

Relay Attacks in EMV Contactless Cards with Android OTS Devices

José Vila[†], Ricardo J. Rodríguez[‡]
pvtolkien@gmail.com, rj.rodriguez@unileon.es

© All wrongs reversed



Universidad
Zaragoza

[†] *Computer Science and
Systems Engineering Dept.*
University of Zaragoza, Spain



universidad
de león

[‡] *Research Institute of
Applied Sciences in Cybersecurity*
University of León, Spain

May 28, 2015

Hack in the Box 2015
Amsterdam (Nederland)

About us



Pepe Vila

Security Consultant at E&Y

tw: @cgvwzq

<http://vwzq.net>



Dr. Ricardo J. Rodríguez

Senior Security Researcher at ULE

tw: @RicardoJRodriguez

<http://www.ricardojrodriguez.es>

Main research interests

- </JavaXSScript> and client-side attacks
- NFC security
- Android internals

Main research interests

- Security/safety modelling and analysis of ICS
- Advanced malware analysis
- NFC security

Agenda

1 Introduction

2 Background

- EMV Contactless Cards
- Relay Attacks and Mafia Frauds

3 Android and NFC: A Tale of L♥ve

- Evolution of NFC Support in Android
- Practical Implementation Alternatives in Android

4 Relay Attack Implementation

- Demo experiment
- Threat Scenarios
- Resistant Mechanisms

5 Related Work

6 Conclusions

Agenda

1 Introduction

2 Background

- EMV Contactless Cards
- Relay Attacks and Mafia Frauds

3 Android and NFC: A Tale of L♥ve

- Evolution of NFC Support in Android
- Practical Implementation Alternatives in Android

4 Relay Attack Implementation

- Demo experiment
- Threat Scenarios
- Resistant Mechanisms

5 Related Work

6 Conclusions

Introduction to NFC (I)

What is NFC?

- Bidirectional short-range contactless communication technology
 - Up to 10 cm
- Based on RFID standards, works in the 13.56 MHz spectrum
- Data transfer rates vary: 106, 216, and 424 kbps



Introduction to NFC (I)

What is NFC?

- Bidirectional short-range contactless communication technology
 - Up to 10 cm
- Based on RFID standards, works in the 13.56 MHz spectrum
- Data transfer rates vary: 106, 216, and 424 kbps



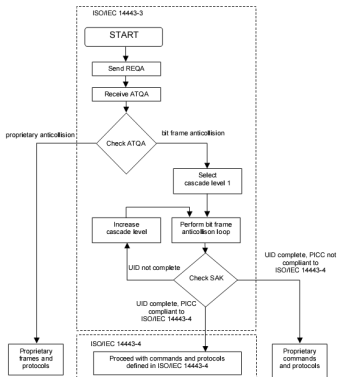
Security based on proximity concern: physical constraints

Introduction to NFC (II)

Wow! NFC sounds pretty hipster!

- Two main elements:
 - Proximity Coupling Device (PCD, also NFC-capable device)
 - Proximity Integrated Circuit Cards (PICC, also NFC tags)
- Three operation modes:
 - Peer to peer: direct communication between parties
 - Read/write: communication with a NFC tag
 - Card-emulation: an NFC device behaves as a tag

Introduction to NFC (III)



ISO/IEC 14443 standard

- Four-part international standard for contactless smartcards
 - 1 Size, physical characteristics, etc.
 - 2 RF power and signalling schemes (Type A & B)
 - Half-duplex, 106 kbps rate
 - 3 Initialization + anticollision protocol
 - 4 Data transmission protocol
- IsoDep cards: compliant with the four parts
 - Example: contactless payment cards

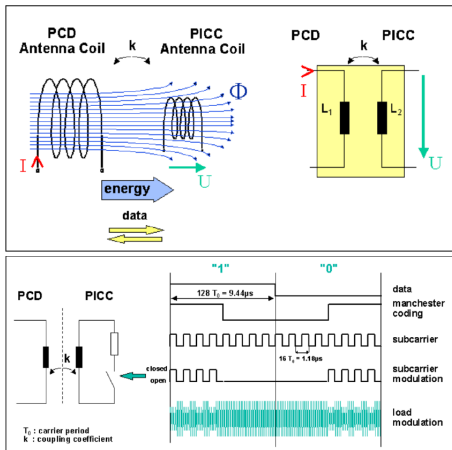
Introduction to NFC (IV)



ISO/IEC 7816

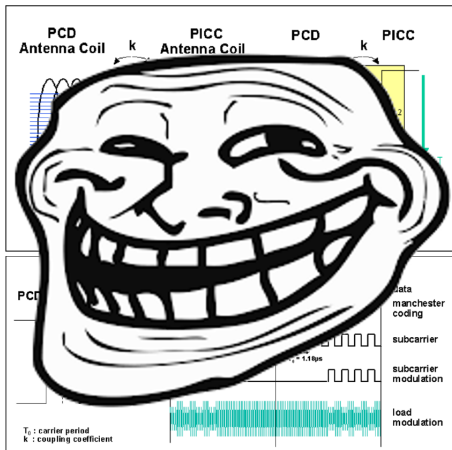
- Fifteen-part international standard related to contactless integrated circuit cards, especially smartcards
- [Application Protocol Data Units \(APDUs\)](#)

Introduction to NFC (V)



[Taken from 13.56 MHz RFID Proximity Antennas (http://www.nxp.com/documents/application_note/AN78010.pdf)]

Introduction to NFC (V)



[Taken from 13.56 MHz RFID Proximity Antennas (http://www.nxp.com/documents/application_note/AN78010.pdf)]

Introduction to NFC (VI)



Ticketing



Time & Attendance



Loyalty & Memberships

NFC



Physical Access

Cashless Payment



Transit



Secure PC Log-On



Introduction to NFC (VII)

Ok. . . So, is it secure, right? Right??

Introduction to NFC (VII)

Ok. . . So, is it secure, right? Right??

If it were *so* secure, you would not be staring at us 😊

Introduction to NFC (VII)

Ok... So, is it secure, right? Right??

If it were *so* secure, you would not be staring at us 😊

NFC security threats

- **Eavesdropping**
 - Secure communication as solution
- **Data modification** (i.e., alteration, insertion, or destruction)
 - Feasible in theory (but requires quite advanced RF knowledge)
- **Relays**
 - Forwarding of wireless communication
 - Two types: passive (just forwards), or active (forwards and alters the data)

Introduction to NFC (VII)

Ok... So, is it secure, right? Right??

If it were *so* secure, you would not be staring at us 😊

NFC security threats

- **Eavesdropping**
 - Secure communication as solution
- **Data modification** (i.e., alteration, insertion, or destruction)
 - Feasible in theory (but requires quite advanced RF knowledge)
- **Relays**
 - Forwarding of wireless communication
 - Two types: passive (just forwards), or active (forwards and alters the data)

We focus on passive relay attacks

Introduction to NFC (VIII)



- NFC brings “cards” to mobile devices
- Payment sector is quite interested in this new way for making payments
 - 500M NFC payment users expected by 2019
- Almost 300 smart phones available at the moment with NFC capabilities
 - Check <http://www.nfcworld.com/nfc-phones-list/>
 - Most of them runs **Android OS**

Introduction to NFC (VIII)



- NFC brings “cards” to mobile devices
- Payment sector is quite interested in this new way for making payments
 - 500M NFC payment users expected by 2019
- Almost 300 smart phones available at the moment with NFC capabilities
 - Check <http://www.nfcworld.com/nfc-phones-list/>
 - Most of them runs **Android** OS

Research Hypothesis

- *Can a passive relay attack be performed in contactless payment cards, using an Android NFC-capable device?*
- *If so, what are the constraints? (whether any exists)*

Agenda

1 Introduction

2 Background

- EMV Contactless Cards
- Relay Attacks and Mafia Frauds

3 Android and NFC: A Tale of L♥ve

- Evolution of NFC Support in Android
- Practical Implementation Alternatives in Android

4 Relay Attack Implementation

- Demo experiment
- Threat Scenarios
- Resistant Mechanisms

5 Related Work

6 Conclusions

Background (I)

EMV contactless cards



- Europay, Mastercard, and VISA standard for inter-operation of IC cards, Point-of-Sale terminals and automated teller machines
- Authenticating credit and debit card transactions
- Commands defined in ISO/IEC 7816-3 and ISO/IEC 7816-4 (<http://en.wikipedia.org/wiki/EMV>)
 - Application ID (AID) command

Background (II)

MasterCard PayPass, VISA payWave, and AmericanExpress ExpressPay



Are they secure?

Background (II)

MasterCard PayPass, VISA payWave, and AmericanExpress ExpressPay



Are they secure?

- Amount limit on a single transaction
 - Up to £20 GBP, 20€, US\$50, 50CHF, CAD\$100, or AUD\$100

Background (II)

MasterCard PayPass, VISA payWave, and AmericanExpress ExpressPay



Are they secure?

- Amount limit on a single transaction

- Up to £20 GBP, 20€, US\$50, 50CHF, CAD\$100, or AUD\$100
- *cof, cof*

(<http://www.bankinfosecurity.com/android-attack-exploits-visa-emv-flaw-a-7516/op-1>)

Background (II)

MasterCard PayPass, VISA payWave, and AmericanExpress ExpressPay

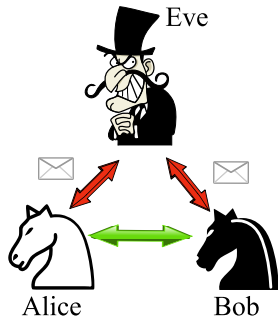


Are they secure?

- Amount limit on a single transaction
 - Up to £20 GBP, 20€, US\$50, 50CHF, CAD\$100, or AUD\$100
 - *cof, cof*

(<http://www.bankinfosecurity.com/android-attack-exploits-visa-emv-flaw-a-7516/op-1>)
- Sequential contactless payments limited – it asks for the PIN
- Protected by the same fraud guarantee as standard transactions (hopefully)

Background (III)



Relay attacks

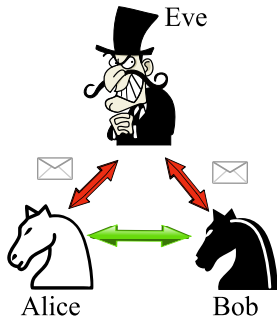
- “On Numbers and Games”, J. H. Conway (1976)

Mafia frauds – Y. Desmedt (SecuriCom’88)

$$\mathcal{P} \rightarrow \bar{\mathcal{V}} \ll \text{communication link} \gg \bar{\mathcal{P}} \rightarrow \mathcal{V}$$

- Real-time fraud where a fraudulent prover $\bar{\mathcal{P}}$ and verifier $\bar{\mathcal{V}}$ cooperate

Background (III)



Relay attacks

- “On Numbers and Games”, J. H. Conway (1976)

Mafia frauds – Y. Desmedt (SecuriCom'88)

$$\mathcal{P} \rightarrow \overline{\mathcal{V}} \ll\text{communication link}\gg \overline{\mathcal{P}} \rightarrow \mathcal{V}$$

- Real-time fraud where a fraudulent prover $\overline{\mathcal{P}}$ and verifier $\overline{\mathcal{V}}$ cooperate
 - Honest prover and verifier: contactless card and Point-of-Sale terminal
 - Dishonest prover and verifier: two NFC-enabled Android devices

Agenda

1 Introduction

2 Background

- EMV Contactless Cards
- Relay Attacks and Mafia Frauds

3 Android and NFC: A Tale of L♥ve

- Evolution of NFC Support in Android
- Practical Implementation Alternatives in Android

4 Relay Attack Implementation

- Demo experiment
- Threat Scenarios
- Resistant Mechanisms

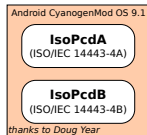
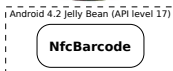
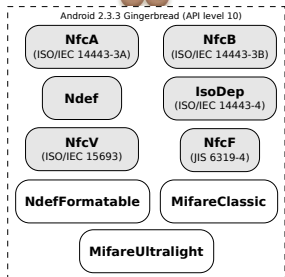
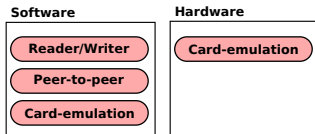
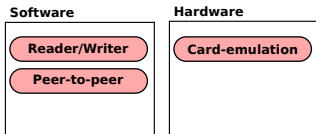
5 Related Work

6 Conclusions

Android and NFC: A Tale of Love (I)

Recap on evolution of Android NFC support

NFC operation modes supported



Android and NFC: A Tale of L♥ve (II)

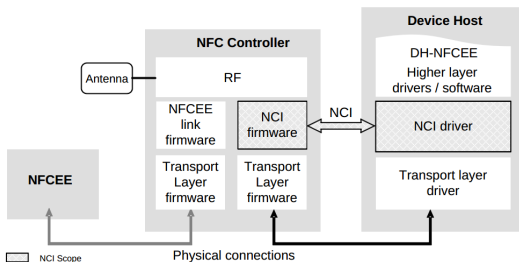
Digging into Android NFC stack

- Event-driven framework, nice API support
- Two native implementations (depending on built-in NFC chip)
 - `libnfc-nxp`
 - `libnfc-nci`

Android and NFC: A Tale of L♥ve (II)

Digging into Android NFC stack

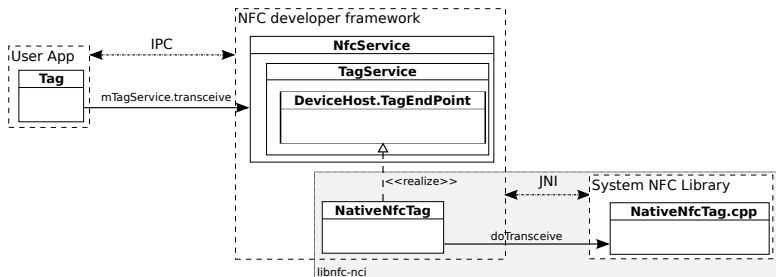
- Event-driven framework, nice API support
- Two native implementations (depending on built-in NFC chip)
 - libnfc-nxp
 - libnfc-nci
- NXP dropped in favour of NCI:
 - Open architecture, not focused on a single family chip
 - Open interface between the NFC Controller and the DH
 - Standard proposed by NFC Forum



Android and NFC: A Tale of L♥ve (III)

Digging into Android NFC stack – Reader/Writer mode

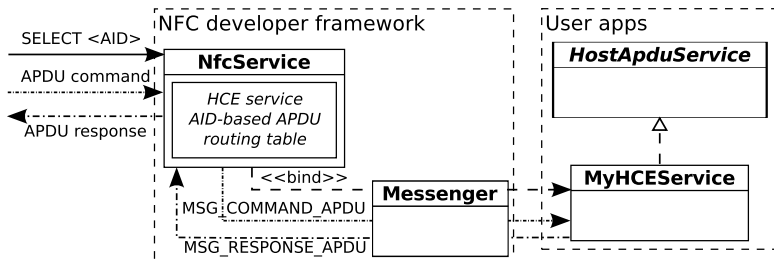
- Not allowed to be set directly → Android activity
- Android NFC service selects apps according to tag definition of Manifest file
- In low-level, libnfc-nci uses reliable mechanism of queues and message passing – General Kernel Interface (GKI)
 - Makes communication between layers and modules easier



Android and NFC: A Tale of L♥ve (IV)

Digging into Android NFC stack – HCE mode

- A service must be implemented to process commands and replies
- HostApduService abstract class, and processCommandApdu method
- AID-based routing service table
 - This means you need to declare in advance what AID you handle!



Android and NFC: A Tale of L♥ve (V)

Digging into Android NFC stack – Summary

Description	Language(s)	Dependency	OSS
NFC developer framework (com.android.nfc package)	Java, C++	API level	Yes
System NFC library (libnfc-ncp or libnc-nci)	C/C++	Manufacturer	Yes
NFC Android kernel driver	C	Hardware and manufacturer	Yes
NFC firmware (/system/vendor/firmware directory)	ARM Thumb	Hardware and manufacturer	No

Some useful links

- <https://android.googlesource.com/platform/frameworks/base/+master/core/java/android/nfc/>
- <https://android.googlesource.com/platform/packages/apps/Nfc/+master/src/com/android/nfc>
- <https://android.googlesource.com/platform/packages/apps/Nfc/+master/nci/>
- <https://android.googlesource.com/platform/external/libnfc-nci/+master/src/>
- <http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/nfc-controller-interface-nci-specifications/>
- [http://www.cardsys.dk/download/NFC_Docs/NFC%20Controller%20Interface%20\(NCI\)%20Technical%20Specification.pdf](http://www.cardsys.dk/download/NFC_Docs/NFC%20Controller%20Interface%20(NCI)%20Technical%20Specification.pdf)
- <http://www.datasheet4u.com/PDF/845670/BCM20793S.html>
- <http://www.datasheet4u.com/PDF/845671/BCM20793SKMLG.html>

Android and NFC: A Tale of L♥ve (VI)

Some remarkable limitations

Limitation 1

- DISHONEST VERIFIER COMMUNICATES WITH A MIFARE CLASSIC
- `libnfc-nci` do not allow sending raw ISO/IEC 14443-3 commands
 - Caused by the CRC computation, performed by the NFCC
- Overcome whether NFCC is modified
- EMV contactless cards are IsoDep: *fully ISO/IEC 14443-compliant*

Android and NFC: A Tale of L♥ve (VI)

Some remarkable limitations

Limitation 1

- DISHONEST VERIFIER COMMUNICATES WITH A MIFARE CLASSIC
- libnfc-nci do not allow sending raw ISO/IEC 14443-3 commands
 - Caused by the CRC computation, performed by the NFCC
- Overcome whether NFCC is modified
- EMV contactless cards are IsoDep: *fully ISO/IEC 14443-compliant*

Limitation 2

- DISHONEST PROVER COMMUNICATES WITH A HONEST VERIFIER
- Device in HCE mode
 - AID must be known in advance
- Overcome whether device is rooted
- Xposed framework may help to overcome this issue, but needs root permissions

Android and NFC: A Tale of L♥ve (V)

Some remarkable limitations and remarks

Limitation 3

- DISHONEST PROVER AND A DISHONEST VERIFIER COMMUNICATE THROUGH A NON-RELIABLE PEER-TO-PEER RELAY CHANNEL
- ISO/IEC 14443-4 defines the Frame Waiting Time as $FWT = 256 \cdot (16/f_c) \cdot 2^{FWI}$, $0 \leq FWI \leq 14$, where $f_c = 13.56$ MHz

Android and NFC: A Tale of L♥ve (V)

Some remarkable limitations and remarks

Limitation 3

- DISHONEST PROVER AND A DISHONEST VERIFIER COMMUNICATE THROUGH A NON-RELIABLE PEER-TO-PEER RELAY CHANNEL
- ISO/IEC 14443-4 defines the Frame Waiting Time as $FWT = 256 \cdot (16/f_c) \cdot 2^{FWI}$, $0 \leq FWI \leq 14$, where $f_c = 13.56$ MHz
 - $FWT \in [500\mu s, 5s] \rightarrow$ relay is *theoretically* possible when delay is $\leq 5s$

Concluding Remarks

- *Any NFC-enabled device running OTS Android ≥ 4.4 can perform an NFC passive relay attack at APDU level when the specific AID of the honest prover is known and an explicit SELECT is performed*

Android and NFC: A Tale of L♥ve (V)

Some remarkable limitations and remarks

Limitation 3

- DISHONEST PROVER AND A DISHONEST VERIFIER COMMUNICATE THROUGH A NON-RELIABLE PEER-TO-PEER RELAY CHANNEL
- ISO/IEC 14443-4 defines the Frame Waiting Time as $FWT = 256 \cdot (16/f_c) \cdot 2^{FWI}$, $0 \leq FWI \leq 14$, where $f_c = 13.56$ MHz
 - $FWT \in [500\mu s, 5s] \rightarrow$ relay is *theoretically possible* when delay is $\leq 5s$

Concluding Remarks

- *Any NFC-enabled device running OTS Android ≥ 4.4 can perform an NFC passive relay attack at APDU level when the specific AID of the honest prover is known and an explicit SELECT is performed*
- *Any communication involving a APDU-compliant NFC tag (i.e., MIFARE DESFire EV1, Inside MicroPass, or Infineon SLE66CL) can also be relayed*

Android and NFC: A Tale of L♥ve (V)

Some remarkable limitations and remarks

Limitation 3

- DISHONEST PROVER AND A DISHONEST VERIFIER COMMUNICATE THROUGH A NON-RELIABLE PEER-TO-PEER RELAY CHANNEL
- ISO/IEC 14443-4 defines the Frame Waiting Time as $FWT = 256 \cdot (16/f_c) \cdot 2^{FWI}$, $0 \leq FWI \leq 14$, where $f_c = 13.56$ MHz
 - $FWT \in [500\mu s, 5s] \rightarrow$ relay is *theoretically possible* when delay is $\leq 5s$

Concluding Remarks

- *Any NFC-enabled device running OTS Android ≥ 4.4 can perform an NFC passive relay attack at APDU level when the specific AID of the honest prover is known and an explicit SELECT is performed*
- *Any communication involving a APDU-compliant NFC tag (i.e., MIFARE DESFire EV1, Inside MicroPass, or Infineon SLE66CL) can also be relayed*

And now, let's move to the practice 😊

Agenda

1 Introduction

2 Background

- EMV Contactless Cards
- Relay Attacks and Mafia Frauds

3 Android and NFC: A Tale of L♥ve

- Evolution of NFC Support in Android
- Practical Implementation Alternatives in Android

4 Relay Attack Implementation

- Demo experiment
- Threat Scenarios
- Resistant Mechanisms

5 Related Work

6 Conclusions

Relay Attack Implementation (I)

Experiment configuration

- PoS device: Ingenico IWL280 with GRPS + NFC support
- Android app developed (± 2000 LOC)
- Two OTS Android NFC-capable devices
 - One constraint only: dishonest prover must run an Android ≥ 4.4

Relay Attack Implementation (I)

Experiment configuration

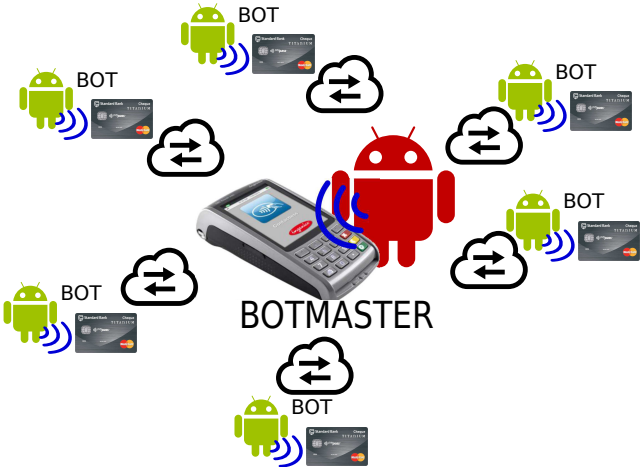
- PoS device: Ingenico IWL280 with GRPS + NFC support
- Android app developed (± 2000 LOC)
- Two OTS Android NFC-capable devices
 - One constraint only: dishonest prover must run an Android ≥ 4.4



Relay Attack Implementation (II)

Threat Scenarios – Scenario 1

DISTRIBUTED MAFIA FRAUD



Relay Attack Implementation (III)

Threat Scenarios – Scenario 2

HIDING FRAUD LOCATIONS



Relay Attack Implementation (IV)

Resistant Mechanisms

Brief summary of resistant mechanisms

- **Distance-bounding protocols**
 - Upper bounding the physical distance using Round-Trip-Time of cryptographic challenge-response messages
- **Timing constraints**
 - Not enforced in current NFC-capable systems
 - The own protocol allows timing extension commands
- **Physical countermeasures**
 - Whitelisting/Blacklisting random UID in HCE mode → unfeasible
 - RFID blocking covers
 - Physical button/switch activation
 - Secondary authentication methods (e.g., on-card fingerprint scanners)

Agenda

1 Introduction

2 Background

- EMV Contactless Cards
- Relay Attacks and Mafia Frauds

3 Android and NFC: A Tale of L♥ve

- Evolution of NFC Support in Android
- Practical Implementation Alternatives in Android

4 Relay Attack Implementation

- Demo experiment
- Threat Scenarios
- Resistant Mechanisms

5 Related Work

6 Conclusions

Related Work

On relay attacks

2005-2009 First works built on [specific hardware](#)

2010 [Nokia mobile phones with NFC capability plus a Java MIDlet app](#)

2012-2013 [Relay attacks on Android accessing to Secure Elements](#)

- [A SE securely stores data associated with credit/debit cards](#)
- [Needs a non-OTS Android device](#)

2014 [Active relay attacks with custom hardware and custom Android firmware](#)

- Several works studied delay upon relay channel:

[Relay over long distances are feasible](#) → latency isn't a hard constraint

*Ask us for *specific* references, too many names for a single slide!*

Agenda

1 Introduction

2 Background

- EMV Contactless Cards
- Relay Attacks and Mafia Frauds

3 Android and NFC: A Tale of L♥ve

- Evolution of NFC Support in Android
- Practical Implementation Alternatives in Android

4 Relay Attack Implementation

- Demo experiment
- Threat Scenarios
- Resistant Mechanisms

5 Related Work

6 Conclusions

Conclusions (I)

Security of NFC is based on the physical proximity concern

- NFC threats: eavesdropping, data modification, relay attacks
- Android NFC-capable devices are rising
 - Abuse to interact with cards in its proximity

Conclusions (I)

Security of NFC is based on the physical proximity concern

- NFC threats: eavesdropping, data modification, relay attacks
- Android NFC-capable devices are rising
 - Abuse to interact with cards in its proximity

Conclusions

- Review of Android NFC stack
- Proof-of-Concept of relay attacks using Android OTS devices
 - Threat scenarios introduced

Conclusions (I)

Security of NFC is based on the physical proximity concern

- NFC threats: eavesdropping, data modification, relay attacks
- Android NFC-capable devices are rising
 - Abuse to interact with cards in its proximity

Conclusions

- Review of Android NFC stack
- Proof-of-Concept of relay attacks using Android OTS devices
 - Threat scenarios introduced

Virtual pickpocketing attack may appear before long!

Conclusions (II)

But then, what the hell can I do?? Should I run away?

Conclusions (II)

But then, what the hell can I do?? Should I run away?

The screenshot shows a website's top navigation bar with the following links: Home, Products, Protect Your Information, About Us, Contact, News Stories, Why It's Needed/FAQ, and Add Your Logo. Below the navigation is a large banner advertisement. The banner features a man in a suit holding a credit card, with a background of green binary code. The text in the banner reads: "YOUR PERSONAL DATA IS AT RISK" in large green letters, followed by "Over 13 million Americans were victims of identity theft related fraud last year. Don't be next." and a "Learn More" button. Below this, it says "Our mission is to inform you about RFID technology risks, and provide you with protective products." Below the banner is a "Product Categories" section with six items: Women's RFID Wallet Styles (red wallet), Men's RFID Wallet Styles (black wallet), Secure Wallet™ Mini RFID wallets (brown wallet), Secure Passport Products (passport holder), Secure Sleeve® Packs (green sleeve), and RFID Blocking Badge Holders (white badge holder). To the right of the product categories is a "Need Ideas? Check out our Gift Guide" link. Below the product categories is a "Protect Yourself from Electronic Pickpocketing" section. To the right of the product categories is a "Pebbled Leather Wallets" advertisement with the text "Buy ONE at Regular Price, & Get the SECOND one FREE*" and "Orders over \$50 ship FREE (*equal or lesser value)".

Home Products Protect Your Information About Us Contact News Stories Why It's Needed/FAQ Add Your Logo

YOUR PERSONAL DATA IS AT RISK

Over 13 million Americans were victims of identity theft related fraud last year. Don't be next.

[Learn More](#)

Our mission is to inform you about RFID technology risks, and provide you with protective products.

Product Categories

[Need Ideas? Check out our Gift Guide](#)

Women's RFID Wallet Styles

Men's RFID Wallet Styles

Secure Wallet™ Mini RFID wallets

Secure Passport Products

Secure Sleeve® Packs

RFID Blocking Badge Holders

Protect Yourself from Electronic Pickpocketing

Pebbled Leather Wallets
Buy ONE at Regular Price, & Get the SECOND one FREE*
Orders over \$50 ship FREE (*equal or lesser value)

Conclusions (II)

But then, what the hell can I do?? Should I run away?



Conclusions (III)

Future Work

- *Develop a botnet infrastructure and earn money*
- Timing constraints of Android HCE mode
- Try active relay attacks within EMV contactless cards

Acknowledgments

- Spanish National Cybersecurity Institute (INCIBE)
- University of León under contract X43
- HITB staff

Conclusions (III)

Future Work

- ~~Develop a botnet infrastructure and earn money~~
- Timing constraints of Android HCE mode
- Try active relay attacks within EMV contactless cards

Acknowledgments

- Spanish National Cybersecurity Institute (INCIBE)
- University of León under contract X43
- HITB staff
- And thanks to all for hearing us!

Visit <http://vwzq.net/relaynfc> for more info about the project

Relay Attacks in EMV Contactless Cards with Android OTS Devices

José Vila[†], Ricardo J. Rodríguez[‡]
pvtolkien@gmail.com, rj.rodriguez@unileon.es

© All wrongs reversed



Universidad
Zaragoza

[†] *Computer Science and
Systems Engineering Dept.*
University of Zaragoza, Spain



universidad
de león

[‡] *Research Institute of
Applied Sciences in Cybersecurity*
University of León, Spain

May 28, 2015

Hack in the Box 2015
Amsterdam (Nederland)