Relay attacks in EMV contactless cards with Android OTS devices

Ricardo J. Rodríguez

@RicardoJRdez ※ rjrodriguez@unizar.es ※ www.ricardojrodriguez.es

Centro Universitario de la Defensa Zaragoza

Centro Universitario de la Defensa,
Academia General Militar (AGM)

March 31, 2017

Escuela de Doctorado – Universidad de Valladolid
Valladolid, Spain

Vila, J. & Rodríguez, R. J. *Practical Experiences on NFC Relay Attacks with Android: Virtual Pickpocketing Revisited*. Proceedings of the 11th International Workshop on RFID Security (RFIDsec), Springer, LNCS vol. 9440, 87-103. doi: 10.1007/978-3-319-24837-0_6

Agenda

CUD Zaragoza

Agenda

CUD Zaragoza

Introduction to NFC

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

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

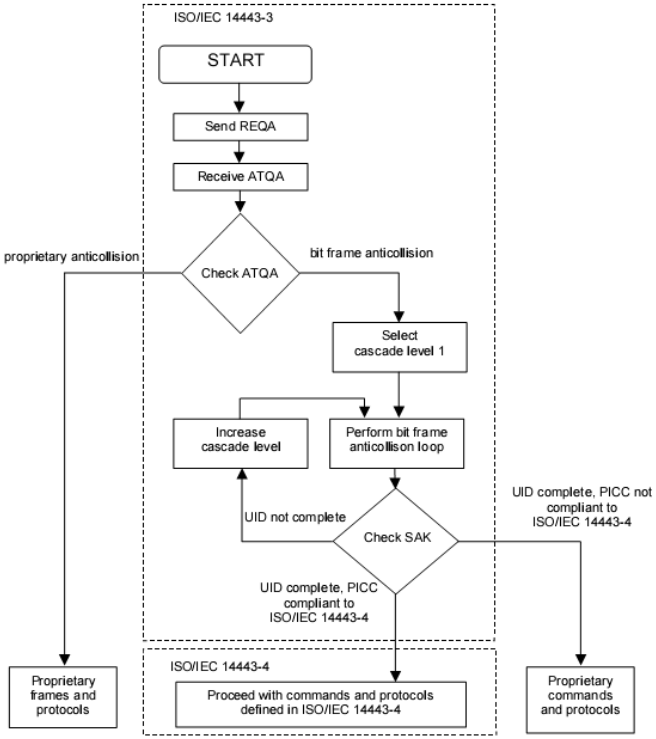
Wow! NFC sounds pretty hipster!

- 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

CUD Zaragoza

Introduction to NFC

Related standards



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

CUD Zaragoza

Introduction to NFC

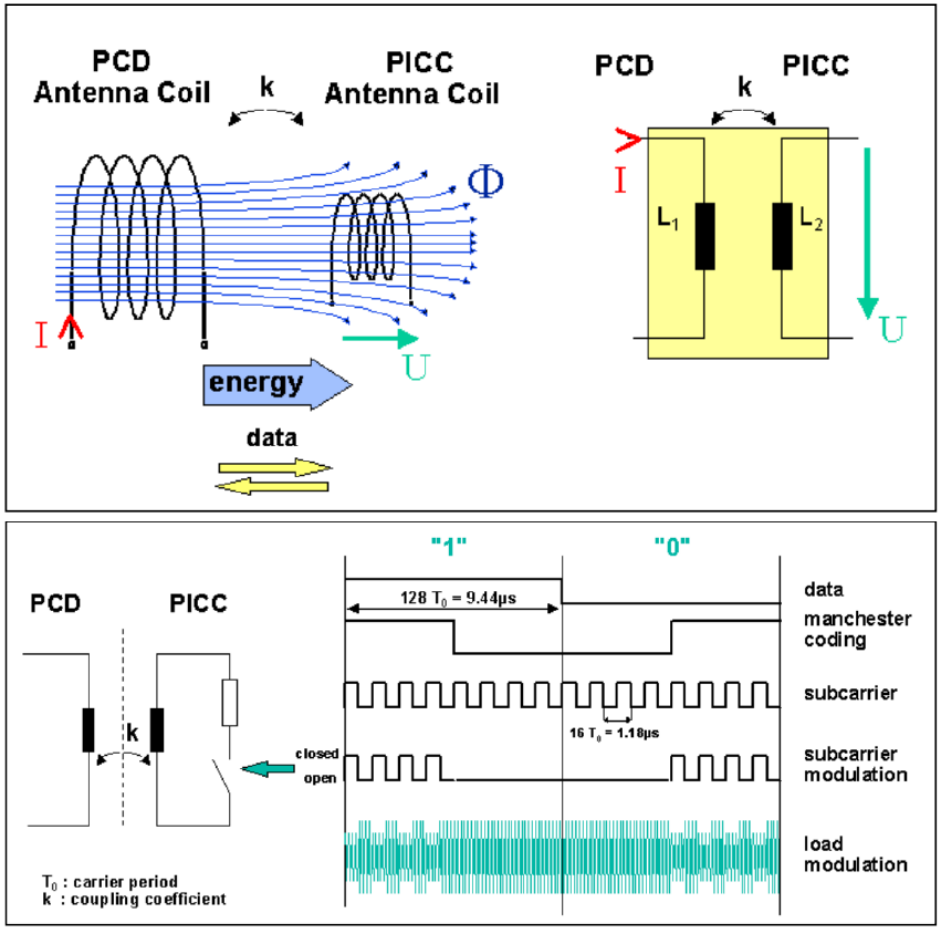
Related standards

ISO/IEC 7816

- Fifteen-part international standard related to contacted integrated circuit cards, especially smartcards
- Application Protocol Data Units (APDUs)

Introduction to NFC

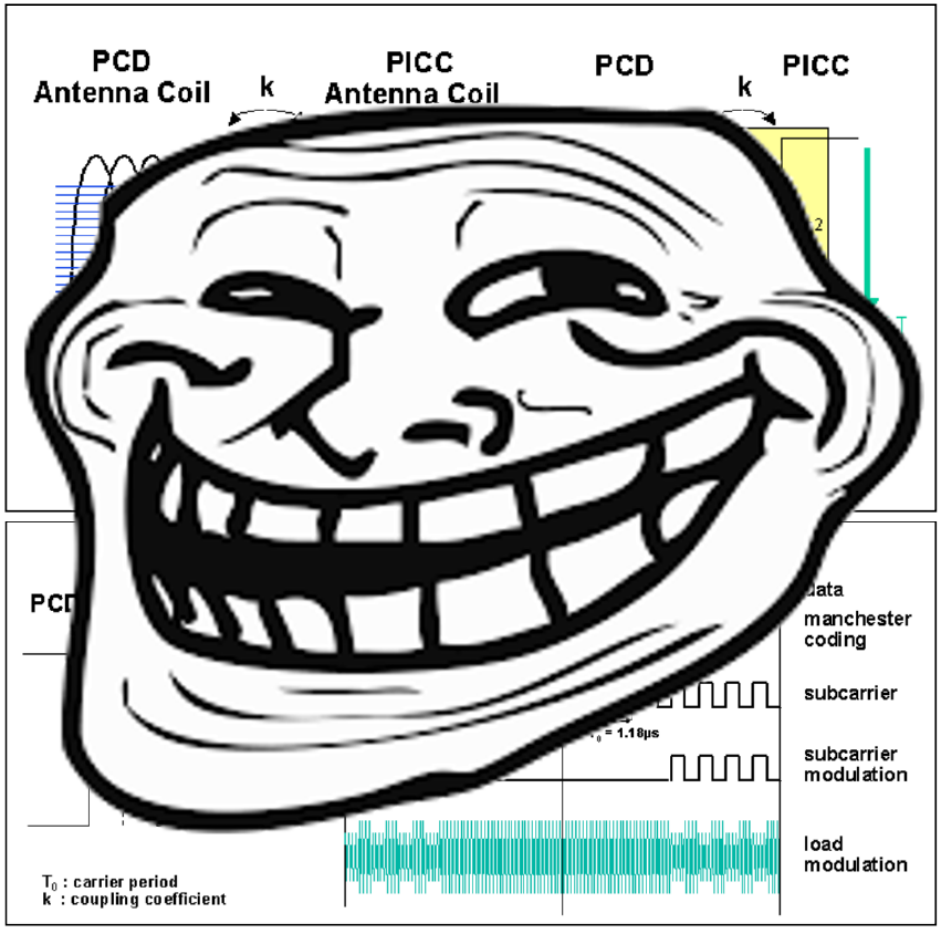
Let's make some physics



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

Introduction to NFC

Let's make some physics



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

Introduction to NFC

Ticketing

Identification

Time & Attendance

NFC

Loyalty & Memberships

Physical Access

Cashless Payment

Transit

Secure PC Log-On

Introduction to NFC

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

Introduction to NFC

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

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)

CUD Zaragoza

Introduction to NFC

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

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 only focus on passive relay attacks

Introduction to NFC

- 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
  - See `http://www.nfcworld.com/nfc-phones-list/`
  - Most of them runs Android OS

Introduction to NFC

- 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
  - See `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

CUD Zaragoza

EMV: What is it?

Europay, Mastercard, and VISA standard for inter-operation of IC cards, Point-of-Sale terminals, and automated teller machines

EMV: What is it?

Europay, Mastercard, and VISA standard for inter-operation of IC cards, Point-of-Sale terminals, and automated teller machines

Owners (with joining dates)

(Sept 2013)

(Feb 2009)

(May 13)

EMV: What is it?

- Standard initially written in 1993-1994
- Different deployment dates (e.g., 2003 at UK)
- Required for Single Euro Payment Area (SEPA)
- Why?
  - Tying to reduce fraud:
    - Skimming
    - Stolen credit cards with forged signatures
    - Card-Not-Present (CNP) fraud
  - Liability shift
    - Merchant: when no EMV card is used
    - Customer: when PIN is used

CUD Zaragoza

EMV contactless cards

- 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

EMV contactless cards

MasterCard PayPass, VISA payWave, and AmericanExpress ExpressPay

Are they secure?

EMV contactless cards

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

EMV contactless cards

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)

EMV contactless cards

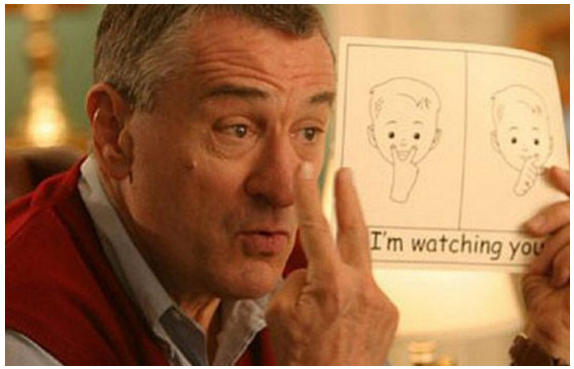
MasterCard PayPass, VISA payWave, and AmericanExpress ExpressPay

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)

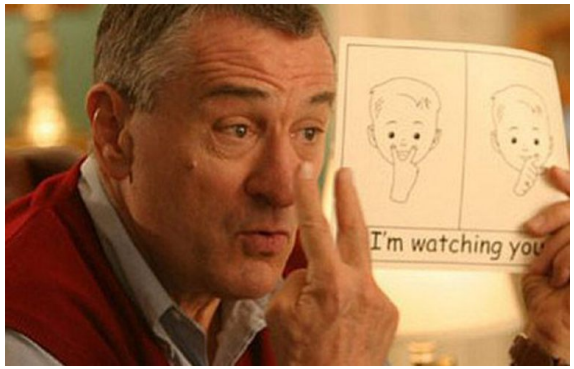
NFC Eavesdropping and EMV Contactless Cards



What data are being transmitted from my card?

(**without any reader verification, it rocks!**)

NFC Eavesdropping and EMV Contactless Cards

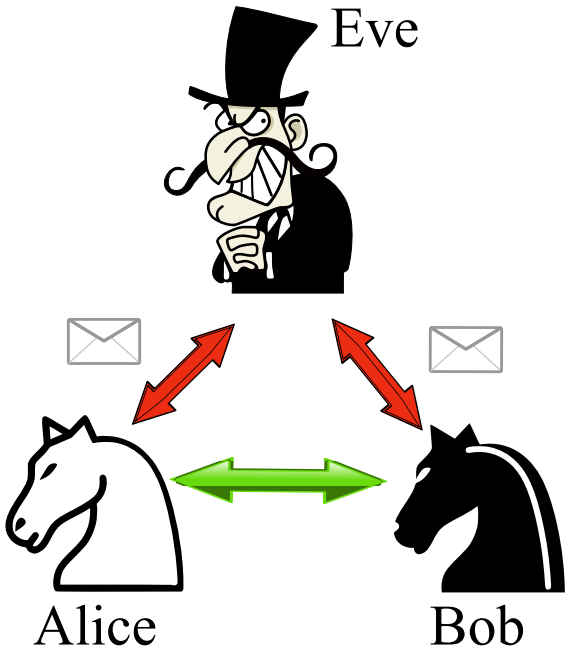


What data are being transmitted from my card?

(**without any reader verification, it rocks!**)

- **Primary Account Number** (PAN)
- **Name**
- **Expiration date**
- Transaction history
  - Data come from NFC plus chip payments. . . – **NFC is just a wireless interface** for accessing the chip!

Background



Relay attacks

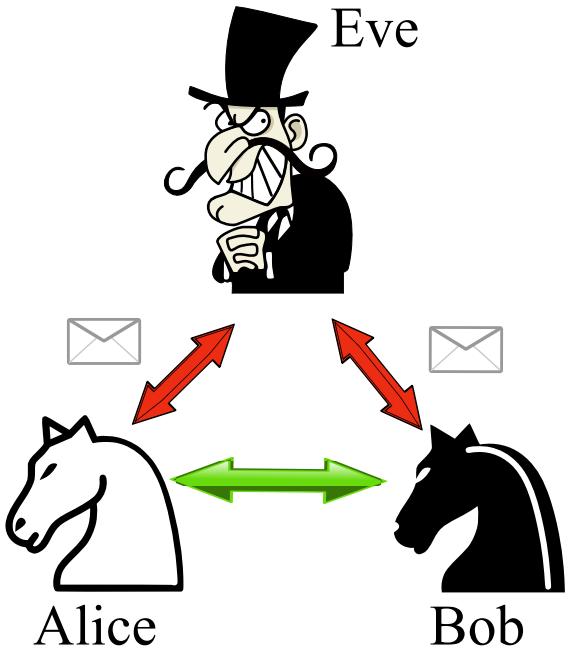
- "On Numbers and Games", J. H. Conway (1976)

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

Background



Relay attacks

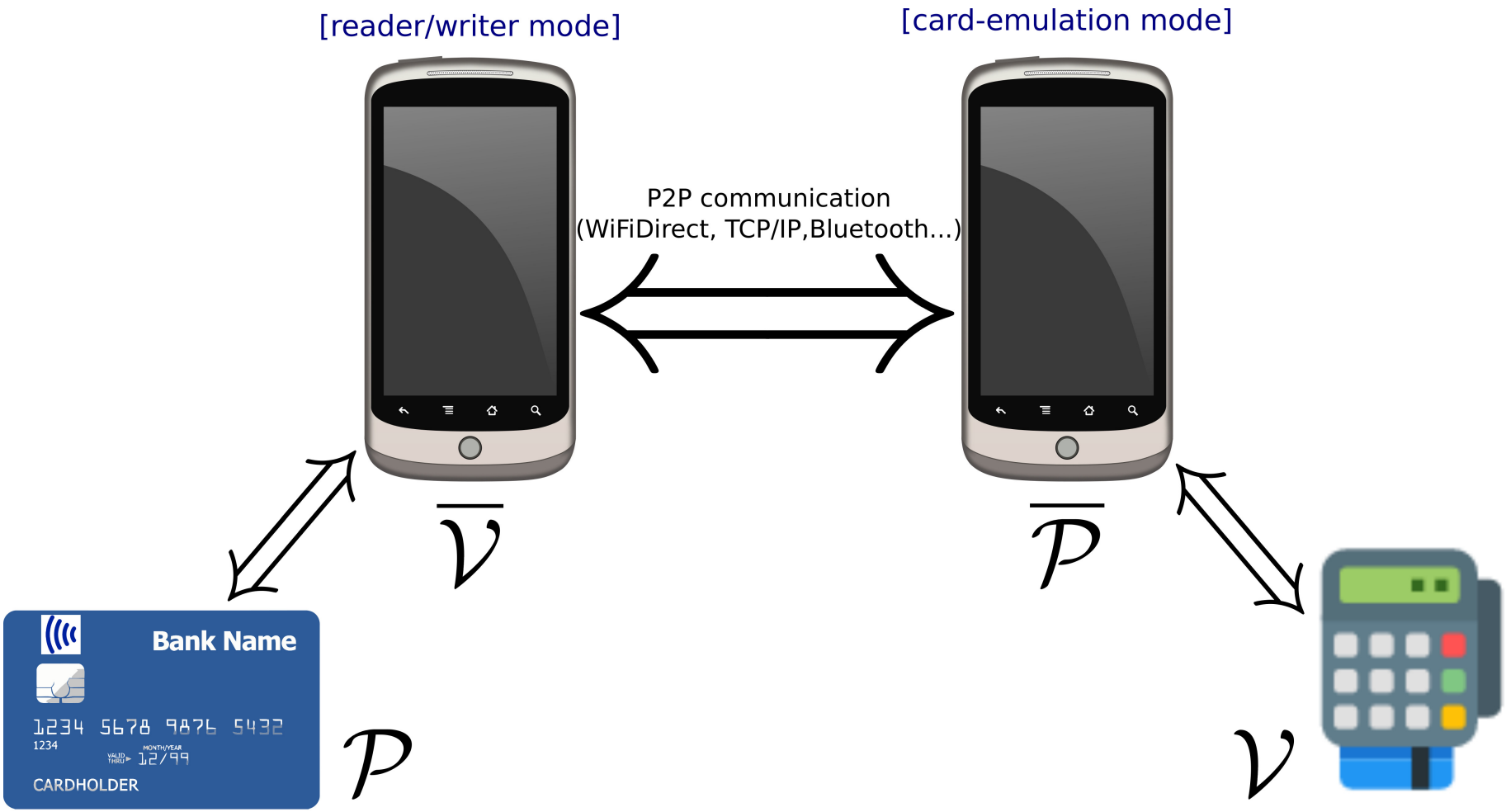
- "On Numbers and Games", J. H. Conway (1976)

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

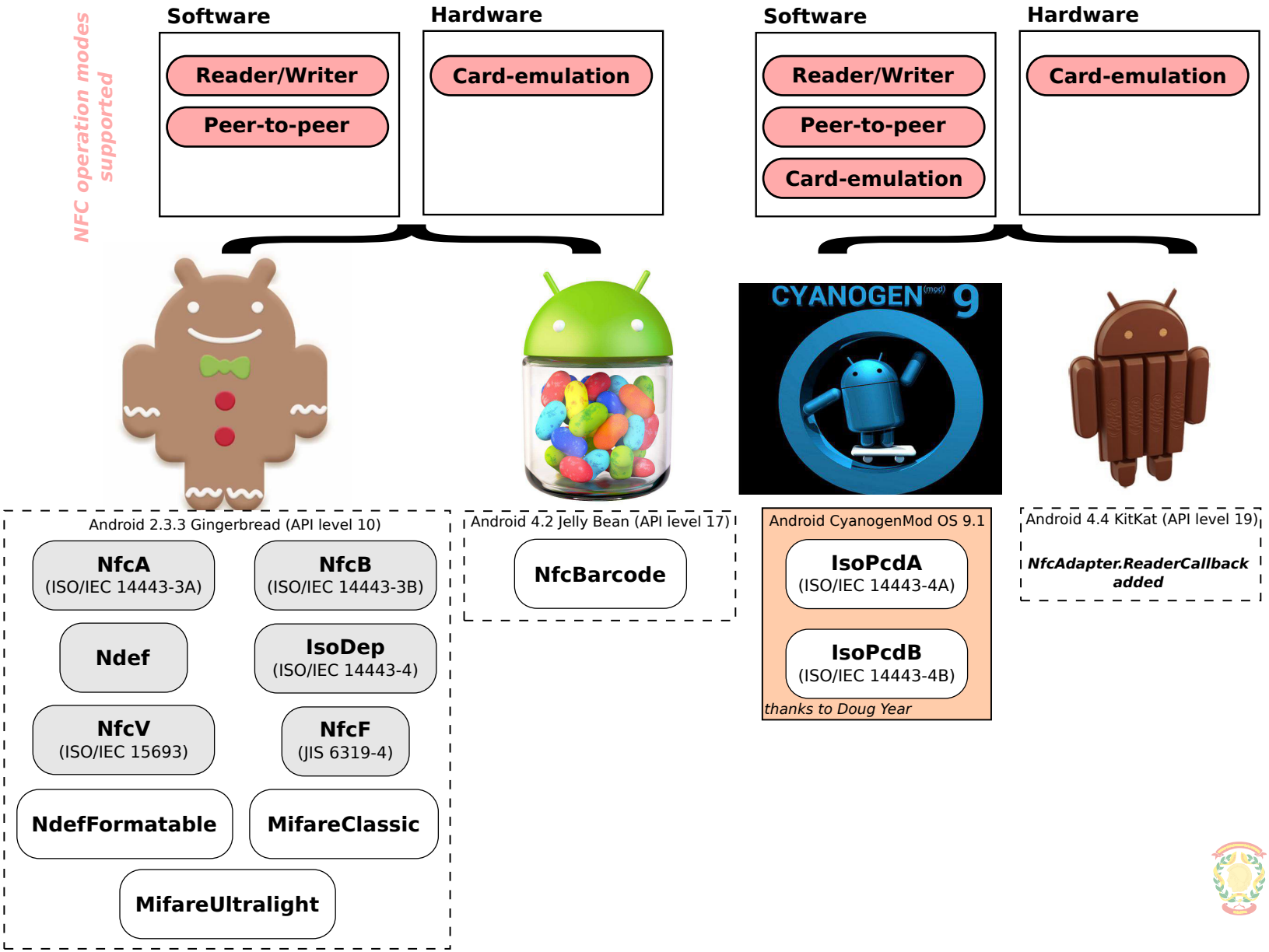

[reader/writer mode]
[card-emulation mode]
P2P communication
(WiFiDirect, TCP/IP,Bluetooth...)
$\overline{\mathcal{V}}$
$\overline{\mathcal{P}}$
Bank Name
1234 5678 9876 5432
1234
MONTH/YEAR
VALID THRU 12/99
CARDHOLDER
$\mathcal{P}$
$\mathcal{V}$

Agenda

CUD Zaragoza

Android and NFC: A Tale of L♥ve

Recap on evolution of Android NFC support



Android and NFC: A Tale of L♥ve

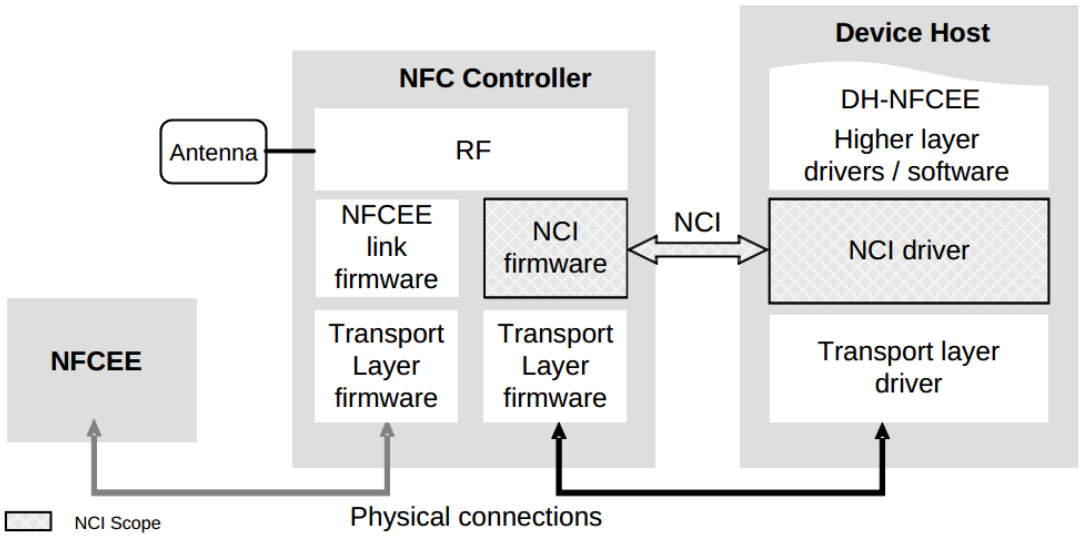
Digging into Android NFC stack

- **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

Digging into Android NFC stack

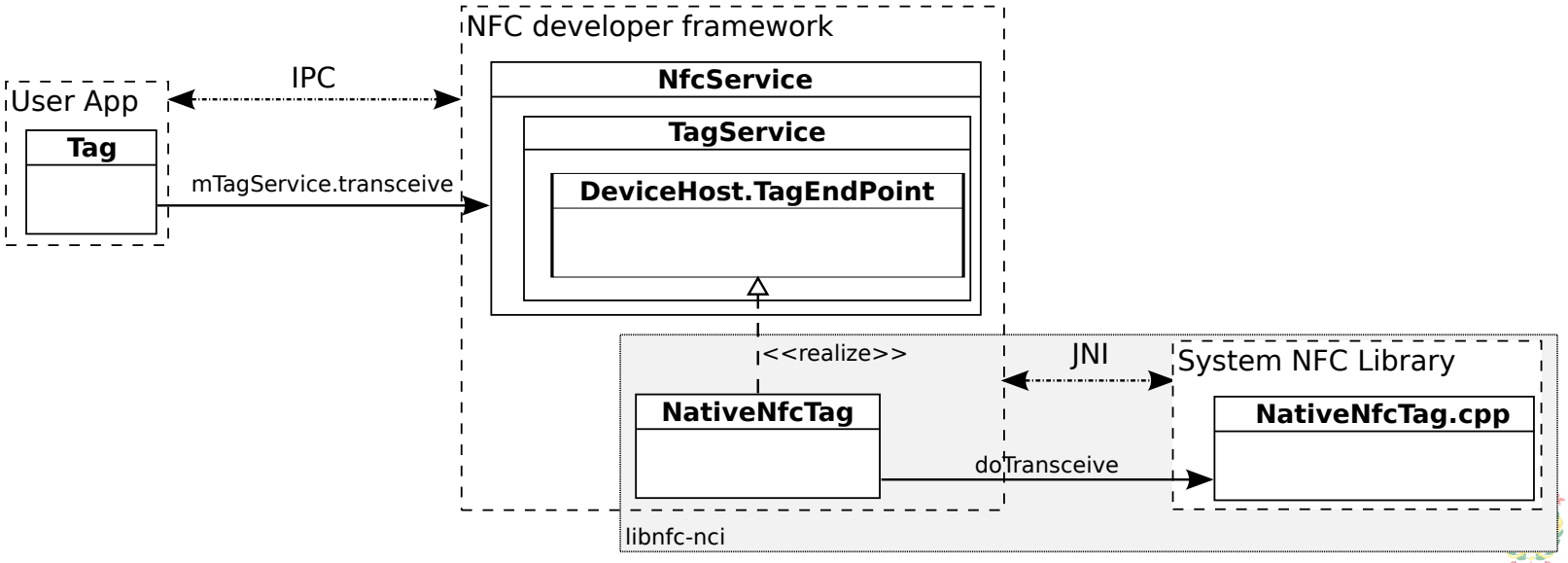
- **Event-driven framework**, nice API support
- Two native implementations (depending on built-in NFC chip)
  - `libnfc-nxp`
  - `libnfc-nci`
- **NXP was dropped in favour of NCI**:
  - Open architecture, not focused on a single family chip
  - Open interface between the NFC Controller and the DH
 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



Android and NFC: A Tale of L♥ve

Digging into Android NFC stack – Reader/Writer mode

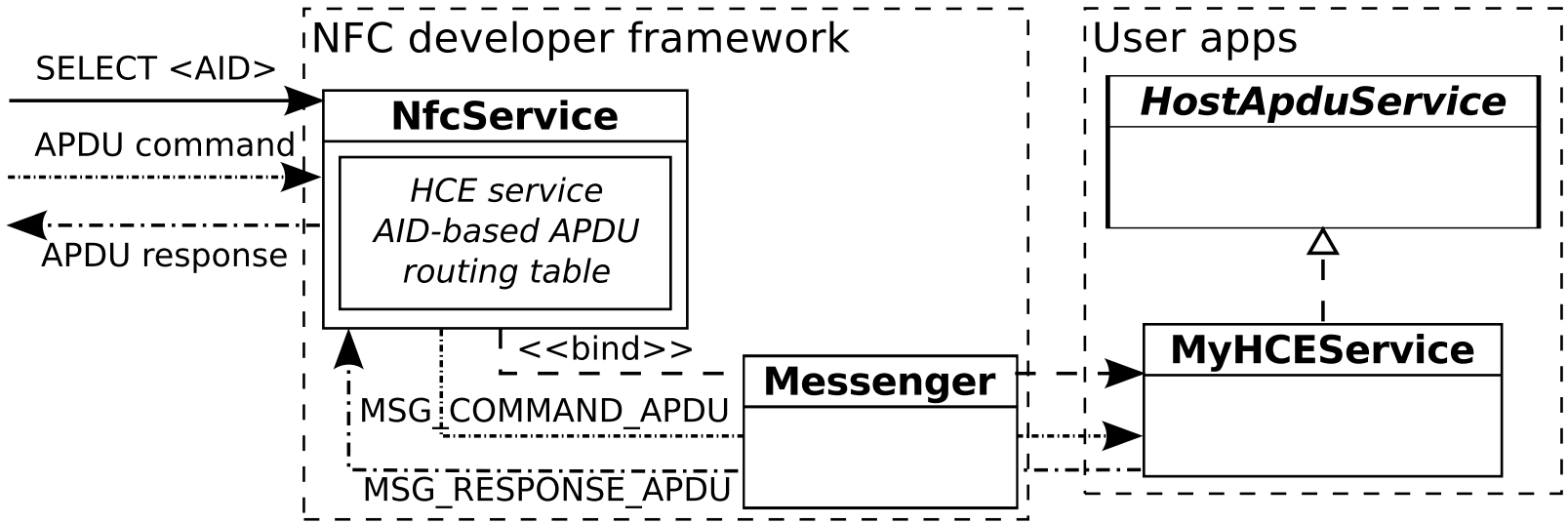
- Not allowed to be set directly → Android activity
- Android NFC service selects apps according to tag definition of Manifest file
- In low-level, `libnfc-nci` uses reliable mechanism of queues and message passing – General Kernel Interface (GKI)
  - Makes communication between layers and modules easier



Android and NFC: A Tale of L♥ve

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

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-nxp` 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.datasheet4u.com/PDF/845670/BCM20793S.html`
- `http://www.datasheet4u.com/PDF/845671/BCM20793SKML.html`

Android and NFC: A Tale of L♥ve

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

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

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

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

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

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* ≥ 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

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

CUD Zaragoza

Relay Attack Implementation

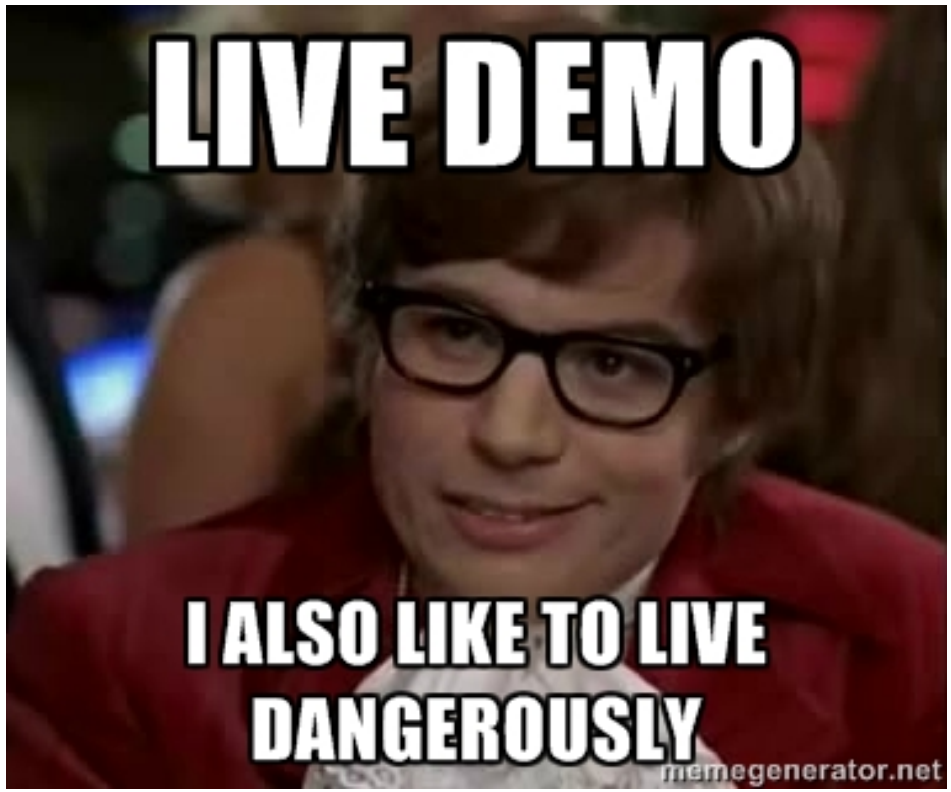
Experiment configuration

- 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

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 $\geq$ 4.4



Relay Attack Implementation

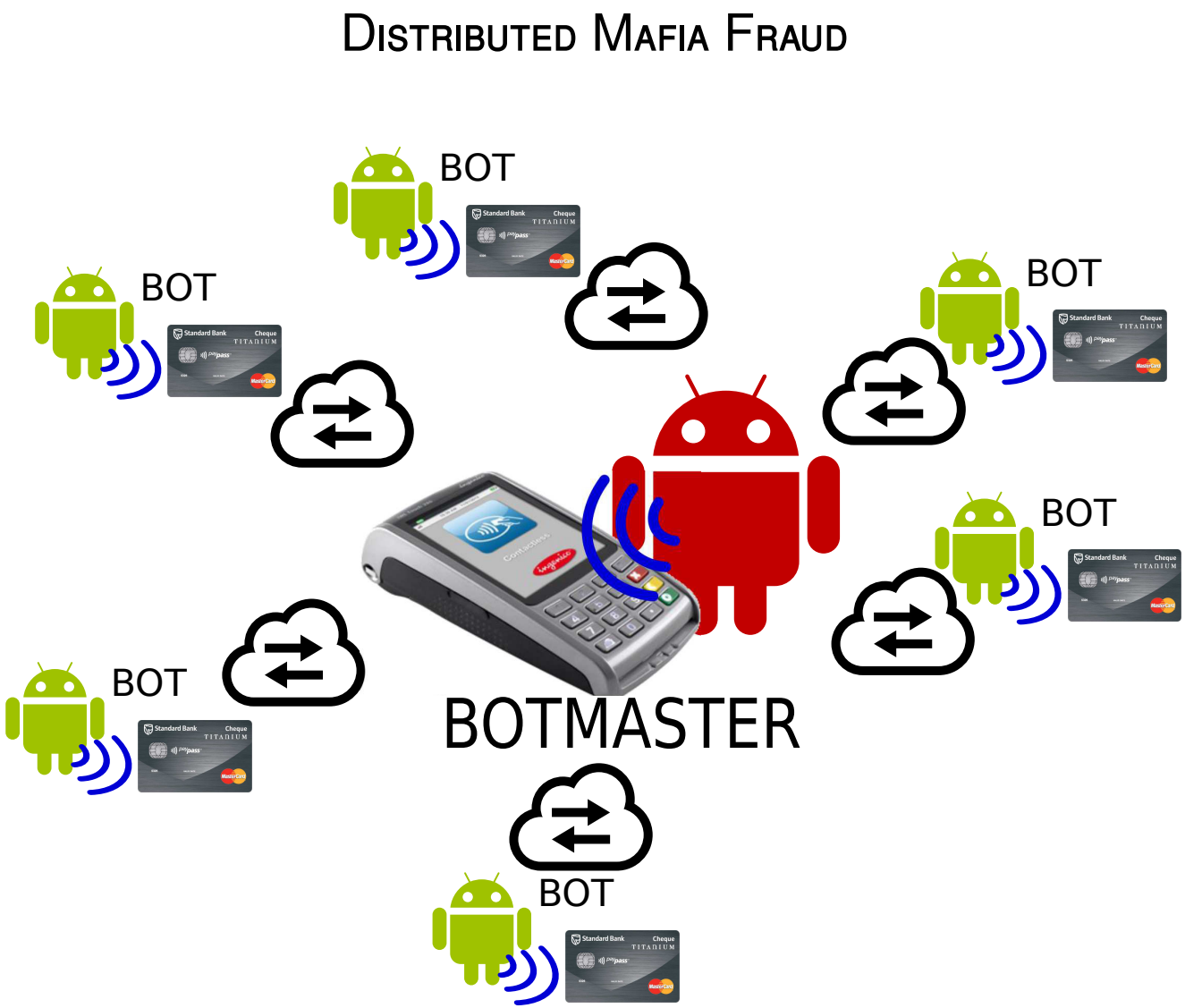
Experiment configuration

- 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

$\mathcal{V} \rightarrow \mathcal{P}$	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 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 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 9000
$\mathcal{V} \rightarrow \mathcal{P}$	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 001F 03
$\mathcal{P} \rightarrow \mathcal{V}$	7729 9F27 01XX 9F36 02XX XX9F 2608 XXXX XXXX XXXX XXXX 9F10 12XX ...XX90 00

Relay Attack Implementation

Threat Scenarios – Scenario 1



Relay Attack Implementation

Threat Scenarios – Scenario 2

Hiding Fraud Locations

Relay Attack Implementation

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

CUD Zaragoza

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

CUD Zaragoza

Conclusions

Security of NFC is based on the physical proximity concern

Conclusions

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

CUD Zaragoza

Conclusions

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
  - (likely) Threat scenarios introduced

CUD Zaragoza

Conclusions

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
  - (likely) Threat scenarios introduced

Virtual pickpocketing attack may appear before long!

Conclusions

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

Conclusions

Conclusions

Conclusions

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

CUD Zaragoza

Conclusions

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
- Thanks for hearing me!

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

Current work

- **Effect of WTX messages** to extend reply timing
- **Feasibility under other wireless technologies**

Relay attacks in EMV contactless cards with Android OTS devices

Ricardo J. Rodríguez

@RicardoJRdez ※ rjrodriguez@unizar.es ※ www.ricardojrodriguez.es

Centro Universitario de la Defensa Zaragoza

Centro Universitario de la Defensa,
Academia General Militar (AGM)

March 31, 2017

Escuela de Doctorado – Universidad de Valladolid
Valladolid, Spain

Vila, J. & Rodríguez, R. J. *Practical Experiences on NFC Relay Attacks with Android: Virtual Pickpocketing Revisited*. Proceedings of the 11th International Workshop on RFID Security (RFIDsec), Springer, LNCS vol. 9440, 87-103. doi: 10.1007/978-3-319-24837-0_6