

# Experiences on NFC Relay Attacks with Android: Virtual Pickpocketing Revisited

José Vila<sup>†</sup>, **Ricardo J. Rodríguez**<sup>‡</sup>  
594190@unizar.es, rj.rodriguez@unileon.es

© All wrongs reversed



**Universidad**  
Zaragoza

<sup>†</sup> University of Zaragoza, Spain



**universidad**  
**de león**

<sup>‡</sup> RIASC, University of León, Spain

14 de Septiembre, 2015

**I Jornadas Nacionales de Investigación en Ciberseguridad**  
León (España)

IN PROCEEDINGS OF THE 11TH INTERNATIONAL WORKSHOP ON RFID 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? – Near Field Communication

- 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? – Near Field Communication

- 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 (I)

## What is NFC? – Near Field Communication

- 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

## Main elements & operation modes

- 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 (II)

## NFC-related ISO/IEC standards

- ISO/IEC 14443 standard
  - Four-part international standard: [Half-duplex communication, 106 kbps](#)
  - [IsoDep cards](#): compliant with the four parts
    - Example: [contactless payment cards](#)
- ISO/IEC 7816: Fifteen-part international standard
  - [Application Protocol Data Units](#) (APDUs)



# Introduction to NFC (II)

## NFC-related ISO/IEC standards

- ISO/IEC 14443 standard
  - Four-part international standard: [Half-duplex communication, 106 kbps](#)
  - [IsoDep cards](#): compliant with the four parts
    - Example: [contactless payment cards](#)
- ISO/IEC 7816: Fifteen-part international standard
  - [Application Protocol Data Units](#) (APDUs)

## 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)



# Introduction to NFC (II)

## NFC-related ISO/IEC standards

- ISO/IEC 14443 standard
  - Four-part international standard: [Half-duplex communication, 106 kbps](#)
  - [IsoDep cards](#): compliant with the four parts
    - Example: [contactless payment cards](#)
- ISO/IEC 7816: Fifteen-part international standard
  - [Application Protocol Data Units](#) (APDUs)

## 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

# Introduction to NFC (II)

## NFC-related ISO/IEC standards

- ISO/IEC 14443 standard
  - Four-part international standard: [Half-duplex communication, 106 kbps](#)
  - [IsoDep cards](#): compliant with the four parts
    - Example: [contactless payment cards](#)
- ISO/IEC 7816: Fifteen-part international standard
  - [Application Protocol Data Units](#) (APDUs)

## 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
  - Types: [passive](#) (just forwards); and active (forwards and alters the data)

# Introduction to NFC (III)



- 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 (III)



- 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 OTS device?*
- *Is there any constraints?*

# 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 (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

## Security on contactless payments

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

# 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

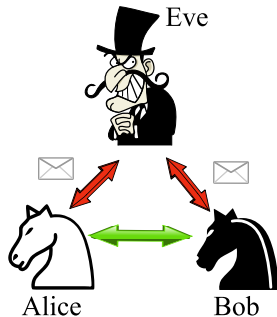
## Security on contactless payments

- Amount limit on a single transaction
  - Up to £20 GBP, 20€, US\$50, 50CHF, CAD\$100, or AUD\$100
- Sequential contactless payments limited – asks for PIN after some payments
- Protected by the same fraud guarantee as standard transactions





## Background (II)



### Relay attacks

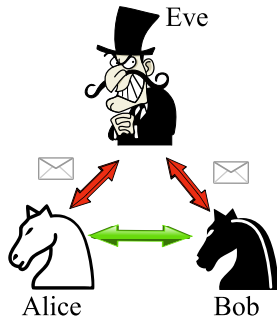
- “On Numbers and Games”, J. H. Conway (1976)

### 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

## Background (II)



### Relay attacks

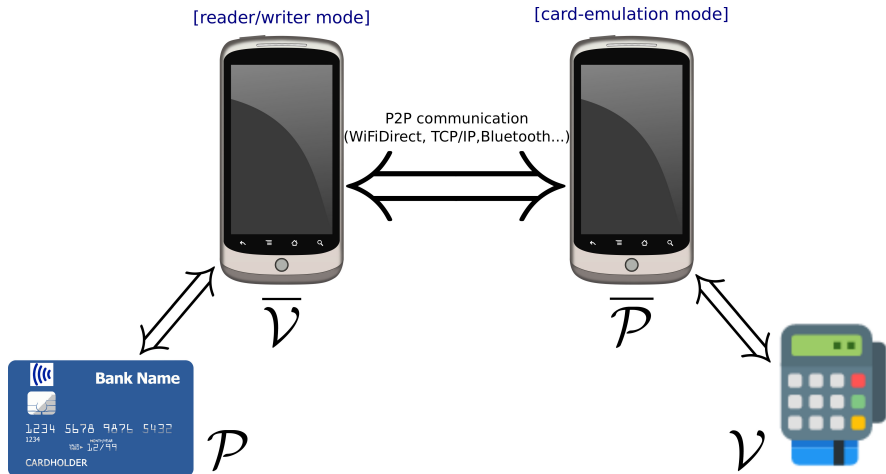
- “On Numbers and Games”, J. H. Conway (1976)

### Mafia frauds – Y. Desmedt (SecuriCom’88)

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

- 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

# Background (III)



# 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

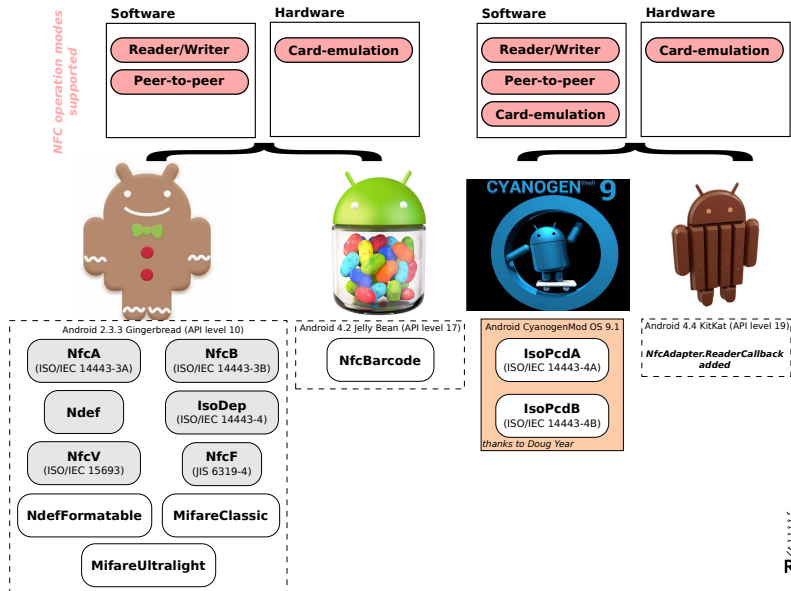
## 5 Related Work

## 6 Conclusions



# Android and NFC: A Tale of L♥ve (I)

## Recap on evolution of Android NFC support



# Android and NFC: A Tale of L♥ve (II)

## Digging into Android NFC stack

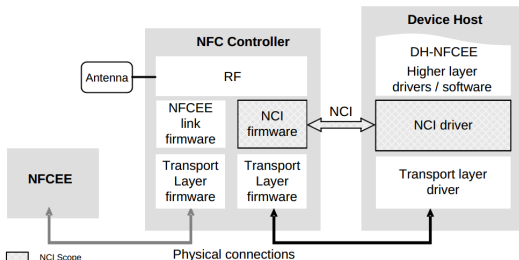
- Event-driven framework, nice API support
- Two native implementations (depending on built-in NFC chip)
  - `libnfc-nxp`
  - `libnfc-nci`



# Android and NFC: A Tale of L♥ve (II)

## Digging into Android NFC stack

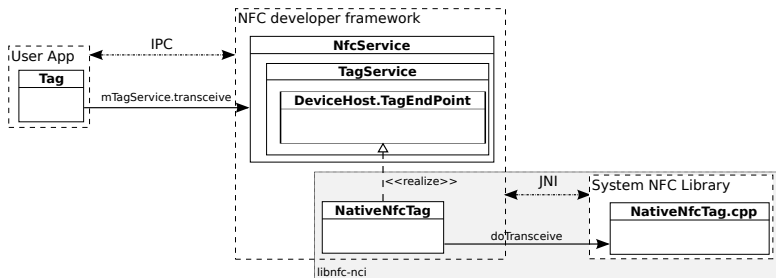
- Event-driven framework, nice API support
- Two native implementations (depending on built-in NFC chip)
  - libnfc-nxp
  - libnfc-nci
- NXP dropped in favour of NCI:
  - Open architecture, not focused on a single family chip
  - Open interface between the NFC Controller and the DH
  - Standard proposed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

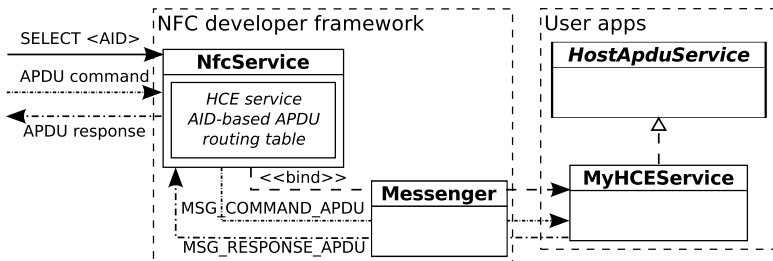




# Android and NFC: A Tale of L♥ve (IV)

## 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<br>(com.android.nfc package) | Java, C++   | API level                 | Yes |
| System NFC library<br>(libnfc-ncp or libnci-nci)     | C/C++       | Manufacturer              | Yes |
| NFC Android kernel driver                            | C           | Hardware and manufacturer | Yes |
| NFC firmware<br>(/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.latchesheet4u.com/PDF/845670/BCH20793S/Html>
- <http://www.latchesheet4u.com/PDF/845671/BCH20793SKMLG/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 (only on Type A cards, apparently on Type B cards is computed by software)
- 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 (only on Type A cards, apparently on Type B cards is computed by software)
- 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 (VII)

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 (VII)

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  $\leq 5s$



# Android and NFC: A Tale of L♥ve (VII)

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  $\leq 5s$
- In HCE mode, NFCC in Android sets  $FWI = 7 \rightarrow FWT = 0.0386$  s
- WTX commands are automatically sent by NFCC (work in progress!)



# Android and NFC: A Tale of L♥ve (VII)

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  $\leq 5s$
- In HCE mode, NFCC in Android sets  $FWI = 7 \rightarrow FWT = 0.0386$  s
- WTX commands are automatically sent by NFCC (work in progress!)

## Concluding Remarks

- *Any NFC-enabled device running OTS Android  $\geq 4.4$  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 (VII)

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  $\leq 5s$
- In HCE mode, NFCC in Android sets  $FWI = 7 \rightarrow FWT = 0.0386$  s
- WTX commands are automatically sent by NFCC (work in progress!)

## Concluding Remarks

- Any NFC-enabled device running OTS Android  $\geq 4.4$  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 of APDU-compliant NFC tags (i.e., DESFire EV1, Inside MicroPass, or Infineon SLE66CL) can be relayed

# 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 ( $\pm 2000$  LOC)
- Two OTS Android NFC-capable devices
  - One constraint only: dishonest prover must run an Android  $\geq 4.4$



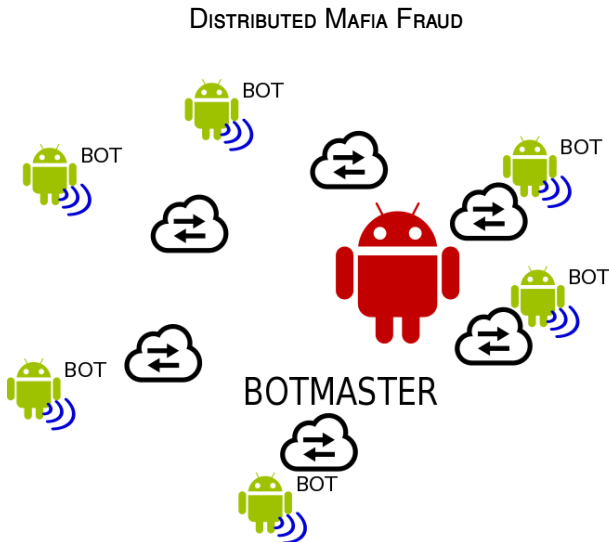
## Relay Attack Implementation (I)

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

|                                       |      |      |      |      |      |      |      |         |      |      |      |      |         |      |         |      |      |      |      |      |      |      |      |      |      |      |  |  |
|---------------------------------------|------|------|------|------|------|------|------|---------|------|------|------|------|---------|------|---------|------|------|------|------|------|------|------|------|------|------|------|--|--|
| $\mathcal{V} \rightarrow \mathcal{P}$ | 00A4 | 0400 | 0E32 | 5041 | 592E | 5359 | 532E | 4444    | 4630 | 3100 |      |      |         |      |         |      |      |      |      |      |      |      |      |      |      |      |  |  |
| $\mathcal{P} \rightarrow \mathcal{V}$ | 6F30 | 840E | 3250 | 4159 | 2E53 | 5953 | 2E44 | 4446    | 3031 | A51E | BF0C | 1B61 | 194F    | 08A0 | 0000    | 0004 | 1010 | 0250 | 0A4D | 4153 | 5445 | 5243 | 4152 | 4487 | 0101 | 9000 |  |  |
| $\mathcal{V} \rightarrow \mathcal{P}$ | 00A4 | 0400 | 08A0 | 0000 | 0004 | 1010 | 0200 |         |      |      |      |      |         |      |         |      |      |      |      |      |      |      |      |      |      |      |  |  |
| $\mathcal{P} \rightarrow \mathcal{V}$ | 6F20 | 8408 | A000 | 0000 | 0410 | 1002 | A514 | 8701    | 0150 | 0A4D | 4153 | 5445 | 5243    | 4152 | 445F    | 2D02 | 6361 | 9000 |      |      |      |      |      |      |      |      |  |  |
| $\mathcal{V} \rightarrow \mathcal{P}$ | 80A8 | 0000 | 0283 | 0000 |      |      |      |         |      |      |      |      |         |      |         |      |      |      |      |      |      |      |      |      |      |      |  |  |
| $\mathcal{P} \rightarrow \mathcal{V}$ | 7716 | 8202 | 1880 | 9410 | 0801 | 0100 | 1001 | 0100    | 1801 | 0200 | 2001 | 0200 | 9000    |      |         |      |      |      |      |      |      |      |      |      |      |      |  |  |
| $\mathcal{V} \rightarrow \mathcal{P}$ | 00B2 | 0114 | 00   |      |      |      |      |         |      |      |      |      |         |      |         |      |      |      |      |      |      |      |      |      |      |      |  |  |
| $\mathcal{P} \rightarrow \mathcal{V}$ | 7081 | 9357 | 13XX | XXXX | XXXX | XXXX | XXXX | XXXX    | XXXX | XXXX | XXXX | XXXX | 5A08    | XXXX | XXXX    | XXXX | XXXX | 5F24 | 03XX | XXXX | 5F28 | 0207 | 245F | 3401 | 018C |      |  |  |
| $\mathcal{V} \rightarrow \mathcal{P}$ | 219F | 0206 | 9F03 | 069F | 1A02 | 9505 | 5F2A | 029A    | 039C | 019F | 3704 | 9F35 | 019F    | 4502 | 9F4C    | 089F | 3403 | 8D0C | 910A | 8A02 | 9505 | 9F37 | 049F | 4C08 | 8E0C |      |  |  |
| $\mathcal{P} \rightarrow \mathcal{V}$ | 0000 | 0000 | 0000 | 0000 | 4203 | 1F03 | 9F07 | 023D    | 009F | 0802 | 0002 | 9F0D | 05B0    | 50AC | 8000    | 9F0E | 0500 | 0000 | 0000 | 9F0F | 05B0 | 70AC | 9800 | 9F4A | 0182 |      |  |  |
| $\mathcal{V} \rightarrow \mathcal{P}$ | 00B2 | 011C | 00   |      |      |      |      |         |      |      |      |      |         |      |         |      |      |      |      |      |      |      |      |      |      |      |  |  |
| $\mathcal{P} \rightarrow \mathcal{V}$ | 7081 | C28F | 0105 | 9F32 | 0301 | 0001 | 9204 | 3DD0    | 2519 | 9081 | B034 | 45XX | ...XX62 | 9000 |         |      |      |      |      |      |      |      |      |      |      |      |  |  |
| $\mathcal{V} \rightarrow \mathcal{P}$ | 00B2 | 021C | 00   |      |      |      |      |         |      |      |      |      |         |      |         |      |      |      |      |      |      |      |      |      |      |      |  |  |
| $\mathcal{P} \rightarrow \mathcal{V}$ | 7081 | B393 | 81B0 | 3445 | XXXX | XXXX | XXXX | ...XXXX | XXXX | XX62 | 9000 |      |         |      |         |      |      |      |      |      |      |      |      |      |      |      |  |  |
| $\mathcal{V} \rightarrow \mathcal{P}$ | 00B2 | 0124 | 00   |      |      |      |      |         |      |      |      |      |         |      |         |      |      |      |      |      |      |      |      |      |      |      |  |  |
| $\mathcal{P} \rightarrow \mathcal{V}$ | 7033 | 9F47 | 0301 | 0001 | 9F48 | 2A3E | XXXX | ...XXXX | XXXX | XX6D | 9000 |      |         |      |         |      |      |      |      |      |      |      |      |      |      |      |  |  |
| $\mathcal{V} \rightarrow \mathcal{P}$ | 00B2 | 0224 | 00   |      |      |      |      |         |      |      |      |      |         |      |         |      |      |      |      |      |      |      |      |      |      |      |  |  |
| $\mathcal{P} \rightarrow \mathcal{V}$ | 7081 | 949F | 4681 | 9018 | XXXX | XXXX | XXXX | ...XXXX | XXXX | XXF5 | 9000 |      |         |      |         |      |      |      |      |      |      |      |      |      |      |      |  |  |
| $\mathcal{V} \rightarrow \mathcal{P}$ | 80AE | 8000 | 2B00 | 0000 | 0000 | 0100 | 0000 | 0000    | 0007 | 2480 | 0000 | 8000 | 0978    | 1502 | 2400    | 37FB | 88BD | 2200 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 |      |  |  |
| $\mathcal{P} \rightarrow \mathcal{V}$ | 7729 | 9F27 | 01XX | 9F36 | 02XX | XX9F | 2608 | XXXX    | XXXX | XXXX | XXXX | XXXX | 9F10    | 12XX | ...XX90 | 00   |      |      |      |      |      |      |      |      |      |      |  |  |

# Relay Attack Implementation (II)

## Threat Scenarios – Scenario 1



# 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 (WTX)
- 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** Built on [specific hardware](#) (Hancke et al., Kfir & Wool)
- 2010** [NFC-enabled Nokia mobile phones plus a Java MIDlet app](#) (Francis et al., Verdult & Kooman)
- 2012-2013** [Relay attacks on Android Secure Elements](#) (Roland et al.)
- Secure storage for credit/debit cards data
  - Needs a non-OTS Android device
- 2013** Delay upon relay channel: (Oren et al., Sportiello & Ciardulli)
- [Latency of the relay channel isn't a hard constraint at all](#)
- 2014** Active relay attacks with [custom hardware and custom Android firmware](#) (Korak & Hutter)

## Android apps available (SF and Google Play)

- 2012** [nfcproxy](#) (Cyanogen Mod, card-emulation support)
- 2014** [nfcspy](#) (catch-all AID module from Xposed framework)

# 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



# Conclusions (I)

Security of NFC is based on the physical proximity concern

**Definitely, physical proximity is not a reliable constraint anymore**

- 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  
**Definitely, physical proximity is not a reliable constraint anymore**

- 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  
**Definitely, physical proximity is not a reliable constraint anymore**

- 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)

What can I do to prevent myself to be a mafia fraud victim?



# Conclusions (II)

[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

### Pebbled Leather Wallets

Buy ONE at Regular Price,  
& Get the SECOND one FREE\*



Clutches Men's Minis

Orders over \$50 ship FREE  
(\*equal or lesser value)

**Protect Yourself from Electronic Pickpocketing**





# Conclusions (II)



# Conclusions (III)

## Future Work

- ~~Develop a botnet infrastructure and earn money~~
- Timing constraints of Android HCE mode

# Conclusions (III)

## Future Work

- ~~Develop a botnet infrastructure and earn money~~
- Timing constraints of Android HCE mode
  - First experiments are promising. . . stay tuned!
- Try active relay attacks within EMV contactless cards

## Acknowledgments

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

# Conclusions (III)

## Future Work

- ~~Develop a botnet infrastructure and earn money~~
- Timing constraints of Android HCE mode
  - First experiments are promising... stay tuned!
- Try active relay attacks within EMV contactless cards

## Acknowledgments

- Spanish National Cybersecurity Institute (INCIBE)
- University of León under contract X43
- Thanks for hearing me!

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



# Experiences on NFC Relay Attacks with Android: Virtual Pickpocketing Revisited

José Vila<sup>†</sup>, **Ricardo J. Rodríguez**<sup>‡</sup>  
594190@unizar.es, rj.rodriguez@unileon.es

© All wrongs reversed



**Universidad**  
Zaragoza

<sup>†</sup> University of Zaragoza, Spain



**universidad**  
**de león**

<sup>‡</sup> RIASC, University of León, Spain

14 de Septiembre, 2015

**I Jornadas Nacionales de Investigación en Ciberseguridad**  
León (España)

IN PROCEEDINGS OF THE 11TH INTERNATIONAL WORKSHOP ON RFID SECURITY