BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2016
http://excel.fit.vutbr.cz

Analýza NFC relay útoku

Petr Holubec*

Abstrakt
Článek se zabývá bezpečností bezkontaktních plateb. Popisuje návrh a implementaci systému, který demonstruje jednoduchost provedení tzv. NFC relay útoku na bezkontaktní platební karty. Systém se skládá z mobilní aplikace pro Android a serverové části realizující samotné přeposílání komunikace. Tento výzkum si klade za cíl analýzu provedení tohoto útoku v reálném prostředí bezkontaktních platebních transakcí.

Klíčová slova: NFC — Android — bezpečnost — bezkontaktní platby

Přiložené materiály: *N/A*

* xholub26@stud.fit.vutbr.cz, *Fakulta informačních technologií, Vysoké učení technické v Brně*

1. Úvod

Česká republika patří ve světovém měřítku na první pozice ve využívání bezkontaktních platebních karet. Pro mnohé z nás je tento způsob platby příjemným zjednodušením a také vítaným zrychlením při nákupu nejrůznějšího zboží. Málokdo si však uvědomuje i rizika spojená s touto technologií a její snadné zneužití případným útočníkem. Tomu velice usnadňuje práci kompatibilita bezkontaktních platebních karet s technologií NFC, jejíž podpora je v mobilních telefonech čím dál běžnější.

Článek popisuje návrh a implementaci systému, který demonstruje možnost realizace tzv. NFC relay útoku v prostředí bezkontaktních platebních transakcí. Jedná se o jeden ze způsobů zneužití bezkontaktní technologie v oblasti platebních karet.

2. Využité technologie a protokoly

Pokud chce bezkontaktní terminál nebo mobilní zařízení s NFC komunikovat s čipovou platební kartou, ve většině případů využije protokol EMV (zkratka z Europay, Mastercard, Visa). O tuto specifikaci se v současné době stará organizace EMVCo, jejímiž členy jsou rovným podílem společnosti American Express, Discover, JCB, MasterCard, UnionPay a Visa[1]. Jednotlivé specifikace jsou průběžně aktualizovány a v několika knihách popisují komunikační protokol od nejnižších vrstev (např. přenos a časování jednotlivých bitů nebo řešení kolizí) až po aplikační rozhraní (příkazy a odpovědi platební karty).

V rámci této práce nás zajímá především komunikace s kartou na úrovni aplikace. Ta probíhá binárně stylem výzva – odpověď. Jednotlivé příkazy jsou formátovány způsobem TLV (Type, Length, Value), kdy v prvních dvou položkách fixní délky (typicky 1-4 byty) je přenášen typ resp. délka obsahu a poté teprve následují samotná data[2]. Celý takto vytvořený paket je zapouzdřen do APDU (Application Protocol Data Unit, definován v ISO/IEC 7816-4). Jeho hlavička obsahuje třídu a typ příkazu a dva parametry. Volitelně mohou následovat velikost dat, data samotná a očekávaná délka dat v odpovědi. Ta obsahuje pouze návratová data a 2 byty určující úspěch, neúspěch či jiný stav zaslaného příkazu. Například dvojice `90,00` znamená úspěšné provedení příkazu. Přesnou strukturu obou typů APDU znázorňuje obrázek 1.

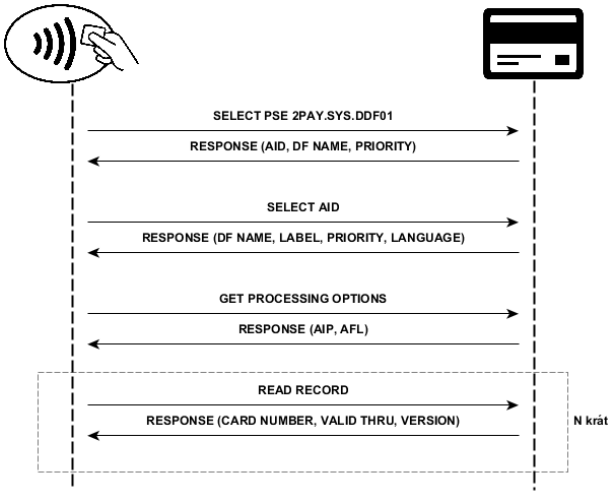
Příkaz APDU						
CLA	INS	P1	P2	Lc	*Data*	Le
Požadováno				Volitelné		

Odpověď APDU		
Data	SW1	SW2
Volitelné	Požadováno	

Obrázek 1. Formát příkazu a odpovědi APDU.

Ve chvíli, kdy je platební karta přiložena k terminálu požadujícímu provedení transakce, je navázáno

spojení a zahájena výměna série příkazů, která v ideálním případě skončí úspěšným zaplacením. Nejprve je nutné příkazem `SELECT` vybrat správné PPSE (Proximity Payment Systems Environment), které je v případě bezkontaktních platebních transakcí reprezentováno řetězcem `2PAY.SYS.DDF01`. V odpovědi je vrácen identifikátor AID (Application ID), který využijeme v dalším příkazu pro výběr požadované aplikace. Následuje příkaz `GET PROCESSING OPTIONS`, kterým jsou získány AIP (Application Interchange Profile) a AFL (Application File Locator), které slouží mimo jiné jako informace o počtu souborů a záznamů aktuálně vybrané aplikace[2]. Ty mohou být poté postupně přečteny pomocí příkazu `READ RECORD`. Dále následují příkazy nutné pro samotnou platbu, které jsou specifické pro každý typ karty[3]. Výše popsaná úvodní fáze bezkontaktní platby je znázorněna na obrázku 2.

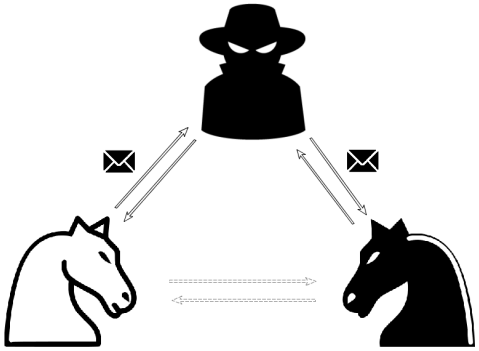


Obrázek 2. Komunikace mezi bezkontaktní čtečkou a platební kartou pomocí protokolu EMV.

3. Popis útoku

Základní princip relay útoku lze snadno ukázat na problému hráče šachů popsaném v [4], který chce vyhrát proti šachovému mistrovi. Představme si podvodníka, který hraje na dálku 2 partie šachů se dvěma různými šachovými mistry. Podvodník vůbec nemusí znát pravidla hry, důležité je, aby v každé partii hrál za jinou barvu. Poté pouze přeposílá tahy jednoho hráče hráči druhému dokud hra neskončí. Ti, přestože si oba myslí, že hrají proti našemu podvodníkovi, ve skutečnosti hrají navzájem proti sobě[5]. Situaci znázorňuje obrázek 3.

V nejběžnějším případě NFC relay útoku jsou zapotřebí dvě zařízení pod kontrolou útočníka. První z nich bude sloužit jako falešná čtečka bezkontaktní karty a druhé využijeme pro emulaci karty. Mezi těmito dvěma zařízeními je nutné vytvořit spolehlivý a především rychlý komunikační kanál bez zbytečných zpoždění. Dále jsou zapotřebí bezkontaktní karta oběti a terminál, který hodláme obelstít naší emulovanou kartou. Protože je v České Republice aktuálně zaveden limit 500 Kč pro platbu bez zadání kódu PIN, uvažujme dále pouze částky do tohoto limitu.



Obrázek 3. Znázornění problému hráče šachů.

4. Existující výzkumy

Ukázkou realizace relay útoku na technologii NFC se v minulosti zabývalo mnoho prací. Liší se především volbou přenosového kanálu, použitými zařízeními a přenášenými daty resp. užitím. V této části si v rychlosti představíme myšlenky a úspěchy některých vybraných prací.

První prací je [6]. Zde se autorům podařilo uskutečnit útok pomocí 4 mobilních telefonů HTC One X se systémem Android verze 4.0 Ice Cream Sandwich. Vzhledem k tomu, že Android Beam používá jako fyzické přenosové médium Bluetooth a ten nepodporuje více spojení najednou, musela být jako relay kanál zvolena bezdrátová síť. Pro demonstraci funkčnosti byla napsána mobilní aplikace, která celé přeposílání dat implementovala.

V práci [7] využili autoři NFC relay útoku na obelstění přístupového systému. Pomocí mobilní aplikace a jediného mobilního telefonu přepnutého do režimu Peer-To-Peer útočník zachytí autentizační klíč ze zařízení oběti. Poté se telefon přepne do režimu emulace karty a při komunikaci se čtečkou využije již zachycený klíč pro získání přístupu do střeženého objektu. Specifikem této práce je využití pouze jediného zařízení. Uplatnění tato metoda najde v prostředích, kde není nutné zprostředkovávat přímý komunikační kanál, ale stačí jednou získat potřebné oprávnění, které je po přepnutí zařízení do režimu emulace karty možné využít později.

Praktickou ukázku NFC relay útoku hned na několika typech dat představili autoři z londýnské univerzity v [8]. Pomocí dvou mobilních telefonů s podporou NFC, mezi kterými vytvořili Bluetooth spojení,

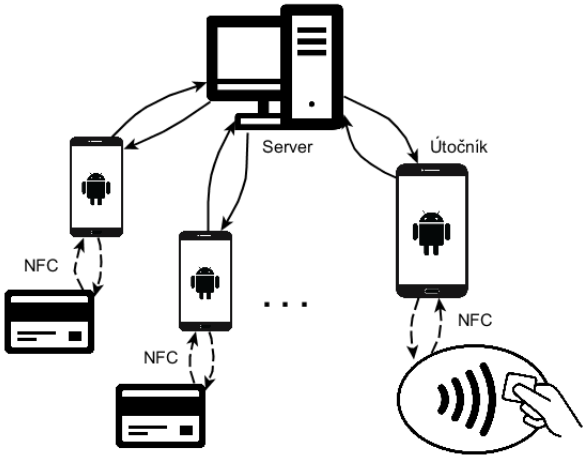
dokázali ošálit bezkontaktní čtečku. Pro otestování bylo nejprve vyzkoušeno přenesení tokenu a další operace s bezkontaktní kartou. Poté bylo otestováno provedení platby pomocí karty se statickou autentizací práv a přečtení dat z elektronického pasu. Všechny pokusy skončili úspěchem i přes nejistotu, zda bude delší prodleva (především u větších APDU obsahujících JPEG fotografii z pasu) čtečkou akceptována. V práci jsou dále diskutovány možnosti, jak podobným útokům předcházet a to jak z pohledu bezkontaktního systému, tak z pohledu mobilního telefonu.

Velice zajímavou a poměrně aktuální prací je [9]. Autor využívá dvě zařízení Nexus 7 k přemostění komunikace mezi bezkontaktní platební kartou a NFC čtečkou připojenou k notebooku. Nejzajímavější částí jsou provedené optimalizace samotného přenosu a díky těmto úpravám dosažené časy. Z analýzy protokolu EMV vyplynulo, že prvních několik přenášených zpráv se pro jednu konkrétní kartu v každé transakci stále opakuje. Proto je možné tyto zprávy uložit a při další transakci je již na každé straně provést lokálně bez nutnosti jejich přenosu. Poté se přenese pouze několik málo zpráv, které jsou pro každou platbu jedinečné. Díky tomuto vylepšení bylo při útoku dosaženo srovnatelných časů jako při skutečné platbě, což dokazuje, že detekce relay útoku na základně rychlosti odezvy nemusí být dostatečná.

Poslední, avšak neméně zajímavou prací je [5]. Autoři vytvořili mobilní aplikaci pro systém Android, která zastane roli bezkontaktní čtečky nebo emulované karty (podle volby uživatele). Dvě zařízení (od každé role jedno) jsou poté spojeny peer-to-peer komunikačním kanálem. Autorům se úspěšně podařilo uskutečnit platbu na vlastním platebním terminálu (Ingenico IWL280), navíc několika různými telefony (Nexus 4, Nexus 5, Samsung Galaxy Nexus a Sony Xperia S). V práci je také zmíněna zajímavá myšlenka zneužití tohoto útoku v podobě tzv. botnetu napadených zařízení. To při detekci platební karty kontaktuje útočníka, který může provést transakci ve svůj prospěch.

5. Obecný návrh systému

Celý systém je navržen s ohledem na maximální škálovatelnost. Cílem není dosáhnout pouze ad-hoc spojení mezi dvěma zařízeními, nýbrž vytvořit centralizovaný systém, ve kterém bude moci figurovat teoreticky neomezené množství platebních karet a útočník si pouze vybere, kterou z aktivních karet využije k platbě. Proto se jednotlivá zařízení budou registrovat vůči serveru a v případě, že jsou v režimu čtečky a detekují ve své blízkosti platební kartu, odešlou její základní údaje na server. V pravidelných intervalech bude server dostávat oznámení, zda je karta stále k dispozici nebo již není v dostatečné blízkosti. Zařízení v roli emulace karty se pak může dotázat serveru na seznam právě aktivních karet, ze kterého si uživatel vybere jednu kartu, s níž se vytvoří spolehlivé spojení.



Obrázek 4. Schéma navrženého systému.

6. Volba přenosového kanálu

V našem případě využijeme jako relay kanál mezi dvěma mobilními telefony Wi-Fi a mobilní datovou síť LTE. Protože nám jde o vyzkoušení reálného útoku, nikoliv pouze o potvrzení proveditelnosti v domácích a předem definovaných podmínkách, musíme uvažovat i fyzickou vzdálenost obou zařízení. Proto by bylo chybné spoléhat pouze na Wi-Fi připojení a z toho důvodu předpokládáme i možnost spojení pomocí mobilní datové sítě. To nám bohužel přináší komplikaci, protože zařízení mohou být v rámci svých sítí za překladem adres (například NAT[10]) a bylo by tedy velice náročné, ne-li dokonce nemožné, propojit telefony přímo. Proto je jako prostředník implementován server, který zajistí spojení obou zařízení a přeposílá veškerou komunikaci. Nejvíce kritickým faktorem konkrétního typu připojení je rychlost odezvy, která může být při komunikaci s bezdrátovou čtečkou klíčová.

Pro přenos jednotlivých příkazů mezi čtečkou a platební kartou, který musí být už z principu obousměrný, slouží protokol WebSocket (RFC 6455). Ten umožňuje pomocí HTTP[11] požadavku vytvořit obousměrné spojení, které pro samotný přenos využívá protokolu TCP[11]. Výhodou je, že na serveru nemusí být otevřen další port a spojení se iniciuje přes již otevřený port využívaný webovou aplikací. Dalším přínosem je, že vrstva protokolu WebSocket sama skládá a kompletuje fragmentované zprávy a aplikaci je doručuje již kompletní, což zjednodušuje zpracování dat v aplikaci.

7. Návrh komponent systému

K provedení útoku lze použít dvě zařízení se systémem Android verze 4.4 Kitkat nebo vyšší. Jeden telefon slouží jako falešná bezkontaktní čtečka karet a druhý v NFC režimu emulace karty vystupuje jako falešná bezkontaktní karta. V případě, že má první telefon ve své blízkosti bezkontaktní kartu, druhé zařízení je schopné se za tuto kartu vydávat. Veškerou komunikaci obdrženou od skutečné čtečky druhé zařízení přeposílá na server, který ji dále předává prvnímu telefonu. Ten komunikaci odesílá bezkontaktní kartě, pro kterou se nyní první telefon tváří jako legitimní čtečka. Jakmile karta na obdrženou komunikaci odpoví, celý řetěz se opakuje, pouze v obráceném pořadí. Tímto způsobem jsou legitimní čtečka a skutečná bezkontaktní karta schopny komunikovat, dokud jedna ze stran komunikaci neukončí nebo nedojde k přerušení spojení.

Jako serverová část systému slouží aplikace napsaná pro platformu Java EE. Ta běží na virtuálním serveru s veřejnou IP adresou a je tak přístupná z internetu. Spojení je zabezpečeno pomocí TLS protokolu HTTPS[11]. Aplikace pracuje s databází MySQL, která je využita pro ukládání informací o jednotlivých zařízeních, kartách a spojeních mezi nimi. Pro mapování informací z databáze na Java objekty je využit framework Hibernate, který je nejrozšířenější implementací specifikace Java Persistence API (JPA).

Pro základní komunikaci se serverem je vytvořeno REST API, které klientovi nabízí několik metod, jak ze serveru získat potřebná data pomocí HTTP metody GET, nebo naopak uložit informace metodou POST (popsáno v RFC 2616). Pokud je třeba v těle dotazu či odpovědi přenášet data, jsou tato data vložena v textové podobě ve formátu JSON (RFC 4627). Jednotlivé dotazy jsou pro snazší práci na serveru automaticky konvertovány na korespondující objekty.

8. Experimenty

Mobilní aplikace byla testována na několika různých zařízeních s odlišnými parametry i verzemi systému Android. Jmenovitě například LG Nexus 4, LG Nexus 5, LG Nexus 5X, Sony Xperia Z3 Compact, Sony Xperia Z5 Compact, Samsung Galaxy S5 mini a další.

První fáze testování probíhala v domácích podmínkách, kde místo reálné čtečky posloužil telefon s aplikací pro čtení bezkontaktních platebních karet. Příkladem takovéto aplikace mohou být *Credit Card Reader NFC (EMV)*, *cardme* nebo obecnější *NFC TagInfo by NXP*. Přeposílání komunikace probíhalo bez problémů a přesně tak, jak se očekávalo. Zkoušena byla různá zařízení v různých rolích, stejně tak jako byl systém otestován na Wi-Fi i datové síti LTE.

Následovat budou experimenty na reálných platebních terminálech. Testování může probíhat například tak, že doma bude zanecháno zařízení s platební kartou v jeho bezprostřední blízkosti a druhým telefonem bude zaplaceno zboží v obchodě.

Toto je samozřejmě pouze testovací případ, jak lze implementovaný systém využít pro platby mobilním telefonem, nicméně reálný útok by vypadal poněkud odlišně. Typickým použitím by bylo například přiblížení telefonu k tašce nebo kabelce oběti v prostředcích MHD, zatímco druhý útočník by na druhém konci města platil vybranou kartou za zboží. Zobecněním tohoto scénáře by pak byla rozsáhlá síť útočníků, případně zařízení vhodně rozmístěných po městě či v MHD, kteří by zajišťovali komunikaci s kartami obětí, zatímco další skupina útočníků by aktuálně dostupnými kartami prováděla platební transakce.

V kapitole 4 je stručně popsáno několik prací, které se mimo jiné zabývají i návrhem vhodných opatření pro zabránění tomuto typu útoku. Zřejmě nejjednodušší a také nejčastěji uvažované řešení na straně terminálu je založeno na rychlosti odezvy platební karty, která by při přenosu komunikace přes internet měla být snadno rozpoznatelná. O neúčinnosti a možnosti překonání této obranné metody se píše v práci [9].

Z pohledu vlastníka bezkontaktní platební karty se zdá nejúčinnější obrana v podobě speciálního pouzdra, které dokáže odstínit pokusy o komunikaci s bezkontaktní kartou. V reálných podmínkách typicky stačí mít v peněžence či kabelce více bezkontaktních karet (například další platební kartu nebo věrnostní karty obchodních řetězců), které se navzájem zaruší a znemožní tak komunikaci s jednotlivými kartami.

9. Závěr

V této práci byl představen a stručně popsán útok typu NFC relay, který umožňuje využití platební nebo jiné bezkontaktní karty i na fyzickou vzdálenost, která u karet tohoto typu není brána v úvahu. Pomocí dvou mobilních zařízení pod kontrolou útočníka lze přeposílat komunikaci mezi terminálem a platební kartou i na obrovské vzdálenosti díky spojení přes internet. Dále byly stručně představeny vybrané práce, které se zabývají podobnou problematikou.

Pro demonstraci a analýzu tohoto útoku byl navržen a implementován systém, který se skládá z mobilní aplikace pro Android a serverové části na platformě Java EE. Ten umožňuje propojit dvě zařízení připojená pomocí Wi-Fi nebo mobilní datové sítě a přeposílat jednotlivé příkazy od terminálu ke kartě a zase zpět. V systému je možné registrovat teoreticky neomezené množství platebních karet a útočník si pouze vybere

jednu aktivní, kterou využije k platbě.

Funkčnost navrženého řešení byla otestována pomocí aplikace pro načítání informací z platebních karet. Během těchto experimentů se ukázalo, že registrace zařízení a karet i přeposílání komunikace funguje správně a bez problémů. Následovat bude testování na reálných platebních terminálech.

Poděkování

Rád bych poděkoval Ing. Lukáši Aronovi za spoustu užitečných rad a připomínek k mé práci. Dále velice děkuji přítelkyni Pavle Pichové za podporu a obětavou pomoc s vytvářením doplňujících materiálů.

Literatura

[1] EMVCo. About emvco. [online], 2016 [cit. 2016-04-09].

[2] EMVCo. Book 3 – application specification. [online], listopad 2011.

[3] EMVCo. Book 1 – application independent icc to terminal interface requirements. [online], listopad 2011.

[4] John Horton Conway. *On numbers and games*. A K Peters, Natick, 2. edition, 2001.

[5] José Vila and Ricardo J. Rodríguez. Practical experiences on nfc relay attacks with android. In *Radio Frequency Identification*, volume 9440 of *Lecture Notes in Computer Science*, pages 87–103. Springer International Publishing, 2015.

[6] Zhao Wang, Zhigang Xu, Wei Xin, and Zhong Chen. Implementation and analysis of a practical nfc relay attack example. In *Instrumentation, Measurement, Computer, Communication and Control (IMCCC), 2012 Second International Conference on*, pages 143–146, prosinec 2012.

[7] D. Cavdar and E. Tomur. A practical nfc relay attack on mobile devices using card emulation mode. In *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015 38th International Convention on*, pages 1308–1312, květen 2015.

[8] Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. Practical relay attack on contactless transactions by using nfc mobile phones. [online], 2011 [cit. 2016-01-05].

[9] Jordi van den Breekel. Relaying emv contactless transactions using off-the-shelf android devices. březen 2015.

[10] Dhiman D. Chowdhury. *Unified IP internetworking*. Springer, Berlin, vyd. 1. edition, 2001.

[11] Adrian Farrel. *Internet and its protocols: a comparative approach*. Morgan Kaufmann, San Francisc, 2004.