elektrorevue
ISSN 1213 - 1539

Rok / Year:	Svazek / Volume:	Číslo / Number:	Jazyk / Language
2021	23	3	CZ

Demonstrátor útoků na bezkontaktní kartové systémy

Attack demonstrator for contactless card-based systems

Petr Dzurenda[1], *Minh Tran*[1], *Jan Hajný*[1], *Vlastimil Beneš*[2], *Pavel Krištof*[2]

dzurenda@vut.cz

[1] Ústav telekomunikací, Fakulta elektrotechniky a komunikačních technologií, Vysoké učení technické v Brně
[2] Institut mikroelektronických aplikací s.r.o.

DOI: -

Abstract: The article focuses on security issues and attacks on existing card systems using contactless smart cards, including payment systems. The focus is on Replay Attacks and Relay Attacks. Only Android smartphones with a publicly available API (Application Programming Interface) are used to implement the attacks. The smartphones have the support of NFC (Near Field Communication) and HCE (Host-based Card Emulation) technologies and therefore they are fully compatible with current contactless cards. The article also includes a description of implemented demonstrator called RRDemo, which enables the actual demonstration of both attacks. The article concludes with a discussion on possible protection techniques and provided experimental tests.

elektrorevue
ISSN 1213 - 1539

Demonstrátor útoků na bezkontaktní kartové systémy

Petr Dzurenda[1], Minh Tran[1], Jan Hajný[1], Vlastimil Beneš[2], Pavel Kristof[2]

[1]Ústav telekomunikací, Fakulta elektrotechniky a komunikačních technologií, Vysoké učení technické v Brně
Email: {dzurenda,xtranm00,hajny}@vut.cz

[2]Institut mikroelektronických aplikací s.r.o.
Email: {vlastimil.benes,pavel.kristof}@ima.cz

Abstrakt *– Článek se zaměřuje na bezpečnostní rizika a útoky na stávající kartové systémy využívající bezkontaktní čipové karty, a to včetně platebních systémů. Důraz je kladen na útoky typu opakováním zprávy (ang. Replay Attack) a přeposíláním zprávy (ang. Relay Attack). Pro realizaci útoků jsou využity volně prodejné mobilní telefony Android s veřejně dostupným API (Application Programming Interface). Použité telefony mají podporu technologie NFC (Near Field Communication) a HCE (Host-based Card Emulation) a jsou tak plně kompatibilní se současnými bezkontaktními kartami. Součástí článku je i popis vytvořeného demonstrátoru s názvem RRDemo, který umožňuje samotnou realizaci obou útoků. V závěru článku jsou diskutovány možné způsoby ochrany a diskuze k provedeným testům.*

1 Úvod

S čipovými kartami (ang. smart cards) se v běžném životě setkáváme dnes a denně. Naprostá většina z nás může potvrdit, že vlastní nějakou čipovou kartu, pomocí které prokazuje svoji identitu a přistupuje k různým elektronickým službám. Nejtypičtějším příkladem čipových karet jsou SIM (Subscriber Identification Module) karty sloužící k identifikaci účastníka v mobilní síti. Dále jsou to platební karty, v Evropě nejrozšířenější VISA (Visa International Service Association) a MasterCard, umožňující bezhotovostní platby u obchodníků. Čipové karty však nalezneme také v podobě cestovních dokladů, jako jsou cestovní pasy, v podobě jízdenek viz např. česká In-Karta [1], v podobě klubových karet výhod, skipasů, studentských karet ISIC (International Student Identity Card) [2], zaměstnanecké karty či karty používané v rámci tzv. eGovernment, které umožňují bezpečnou komunikaci občana se státními úřady. V České republice je k tomuto využívána tzv. eObčanka [3]. Dle průzkumu [4] bylo do června 2021 v oběhu mezi 30 a 50 miliardami kusů čipových karet. Z toho se vydalo přibližně 10 miliard karet v roce 2020, což svědčí o narůstajícím trendu čipových karet. Přibližně 52 % těchto karet pak připadá na SIM karty, 34 % platební karty, 4 % eGovernment (elektronické občanky a pasy) a zbylých 10 % připadá na další aplikace (předplacené TV, parkování, mýtné či jízdenky).

Čipové karty se vyrábí v různém provedení. Může se jednat o standardní plastovou kartu ve formě kreditní karty, klíčenky či nálepky. V současné době zažívají velký rozmach tzv. bezkontaktní (ang. contactless) čipové karty. Je to zejména díky jejich větší uživatelské komfortnosti, kdy uživateli stačí pouze přiložit kartu k čtecímu terminálu a dveře se otevřou, dojde k zaplacení útraty u obchodníka či přihlášení občana do elektronické státní služby. Bezkontaktní přenos dat z čipových karet však umožňuje útočníkům snazší odposlech případně modifikaci přenášených dat. S nástupem veřejně dostupných technologií, jako jsou chytré telefony s podporou technologie NFC (Near Field Communication), jsou tato rizika o to závažnější.

Tento článek se zaměřuje na současná bezpečnostní rizika bezkontaktních kartových systémů. V článku je prezentován vyvinutý demonstrátor útoků s názvem RRDemo, který umožňuje prakticky realizovat útoky opakováním zprávy (ang. Replay Attack) a přeposláním zprávy (ang. Relay Attack). Oba útoky jsou aplikovatelné na všechny bezkontaktní čipové karty podporující APDU (Application Protocol Data Unit) formát zpráv dle normy ISO 7816-4 [5]. K realizaci útoků jsou využity volně prodejné Android mobilní telefony s podporou technologií NFC a HCE (Host-based Card Emulation). Technologie NFC umožňuje telefonu komunikovat s čipovou kartou, zatímco funkce HCE umožňuje telefonu emulovat čipovou kartu a vystupovat tak v systému namísto čipové karty.

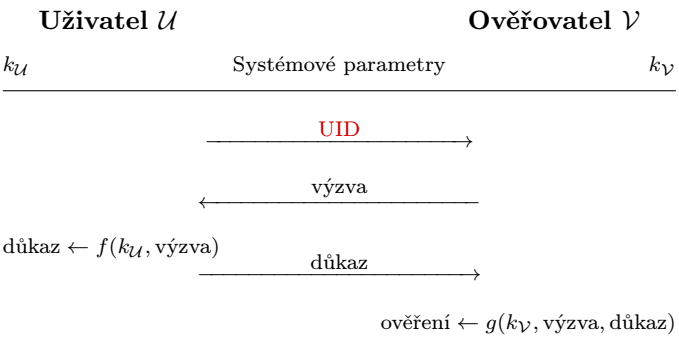
2 Současný stav

Bezpečnost čipových karet zkoumá řada vědeckých článků [6, 7, 8, 9, 10]. Tyto práce analyzují bezpečnostní slabiny samotných implementací čipových karet. K tomu využívají více či méně invazivní a finančně náročné techniky. Jedná se především o 1) `fyzické útoky` zaměřené na fyzickou manipulaci s kartou, např. fyzický přístup k čipu karty či měření postranních kanálů a 2) `logické útoky` využívající chyb vyvinutého softwaru karty. Další články [11, 12] se zaměřují na prolomení autentizačního mechanismu karet, viz prolomení šifry CRIPTO1 u karet Mifare Classic. V pracích [13, 14, 15] se pak autoři zaměřují na možnosti útoku přeposláním dat u platebních EMV (Europay, MasterCard a VISA) systémů. Tyto útoky fungovaly na tehdejší implementaci platebních systémů.

elektrorevue
ISSN 1213 - 1539

3 Bezpečnost identifikačních systémů

Identifikační systémy jsou součástí procesu řízení přístupu k aktivům uživatele. Může se jednat o přístup do chráněných prostor v rámci zaměstnaní či přístup do elektronického bankovnictví. Bezpečný systém řízení přístupu by měl být složen z části 1) `identifikace`, tj. odhalení elektronické identity a 2) `autentizace`, tj. prokázání proklamované identity ověřovateli, viz obrázek 1. Uživatel se obvykle identifikuje pomocí svého jedinečného identifikátoru UID (User IDentifier). Ověřovatel pak zahájí autentizační fázi výzvou v podobě náhodného čísla. Na tuto výzvu musí uživatel vypočítat s pomocí svého tajného klíče $k_{\mathcal{U}}$ autentizační důkaz. Ověřovatel na základě UID vyhledá ve své databázi odpovídající ověřovací klíč $k_{\mathcal{V}}$ a s jeho pomocí ověří validitu důkazu. Pokud je důkaz validní, je uživatelská identita ověřena.



Obrázek 1: Princip identifikačního protokolu.

Některé současné identifikační systémy však autentizační fázi nevyužívají. K řízení přístupu je vyžadována pouze znalost hodnoty UID validního uživatele. Toto je běžnou praxí u čipových karet Mifare Classic, kde se vychází z toho, že hodnota UID je uložena v nepřepisovatelném bloku 0 v paměti karty. V současnosti však lze přepisovatelné Mifare Classic karty snadno zakoupit. To umožňuje kopírování těchto karet a praktickou realizaci útoku opakováním UID v těchto kartových systémech, viz článek [16]. S využitím chytrých telefonů s podporou technologie NFC a HCE je pak snadné realizovat útoky na tyto systémy. Kromě útoku opakováním (ang. Replay Attack) lze realizovat i útoky přeposíláním zpráv (ang. Relay Attack).

3.1 Replay Attack

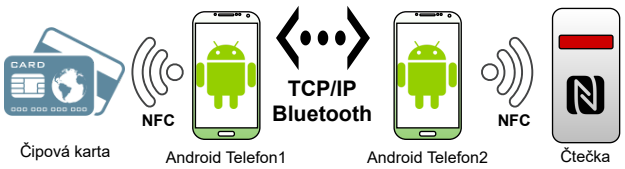
Replay Attack (česky útok opakováním) je založen na principu, že je možné z čipové karty načíst hodnotu UID, která je útočníkem využita v budoucnu. Útok je tak prakticky realizovatelný na kartové systémy využívající Mifare Classic karty. K tomuto útoku je zapotřebí jedno až dvě zařízení. Prvním zařízením je aktivní NFC zařízení (chytrý telefon) umožňující čtení dat z identifikační karty. Druhým zařízením je NFC pasivní zařízení. Na pasivní zařízení budou uložena data, která byla přečtena z identifikační karty. Pasivní zařízení musí mít stejnou strukturu jako originální karta nebo se dokázat chovat jako tato karta. Může se tedy jednat o prázdnou kartu (např. přepisovatelnou Mifare Classic kartu) nebo o chytrý telefon podporující funkci HCE. Princip útoku opakováním je zobrazen na obrázku 2.

Obrázek 2: Princip útoku opakováním zprávy.

3.2 Relay Attack

Relay Attack (česky útok přeposláním) je založen na principu přeposílání zpráv mezi dvěma legitimními stranami přes nějaký komunikační kanál. Legitimní strany u kartových systémů představují čipová karta a čtecí terminál. Mezi těmito zařízeními jsou přeposílána autentizační data v rámci plného autentizačního protokolu, viz obrázek 1. Útok nastává v momentě, kdy útočník vstoupí mezi tyto dvě komunikující strany a přeposílá jejich data. Z jedné strany posílá data z terminálu na kartu a z druhé strany data z karty na terminál.

K tomuto útoku je zapotřebí dvou zařízení, jedno NFC aktivní zařízení vystupující v roli terminálu `Telefon1` a jedno NFC pasivní zařízení (s funkcí HCE) vystupující v roli karty `Telefon2`. Útok začíná útočník. Útočník přiloží `Telefon2` k legitimnímu čtecímu terminálu. Terminál následně pošle na `Telefon2` APDU příkaz, který `Telefon2` přepošle na `Telefon1`, který dále přepošle příkaz na legitimní čipovou kartu. V tuto chvíli si karta myslí, že komunikuje s legitimním terminálem, protože dostává data, která očekává. Jako reakci na APDU příkaz odešle karta APDU odpověď, kterou pošle na `Telefon1`, ten data přepošle na `Telefon2` a ten je přepošle do legitimního terminálu. Tím, že terminál obdržel validní odpověď od legitimní karty, tak také věří tomu, že komunikuje přímo s legitimní čipovou kartou. Telefony `Telefon1` a `Telefon2` si přeposílají data do té doby, dokud není ukončen autentizační protokol jednou z legitimních komunikujících stran. Jako komunikační kanál mezi telefony lze využít Bluetooth, Wi-Fi či internetové připojení. Princip útoku přeposláním je zobrazen na obrázku 3.



Obrázek 3: Princip útoku přeposláním zprávy.

elektrorevue
ISSN 1213 - 1539

4 Čipové karty

Čipové karty jsou malá přenosná zařízení o velikosti platební karty. Karty jsou vybaveny integrovaným obvodem, který je chráněn plastovým tělem karty. Identifikační karty s integrovanými obvody jsou standardizovány normou ISO/IEC 7816-1 [17]. Karty se mohou lišit svými fyzickými rozměry či výpočetními, paměťovými nebo kryptografickými prostředky. Podle schopnosti karty provádět výpočty rozlišujeme karty na `paměťové` (data pouze uchovávají), `procesorové` (data zpracovávají) či `kryptografické` (obsahují kryptografický procesor pro hardwarovou akceleraci kryptografických algoritmů). S kartou lze komunikovat prostřednictvím kontaktního či bezkontaktního rozhraní. Identifikační bezkontaktní RFID (Radio Frequency Identification) karty s integrovanými obvody jsou standardizovány normou ISO/IEC 14443-2 [18]. Tyto karty pracují na frekvenci 13,56 MHz a jsou s NFC plně kompatibilní.

Čipové karty jako např. Java Card, MultOS, Basic Card či .NET card jsou programovatelné a mají vlastní operační systém.Vývojáři mají tak možnost navrhnout a implementovat si vlastní identifikační protokol běžící na kartě. Jiné karty nabízí již hotové proprietární řešení pro identifikační systémy. Sem patří technologie jako je Mifare, HID či Legic, viz článek [19].

Komunikace s čipovou kartou je typu klient-server, kdy karta vystupuje v roli serveru odpovídajícího na požadavky klienta. Po připojení karty ke čtečce vrátí karta zprávu ATR (Answer To Reset) a resetuje se. ATR zprostředkovává informace o komunikačních parametrech navržených kartou, povaze a stavu karty. Následně dojde k sjednání transportních protokolů a parametrů pomocí zpráv PPS (Protocol and Parameters Selection). Následující komunikace pak již probíhá pomocí výměny APDU zpráv dle standardu ISO/IEC 7816-4 [5]. V případě, že se jedná o multiaplikační kartu, je nutné aplikaci předem vybrat na základě jejího identifikátoru AID (Application Identifier) dle standardu ISO/IEC 7816-5 [20].

Mifare karty mají největší zastoupení na trhu s identifikačními systémy [19]. Mifare karty se vyrábí v různých typech s různou úrovní zabezpečení:

- `Classic` - mají proprietární komunikační protokol, který je nekompatibilní s APDU formátem zpráv dle ISO/IEC 7816-4 [5]. Karty používají také proprietární autentizační a šifrovací (CRIPTO1) protokoly.
- `Plus` - nahrazují karty Classic. Používají šifrování AES-128 či CRIPTO1 pro zpětnou kompatibilitu. Od verze EV1 je zajištěna podpora APDU zpráv dle ISO/IEC 7816-4 [5] a kontrola vzdálenosti od čtečky.
- `Ultralight` - jsou nízkonákladové jednoúčelové karty bez kryptografické podpory.
- `DESFire` - plně podporují komunikaci dle ISO/IEC 7816-4 [5]. Šifrování zajišťuje šifra 3DES či AES-128. Karty podporují více aplikací (od EV2 neomezený počet), kontrolu vzdálenosti (od EV2) a časovač transakce (od EV3) proti útoku mužem uprostřed.

5 Android platforma a NFC

Android představil technologii NFC v roce 2010 v rámci verze Gingerbread - Android 2.3 na mobilním telefonu Nexus S [21]. NFC umožňovalo pouze `Read/Write mode` dovolující telefonu zapisovat na NFC tag a číst z něho data. Od verze Ice Cream Sandwich - Android 4.0 je podporován `Peer-to-Peer mode` umožňující posílání dat mezi dvěma telefony pomocí NFC rozhraní. Od verze KitKat - Android 4.4 je pak k dispozici `Card emulation mode` umožňující telefonu emulovat čipovou kartu a komunikovat s ní dle standardu ISO/IEC 7816-4 [5]. Telefon je tedy možné použít v stávajících RFID identifikačních systémech namísto čipových karet. Na rozdíl od RFID komunikace, kde je pracovní vzdálenost řádově do 15 cm, je u NFC vyžadovaná komunikační vzdálenost jen řádově do 2 cm. NFC je standardizováno dle normy ISO/IEC 18092 [22].

NFC zařízení spolu komunikují obdobně jako RFID zařízení. Na jedné straně je NFC aktivní zařízení a na druhé NFC pasivní zařízení. Komunikaci iniciuje vždy aktivní zařízení. Pracovní frekvence NFC je stejná jako pro RFID identifikační systémy, tj. 13,56 MHz. Je-li NFC služba zapnutá, zařízení nepřetržitě hledá ve svém okolí NFC tagy, ke kterým by se mohla připojit a začít s nimi komunikovat. Různé tagy podporují různé technologie, proto je nutné tagy filtrovat, podle toho se kterými tagy má aplikace komunikovat. Android definuje tyto třídy tagů [23]:

- `IsoDep` - Třída zajišťuje komunikaci s tagy dle ISO/IEC 7816-4.
- `MifareClassic` - Třída zajišťuje funkce pro komunikaci s Mifare Classic kartami.
- `MifareUltralight` - Třída zajišťuje funkce pro komunikaci s Mifare Ultralight kartami.
- `Ndef` - Třída umožňuje komunikovat se zařízeními respektujícími doporučení NFC fóra pomocí NDEF (NFC Data Exchange Format) zpráv.
- `NdefFormatable` - Třída poskytuje přístup k funkcím pro formatovatelné NDEF zprávy.
- `NfcA` - Třída poskytuje funkce pro komunikaci s tagy dle ISO 14443-3A.
- `NfcB` - Třída poskytuje funkce pro komunikaci s tagy dle ISO 14443-3B.
- `NfcBarcode` - Třída poskytuje přístup do tagů obsahujících pouze čárový kód.
- `NfcF` - Třída poskytuje funkce pro komunikaci s tagy dle JIS 6319-4.
- `NfcV` - Třída poskytuje funkce pro komunikaci s tagy dle ISO 15693.

Třídy `IsoDep` a `MifareClassic` jsou tedy nejvhodnější pro komunikaci s většinou identifikačních karet, jako jsou Java Card, MultOS, Mifare DESFire či Classic.

elektrorevue
ISSN 1213 - 1539

6 Demonstrátor útoků - RRDemo

Demonstrátor útoků implementuje řadu funkcí umožňujících práci se současnými kartovými systémy využívajícími čipové karty Mifare Classic a karty s podporou APDU zpráv dle ISO/IEC 7816-4. Mimo to je demonstrátor schopen prakticky realizovat útoky opakováním zprávy (ang. Replay Attack) či přeposláním zprávy (ang. Relay Attack). Útok přeposláním zprávy je aplikovatelný i na současné EMV platební systémy. Výčet základních funkcí demonstrátoru je uveden v tabulce 1.

Tabulka 1: Výčet hlavních funkcí demonstrátoru útoků.

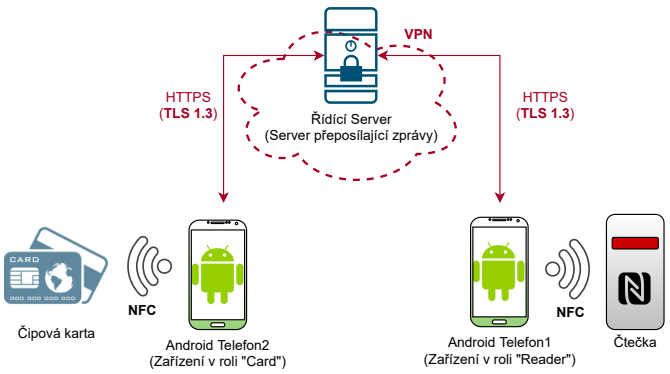
Funkce	Technologie	Podpora
Scan Reader	ISO/IEC 7816-4 APDU Mifare Classic EMV	✓/✓ ✗/✗ ✗/✗
Scan Card	ISO/IEC 7816-4 APDU Mifare Classic EMV	✗/✓ ✗/✗ ✗/✗
Replay Attack	ISO/IEC 7816-4 APDU Mifare Classic EMV	✓!/✓ ✓!/✓ ✗/✗
Relay Attack	ISO/IEC 7816-4 APDU Mifare Classic EMV	✓/✓ ✗/✓ ✓/✓

Poznámka: Podpora x/y značí podporovanou funkci, kde x = podpora funkce a y=požadavek na podporu, ✗značí nepodporovanou funkci, ✓značí podporovanou funkci a ✓! značí podporovanou funkci s omezením.

Multiaplikační karty (včetně EMV platebních karet) podporují APDU zprávy dle ISO/IEC 7816-4. Karty obvykle implementují proprietární kryptografický protokol typu výzva-odpověď, viz obrázek 1. To zabraňuje kopírování karet a tedy realizaci útoku opakováním. V případě, že by implementovaný protokol nebyl typu výzva-odpověď, je možné pomocí demonstrátoru útok opakováním realizovat. Demonstrátor umožňuje kopírovat Mifare Classic karty, tj. čtení a zápis do sektoru 0. Funkce je označena jako částečně podporovaná, jelikož neumožňuje telefonu emulovat Mifare Classic. K tomuto je zapotřebí root telefonu a telefon se specifickou HW podporou NFC [24]. Útok přeposláním není podporován u Mifare Classic karet, jelikož Android HCE funkce dokáže emulovat pouze karty komunikující pomocí APDU zpráv dle ISO/IEC 7816-4, mezi které karty Classic nepatří. U multiaplikačních karet je pro realizaci útoku nutné znát AID aplikace. K tomu slouží funkce demonstrátoru `Scan Reader` a `Scan Card`. V případě skenování čtečky stačí pouze přiložit telefon ke čtečce, která automaticky vyšle zprávu `SELECT AID`, kterou si telefon uloží. V případě platebních systémů EMV toto AID čtečka nezná (může se jednat o VISA či MasterCard). Zpráva `SELECT AID` se zašle až podle toho jaká karta je přiložena. V tomto případě jsou však všechny AID veřejně známé [25], tudíž je možné je do aplikace staticky nahrát, což demonstrátor umožňuje. Mifare Classic karty nemají žádné AID, proto také pro ně není tato funkce demonstrátorem podporována. Princip skenování karty je ekvivalentní ke skenování terminálu. Telefon se přiloží ke kartě, ze které jsou načtena všechna AID všech aplikací uložených na kartě.

6.1 Architektura systému

Demonstrátor RRDemo se skládá z mobilní aplikace a aplikace řídícího serveru. Pro vývoj mobilní aplikace byl využit program Android Studio. Aplikace je psána v jazyce Kotlin s minimální verzí API 22: Android 5.1 Lollipop, která by měla spolehlivě fungovat na 92,3 % všech Android zařízení. Serverová část byla vyvinuta pomocí vývojových prostředí Visual Studio Code a NodeJS. Server je psaný v jazyce JavaScript a je implementován v jediném souboru `server.js`. Cílem bylo vytvořit zabezpečený server zajišťující co nejrychlejší přeposílání komunikace a ukládání logů pro případnou analýzu autentizačního protokolu kompromitovaného systému. Z důvodu dostupnosti a bezpečnosti je server virtuálně hostován v privátní VPN (Virtual Private Network) síti na VUT v Brně. Server běží na operačním systému Ubuntu. Architektura systému je zobrazena na obrázku 4.



Obrázek 4: Architektura demonstrátoru RRDemo.

Mobilní aplikace RRDemo podporuje dva základní útoky (R)eplay a (R)elay. Řídící server je využit pouze pro účely přeposílání komunikace mezi telefony v rámci útoku přeposláním zprávy. Útok opakováním (Replay) dokáže kopírovat karty Mifare Classic na přepisovatelné karty podporující Classic technologii. Útok přeposláním (Relay) zpráv je funkční pro karty s komunikačním rozhraním definovaným dle ISO/IEC 7816-4. V případě demonstrátoru RRDemo byly testovány karty Java Card a EMV.

elektrorevue
ISSN 1213 - 1539

6.2 Aplikace Replay Attack

K realizaci útoku je zapotřebí vlastnit přepisovatelnou GEN2 kartu a NFC hardware podporující Mifare Classic, což jsou například čipové sety NXP nebo Samsung čipy [26]. Uživatelské rozhraní aktivity je zobrazeno na obrázku 5. Aplikace implementuje funkce `Scan Mifare` pro načtení dat z karty, `Saved Cards` pro načtení již uložených karet a `Clone to card` pro zkopírování vybrané karty na přepisovatelnou Mifare Classic kartu. V aktivitě `Scan Mifare` viz obrázek 5 (vpravo), je pak možné pomocí tlačítek `Save UID` uložit načtenou kartu, `Add Keys` uložit vlastní klíče karty či `Keys` zobrazit klíče.

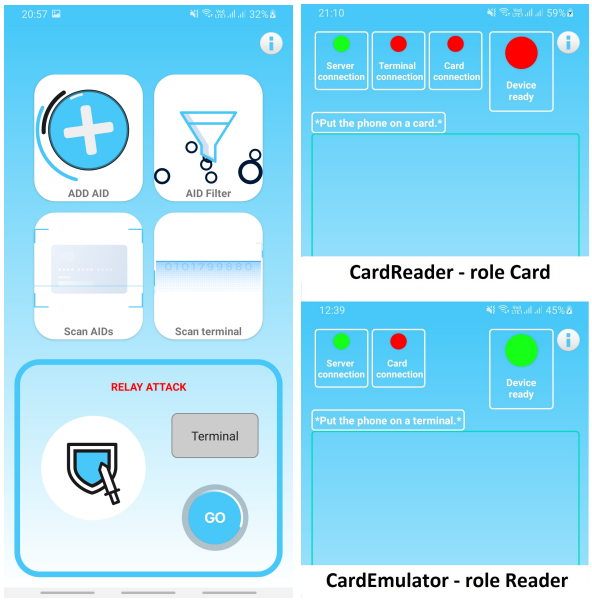
Obrázek 5: Uživatelské rozhraní aktivity Replay Attack (zleva: hlavní aktivita, Scan Mifare).

K testování byla zvolena instituce využívající Mifare Classic ve formě ISIC průkazů. Nejdříve byl vyzkoušen přístup s prázdnou GEN2 kartou, viz obrázek 6 (vlevo) a poté se zkopírovanou ISIC kartou, viz obrázek 6 (vpravo). V prvním případě byla karta zamítnuta, v druhém případě došlo k povolení přístupu.

Obrázek 6: Kopírování Mifare Classic karet.

6.3 Aplikace Relay Attack

Pro správnou funkci demonstrátoru je nutné do aplikace nahrát AID aplikace čipové karty. Pro tento útok jsou nutné dva mobilní telefony s podporou NFC a HCE a internetové připojení. Architektura systému je zobrazena na obrázku 4. Jeden telefon vystupuje v roli `Card`, druhý telefon pak v roli `Terminal`. Telefon v roli `Card` je přiložen ke kartě oběti a telefon v roli `Terminal` je přiložen k terminálu. Komunikace mezi telefony je zprostředkována WebSocket serverem (řídícím serverem), který je připojený k zabezpečené webové stránce v privátní VPN síti VUT.



Obrázek 7: Uživatelské rozhraní aktivity Relay Attack (zleva: hlavní aktivita, CardReader a CardEmulator).

Uživatelské rozhraní aktivity je zobrazeno na obrázku 7 (vlevo). Funkce `ADD AID` umožňuje manuální uložení známých AID. Kód aplikace již obsahuje některé předdefinované AID např. pro karty Mifare DESFire či EMV platební karty MasterCard a VISA a jejich startovací příkazy transakce PSE (Payment System Environment) a PPSE (Proximity PSE). Pro rootnuté telefony je zde vložen také speciální AID pro filtraci všech AID (Xposed modul [27]).

```
val startAIDList = mutableListOf<String>(
    "325041592E5359532E4444463031",// PPSE
    "315041592E5359532E4444463031",// PSE
    "A0000000041010",// MasterCard
    "A0000000031010",// VISA
    "D2760000850100",// Mifare DESFire
    "F04E66E75C02D8"// specialni AID (Xposed
    modul)
)
```

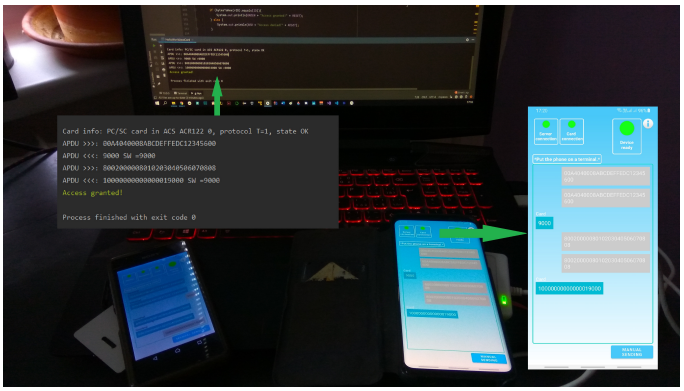
Kód 1: Startovací seznam s AIDs.

elektrorevue
ISSN 1213 - 1539

Funkce `AID Filter` umožňuje uživateli zjistit, která AID jsou již v aplikaci uložena. `Scan AIDs` umožňuje skenování karty a načtení všech AID na ní uložených. `Scan terminal` umožňuje získat AID přímo z terminálu. Podmínkou použití této funkcionality je rootnutý telefon. Terminály obvykle posílají jako první APDU zprávu výběr AID. Zařízení přiložené na terminálu musí tedy filtrovat dotazy na všechny AID, aby mohlo tuto zprávu zachytit a přijmout. Z toho důvodu je nutné mít nainstalován modul `NFC HCE Catch-All-Routing`. Na obrázku 7 (vpravo) jsou pak zobrazeny aktivity rolí telefonu `Card` a `Terminal`. Obě aktivity mají stejnou strukturu, liší se pouze ve funkcionalitě:

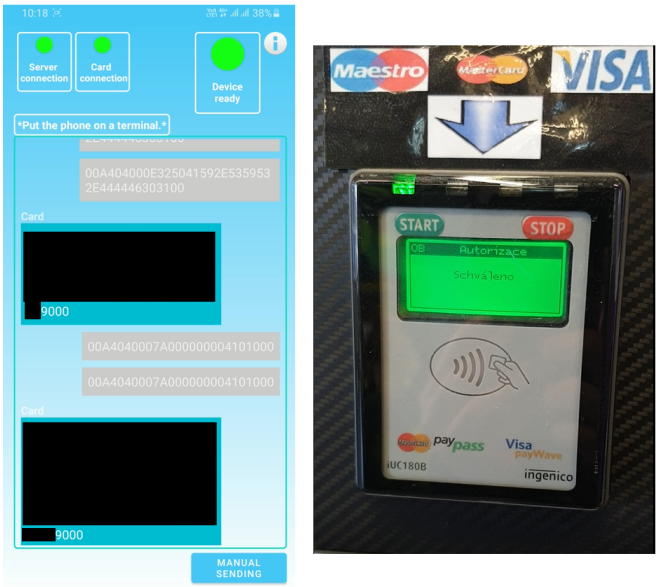
- `CardReader - role Card` - telefon je nastaven na roli `Card`, tj. přikládá se na čipovou kartu. Po spuštění aktivity se zkontroluje připojení k řídícímu serveru. Aktivní připojení je indikováno zeleným indikátorem `Server connection`. Indikátor `Terminal connection` informuje, zda je k dispozici druhý telefon v roli `Reader`, indikátor `Card connection` informuje, zda bylo vytvořeno spojení telefonu s kartou oběti. Pokud jsou všechny podmínky útoku splněny, je o tom uživatel informován indikátorem `Device ready`. Role `Card` vyžaduje funkční NFC hardware schopný číst karty a funkční internetové připojení.
- `CardEmulator - role Reader` - telefon je nastaven na roli `Reader`, tj. přikládá se k čtecímu terminálu. Po spuštění aktivity se zkontroluje připojení k řídícímu serveru. Aktivní připojení je indikováno zeleným indikátorem `Server connection`. Indikátor `Card connection` informuje, zda je k dispozici druhý telefon v roli `Card`. Pokud jsou všechny podmínky útoku splněny, je o tom uživatel informován indikátorem `Device ready`. Zařízení zastupující roli `Terminal` by mělo ideálně mít root a `NFC HCE Catch-All-Routing`. Není to však nutností. Je však nutné mít v aplikaci nahrán příslušné AID.

Demonstrátor byl prakticky testován na identifikačním systému vyvinutém v rámci projektu MPO s reg. č. FV40340 a také na současných EMV platebních systémech. Pro testování byl v roli `Terminal` použit rootnutý telefon s nainstalovaným modulem `NFC HCE Catch-All-Routing` a vypnutou aplikací `Google Pay`. Na obrázku 8 je zobrazeno testování demonstrátoru na přístupovém systému. Pro testování byl využit mobilní telefon Sony Xperia Z1 Compact D5503, který byl v roli `Card` a rootnutý telefon Samsung Galaxy S9+ s modulem `NFC HCE Catch-All-Routing`, který byl v roli `Terminal`. Prvním krokem útoku bylo přiložení telefonu Sony ke kartě. Druhým krokem bylo přiložení telefonu Samsung na čtecí terminál. V momentě, kdy terminál detekoval přítomnost telefonu, zaslal na něj APDU příkazy a začala se přeposílat komunikace. Přeposílání zpráv lze vidět na části obrázku se snímkem obrazovky telefonu. Terminál po útoku zobrazuje `"Access granted!"`, což znamená, že útok na testovací autentizační systém proběhl úspěšně.



Obrázek 8: Útok přeposláním zprávy na identifikační systém.

Speciálním případem je útok na EMV platební systémy. Jako první zpráva se zpravidla posílá PPSE, která na OS Android zařízeních automaticky vyvolává aplikaci `Google Pay`. Proto nelze v aplikaci RRDemo útok přímo realizovat. Důvodem je, že Android rozpoznává PPSE jako inicializační APDU příkaz pro platby a aplikace `Google Pay` je jediná legitimní aplikace pro platby pomocí HCE módu. Tento problém však lze obejít tím, že se deaktivuje aplikace `Google Pay`. Po deaktivaci `Google Pay` je možné již realizovat útok. Testování bylo provedeno na automatu na kávu. Na obrázku 9 (vlevo) lze vidět obrazovku zařízení v roli `Terminal`. Všechny indikátory jsou zelené. Vše je tedy v pořádku a je možné provést útok. V textovém poli lze vidět dvě prvotní zprávy z terminálu, a to PPSE a `SELECT APDU`, na které bylo úspěšně (kód 9000) odpovězeno ze zařízení v roli `Card` přiložené k platební kartě. Po předání všech zpráv terminál schválil transakci, viz obrázek 9 (vpravo).



Obrázek 9: Útok přeposláním zprávy na EMV platební systém.

elektrorevue
ISSN 1213 - 1539

Při útoku byly použity mobilní telefony Samsung Galaxy S9+ v roli `Terminal` a Xiaomi Redmi Note 8 Pro bez rootu v roli `Card`. Útok byl úspěšný a trval přibližně 4 sekundy.

7 Možnosti ochrany proti RR útokům

V případě útoku opakováním zprávy (ang. Replay Attack) je řešením využít pro identifikaci autentizační protokol typu výzva-odpověď, viz obrázek 1. V případě útoku přeposláním zprávy (ang. Relay Attack) je řešením kontrola zpoždění komunikace. Případný útočník, který vstoupí do komunikace mezi dvě legitimní zařízení, vždy zavádí určité zpoždění do komunikace z důvodu nutné režie přeposílání zpráv. Toto zpoždění je o to významnější, komunikují-li zařízení útočníka přes internet. Řešením může být tedy kontrola zpoždění na straně přístupového terminálu či přímo v čipové kartě, viz funkce kontroly vzdálenosti a časovače transakcí u karet Mifare DesFire EV3. Bezpečnost může zvýšit i vícefaktorová autentizace, kdy uživatel musí kartovou transakci potvrdit PIN kódem či heslem. Mobilní telefony umožňují emulaci čipových karet, přičemž pro komunikaci s čtečkou karet musí být alespoň v pohotovostním režimu. To chrání telefon proti neoprávněné komunikaci s okolím bez vědomí uživatele. K tomu by mohlo teoreticky dojít v přeplněných prostředcích hromadné dopravy (tramvaje či autobusy). Útočník by pouze přiložil telefon ke kapse oběti, v které se nachází čipová karta (nebo telefon) a mohl by tak teoreticky realizovat útok. Proti neoprávněnému přečtení čipových karet tak pomohou i speciální pouzdra či peněženky absorbující elektromagnetické vlny a tím znemožňující komunikaci s kartou.

8 Závěr

V článku byly popsány a diskutovány možnosti útoků na kartové systémy využívající bezkontaktní RFID identifikační karty. Tyto karty jsou plně kompatibilní s technologií NFC používané u současných chytrých telefonů. Článek se zaměřuje na konkrétní útoky typu 1) opakováním zprávy (ang. Replay Attack) a 2) přeposláním zprávy (ang. Relay Attack). Útoky necílí na softwarovou ani hardwarovou implementaci čipové karty ani na slabinu kryptografického protokolu. Oba tyto útoky byly implementovány v rámci demonstrátoru útoků s názvem RRDemo. Výsledky testování ukázaly, že útoky typu RR (Relay a Replay) jsou i v současné době velmi relevantní v řadě identifikačních tak i EMV platebních systémů typu VISA či MasterCard. Ochran proti těmto útokům existuje celá řada. Většina je však v rukou poskytovatele služby, který musí implementovat bezpečnostní funkce do samotného identifikačního systému, tj. čtecích terminálů či čipových karet. Uživatelé mají pouze základní možnost ochrany proti útoku, a to mít karty stále pod kontrolou a chránit je proti neoprávněnému přečtení, např. pomocí speciálních pouzder či peněženek pohlcujících elektromagnetické vlnění.

Poděkování

Článek vznikl na základě výsledků projektu s názvem Modulární systém pro bezpečný sběr dat v prostředí Průmyslu 4.0, reg. č. FV40340, podpořeno Ministerstvem průmyslu a obchodu ČR v rámci programu TRIO.

Literatura

[1] In Karta: Co je to In Karta?, c2016. *České dráhy* [online]. Praha: České dráhy [cit. 2021-12-04]. Dostupné z: https://www.cd.cz/jizdne/in-karta/

[2] *ISIC international student identity card* [online], c2021. Praha: GTS ALIVE [cit. 2021-12-04]. Dostupné z: https://www.isic.cz/

[3] EObčanka, c2021. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů [cit. 2021-12-04]. Dostupné z: https://info.identitaobcana.cz/eop/

[4] Smart card basics — A short illustrated guide (June 2021), 2021. *Thales - Building a future we can all trust* [online]. La Défense, Francie: Thales Group [cit. 2021-12-04]. Dostupné z: https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/smart-cards-basics

[5] *ISO/IEC 7816-4:2020 Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange*, 2020. 4. Ženeva, Švýcarsko: International Organization for Standardization. Dostupné také z: https://www.iso.org/standard/77180.html

[6] BARBU, Guillaume, Hugues THIEBEAULD a Vincent GUERIN, 2010. Attacks on java card 3.0 combining fault and logical attacks. *Springer: Lecture Notes in Computer Science, 9th IFIP WG 8.8/11.2 International Conference, CARDIS 2010, Passau, Germany, April 14-16, 2010. Proceedings.* Berlin, Heidelberg, **6035**(1), 148-163. ISSN 978-3-642-12510-2.

[7] CALAFATO, Andrew, 2012. *An analysis of the vulnerabilities introduced with the java card 3.* Londýn. Diplomová práce. Royal Holloway, University of London. Vedoucí práce Dr. Kostantinos Markantonakis.

[8] OSWALD, David a Christof PAAR, 2011. Breaking Mifare DESFire MF3ICD40: Power analysis and templates in the real world. *Springer: Lecture Notes in Computer Science, 13th International Workshop, Nara, CHES 2011, Japan, September 28 — October 1, 2011. Proceedings.* Berlin, Heidelberg, **6917**(1), 207-222. ISSN 978-3-642-23951-9.

[9] FLYNN, Rory, 2019. *An investigation of possible attacks on the MIFARE DESFire EV1 smartcard used in public transportation.* Dublin. Bakalářská práce. Trinity College Dublin, School of Computer Science and Statistics. Vedoucí práce Dr. Stephen Farrell.

elektrorevue
ISSN 1213 - 1539

[10] FUJINO, Takeshi, Takaya KUBOTA a Mitsuru SHIOZAKI, 2017. Tamper-resistant cryptographic hardware. *IEICE Electronics Express*. Tokio, Japonsko, **14**(2), 1—13. ISSN 1349-2543.

[11] COURTOIS, Nicolas T., Karsten NOHL a Sean O'NEIL, 2008. Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards. *IACR cryptology: Cryptology ePrint Archive: Report 2008/166*. 3.

[12] COURTOIS, Nicolas T., 2009. The dark side of security by obscurity and cloning Mifare Classic rail and building passes, anywhere, anytime: Prezentace. *UCL Discovery: The 5th Workshop on RFID Security*. Leuven, Belgie, 1-109.

[13] VILA, José a Ricardo J. RODRÍGUEZ, 2015. Practical experiences onNFC relay attacks with android. *Springer: Lecture Notes in Computer Science, 10th International Workshop, RFIDSec 2014, Oxford, UK, July 21-23, 2014, Revised Selected Papers*. Berlin, Heidelberg, **9440**(1), 87-103. ISSN 978-3-319-24836-3.

[14] FRANCIS, Lishoy, Gerhard HANCKE, Keith MAYES a Konstantinos MARKANTONAKIS, 2012. Practical re-lay attack on contactless transactions by using NFCmobile phones. *IACR cryptology: Cryptology ePrint Archive: Report 2011/618*. 1-16.

[15] GIESE, Dennis, Kevin LIU, Michael SUN, Tahin SYED a Linda ZHANG, 2018. Security analysisof near-field communication (NFC) payments. *ArXivpreprint: arXiv:1904.10623*. 1-10.

[16] LIESKOVAN, Tomáš, 2019. Bezpečnost autentizačních systémů založených na kartách Mifare Classic a ověřování pomocí UID. *Elektrorevue*. **21**(1), 16-20. ISSN 1213-1539.

[17] *ISO/IEC 7816-1:2011 Identification cards - Integrated circuit cards - Part 1: Cards with contacts - Physical characteristics*, 2011. 2. Ženeva, Švýcarsko: International Organization for Standardization. Dostupné také z: https://www.iso.org/standard/54089.html

[18] *ISO/IEC 14443-2:2020 Cards and security devices for personal identification - Contactless proximity objects - Part 2: Radio frequency power and signal interface*, 2020. 4. Ženeva, Švýcarsko: International Organization for Standardization. Dostupné také z: https://www.iso.org/standard/73597.html

[19] DZURENDA, Petr, Jan HAJNY, Vaclav ZEMAN a Kamil VRBA, 2015. Modern physical access control systems and privacy protection. *IEEE Xplore: 2015 38th International Conference on Telecommunications and Signal Processing (TSP), Prague, Czech Republic*. New York, USA, 1-5. ISSN 978-1-4799-8498-5.

[20] *ISO/IEC 7816-5:2004 Identification cards - Integrated circuit cards - Part 5: Registration of application providers*, 2004. 2. Ženeva, Švýcarsko: International Organization for Standardization. Dostupné také z: https://www.iso.org/standard/34259.html

[21] Gingerbread, 2020. *Android for Developers* [online]. Mountain View, USA: Google [cit. 2021-12-04]. Dostupné z: https://developer.android.com/about/versions/android-2.3-highlights

[22] *ISO/IEC 18092:2013 Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1)*, 2013. 2. Ženeva, Švýcarsko: International Organization for Standardization. Dostupné také z: https://www.iso.org/standard/56692.html

[23] Android.nfc.tech, 2021. *Android for Developers* [online]. Mountain View, USA: Google [cit. 2021-12-04]. Dostupné z: https://developer.android.com/reference/android/nfc/tech/package-summary

[24] SLAWOMIR, Jasek, 2018. A 2018 practical guide to hacking NFC/RFID: Prezentace. *SecuRing 15 yrs*. Confidence, Kraków: SecuRing, 1-148. Dostupné také z: https://smartlockpicking.com/slides/Confidence_A_2018_Practical_Guide_To_ Hacking_RFID_NFC.pdf

[25] COMPLETE LIST OF APPLICATION IDENTIFIERS (AID), c2011. *EFTLab - Breakthrough Payment Technologies* [online]. London, UK: EFTLab [cit. 2021-12-04]. Dostupné z: https://www.eftlab.com/knowledge-base/ 211-emv-aid-rid-pix/

[26] NFC Compatibility, 2021. *NFC Tags, Cards, Readers and other NFC Products - Shop NFC* [online]. Lecco, Itálie: Shop NFC [cit. 2021-12-04]. Dostupné z: https://www.shopnfc.com/en/content/ 7-nfc-compatibility

[27] ZWENG, Johannes, 2018. Xposed Module NFC HCE Catch-All-Routing. *GitHub* [online]. [cit. 2021-12-04]. Dostupné z: https://github.com/johnzweng/ Xposed-ModifyAidRouting