aktivní, ve scénáři, kdy by obě napadená zařízení byli aktivními prvky by si útočník musel být jistý, že dokáže zajistit komunikaci v reálném čase, aby komunikující strany nezjistily narušení či zpoždění komunikace a následné od ní odstoupily a tím zmařily šance na útočníkův úspěch [4].

5.2.7. Replay Attack – Opakované přenášení

Základní myšlenkou opakovaného přenosu je odposlechnutí komunikace mezi dvěma zařízeními a její uložení, aby poté mohla být znovu opakovaně přehrána a tím se vydávat za zprávu z originálního transpondéru.

Jednou z výhod tohoto útoku je, že útočník nemusí rozumět nebo upravovat odposlechnutá data z komunikace. Toto platí pouze pokud je komunikace nešifrovaná, pokud ano musí ji útočník nejdříve rozšifrovat pomocí příslušných klíčů. Tento útok je možné provádět na NFC karty používané v městské hromadné dopravě, kdy útočníkovi stačí odposlechnout komunikaci probíhající platby za jízdenku a poté odposlechnutou zprávu čtecímu zařízení. Dále také může útočník odposlechnout a zopakovat ověřovací sekvenci u bezkontaktních plateb debetní/kreditní kartou a mít přístup k bankovnímu účtu. To se týká pouze bezkontaktních plateb, které nepotřebují pro potvrzení zadání PIN kódu.

Ochranou proti opakovanému přenášení může být použití časových razítek, pořadových čísel datových jednotek nebo i čítač transakcí, který se bude inkrementovat při navázání nového spojení.

Více zabezpečenou možností je použití generátoru náhodného čísla, které bude číslo generovat při každém novém spojení. Náhodné číslo by se mělo odvozovat od šifrovacího klíče, kterým bude zabezpečena celá komunikace [4].

5.2.8. Ztráta zařízení

Přestože ztráta NFC zařízení nepatří k běžným útokům, které jsou prováděny na bezdrátové komunikace, i jí musíme zařadit jako hrozbu pro technologii NFC. Ztracená bezkontaktní karta bude sloužit nálezci stejně tak jako sloužila svému původnímu majiteli. Její nálezce s ní bude moci překonávat autentizační mechanismy. Stejně jako mobilní telefony vybavené NFC technologií a používané pro bezkontaktní platby bude nálezci sloužit jako původnímu majiteli, pokud nebudou použity ochranné mechanismy jako hesla, PIN kódy nebo gesta pro uzamčení telefonu. NFC nelze používat, pokud je obrazovka telefonu zamčena či vypnuta.

Jako ochranu proti zneužití u případné ztráty zařízení lze jen doporučit používání aplikací disponujících šifrovacími algoritmy a používat silná hesla, které je nutné bezpečně uložit v paměti zařízení. U mobilních telefonů jsou to bezpečností mechanizmy pro zamykání obrazovky telefonu jako hesla, PIN kódy, gesta nebo i biometrie. Také je doporučeno mít NFC funkci u svého telefonu vypnutou a zapínat jen ve chvílích nutných pro použití.

5.2.9. Další možné hrozby pro NFC

V této podkapitole jsou uvedeny další hrozby pro NFC, které nejsou až tak známé a spíše se týkají mobilních telefonů vybavených NFC, protože můžeme NFC považovat za další možný vektor pro napadení mobilních telefonů.

Malicious tags – Škodlivé tagy

Škodlivými tagy se rozumí speciální tagy s NDEF záznamy, které jsou určené k poškození uživatelů. Mohou se objevovat na veřejných místech a to způsobem, že útočník přelepí originální tag svým vlastním tagem a odstíní jej hliníkovou fólií, aby jej nebylo možno přečíst, či zformátováním originálního tagu a nahráním své škodlivé zprávy na tag. Tato hrozba je závažnější, než se zdá, protože se NFC tagy začínají čím dál tím více objevovat na veřejných místech například ve formě „smart posters“ nebo v restauracích zabudované ve stolech kde si poté mohou zákazníci přečíst marketingové materiály či získat přístup k Wi-Fi.

Tato hrozba je velmi závislá na obezřetnosti dnešních uživatelů „chytrých“ telefonů, zda kontrolují notifikační zprávy na obrazovkách jejich telefonů a zda je pouze dále nepotvrzují. Toto může vést k situacím, kdy se uživatelé dostanou na podvržené webové stránky určené k „phishingu“ a jiným nekalým aktivitám, či načtení různých příkazů pro mobilní telefon z tagu, které mohou vyvolat akce jako volání různých čísel, odesílání zpráv a emailů nebo

stahování dodatečného nevyžádaného obsahu. Takovéto tagy vytvořil Collin Mulliner pro konferenci NinjaCON v roce 2011 v rámci výzkumu bezpečnosti NFC a NDEF v mobilních telefonech [13].

Název hrozby	**Teoretická proveditelnost**	**Praktická proveditelnost**	**Úspěšně vyzkoušeno**	**Technologie**
Eavesdropping	ANO	ANO	ANO	Shield, TagInfo
Data Corruption	ANO	ANO	ANO	Shield, TagInfo
Data Modification	ANO	ANO ale pouze v laboratorních podmínkách	NE	
Data Insertion	ANO	ANO ale pouze v laboratorních podmínkách	NE	
Man – in – the Middle	NE	NE	NE	
Relay Attack	ANO	ANO ale pouze v laboratorních podmínkách	NE	
Replay Attack	ANO	ANO	NE	NFCProxy
Ztráta zařízení	ANO	ANO	ANO	
Lock Attack	ANO	ANO	ANO	NFCuIT
Malicious Tags	ANO	ANO	ANO	TagWriter

Tabulka 1 - Hrozby a jejich proveditelnosti

6. Praktická část

Praktická část obsahuje nejprve přípravnou část s průzkumem trhu, poté testovací část, kde jsou popsány jednotlivé testovací scénáře a jejich průběh. V závěru praktické části se nachází diskuze výsledků testování bezpečnosti NFC technologie, ve které jsou shrnuty poznatky získané během testování.

6.1. Analýza trhu

Pro práci s NFC se na dnešním trhu vyskytuje velké množství zařízení schopných komunikovat s NFC tagy a dají se rozdělit do dvou kategorií. První kategorií jsou speciální čtecí zařízení pro práci s NFC a druhou jsou mobilní telefony se zabudovanými moduly technologie NFC.

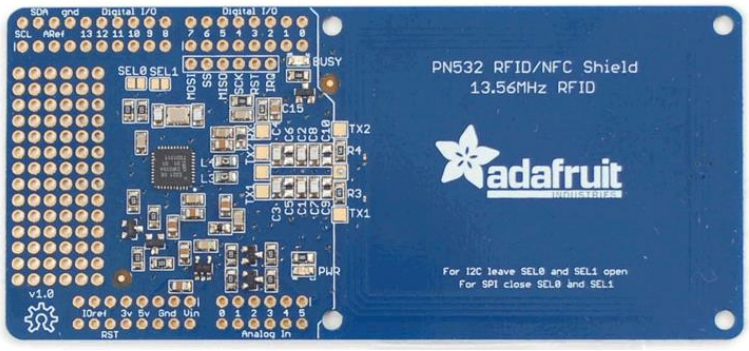
6.1.1. Čtecí zařízení

Tato čtecí zařízení jsou speciálně vytvářena pro práci s NFC a na trhu se vyskytuje široký sortiment takových čtecích zařízení. Kromě čtecích zařízení, která jsou opravdu schopna jen „přečíst“ obsahy tagů, jsou k dispozici složitější zařízení, která mohou jejich uživatelé programovat. Tato zařízení lze dále rozdělit do tří skupin.

První jsou NFC zařízení, která se používají/programují po připojení k osobnímu počítači jako například ACR122U a jemu podobné a jsou schopna komunikovat se všemi čtyřmi typy NFC tagů.

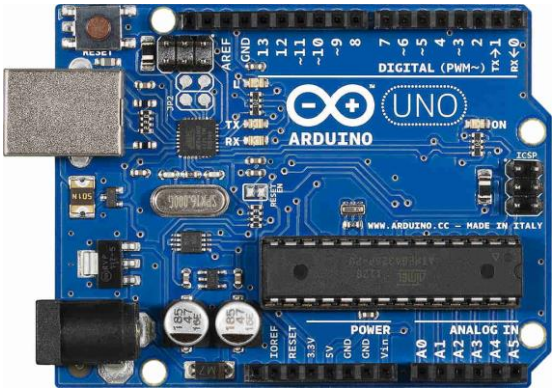
Obrázek 6 - ACR122U

Druhou skupinou zařízení jsou rozšíření pro vývojové desky neboli „shieldy“, které se dají připojit a programovat pomocí Arduina nebo Rapsberry Pi, mezi které patří Adafruit PN532, Saeed Studio NFC Shield a NFC Shield v2.0. Každý shield má programovou podporu pro určitou vývojovou platformu například knihovny od společnosti Adafruit pro Arduino. Samostatné shieldy jsou jen o málo levnější než samostatná zařízení, ale dále je nutné společně s nimi použít i vývojovou desku jako je například Arduino UNO.



Obrázek 7 - Adafruit PN532 NFC Shield

Arduino je malý jednodeskový počítač založený na mikrokontrolerech ATmega od firmy Atmel, společeně s vývojovým prostředním Arduino IDE. Na rozdíl od Rapsberry Pi není zamýšleno jako plnohodnotný počítač. Programy jsou vytvářeny zvlášť, poté jsou nahrány do Arduina a následně spuštěn.



Obrázek 8 - Arduino UNO

Třetí skupinou jsou speciálně vytvořené sety pro exploitaci NFC technologie v čele s kitem Proxmark3 od společnosti RyscCorp., který obsahuje vše potřebné pro výzkum a vývoj bezpečnosti NFC technologie a bezkontaktních plateb. Tento kit je však velice finančně nákladný, je to nástroj určený pouze pro výzkum a vývoj, proto se musí jeho

majitel, nebo osoba, která si tuto sadu chce opatřit, ujistit, zda neporušuje jeho použitím zákony své země. Toto varování uvádí i výrobce na svých webových stránkách, kde je Proxmark3 k dispozici ke koupi.

Obrázek 9 - Proxmark3 Kit od společnosti RyscCorp.

6.1.2. Mobilní telefony a jejich aplikace

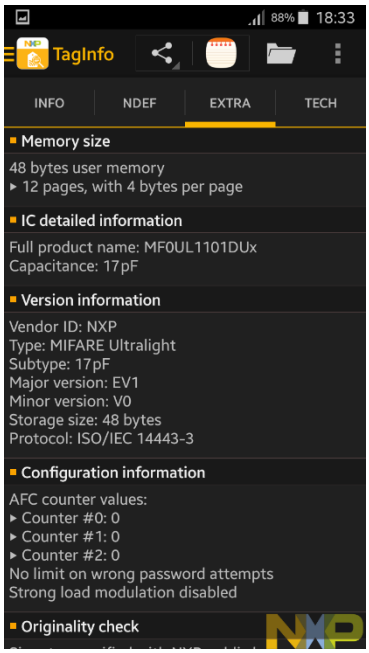
Mobilní telefony jako zařízení schopná komunikovat pomocí NFC jsou dnes mnohem větší skupinou než specializovaná čtecí zařízení. Aktuální seznamy mobilních zařízení vybavených NFC je možné najít na webových stránkách www.nfcworld.com nebo www.unitag.io, kde jsou denně aktualizovány.

Ne každý chytrý telefon a jeho operační systém však podporuje všechny typy vyráběných NFC tagů, v některých případech dokáží mobilní telefony přečíst pouze UID daného NFC tagu. Další úkony je v případě nekompatibility nemožné provést, například čtení a změna obsahu tagu a v nich uložených NDEF zpráv.

Veškerou funkcionalitu přesahující přečtení obsahu tagu a provedení zapsaných operací je nutné implementovat do mobilního telefonu pomocí doprovodných aplikací. Aplikace pro telefony s operačním systémem Android je možné stáhnout buď z obchodu Google Play a jednoduše je nainstalovat, nebo je stáhnout z GitHubu či jiných serverů přímo od jejich vývojářů. Takto opatřené aplikace je někdy nutné zkompilovat, aby mohli být naistalovány na mobilní telefon, nebo pro některé aplikace je nutné provést úpravy přímo na mobilním telefonu pro jejich správnou funkcionalitu, například instalace CyanogenModu.

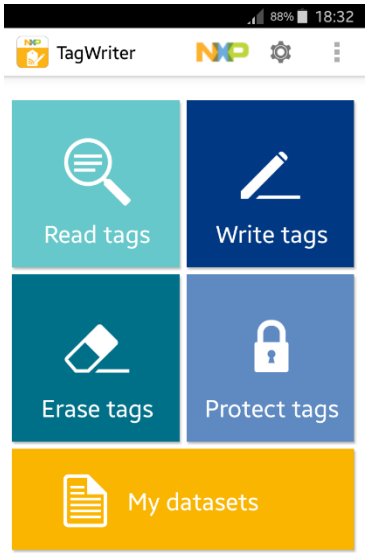
NFC aplikace určené speciálně pro operační systém Android mohou být rozděleny do dvou kategorií. První jsou základní aplikace pro práci s NFC, které vytvářejí samy společnosti zabývající se NFC vývojem. Společnost NXP Semiconductors, zabývající se výrobou NFC tagů, vydala dvě NFC aplikace jménem TagWriter a TagInfo.

TagInfo je aplikace pro čtení tagů, která podává o tagu velice podrobné informace, jako jsou například: výrobce, typ, standart NFC fóra, velikost, rozdělení a obsah paměti tagu, jaké technologie tag podporuje (NFC knihovny pro Android, a tedy i příkazy obsaženy v NDEF záznamech) a také způsob ochrany sektoru paměti tagu proti přepsání heslem nebo je zamknutý natrvalo.



Obrázek 10 - Snímek obrazovky s aplikací TagInfo

Další aplikací od NXP Semiconductors je TagWriter. TagWriter je aplikací, která umožnuje vytvářet obsah tagů, zabezpečovat je heslem a mazat obsah tagů, pokud nejsou chráněny proti přepsání. Obsahem tagů mohou být příkazy podobě NDEF záznamů k nastavení telefonu, spuštění jiných nainstalovaných aplikací, nebo odkazy na webové stránky, které se mohou pouze zobrazit jako link či se hned spustit v internetovém prohlížeči, eventuálně pouze text, který se zobrazí na obrazovce telefonu k přečtení.



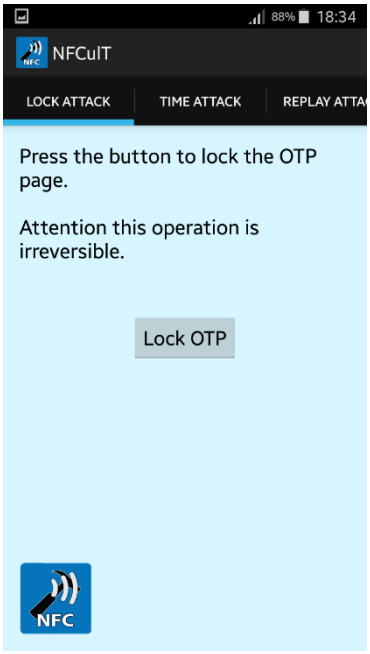
Obrázek 11 - Snímek obrazovky s aplikací TagWriter

Druhou kategorií jsou NFC aplikace zabývající se výzkumem bezpečnosti NFC technologie. Jsou to speciální aplikace, které byly vytvořeny pro exploitaci NFC technologie a byly předvedeny na konferencích o bezpečnosti informačních technologií jako je například DEF CON. Dvě zajímavé aplikace z této kategorie jsou NFCuIT a NFCProxy.

NFCuIT je aplikací speciálně vytvořenou pro exploataci tagu Mifare Classic Ultralight, která bývá často používána jako bezkontaktní nabíjecí jízdenka pro městkou hromadnou dopravu z důvodu její cenové dostupnosti. Díky aplikaci NFCuIT je možno jízdenku upravit, aby jí bylo možné používat opakovaně bez nutnosti dobíjení, a to několika způsoby.

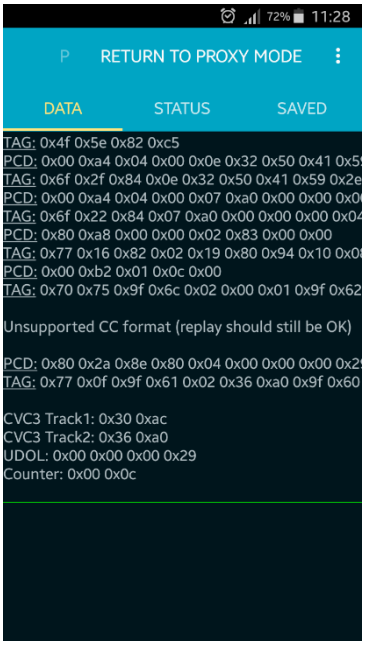
Prvním způsobem je Lock Attack, jenž na tagu zamkne OTP sektor, který je možné upravovat pouze jednou. Tímto se zamkne celá jízdenka proti úpravám a terminál, který odečítá jízdy z jízdenky, správně načte UID tagu a povolí jízdu, ale už není schopen změnit paměť jízdenky a odečíst jízdu.

Dále aplikace obsahuje možnost změnit časovou známku obsaženou na tagu. Poté aplikace umožňuje provést Replay Attack, kdy načte jízdenku, uloží její otisk a poté je možné jí znovu přehrát.



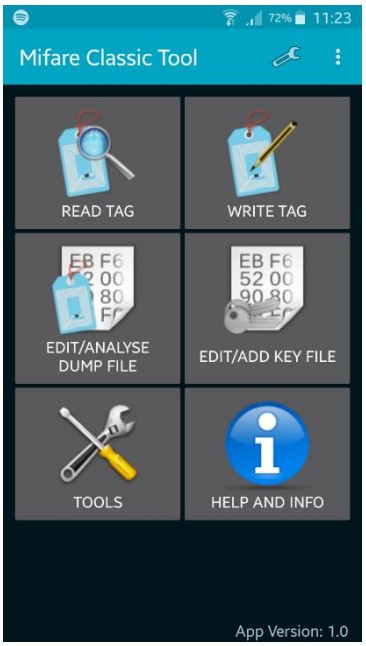
Obrázek 12 - Snímek obrazovky s aplikací NFCuIT

Aplikace NFCProxy je aplikací zaměřenou na exploataci bezkontaktních platebních karet. Ty je možné načíst do paměti telefonu a následně je znovu přehrát v režimu Card Emulation. Další možností je otisk karty odeslat pomocí Wi-Fi na jiný telefon s nainstalovanou aplikací NFCProxy a přehrát ho na jiném místě. Tento způsob se nazývá Relay Attack, který velice podobný technice Man-in-the-Middle jen s tím rozdílem, že komunikaci s oběma stranami navazuje útočník a poté pouze přeposílá zprávy mezi nimi.



Obrázek 13 - Snímek obrazovky s aplikací NFCProxy

Poslední zajímavou aplikací je Mifare Classic Tool, která není aplikací přímo k testování bezpečnosti NFC, obsahuje však několik zajímavých funkcí. První je vytváření „memory dump“ souborů z přečtených tagů a poté také rozšifrování obsahu tagu, pokud jsou vloženy oba nutné klíče. Kromě toho aplikace poskytuje i obyčejné funkce jako je čtení a zapisování tagů, ale pouze na tagy typu Mifare Classic.



Obrázek 14 - Aplikace Mifare Classic Tool

6.1.3. NFC Tagy

NFC tagy jsou hlavní způsob dnešního využití NFC technologie. Tagy se objevují v různých variantách, jako jsou karty, čipy na klíče, náramky a v zahraničí i v mnohem exotičtějších formách jako prsteny, dále jako „smart posters“ tedy plakáty s čipem, který obsahuje další informace nebo odkaz na webové stránky, či podkožní čipy, které je možné implantovat do dlaní a poté s nimi otevírat elektronicky zamčené zámky vybavené NFC čtecím zařízením.

6.2. Příprava

Po průzkumu trhu vyplynulo jako nejvhodnější NFC zařízení pro zakoupení Adafruit PN532 Shield s vývojovou deskou Arduino Uno, což byla finančně nejpřívětivější možnost a vývojové prostředí Arduino IDE nabízí široké možnosti pro programování desky.

Deska je klasickým Shieldem (nadstavbou) pro vývojovou platformu Arduino, ale lze ji také připojit a programovat pomocí Rapsberry Pi. Shield obsahuje dnes asi nejvíce rozšířenou anténu PN532 pro NFC komunikaci, která se velice hojně vyskytuje i v mobilních telefonech.

Adafruit PN532 Shield není obvykle k dostání u tuzemských prodejců elektroniky, ale bylo jej možné objednat v zahraničí ze specializovaného online obchodu, www.hackthecar.com, sídlícím ve Francii.

Pro seznámení se základními funkcemi a otestovaní funkčnosti Adafruit PN532 Shieldu byla použita kniha Beginning NFC Near Field Communication with Arduino, Android, and PhoneGap, která obsahuje velice podrobné informace pro začátečníky i pokročilé uživatele, kteří se chtějí zabývat technologií NFC, a praktické ukázky právě pro Adafruit PN532 Shield společně s vývojovou deskou Arduino UNO. Dále také odkazy na knihovny pro vývojové prostředí Arduino IDE, které podporují mnohem více možností než knihovna dodávaná společností Adafruit společně s manuálem k Shieldu PN532.

NFC tagy, které byly opatřeny, pocházejí z našeho trhu, nfcmall.com, který je největším českým e-shopem pro prodej NFC tagů. Tagy z tohoto obchodu jsou obvykle používány jako prostředky pro marketingové účely. Pro testovací účely byly opatřeny NFC tagy Mifare Ultralight, Mifare Classic 1K a NTAG 203, dostupné v obchodě

7. Testování

Pro otestování možné zranitelnosti NFC technologie byla provedena řada testů s různými NFC tagy za pomocí různých mobilních aplikací pro Android a programů pro Arduino UNO s Adafruit PN532 NFC Shield s několika knihovnami pro Arduino IDE.

7.1 Tag Reading

Tag Reading neboli čtení tagů byl prvním spíše pomocným testem, který byl použit k počátečnímu seznámení s technologií a zjištění, co všechno o sobě NFC tagy prozradí pouze za pomoci oficiálních aplikací a později i Adafruit PN532 NFC Shieldu.

Nejvíce informací o NFC tagu dokázala získat aplikace TagInfo od společnosti NXP Semiconductors, která je volně ke stažení v obchodě GooglePlay. Díky této aplikaci bylo možné přečíst data podle toho, co podporuje mobilní telefon, na kterém je aplikace naistalována. Například u Samsungu S5 Mini použitého během testování je podpora NFC tagů typu Mifare Classic 1K velice omezena a aplikace je poté schopna přečíst pouze základní informace jako ATQA (kód výrobce), SAK (kód výrobku) a UID tagu, ale i tyto informace o výrobci nemusí být přesné kvůli nekompatibilitě, na kterou aplikace upozorňuje. Oproti tomu u jiných typů NFC tagů jako Mifare Classic Ultralight a NTAG 203 byla aplikace byla aplikace schopná přečíst mnohem více informací včetně obsahu paměti tagů.

V případě, že by bylo úložiště zablokováno proti čtení jako u platebních či i jiných tagů/karet, je nutné znát klíče pro rozšifrování obsahu.

Při čtení za pomocí Adafruit PN532 NFC Shieldu připojeného k Arduinu UNO bylo možné pomocí jednoduchých programů přečíst tagy, a to mnohem rychleji než za pomoci mobilního telefonu, ale hlavně na mnohem větší vzdálenost. Shield dokázal přečíst tag na vzdálenost až 20 cm, oproti tomu mobilní telefon přečetl tag na vzdálenost asi 2 cm a většinou bylo nutné tag přiložit přímo k zadnímu krytu telefonu, kde se nachází modul pro čtení NFC tagů. Toto lze připisovat zkrácení dosahu NFC u mobilních telefonů a to z důvodu zvýšené bezpečnosti komunikace. Hlavní nevýhodou čtení pomocí Shieldu byla

nutnost nahrát jiný program speciálně zaměřený pro každý typ tagu a při neznalosti typu tagu použít program pro jeho rozeznání.

```
if (uidLength == 4)
{
  Serial.println("Mifare Classic card (4 byte UID)");
  Serial.println("Trying to authenticate block 4 with default KEYA value");
  uint8_t keya[6] = { 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF }; //KeyA: 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF
  success = nfc.mifareclassic_AuthenticateBlock(uid, uidLength, 4, 0, keya); //autentizace pro read/write přístup
  if (success)
  {
    Serial.println("Sector 1 (Blocks 4..7) has been authenticated");
    uint8_t data[16];
    success = nfc.mifareclassic_ReadDataBlock(4, data); //čtení z bloku 4
    if (success)
    {
      Serial.println("Reading Block 4:");
      nfc.PrintHexChar(data, 16);
      Serial.println("");
      delay(1000);
    }
    else
    {
      Serial.println("Unable to read the requested block. Try another key?");
    }
  }
  else
  {
    Serial.println("Authentication failed: Try another key?");
  }
}
```

Obrázek 15 - Úryvek kódu pro čtení Mifare Classic tagu pomocí Adafruit PN532 Shield v Arduino IDE

7.2 Memory dumping

Memory dumping neboli uložení obrazu tagu je jeden z velice důležitých kroků pro provedení Opakovaného přenosu (Replay attack). Během testu byly použity 4 možnosti vytvoření obrazu.

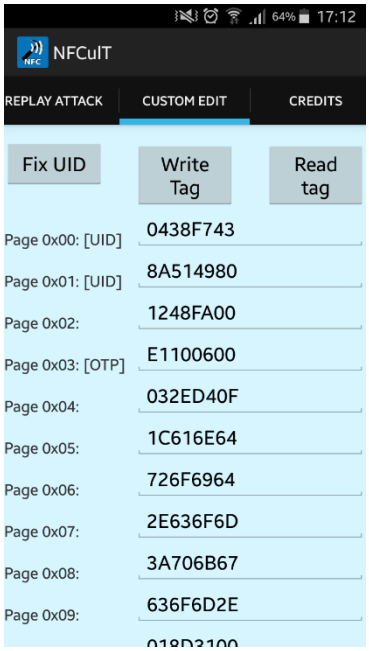
První možností bylo použití Shieldu, kde vytvoření obrazu tagu Mifare Classic bylo díky použitým knihovnám snadné, ale fungovalo pouze na nezamčené tagy, které nepotřebovali k přečtení obsahu klíče.

```
  UID Length: 4 bytes
  UID Value: 0xDB 0x9A 0x69 0x3F

Seems to be a Mifare Classic card (4 byte UID)
------------------------Sector 0-------------------------
Block 0  DB 9A 69 3F 17 08 04 00 01 94 B7 8F B2 1F 3A 1D  Ůši?.....”·Ź¸.:.
Block 1  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 2  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 3  00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF  ......˙.€i˙˙˙˙˙˙
------------------------Sector 1-------------------------
Block 4  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 5  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 6  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 7  00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF  ......˙.€i˙˙˙˙˙˙
------------------------Sector 2-------------------------
Block 8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 9  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 11 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF  ......˙.€i˙˙˙˙˙˙
------------------------Sector 3-------------------------
Block 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 15 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF  ......˙.€i˙˙˙˙˙˙
------------------------Sector 4-------------------------
Block 16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 17 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 19 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF  ......˙.€i˙˙˙˙˙˙
------------------------Sector 5-------------------------
Block 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 21 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 22 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 23 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF  ......˙.€i˙˙˙˙˙˙
------------------------Sector 6-------------------------
Block 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 26 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 27 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF  ......˙.€i˙˙˙˙˙˙
------------------------Sector 7-------------------------
Block 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
Block 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Obrázek 16 - Část výpisu za pomocí Adafruit PN532 Shieldu

Druhou možností bylo použití aplikace NFCuIT, která umožnuje provedení opakovaného přenosu, a tedy i uložení obrazu. Úspěšně i přes počáteční neúspěchy byl načten a uložen obsah tagu typu Mifare Classic Ultralight. Důvodem neúspěchu bylo, že samotné ukládání dump souboru nefungovalo. Aplikace vytvářela soubory dump.mdf, ale nešlo jej již znovu načíst nebo jinak s ním pracovat kromě možností smazání a přejmenování. Ale díky funkci Custom Edit bylo možné obsah tagu načíst a pracovat s ním.



Obrázek 17 - Custom Edit tagu v Aplikaci NFCuIT

Třetí možností použitou během testu bylo vytvoření obrazu pomocí aplikace NFCProxy, která také umožnuje provedení opakovaného přenosu. Vytváření obrazu v tomto případě bezkontaktní karty nebylo úspěšné a to ze dvou důvodů. První a hlavní důvod je absence operačního systému CyanogenMod na mobilním telefonu, kde bylo prováděno testování, díky čemuž nebyla obstarána plná funkcionalita aplikace. Druhým a spíše domnělým důvodem byla neznalost klíčů pro odemčení paměti karty a následně i nemožnosti vytvoření obrazu.

Poslední a asi nejvíce zajímavou možností bylo použití aplikace Mifare Classic Tool, která obsahuje standartní klíče k tagům typu Mifare Classic. Na mobilním telefonu použitém k testování, ale nebylo možné tuto aplikaci použít. Jak již bylo zmíněno, nepodporuje NFC tagy typu Mifare Classic a aplikace byla pouze schopná přečíst údaje o výrobci. Proto byl po dlouhodobém zkoušení a přesvědčování zapůjčen mobilní telefon Samsung Galaxy J5 2015 (verze Androidu 6.0.1) a bylo možné za pomoci aplikace vytvořit obraz tagu typu Mifare Classic 1K, který poté byl přenesen do původního telefonu, kde se s ním po uložení do správného adresáře dalo pracovat stejně jako by byl obraz tagu pořízen na původním telefonu.

Obrázek 18 - Dump soubor přenesený z jiného telefonu do aplikace Mifare Classic Tool

Aplikace také umožňuje přidání vlastních sad dešifrovacích klíčů a bylo by tedy teoreticky možné dešifrovat jakékoliv karty založené na Mifare Classic tagu jako například některé starší typy bezkontaktních platebních karet.

7.3 Lock Attack

Lock Attack neboli zamčení OTP sektoru tagu je možné provést pomocí aplikace NFCuIT. Během testování tohoto útoku nenastaly žádné problémy a tag typu Mifare Classic Ultralight byl zamčen proti jakýmkoli dalším úpravám. Poté byly provedeny pokusy o změnu obsahu, které vždy skončily neúspěchem, a to jak za pomoci aplikace TagWriter, nebo i Adafruit PN532 NFC Shieldu. Takže do dnešní doby je v paměti uložen příkaz pro zapnutí aplikace Jetpack Joyride, který byl dříve vytvořen v aplikaci TagWriter. Zamknutí tagu probíhá změnou příslušného bitu, který označuje zamknutí paměťových sektorů tagů.

```
# Memory content:
[00] *  04:38:F7 43 (UID0-UID2, BCC0)
[01] *  8A:51:49:80 (UID3-UID6)
[02] +  12 48 FA 00 (BCC1, INT, LOCK0-LOCK1)
[03] x  E1:10:06:00 (OTP0-OTP3)
[04] *  03 2E D4 0F |....|
[05] *  1C 61 6E 64 |.and|
[06] *  72 6F 69 64 |roid|
[07] *  2E 63 6F 6D |.com|
[08] +  3A 70 6B 67 |:pkg|
[09] +  63 6F 6D 2E |com.|
[0A] .  01 8D 31 00 |..1.|
[0B] .  62 72 69 63 |bric|
[0C] .  01 8D 31 00 |..1.|
[0D] .  74 70 61 63 |tpac|
[0E] .  6B 6A 6F 79 |kjoy|
[0F] .  72 69 64 65 |ride|
[10]    00 00 00 FF (AUTH0)
[11]    00 05 -- -- (ACCESS, VCTID)
[12] +P FF FF FF FF (PWD0-PWD3)
[13] +P 00 00 -- -- (PACK0-PACK1)

  *:locked & blocked, x:locked,
  +:blocked, .:un(b)locked, ?:unknown
  r:readable (write-protected),
  p:password protected, -:write-only
  P:password protected write-only
```

Obrázek 19 - Výpis obsahu paměti tagu

7.4 Data Corruption

Přerušit spojení během komunikace dvou NFC zařízení lze provést více způsoby. První nejsložitější způsob je vysílání na frekvenci 13,56 MHz a tím „přehlušit“ komunikaci. Tento způsob během testování nebyl použit, protože se jím již úspěšně zabývalo mnoho jiných prací a nebylo jej tedy nutno opakovat, aby byla prokázána jeho proveditelnost.

Dalším způsobem, a to mnohem jednodušším, jak porušit komunikaci a tedy jí i zamezit, je vložení dalšího rušivého prvku do pole čtecího zařízení. Nejjednodušším je vložení jiného vodivého materiálu do cesty během komunikace například obalení NFC tagu hliníkovou fólií. Tento krok zamezil přečtení tagu mobilním telefonem, který byl použit během testování. Naprosto stejně fungují ochranné obaly na bezkontaktní platební karty, které se dají běžně zakoupit.

Další možností zamezení přečtení tagu je vložení dalšího tagu do pole čtecího zařízení. V průběhu testování se tímto způsobem povedlo zamezit mobilnímu telefonu přečíst tag, ale při čtení pomocí Adafruit PN532 NFC Shieldu, byl Shield schopen číst 2 tagy zároveň a jejich obsah střídavě vypisovat na obrazovku.

7.5 Card Cloning

Pro klonování tagů/karet je nutné provést dva kroky. První zajišťuje obraz tagu, jak je popsáno v části Memory dumping, a ve druhém kroku je provedeno nahrání obrazu na tag. Pro vytvoření klonu je nutné použít tag s měnitelným UID, který zajistí, že nový tag bude naprosto identický s originálním tagem.

Kromě prvního způsobu je možné vytvořit tzv. „nedokonalé klony“, v tomto případě je obsah tagu stejný, ale liší se svým UID. Následná funkčnost klonu není zaručena a záleží na návrhu systému, který s tagy pracuje. Zda porovnává UID tagu se záznamy nebo pouze pracuje s daty uloženými na tagu, pak může být nedokonalý klon tagu přijat jako validní.

7.6 Replay Attack

K úspěšnému opakovanému přenosu je nutné nejprve získat obraz tagu, jak je zmíněno v sekci Memory dumping. Během testování byly použity aplikace NFCuIT a NFCProxy, které podporují tento útok, ale u každé byl pojat jinak. U NFCuIT se úplně nejedná o opakovaný přenos, i když je v aplikaci takto nazván, ale o klonování tagů, kdy se obraz tagu ukládá na jiný prázdný tag, i přestože cílový tag nemusí mít měnitelné UID a vytvoří „nedokonalý klon“ tagu.

Při použití NFCProxy se jedná už opravdu o opakovaný přenos. Návod, jak použít aplikaci se nachází v knize Mobile Device Exploitation Cookbook [10], ale není velmi obsáhlý. Pro prvotní vyzkoušení aplikace a jako zdroj s užitečnými odkazy byl dostačující. Během testování nebylo možné vytvořit nový obraz tagu/karty z důvodu absence CyanogenModu na testovacím telefonu. NFCProxy obsahuje několik testovacích obrazů, v tomto případě bezkontaktních platebních karet se kterými byla úspěšně otestována emulace platební karty. Kdy byla karta emulovaná telefonem a poté úspěšně zaznamenána čtecím zařízením, ale díky tomu, že se jednalo pouze o ukázkový příklad nemohla být úspěšně provedena platba.

7.7 Malicious Tags

Škodlivé tagy jsou z odborného hlediska zajímavou hrozbou, která je velice jednoduchá na provedení. Úspěch útoku pomocí škodlivých tagů závisí na uživatelích a jejich pozornosti během čtení tagů na veřejných místech.

Pro účel testování bylo předpokládáno, že uživatel načte tag z vlastní vůle. Pro lepší popis testů byl průběh této hrozby rozdělen do tří částí.

V první části je vytvořen tag se škodlivým kódem, nebo odkazem na webové stránky se škodlivým obsahem, který je díky paměťovým omezením tagů příhodnější, nebo jakoukoliv jinou funkcí, kterou je útočník schopen vložit na tag. Tento krok je naprosto jednoduchý a zvládne jej jakýkoliv začátečník zabývající se technologií NFC. URL je možné vložit na tag pomocí mnoha aplikací například již zmiňovanou TagWriter od společnosti NXP Semiconductors.

Druhou částí pro úspěšné provedení útoku je zajištění dostupnosti tagu. Nejsnazší cestou je umístění škodlivého tagu na veřejné místo, kde je tag naistalován na nové místo nebo přes již existující tag.

Během testovaní při pokusu o překrytí původního tagu novým škodlivým tagem došlo k situaci, kdy k sobě byli tagy přiloženy, původní tag byl obalen aluminiovou fólií a na něm byl v přesném zákrytu přiložený nový škodlivý tag. Mobilní telefon nebyl schopen přečíst ani jeden z tagů. Načtení škodlivého tagu bylo úspěšné až po přidání papírové vrstvy mezi tagy a vytvořením tak alespoň 1 milimetrové mezery.

Jednodušší způsob je originální tag poškodit a vedle nebo přes něj umístit svůj vlastní škodlivý tag.

Ve třetí části testu bylo zjištěno vše, na co bude muset uživatel reagovat, než doopravdy přejde na škodlivý web. Zde byly znovu otestovány tři stupně omezení nebo spíše zjednodušení uživatelovy reakce, aby během načítání tagu uživatel nemohl zasáhnout do zobrazování naší požadované webové stránky.

První možností je pouze vložit URL na tag a v tomto případě se uživateli zobrazí dialog s názvem webové stránky a samotnou URL. Mobilní telefon poté nechá uživatele

rozhodnout, co udělá. Uživatel může zrušit vykonání přechodu na webovou stránku a tím může zabránit úspěchu celého útoku.

Obrázek 20 - Dialog při načítání tagu

Předchozí situaci může útočník zabránit tím, že použije druhou možnost útoku, kdy k adrese tagu přidá ještě povel pro spuštění aplikace webového prohlížeče, ale může zde nastat případ, kdy uživatel bude používat jiný webový prohlížeč, než je předinstalovaný a tím pádem útočník musí odhadnout jaký prohlížeč uživatel používá. V případě, že bude zvolen špatný, odkaz přesměruje uživatele od obchodu Google Play a požádá ho k nainstalování daného prohlížeče.

Tato situace se dá velice elegantně vyřešit třetí možností, a tedy použitím speciálního zkracovače pro URL zaměřeného na NFC tagy, jako je zkracovač na adrese www.nfclink.net. Ten také místo funkce pouhého zkrácení odkazu dokáže, že se odkaz okamžitě spustí v uživatelem používaném webovém prohlížeči, který má nastavený jako výchozí. Obejití interakce s uživatelem se nazývá „Zero click push NFC“. Takový odkaz by mohl vypadat takto http://www.nfclink.net/n/49417e38 – odkaz na stránky Jihočeské univerzity ve zkrácené podobě, které po nahrání na tag bude fungovat bez interakce uživatele.

Po dalším testování bylo zjištěno, že odkaz se spustí stejně jako ve zkracovači, když před něj bude přidán protokol http://.

Poslední podmínkou pro útočníka je už jen taková znalost tvorby webových stránek, aby vytvořil dostatečně uvěřitelnou phishingovou stránku pro uživatele.

Největší zajímavostí útoku „Malicious Tags“ je, že proti němu neexistuje způsob obrany nebo jeho zabránění. Vše záleží pouze na uživateli, jestli bude pozorně kontrolovat tagy umístěné na veřejných místech a poté s obezřetností sledovat interakci se svým mobilním telefonem.

7.8 Ztráta zařízení

Princip ztráty zařízení spočívá v tom, že NFC zařízení slouží nálezci stejně jako originálnímu majiteli. Otestování této hrozby v oblasti bezkontaktních karet a tagů je spíše zbytečné a je zjevné, že pokud budě někomu odcizena čipová karta, nebo bezkontaktní platební karta a není zabezpečena dalším způsobem jako je PIN, biometrie nebo jinými metodami tak jí bude moci útočník/nálezce/zloděj používat stejným způsobem jako majitel. A proto byla tato část testování zaměřena výhradně na mobilní telefony. A to, jak jsou zabezpečeny proti takovéto situaci. Během testování bylo ověřeno že mobilní telefon nepřijímá komunikaci přes NFC, pokud je jeho obrazovka zamčena. Kdyby však byla ochrana telefonu (gesto, PIN, otisk prstu) prolomena. Útočníkovi se ani tak nepodaří provést bezkontaktní platbu, která potřebuje další potvrzení (PIN, otisk prstu).

7.9 Diskuze výsledků testování

Provedené testy byli z velké části zaměřeny na NFC v režimu Reader/Writer, během kterého je NFC vždy v kontaktu s kompatibilním tagem, který je považován za bezpečnější, a bývá doporučeno ho přednostně používat z důvodu horší možnosti odposlechu komunikace.

Z jednotlivých testů vychází, že komunikace pomocí technologie NFC je bezpečná, pokud používá zabezpečený kanál a obsah dat jednotlivých tagů bude šifrován. Tím bude útočníkovi zabráněno odposlechnout, přečíst, zkopírovat a modifikovat data posílaná uživatelem nebo uložená na tagu.

Největší zranitelností zůstává uživatel sám, který si může svojí nepozorností způsobit, že se jeho mobilní telefon dostane pod nadvládu útočníka nebo na sebe vyzradí důležité informace tím, že dobrovolně načte neznámý škodlivý tag.

Protože je pro útok za pomoci škodlivých tagů nutná pouze malá znalost technologie NFC a je možné jej uskutečnit pouze za pomoci veřejně dostupných aplikací. Díky tomu můžeme tuto hrozbu považovat za největší a nejvážnější pro neopatrné uživatele.

Během testování byl tag pro spuštění webové stránky vyzkoušen na 4 různých mobilních telefonech a vždy proběhl úspěšně.

Většina zmíněných hrozeb v teoretické části je z praktického hlediska neproveditelná, nebo pouze za přísných laboratorních podmínek ve kterých by bylo nutno zařídit naprosto bezchybně načasované odpovědi a odposlechy během komunikace bez přeslechů. Pouze poté by napadené čtecí zařízení nebylo schopno zaregistrovat časové prodlevy útočníka a neodstoupit od komunikace.

Testy	Úspěch	Technogie	Závěr
Tag Reading	Ano	Shield, TagInfo	Přečtení obsahu
Memory dumping	Ano	Shield, Mifare Classic tool	Vytvoření dump souboru
Lock Attack	Ano	NFCuIT	Zamčení OTP sektoru
Data Corruption	Ano	Shield, TagInfo	Odstínění tagu
Card Cloning	Ne	NFCuIT	Tag bez měnitelného UID, nedokonalý klon
Replay Attack	Ne	NFCProxy	Chybějící CyanogenMod, test emulace tagu
Malicious Tags	Ano	TagWriter	Spuštení web. stránky bez interakce uživatele
Ztráta zařízení	Ano	Android, NFC tag	Nutnost dalšího zabezpečení

Tabulka 2 - Provedené testy

8. Závěr

Hlavním cílem této práce bylo prozkoumat bezpečnostní rizika technologie NFC, tedy hrozeb a zranitelností.

Teoretická část, která je rozdělena do dvou částí slouží především jako ucelený přehled o technologii NFC. V první části zabývá se jejím vznikem a počátečním vývojem. Poté technologickými specifikace NFC a její funkcionalitou. Dále je zde také uvedeno uplatnění a rozšířenost technologie NFC v dnešní době, tedy kde a v jakých oblastech se vyskytuje a aktivně využívá.

Druhá polovina teoretické části se zabývá otázkami bezpečnosti a hrozbami zneužití NFC při jejím používání, společně s možnostmi zabezpečení. Jednotlivé hrozby jsou vysvětleny společně s popisem, jak je jim možné zabránit, nebo alespoň minimalizovat možnost jejich uskutečnění, včetně možné proveditelnosti jednotlivých hrozeb jak z teoretických, tak i praktických hledisek.

Praktická část obsahuje úvodem dnešní průzkum trhu s hardwarem a aplikacemi pro práci s NFC technologií, které jsou také popsány, a kromě běžných jsou zde i ty, co slouží právě pro výzkum bezpečnosti NFC.

Další částí je příprava před samotným testováním, která sloužila pro seznámení s NFC a jejími možnostmi a vyzkoušení programů s PN532 Shieldem. Následuje testovací část, v níž jsou popsány provedené pokusy, které bylo možné provést za opatřeného hardwaru a aplikací.

Rozšíření práce do budoucnosti by bylo možné několika způsoby, jako například zakoupení více čtecích zařízení a otestovat praktické možnosti Relay Attacku včetně analýzy útoku pro reálné využití. Další možností by bylo opatření nákladného ProxMark3 kitu a vyzkoušení jeho možností s takovým omezením, aby během testování nedošlo k porušení Českých zákonů. Asi poslední možností rozšíření práce by mohla být instalace CyanogenModu na mobilní telefon a tím pádem se pokusit vytvořit co největší kompatibilitu s mobilními aplikacemi pro testování bezpečnosti NFC.

9. Zdroje

9.1. Zdroje a seznam obrázků

9.2. Seznam použitých zdrojů

[1] ROLAND, Michael. *Security Issues in Mobile NFC Devices* [online]. Feb 12 2015. Springer, 2015 [cit. 2017-02-06]. ISBN 978-3-319-15488-6. Dostupné z: http://it-ebooks.directory/book-3319154877.html

[2] IGOE, Tom, Don COLEMAN a Brian JEPSON. *Beginning NFC: Near Field Communication with Arduino, Android and PhoneGap* [online]. Feb 03 2014. 1005 Gravenstein Highway North, Sebastopol, CA 95472: O'Reilly Media, 2014 [cit. 2017-02-06]. ISBN 9781449372064. Dostupné z: http://it-ebooks.directory/book-1449372066.html

[3] SABELLA, Robert P. *NFC For Dummies* [online]. Feb 15 2016. 111 River Street, Hoboken, NJ 07030-5774: Wiley, 2016 [cit. 2017-02-06]. ISBN 978-1-119-18296-2. Dostupné z: http://it-ebooks.directory/book-1119182921.html

[4] *Technologie NFC – popis, bezpečnost a využití* [online]. 2013, **20.04.2013**(22) [cit. 2017-02-06]. ISSN 1213-1539. Dostupné z: http://www.elektrorevue.cz/cz/clanky/informacni-technologie/0/technologie-nfc---popis--bezpecnost-a-vyuziti/

[5] FRANCIS, Lishoy, Gerhard HANCKE, Keith MAYES a Konstantinos MARKANTONAKIS. *Practical NFC Peer-to-Peer Relay Attack Using Mobile Phones*. In: . DOI: 10.1007/978-3-642-16822-2_4. ISBN 10.1007/978-3-642-16822-2_4. Dostupné také z: http://link.springer.com/10.1007/978-3-642-16822-2_4

[6] NUSSEY, John. *Arduino for dummies* [online]. 2013. West Sussex, England: Wiley, 2013 [cit. 2017-02-09]. --For dummies. ISBN 9781118446430. Dostupné z: https://archive.org/details/pdfy--LpbPxUly33g2cjN

[7] *NFC Forum* [online]. [cit. 2017-03-08]. Dostupné z: http://nfc-forum.org/

[8] Near field communications tutorial - Radio-Electronics.com. *Radio-Electronics.com* [online]. [cit. 2017-03-20]. Dostupné z: http://www.radio-electronics.com/info/wireless/nfc/near-field-communications-tutorial.php

[9] MOSTAFA ABD ALLAH, Mohamed. *Strengths and Weaknesses of Near Field Communication (NFC) Technology* [online]. USA: Global Journals, 2011, **2011**(Volume 11 Version 1.0) [cit. 2017-03-25]. ISSN 0975-4172.

[10] VERMA, Prashant a Akshay DIXIT. *Mobile Device Exploitation Cookbook*. BIRMINGHAM - MUMBAI: Packt Publishing Limited, 2016. ISBN 9781783558728. Dostupné také z: https://id.scribd.com/document/342965441/Mobile-Device-Exploitation-Cookbook

[11] NUSSEY, John. *Arduino for dummies* [online]. 2013. West Sussex, England: Wiley, c2013 [cit. 2017-11-06]. --For dummies. ISBN 9781118446430. Dostupné z: https://archive.org/details/pdfy--LpbPxUly33g2cjN

[12] HASELSTEINER, Ernst a Klemens BREITFUß. *Security in Near Field Communication (NFC): Strengths and Weaknesses*. Mikronweg 1, 8101 Gratkorn, Austria: Philips Semiconductors, 2006. Dostupné také z: http://rfidsec2013.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf

[13] MULLINER, Collin . *Hacking NFC and NDEF: why I go and look at it again: Talk at NinjaCon*. Vienna, Austria., 2011. Dostupné také z: http://www.mulliner.org/nfc/feed/nfc_ndef_security_ninjacon_2011.pdf

[14] N - Mark. In: *NFC Forum* [online]. [cit. 2017-11-27]. Dostupné z: http://nfc-forum.org/wp-content/uploads/2016/04/N-Mark_box_blue_TM.png

[15] ACR122U. In: *Synchrotech* [online]. [cit. 2017-11-27]. Dostupné z: http://www.synchrotech.com/product-sc/img/contactless-nfc-smart-card-reader-01-acr122u-usb-a.jpg

[16] Adafruit PN532 NFC Shield. In: *MobileFish.com* [online]. [cit. 2017-11-27]. Dostupné z: http://www.mobilefish.com/images/developer/libnfc_adafruit_large.gif

[17] Proxmark3 Kit: RyscCorp. In: *Shopify* [online]. [cit. 2017-11-27]. Dostupné z: https://cdn.shopify.com/s/files/1/0847/7088/products/Proxmark3_Kit_-_Revised_-_Small.jpg?v=1485956761

[18] Arduino UNO. In: *Robotecho Shop* [online]. [cit. 2017-12-08]. Dostupné z: http://robotechshop.com/wp-content/uploads/2015/12/arduino_uno_large-comp.jpg

9.3 Seznam tabulek

9.4 Seznam příloh

Přiložené CD obsahuje elektronickou verzi práce, scany a dump výpis, kódy programů a návody pro prodení testů z praktické části. Dále také dump soubory tagů a sketche pro Arduino