Contactless Payment Cards: Vulnerabilities, Attacks, and Solutions

Dr. Ricardo J. Rodríguez

ↄ All wrongs reversed

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

Universidad Zaragoza
1542

Department of Computer Science and Systems Engineering
University of Zaragoza, Spain

November 28, 2015

CyberCamp 2015
Madrid (Spain)

$whoami

- Ph.D. on Comp. Sci. (Univ. of Zaragoza, Spain) (2013)
- Assistant Professor at University of Zaragoza
  - Performance analysis on critical, complex systems
  - Secure Software Engineering
  - Advance malware analysis
  - RFID/NFC Security
- Not prosecuted ⌣̈
- Speaker at NcN, HackLU, RootedCON, STIC CCN-CERT, HIP, MalCON, HITB...

Universidad Zaragoza
1542

Agenda

PART 1: Theory on RFID and NFC

PART 2: EMV

PART 3: EMV Contactless cards

PART 4: Solutions, Conclusions, and References

(some slides borrowed from Joeri de Ruiter, University of Birmingham – thanks mate! $\ddot\smile$)

Part I – Theory on RFID and NFC

1. RFID
   - What is it?
   - Where is it used?
2. Near Field Communication (NFC)
   - What is it?
   - Where is it used?
   - NFC vs. RFID
   - NFC vs. Other Wireless Technologies
   - NFC (in)Security
3. ISO/IEC 14443

RFID: What is it? (I)

- Stands for Radio-Frequency IDentification
- Wireless use of electromagnetic fields to transfer data
- Main purposes:
  - Automatically identify objects
  - Automatically track objects

RFID: What is it? (I)

- Stands for Radio-Frequency IDentification
- Wireless use of electromagnetic fields to transfer data
- Main purposes:
  - Automatically identify objects
  - Automatically track objects
- Automatic Identification and Data Capture (AIDC) method
- Its market is $\geq$ *US*\$20 billion (estimation by 2014)

RFID: What is it? (I)

- Stands for Radio-Frequency IDentification
- Wireless use of electromagnetic fields to transfer data
- Main purposes:
  - Automatically identify objects
  - Automatically track objects
- Automatic Identification and Data Capture (AIDC) method
- Its market is $\geq$ *US*$20 billion (estimation by 2014)
- Different types of powered tags:
  - Electromagnetic induction
  - Passive transponder
  - Local power source

Main advantages to barcodes

- No need to be aligned with the reader
- Can be embedded in the tracked object

RFID: What is it? (II)

A bit of history. . .

- 1945: Soviet Union espionage tool that retransmitted incident radio waves with audio information (Léon Theremin, the Great Seal bug)
    - Sound waves vibrated a diaphragm which slightly altered the shape of the resonator, which modulated the reflected radio frequency

RFID: What is it? (II)

A bit of history. . .

- 1945: Soviet Union espionage tool that retransmitted incident radio waves with audio information (Léon Theremin, the Great Seal bug)
  - Sound waves vibrated a diaphragm which slightly altered the shape of the resonator, which modulated the reflected radio frequency

Devices

- Tags: Attached/embedded in the objects
  - Passive, active or battery-assisted passive
  - Read-only, read/write (write-once/read-multiple. . .)
  - Two components: Integrated Circuit (for storing, processing, de/modulating, collecting DC power), and an antenna (for receiving and transmitting the signal)
  - Information stored in non-volatile memory
- Readers
  - Passive: Needs an active tag. Reception range 0.30 to 609.60m
  - Active

RFID: Where is it used? (III)

Band	Regulations	Range	Data speed	Remarks
120–150 kHz (LF)	Unregulated	10 cm	Low	Animal identification, factory data collection
13.56 MHz (HF)	ISM band worldwide	10 cm - 1 m	Low to moderate	Smart cards (MIFARE, ISO/IEC 14443)
433 MHz (UHF)	Short Range Devices	1–100 m	Moderate	Defence applications, with active tags
865-868 MHz (Europe), 902-928 MHz (North America) UHF	ISM band	1–12 m	Moderate to high	EAN, various standards
2450-5800 MHz (microwave)	ISM band	1–20 m	High	802.11 WLAN, Bluetooth standards
3.1–10 GHz (microwave)	Ultra wide band	200 m	High	Requires semi-active or active tags

RFID: Where is it used? (IV)

- Access management
- Tracking of goods
- Tracking of persons and animals
- Toll collection and contactless payment
- Machine readable travel documents
- Smartdust (for massively distributed sensor networks)
- Tracking sports memorabilia to verify authenticity
- Airport baggage tracking logistics
- Timing sporting events

Near Field Communication: What is it? (I)

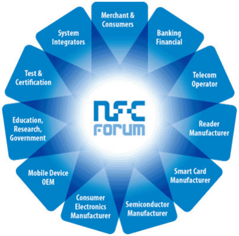
Near Field Communication (NFC)

- Standard to establish radio communication between devices
  - By touching or bringing then into close proximity
- Builds upon RFID
  - Radio-Frequency ID: identify and track (things/animals/people) using radio waves
  - Works at 13.56MHz band on ISO/IEC 18000-3 (no license needed)
- Distance needed: $\leq$ 10cm (theoretically $\leq$ 20)
- Rates: 106 – 424 kbit/s
- Two main actors
  - Initiator: generates a RF field
  - Target
- Two working modes
  - Passive: initiator device provides a carrier field. Target is a transponder
  - Active: initiator + target generate their own fields

Near Field Communication: What is it? (II)

“Big” actors

NFC
NEAR FEILD COMMUNICATION

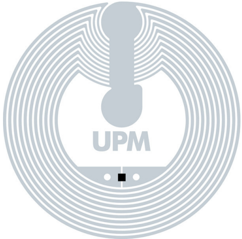


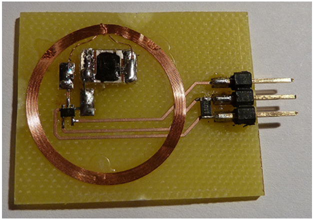
NFC Forum

- Non-profit industry association
- Formed on March 18, 2004
- Founders: NXP Semiconductors (formerly Philips Semiconductors), Sony and Nokia
- Promotes implementation and standardisation of NFC
- 190 member companies (June 2013). Some located at Spain:
  - Applus
  - AT4 Wireless

Near Field Communication: What is it? (III)

Real actors (1)



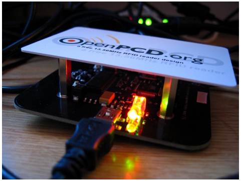


PICC

- Proximity Integrated Circuit Card
- Commonly named as *tag*
- Passive or active (depends on power supply)
  - Widely used (cheaper): passive ones
- It contains:
  - Internal capacitor
    - Stores the energy coming from the reader
  - Resistor

Near Field Communication: What is it? (III)

Real actors (2)

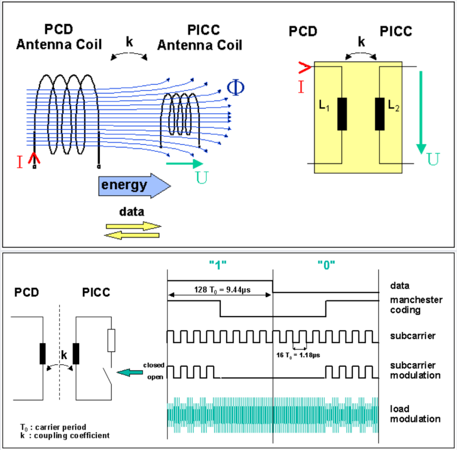


PCD

- Proximity Coupling Device
- Commonly named as *reader/writer*
- Active (forced)
- Contains the antenna
  - Communication at the 13.56MHz (±7kHz) frequency
  - Electronic field

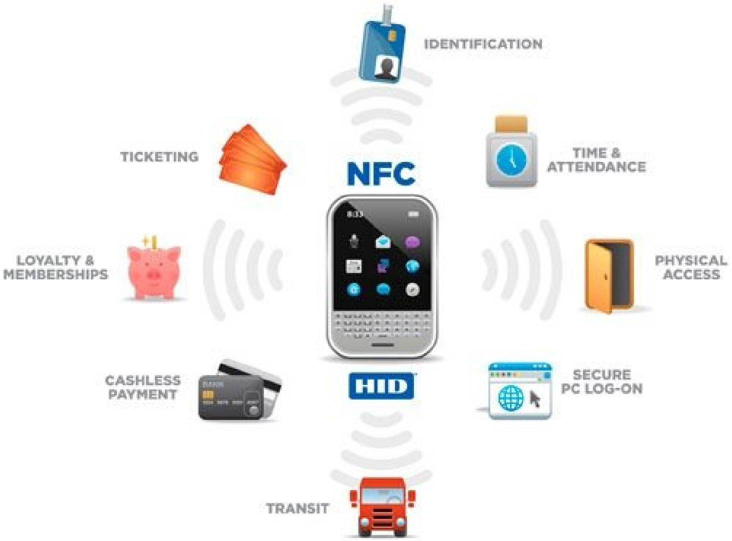
Near Field Communication: What is it? (IV)

An interesting reading on this topic. . .



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

Near Field Communication: Where is it used? (V)

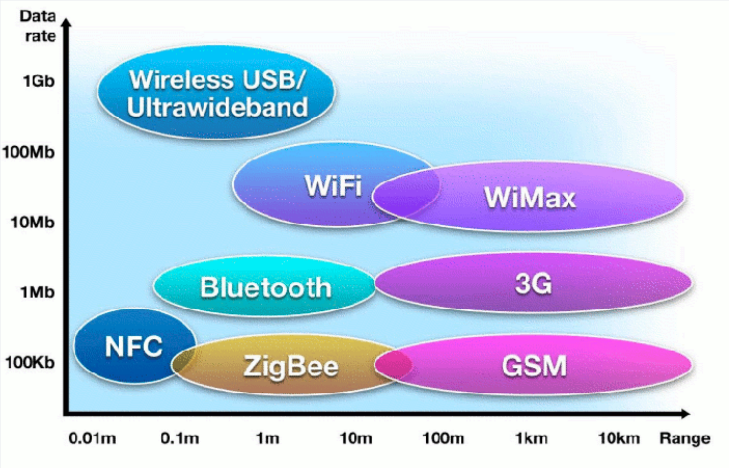


NFC vs. RFID

Remember: NFC operates at 13.56MHz → extension of High Frequency RFID standards

	HF RFID	**NFC**
Operating Frequency	13.56 MHz	13.56 MHz
Communication	One way	Two way
Standards	ISO 14443, 15693, 18000	ISO 14443
Scan Distance	Up to 1 m	Up to 10 cm
Scan Tags Simultaneously	Yes	No

NFC vs. Other Wireless Technologies



(taken from http://www.cnx-software.com/2010/12/28/near-field-communication-nfc/)

Why NFC? Why??

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

We will recall this issue later on. . .

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)

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

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)

Universidad Zaragoza
1542

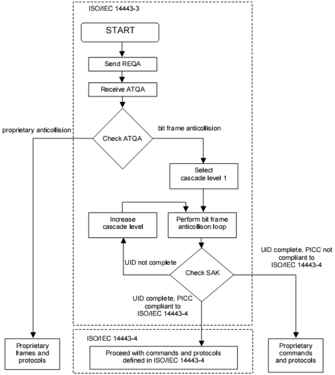
NFC security threats

- 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)

Herein, we focus on eavesdropping and relay threats

ISO/IEC 14443 (I)

Identification cards – Contactless integrated circuit cards – Proximity cards


ISO/IEC 14443-3
START
Send REQA
Receive ATQA
Check ATQA
proprietary anticollision
bit frame anticollision
Select cascade level 1
Increase cascade level
Perform bit frame anticollison loop
UID not complete
Check SAK
UID complete, PICC not compliant to ISO/IEC 14443-4
UID complete, PICC compliant to ISO/IEC 14443-4
ISO/IEC 14443-4
Proceed with commands and protocols defined in ISO/IEC 14443-4
Proprietary frames and protocols
Proprietary commands and protocols

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

ISO/IEC 14443 (II)

ISO/IEC 7816

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

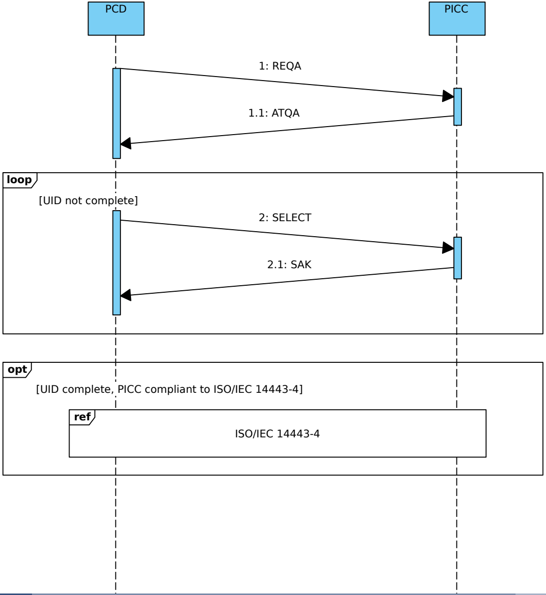
ISO/IEC 14443 (II)

ISO/IEC 7816

- Fifteen-part international standard related to contacted integrated circuit cards, especially smartcards
- Application Protocol Data Units (APDUs)
  - `SELECT` command: AID (App. ID, printed in the card)
    - RID (Registered Application Provider Identifier): 5B
    - PIX (Proprietary Identifier Extension): To distinguish apps

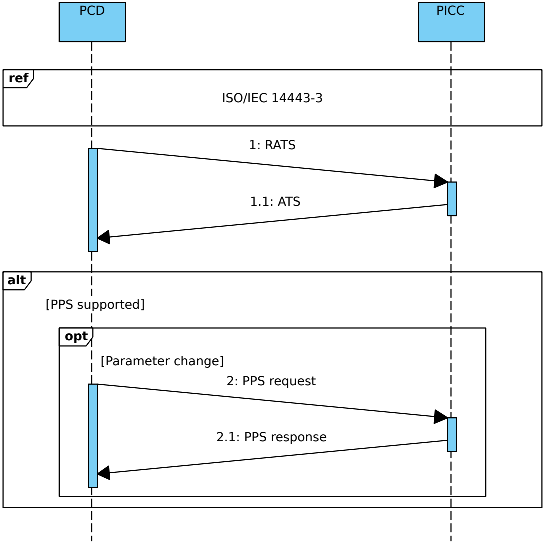
ISO/IEC 14443 (III)

Selection and anti-collision protocol (ISO 14443-3A)



ISO/IEC 14443 (IV)

Transmission protocol – preamble (ISO 14443-4)



ISO/IEC 14443 (V)

- IsoDep cards: Compliant with 4 parts of the ISO/IEC 14443
- But this is not a requirement. . .
    - MIFARE Classic: Fulfills ISO/IEC 14443-1, ISO/IEC 14443-2
        - Some parts of ISO/IEC 14443-3
        - Own ISO/IEC 14443-4 protocol

ISO/IEC 14443 (V)

- IsoDep cards: Compliant with 4 parts of the ISO/IEC 14443
- But this is not a requirement. . .
  - MIFARE Classic: Fulfills ISO/IEC 14443-1, ISO/IEC 14443-2
    - Some parts of ISO/IEC 14443-3
    - Own ISO/IEC 14443-4 protocol

A note on MIFARE Classic. . .

- Nice example for security by obscurity problem
- Well known vulnerabilities (and documented)
- Most critical: low entropy of random number generation
  - Replay attacks

ISO/IEC 14443 (V)

- IsoDep cards: Compliant with 4 parts of the ISO/IEC 14443
- But this is not a requirement…
  - MIFARE Classic: Fulfills ISO/IEC 14443-1, ISO/IEC 14443-2
    - Some parts of ISO/IEC 14443-3
    - Own ISO/IEC 14443-4 protocol

A note on MIFARE Classic…

- Nice example for security by obscurity problem
- Well known vulnerabilities (and documented)
- Most critical: low entropy of random number generation
  - Replay attacks
  - “Darkside” attack
  - Nested attack

ISO/IEC 14443 (V)

- IsoDep cards: Compliant with 4 parts of the ISO/IEC 14443
- But this is not a requirement. . .
  - MIFARE Classic: Fulfills ISO/IEC 14443-1, ISO/IEC 14443-2
    - Some parts of ISO/IEC 14443-3
    - Own ISO/IEC 14443-4 protocol

A note on MIFARE Classic. . .

- Nice example for security by obscurity problem
- Well known vulnerabilities (and documented)
- Most critical: low entropy of random number generation
  - Replay attacks
  - "Darkside" attack
  - Nested attack

Recall: show video demo

ISO/IEC 14443 (V)

- IsoDep cards: Compliant with 4 parts of the ISO/IEC 14443
- But this is not a requirement. . .
  - MIFARE Classic: Fulfills ISO/IEC 14443-1, ISO/IEC 14443-2
    - Some parts of ISO/IEC 14443-3
    - Own ISO/IEC 14443-4 protocol

A note on MIFARE Classic. . .

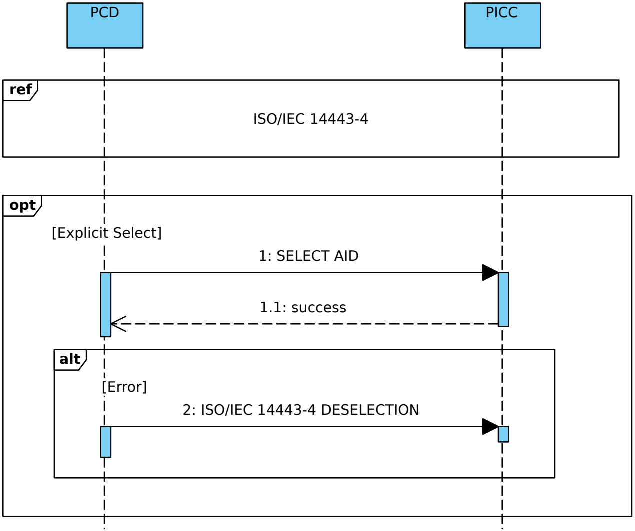
- Nice example for security by obscurity problem
- Well known vulnerabilities (and documented)
- Most critical: low entropy of random number generation
  - Replay attacks
  - "Darkside" attack
  - Nested attack

Recall: show video demo

MFCAB tool: `http://www.bitbucket.org/rjrodriguez/mfcab`

ISO/IEC 14443 (VI)

Optional selection of AID (ISO 14443-4)



ISO/IEC 14443 (VIII)

Examples

- MIFARE cards
- Calypso (electronic ticketing system)
- Biometric passports
- EMV payment cards (PayPass, payWave, ExpressPay)
- Spanish & German identity cards
- ...

Part II – EMV

4 EMV Protocol
- What is it?
- EMV Protocol Details
- Known Weaknesses

EMV: What is it? (I)

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

EMV: What is it? (I)

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

EMVCo

Owners (with joining dates)

AMERICAN EXPRESS

DISCOVER (Sept 2013)

JCB (Feb 2009)

MasterCard Worldwide

UnionPay 银联 中国银联 China UnionPay (May 13)

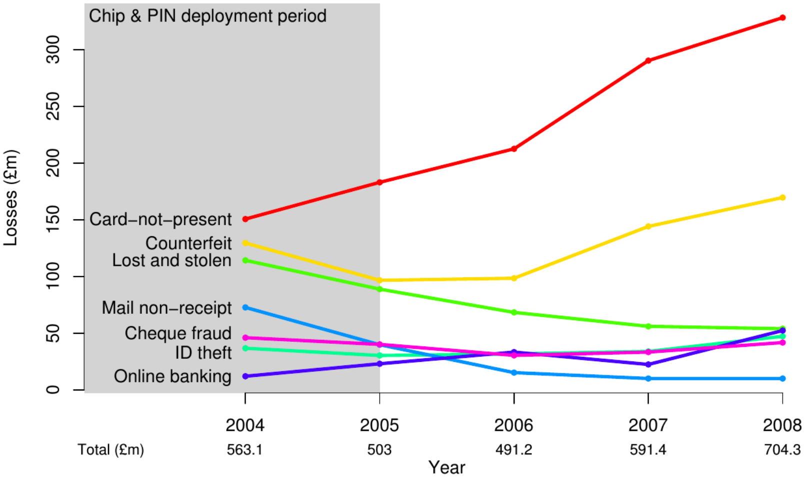
VISA

EMV: What is it? (II)

- 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

Universidad Zaragoza

EMV: What is it? (III)



(taken from *"Chip and PIN is broken"*, S.J. Murdoch et al.; IEEE S&P 2010)

EMV Protocol Details (I)

Since version 4.0. . . (June 2004)

- Standard specification distributed over 4 books (∼ 700 pp.)

Book 1. *Application Independent ICC to Terminal Interface Requirements*
Book 2. *Security and Key Management*
Book 3. *Application Specification*
Book 4. *Cardholder, Attendant, and Acquirer Interface Requirements*

EMV Protocol Details (I)

Since version 4.0. . . (June 2004)

- Standard specification distributed over 4 books (~ 700 pp.)

Book 1. *Application Independent ICC to Terminal Interface Requirements*

Book 2. *Security and Key Management*

Book 3. *Application Specification*

Book 4. *Cardholder, Attendant, and Acquirer Interface Requirements*

We haven't finished yet!

- Four card authentication methods
- Six cardholder verification methods
- Two types of transactions

EMV Protocol Details (I)

Since version 4.0. . . (June 2004)

- Standard specification distributed over 4 books (∼ 700 pp.)

Book 1. *Application Independent ICC to Terminal Interface Requirements*

Book 2. *Security and Key Management*

Book 3. *Application Specification*

Book 4. *Cardholder, Attendant, and Acquirer Interface Requirements*

We haven't finished yet!

- Four card authentication methods
- Six cardholder verification methods
- Two types of transactions

Everything customised using Data Object Lists (DOL)

EMV Protocol Details (I)

Since version 4.0. . . (June 2004)

- Standard specification distributed over 4 books (∼ 700 pp.)

Book 1. *Application Independent ICC to Terminal Interface Requirements*
Book 2. *Security and Key Management*
Book 3. *Application Specification*
Book 4. *Cardholder, Attendant, and Acquirer Interface Requirements*

We haven't finished yet!

- Four card authentication methods
- Six cardholder verification methods
- Two types of transactions

Everything customised using Data Object Lists (DOL)
→ Madness complexity!

EMV Protocol Details (II)

EMV actors

- Card
- Card bank issuer
- Point-of-Sale terminals

EMV Protocol Details (III)

Cryptography used

- Symmetric key (3DES)
    - Between the card (derived key) and issuer/bank (master key)
    - Authenticate transactions to bank

EMV Protocol Details (III)

Cryptography used

- Symmetric key (3DES)
  - Between the card (derived key) and issuer/bank (master key)
  - Authenticate transactions to bank
- Asymmetric keypair (RSA)
  - Payment scheme: authenticate issuers
  - Card Issuer: authenticate cards
  - Cards: authenticate cards/transactions to terminal (optional)

EMV Protocol Details (III)

Cryptography used

- Symmetric key (3DES)
    - Between the card (derived key) and issuer/bank (master key)
    - Authenticate transactions to bank
- Asymmetric keypair (RSA)
    - Payment scheme: authenticate issuers
    - Card Issuer: authenticate cards
    - Cards: authenticate cards/transactions to terminal (optional)

Cryptography setup

- Terminal
    - Payment scheme's public keys

EMV Protocol Details (III)

Cryptography used

- Symmetric key (3DES)
  - Between the card (derived key) and issuer/bank (master key)
  - Authenticate transactions to bank
- Asymmetric keypair (RSA)
  - Payment scheme: authenticate issuers
  - Card Issuer: authenticate cards
  - Cards: authenticate cards/transactions to terminal (optional)

Cryptography setup

- Terminal
  - Payment scheme's public keys
- Card
  - Card issuer's public key certificate, signed by payment scheme
  - Card's public key certificate, signed by card issuer

EMV Protocol Details (IV)

- Based on ISO/IEC 7816
- Application Protocol Data Units (APDUs)
- Command-response / master-slave protocol
  - Command packets
  - Response packets

EMV Protocol Details (V)

ISO/IEC 7816: command APDU

CLA	INS	P1	P2	L_c	Data	L_e

CLA : 1B. Instruction class; type of command (e.g., interindustry or proprietary)

INS : 1B. Instruction code; specific command (e.g., “write data”)

P1-P2 : 2B. Instruction command parameters (e.g., offset into file at which to write the data)

L_c : 0, 1 or 3B. Number (N_c) of bytes of command data

Data : N_cB. Data

L_e : 0, 1 or 3B. Maximum number (N_e) of response bytes

EMV Protocol Details (VI)

ISO/IEC 7816: response APDU

Data	SW1	SW2

Data : N_r ($\leq N_e$) Response data

SW1-SW2 : 2B. Response trailer. Command processing status (e.g., `0x9000` indicates successful operation)

EMV Protocol Details (VII)

ISO/IEC 7816: verifying PIN

```
> 00 20 00 80 08 24 12 34 FF FF FF FF FF
```

Command detailed description

`00 20` : VERIFY command

`00 80` : Plaintext Personal Identification Number (PIN)

`08` : Length data

`24 12 34 FF FF FF FF FF` : Data (yes, your PIN is there in plain text ⌣̈)

EMV Protocol Details (VII)

ISO/IEC 7816: verifying PIN

```
> 00 20 00 80 08 24 12 34 FF FF FF FF FF
```

Command detailed description

00 20	: VERIFY command
00 80	: Plaintext Personal Identification Number (PIN)
08	: Length data
24 12 34 FF FF FF FF FF	: Data (yes, your PIN is there in plain text $\ddot\smile$)

```
< 90 00
```

Response detailed description

90 00	: Command executed without error

NOTE: card may reply with 69 85 to prevent brute force attacks

EMV Protocol Details (VIII)

Establishing a session to communicate

Steps

1. Initialization

Do you see that something is missing?

EMV Protocol Details (VIII)

Establishing a session to communicate

Steps

1. Initialization
2. Card authentication

Do you see that something is missing?

EMV Protocol Details (VIII)

Establishing a session to communicate

Steps

1. Initialization
2. Card authentication
3. Cardholder verification

Do you see that something is missing?

EMV Protocol Details (VIII)

Establishing a session to communicate

Steps

1. Initialization
2. Card authentication
3. Cardholder verification
4. Transaction

Do you see that something is missing?

EMV Protocol Details (VIII)

Establishing a session to communicate

Steps

1. Initialization
2. Card authentication
3. Cardholder verification
4. Transaction

Do you see that something is missing?

EMV Protocol Details (VIII)

Establishing a session to communicate

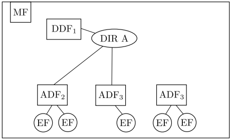
Steps

1. Initialization
2. Card authentication
3. Cardholder verification
4. Transaction

Do you see that something is missing?

EMV Protocol Details (IX)

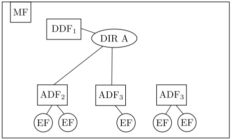
File structure



- Master File (MF): top-most file
  - One (or more) Application Definition Files (ADF)
  - May be distributed in directories
- ADF selected using Application Identifier (AID)
  - Registered application provider IDentifier (RID): 5B (issued by ISO/IEC 7816-5 RA)
  - Proprietary application Identifier eXtension (PIX): differentiate among applications from the same RID
  - AID is printed in receipts

EMV Protocol Details (IX)

File structure



- Master File (MF): top-most file
  - One (or more) Application Definition Files (ADF)
  - May be distributed in directories
- ADF selected using Application Identifier (AID)
  - Registered application provider IDentifier (RID): 5B (issued by ISO/IEC 7816-5 RA)
  - Proprietary application Identifier eXtension (PIX): differentiate among applications from the same RID
  - AID is printed in receipts
- ADF divided in Application Elementary Files (EF)
  - EF contains data
  - Selection of EF thr. Short File Identifier (SFI)

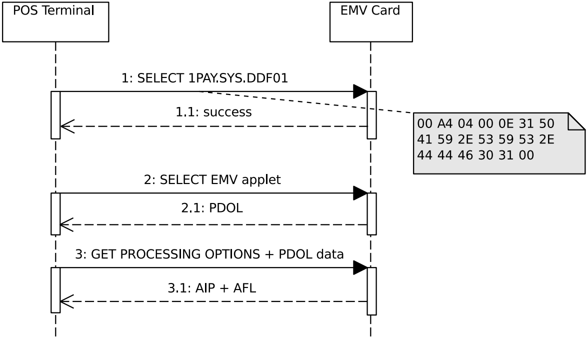
EMV Protocol Details (X)

Example of AIDs

Card issuer	RID	Specific card	PIX	AID
Visa	A000000003	Visa credit or debit	1010	A0000000031010
		Visa Electron	2010	A0000000032010
		V PAY	2020	A0000000032020
		Plus	8010	A0000000038010
MasterCard	A000000004	MasterCard credit or debit	1010	A0000000041010
		MasterCard	9999	A0000000049999
		Maestro (debit card)	3060	A0000000043060
		Cirrus (interbank network)	6000	A0000000046000

EMV Protocol Details (XI)

Initialization (1)



- Processing Option Data Object List (PDOL): data to provide
  - Terminal language, capabilities, country code, etc.
- Application Interchange Profile (AIP): data authentication methods
- Application File Locator (AFL) lists available files

EMV Protocol Details (XII)

Initialization (2)

OK, let’s proceed with the transaction!

EMV Protocol Details (XII)

Initialization (2)

OK, let's proceed with the transaction!

Online or offline transaction? → Card Authentication and Cardholder Verification Methods

EMV Protocol Details (XIII)

Card Authentication Methods (CAM)

Online CAM

- Needs Internet (or phone) connection (obviously)
- Authentications done in issuer's network

EMV Protocol Details (XIII)

Card Authentication Methods (CAM)

Online CAM

- Needs Internet (or phone) connection (obviously)
- Authentications done in issuer's network

Offline CAM – based on RSA

- Terminal performs all authentication processes
- Two types
  - Offline Static CAM: Static Authentication Data (SDA)
  - Offline Dynamic CAM: Dynamic Authentication Data (DDA)
    - Standard DDA
    - Combined DDA/generate AC (also termed as CDA)

EMV Protocol Details (XIV)

Cardholder Verification Method

Method	b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0
Fail CVM processing	X	-	0	0	0	0	0	0
Plaintext PIN verification	X	-	0	0	0	0	0	1
Enciphered online PIN verification	X	-	0	0	0	0	1	0
Plaintext PIN verification and Signature verification	X	-	0	0	0	0	1	1
Enciphered offline PIN verification	X	-	0	0	0	1	0	0
Encipher PIN verification and Signature verification	X	-	0	0	0	1	0	1
Signature verification	X	-	0	1	1	1	1	0
No CVM needed	X	-	0	1	1	1	1	1

CVM list of rules

EMV Protocol Details (XV)

Transaction

Application cryptograms

- Transaction Certificate (TC)
  - Transaction approved
- Authorization Request Cryptogram (ARQC)
  - Online authorization requested
- Application Authentication Cryptogram (AAC)
  - Transaction declined

EMV Protocol Details (XV)

Transaction

Application cryptograms

- Transaction Certificate (TC)
  - Transaction approved
- Authorization Request Cryptogram (ARQC)
  - Online authorization requested
- Application Authentication Cryptogram (AAC)
  - Transaction declined

- Offline mode: GENERATE AC + TC (or AAC)
- Online mode:
  - Terminal initiated: ARQC + ARQC (or AAC)
  - Card initiated: TC + ARQC
  - ARQC forwarded to bank issuer → ATC
  - EXTERNAL AUTH (or second GENERATE AC) + TC (or AAC)

EMV Known Weaknesses (I)

- Skimming
  - Magnetic stripe data also present on chip data

EMV Known Weaknesses (I)

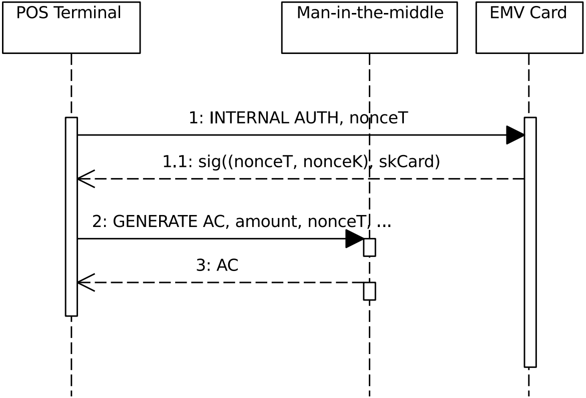
- Skimming
  - Magnetic stripe data also present on chip data
- Cloning SDA cards
  - Possible for offline transactions
  - Only static data authenticated
  - YES-card (accepts any PIN code)

EMV Known Weaknesses (I)

- Skimming
  - Magnetic stripe data also present on chip data
- Cloning SDA cards
  - Possible for offline transactions
  - Only static data authenticated
  - YES-card (accepts any PIN code)
  - SDA no longer allowed for offline-enabled cards

EMV Known Weaknesses (II)

DDA Man-in-the-middle attack



POS Terminal
Man-in-the-middle
EMV Card
1: INTERNAL AUTH, nonceT
1.1: sig((nonceT, nonceK), skCard)
2: GENERATE AC, amount, nonceT, ...
3: AC

- For offline transactions
- Authenticity of a transaction undetermined
- Transaction not connected to card authentication

EMV Known Weaknesses (III)

Murdoch et al., 2010

- For offline and online transactions
  - When card is not blocked
  - When transaction without PIN are accepted
- MITM attack
- YES-card

EMV Known Weaknesses (III)

Murdoch et al., 2010

- For offline and online transactions
  - When card is not blocked
  - When transaction without PIN are accepted
- MITM attack
- YES-card

Barisani et al., 2011

- Rollback attack
  - Force CVM to plaintext PIN
- Online transaction in case of failed data authentication

EMV Known Weaknesses (III)

Murdoch et al., 2010

- For offline and online transactions
  - When card is not blocked
  - When transaction without PIN are accepted
- MITM attack
- YES-card

Barisani et al., 2011

- Rollback attack
  - Force CVM to plaintext PIN
- Online transaction in case of failed data authentication

Bond et al., 2015

- Preplay attack
  - No POS terminal verification
  - Nonce generated by an non-relying party
    - And besides, with low entropy. . .

Part III – EMV Contactless cards

5 What?

6 EMV Contactless Protocol Details

7 Eavesdropping

8 Relay Attack

- Attack Description
- Android and NFC: A Tale of L♥ve
- Demo Experiment
- Threat Scenarios

EMV contactless cards (I)

- 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 (II)

MasterCard PayPass, VISA payWave, and AmericanExpress ExpressPay

Are they secure?

EMV contactless cards (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

EMV contactless cards (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)

EMV contactless cards (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)

EMV Contactless Protocol Details (I)

- Standard specification distributed over 4 books

Book A. *Architecture and General Requirements*
Book B. *Entry Point*
Book C. *Kernel Specification*
Book D. *Contactless Communication Protocol*

- Different variants for book C (seven!)
- Based on ISO/IEC 14443
  - Recall the introduction ⌣̈
- All EMV applications listed in “2PAY.SYS.DDF01” file

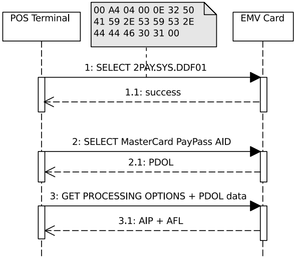
EMV Contactless Protocol Details (II)

MasterCard PayPass (1)

- Kernel 2
- Two modes
  - EMV mode
  - Magnetic stripe mode

EMV Contactless Protocol Details (III)

MasterCard PayPass (2)



POS Terminal

EMV Card

00 A4 04 00 0E 32 50
41 59 2E 53 59 53 2E
44 44 46 30 31 00

1: SELECT 2PAY.SYS.DDF01

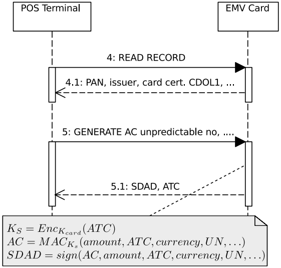
1.1: success

2: SELECT MasterCard PayPass AID

2.1: PDOL

3: GET PROCESSING OPTIONS + PDOL data

3.1: AIP + AFL



POS Terminal

EMV Card

4: READ RECORD

4.1: PAN, issuer, card cert. CDOL1, ...

5: GENERATE AC unpredictable no, ...

5.1: SDAD, ATC

$K_S = Enc_{K_{card}}(ATC)$
$AC = MAC_{K_s}(amount, ATC, currency, UN, \ldots)$
$SDAD = sign(AC, amount, ATC, currency, UN, \ldots)$

EMV mode

- No DDA
- One application cryptogram for online transactions
- RECOVER AC command (to restore torn transactions)
- Data may be temporally stored on card (“scratch pad”)

EMV Contactless Protocol Details (IV)

MasterCard PayPass (3)

Mag-stripe mode

- Backward compatibility (♥♥)
- COMPUTE CRYPTOGRAPHIC CHECKSUM command: generate Card Verification Code (CVC3)
  - Unpredictable number (UN)
  - Application Transaction Number (ATC)
  - Secret Key
- CVC3 + UN used to construct valid mag-stripe data

EMV Contactless Protocol Details (IV)

MasterCard PayPass (3)

Mag-stripe mode

- Backward compatibility (♥♥)
- COMPUTE CRYPTOGRAPHIC CHECKSUM command: generate Card Verification Code (CVC3)
  - Unpredictable number (UN)
  - Application Transaction Number (ATC)
  - Secret Key
- CVC3 + UN used to construct valid mag-stripe data

Pre-play + rollback attack (Roland and Langer, 2013)

- UN length: 1 to 3 digits
- Fallback possible
  - To mag-stripe mode
  - To shorter UN

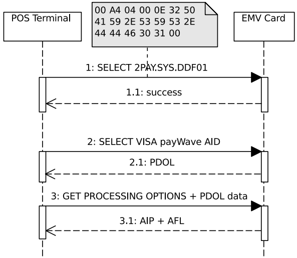
EMV Contactless Protocol Details (V)

VISA payWave (1)

- Kernel 1 and 3
- Two modes
  - EMV modes
    - VSDC: original EMV + minor changes
    - qVSDC: different from original EMV
- No offline plaintext PIN allowed

EMV Contactless Protocol Details (VI)

VISA payWave (2)



POS Terminal

00 A4 04 00 0E 32 50
41 59 2E 53 59 53 2E
44 44 46 30 31 00

EMV Card

1: SELECT 2PAY.SYS.DDF01

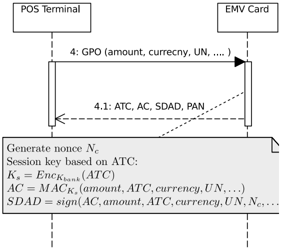
1.1: success

2: SELECT VISA payWave AID

2.1: PDOL

3: GET PROCESSING OPTIONS + PDOL data

3.1: AIP + AFL



POS Terminal

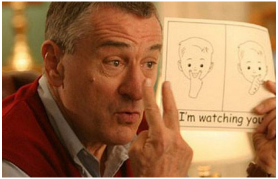
EMV Card

4: GPO (amount, currecny, UN, ...)

4.1: ATC, AC, SDAD, PAN

Generate nonce N_c
Session key based on ATC:
$K_s = Enc_{K_{bank}}(ATC)$
$AC = MAC_{K_s}(amount, ATC, currency, UN, \ldots)$
$SDAD = sign(AC, amount, ATC, currency, UN, N_c, \ldots$

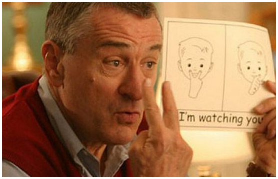
NFC Eavesdropping



What data are being transmitted from my card?

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

NFC Eavesdropping



What data are being transmitted from my card?

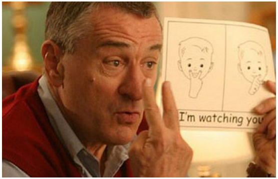
(**without any reader verification, it rocks!**)

- Primary Account Number (PAN)

Recall: demo here

Hw used: Proxmark3 + Google Nexus + NFC-capable MasterCard

NFC Eavesdropping



What data are being transmitted from my card?

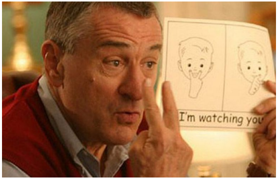
(**without any reader verification, it rocks!**)

- Primary Account Number (PAN)
- Name

Recall: demo here

Hw used: Proxmark3 + Google Nexus + NFC-capable MasterCard

NFC Eavesdropping



What data are being transmitted from my card?

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

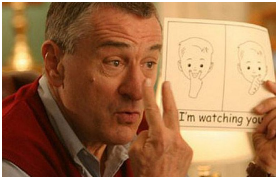
- Primary Account Number (PAN)
- Name
- Expiration date

Recall: demo here

Hw used: Proxmark3 + Google Nexus + NFC-capable MasterCard

Universidad Zaragoza

NFC Eavesdropping



What data are being transmitted from my card?

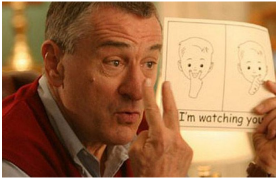
(**without any reader verification, it rocks!**)

- Primary Account Number (PAN)
- Name
- Expiration date
- Transaction history

Recall: demo here

Hw used: Proxmark3 + Google Nexus + NFC-capable MasterCard

NFC Eavesdropping



What data are being transmitted from my card?

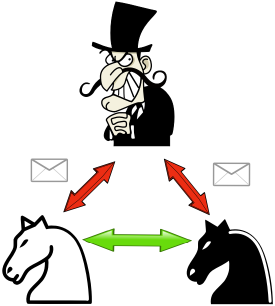
(**without any reader verification, it rocks!**)

- Primary Account Number (PAN)
- Name
- Expiration date
- Transaction history
  - Data from NFC plus chip payments. . .

Recall: demo here

Hw used: Proxmark3 + Google Nexus + NFC-capable MasterCard

NFC Relay Attack Description (I)



Relay attacks

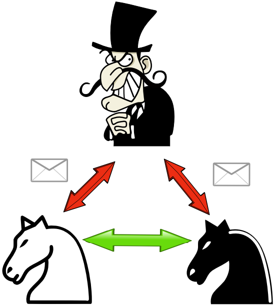
- “On Numbers and Games”, J. H. Conway (1976)

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

NFC Relay Attack Description (I)



Relay attacks

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

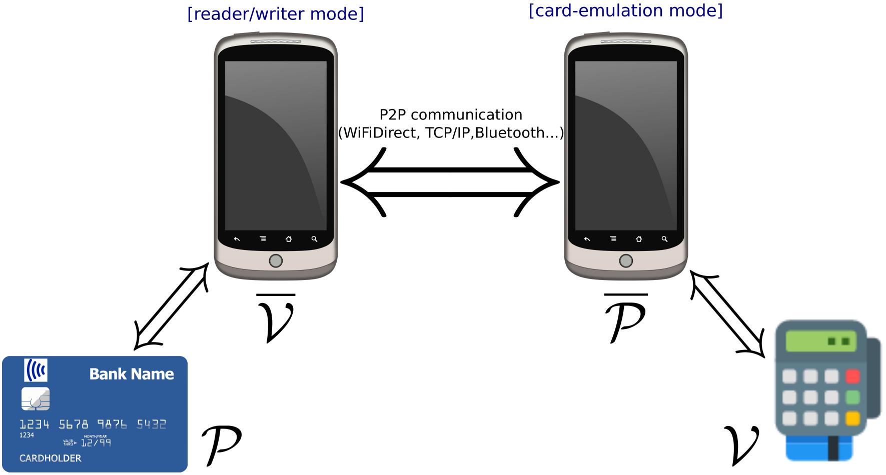
Mafia frauds – Y. Desmedt (SecuriCom’88)

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

- 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

NFC Relay Attack Description (II)

Using Android! ⌣̈



[reader/writer mode]

[card-emulation mode]

P2P communication
(WiFiDirect, TCP/IP,Bluetooth...)

$\overline{\mathcal{V}}$

$\overline{\mathcal{P}}$

$\mathcal{P}$

$\mathcal{V}$

Universidad Zaragoza
1542

Android and NFC: A Tale of L♥ve (I)

Recap on evolution of Android NFC support

NFC operation modes supported

Software
- Reader/Writer
- Peer-to-peer

Hardware
- Card-emulation

Software
- Reader/Writer
- Peer-to-peer
- Card-emulation

Hardware
- Card-emulation

Android 2.3.3 Gingerbread (API level 10)
- **NfcA** (ISO/IEC 14443-3A)
- **NfcB** (ISO/IEC 14443-3B)
- **Ndef**
- **IsoDep** (ISO/IEC 14443-4)
- **NfcV** (ISO/IEC 15693)
- **NfcF** (JIS 6319-4)
- **NdefFormatable**
- **MifareClassic**
- **MifareUltralight**

Android 4.2 Jelly Bean (API level 17)
- **NfcBarcode**

Android CyanogenMod OS 9.1
- **IsoPcdA** (ISO/IEC 14443-4A)
- **IsoPcdB** (ISO/IEC 14443-4B)

thanks to Doug Year

Android 4.4 KitKat (API level 19)

NfcAdapter.ReaderCallback added

Android and NFC: A Tale of L♥ve (II)

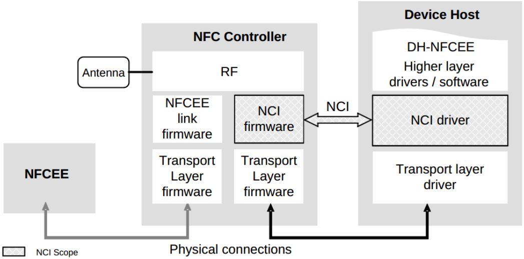
Digging into Android NFC stack – just a bit!

- 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 – just a bit!

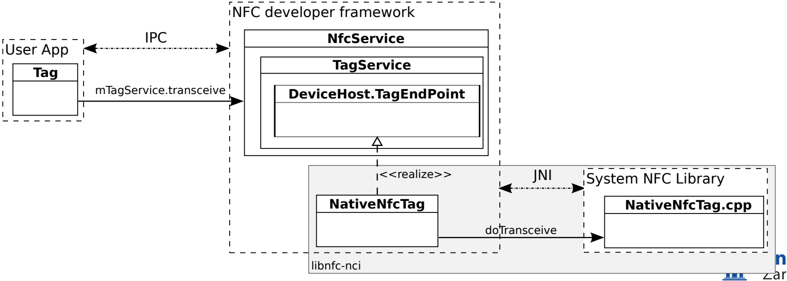
- Event-driven framework, nice API support
- Two native implementations (depending on built-in NFC chip)
  - `libnfc-nxp`
  - `libnfc-nci`
- NXP dropped in favour of NCI:
  - Open architecture, not focused on a single family chip
  - Open interface between the NFC Controller and the DH
  - Standard proposed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



Android and NFC: A Tale of L♥ve (III)

Digging into Android NFC stack – Reader/Writer mode

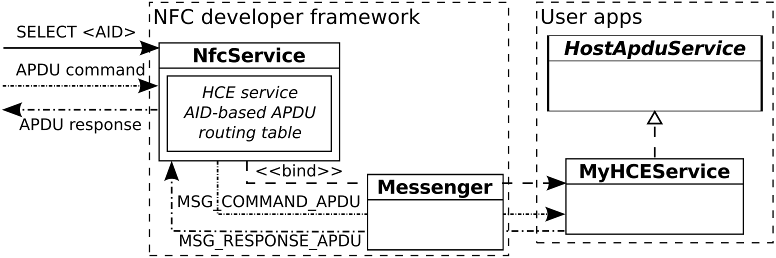
- Not allowed to be set directly → Android activity
- Android NFC service selects apps according to tag definition of Manifest file
- In low-level, `libnfc-nci` uses reliable mechanism of queues and message passing – General Kernel Interface (GKI)
  - Makes communication between layers and modules easier



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 & limitations

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

Android and NFC: A Tale of L♥ve (V)

Digging into Android NFC stack – summary & limitations

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

1. Only valid communication with IsoDep cards
   - `libnfc-nci` do not allow sending raw ISO/IEC 14443-3 commands
   - Caused by the CRC computation, performed by the NFCC

Android and NFC: A Tale of L♥ve (V)

Digging into Android NFC stack – summary & limitations

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

1. Only valid communication with IsoDep cards
   - `libnfc-nci` do not allow sending raw ISO/IEC 14443-3 commands
   - Caused by the CRC computation, performed by the NFCC
   - **Solution**: modify NFCC
2. Device in HCE mode
   - AID must be known in advance

Android and NFC: A Tale of L♥ve (V)

Digging into Android NFC stack – summary & limitations

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

1. Only valid communication with IsoDep cards
   - `libnfc-nci` do not allow sending raw ISO/IEC 14443-3 commands
   - Caused by the CRC computation, performed by the NFCC
   - **Solution**: modify NFCC
2. Device in HCE mode
   - AID must be known in advance
   - **Solution**: `sudo make me a sandwich`
3. Maximum delay allowed in the relay channel:
   $FWT = 256 \cdot (16/f_c) \cdot 2^{FWI}, 0 \leq FWI \leq 14$, where $f_c = 13.56$ MHz

Android and NFC: A Tale of L♥ve (V)

Digging into Android NFC stack – summary & limitations

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

1. Only valid communication with IsoDep cards
   - `libnfc-nci` do not allow sending raw ISO/IEC 14443-3 commands
   - Caused by the CRC computation, performed by the NFCC
   - **Solution**: modify NFCC
2. Device in HCE mode
   - AID must be known in advance
   - **Solution**: `sudo make me a sandwich`
3. Maximum delay allowed in the relay channel:
   $FWT = 256 \cdot (16/f_c) \cdot 2^{FWI}, 0 \leq FWI \leq 14$, where $f_c = 13.56$ MHz
   - $FWT \in [500\mu s, 5s]$ → relay possible if delay is $\leq 5s$

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 $\geq$ 4.4

Relay Attack Implementation (I)

Experiment configuration

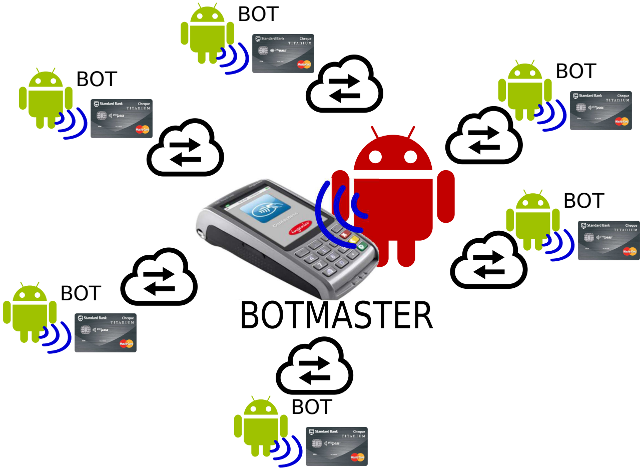
- PoS device: Ingenico IWL280 with GRPS + NFC support
- Android app developed (±2000 LOC)
- Two OTS Android NFC-capable devices
  - One constraint only: dishonest prover must run an Android ≥ 4.4

```
𝒱 → 𝒫   00A4 0400 0E32 5041 592E 5359 532E 4444 4630 3100
𝒫 → 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
𝒱 → 𝒫   00A4 0400 08A0 0000 0004 1010 0200
𝒫 → 𝒱   6F20 8408 A000 0000 0410 1002 A514 8701 0150 0A4D 4153 5445 5243 4152 445F 2D02 6361 9000
𝒱 → 𝒫   80A8 0000 0283 0000
𝒫 → 𝒱   7716 8202 1880 9410 0801 0100 1001 0100 1801 0200 2001 0200 9000
𝒱 → 𝒫   00B2 0114 00
𝒫 → 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
𝒱 → 𝒫   00B2 011C 00
𝒫 → 𝒱   7081 C28F 0105 9F32 0301 0001 9204 3DD0 2519 9081 B034 45XX ...XX62 9000
𝒱 → 𝒫   00B2 021C 00
𝒫 → 𝒱   7081 B393 81B0 3445 XXXX XXXX XXXX ...XXXX XXXX XX62 9000
𝒱 → 𝒫   00B2 0124 00
𝒫 → 𝒱   7033 9F47 0301 0001 9F48 2A3E XXXX ...XXXX XXXX XX6D 9000
𝒱 → 𝒫   00B2 0224 00
𝒫 → 𝒱   7081 949F 4681 9018 XXXX XXXX XXXX ...XXXX XXXX XXF5 9000
𝒱 → 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
𝒫 → 𝒱   7729 9F27 01XX 9F36 02XX XX9F 2608 XXXX XXXX XXXX XXXX 9F10 12XX ...XX90 00
```

Relay Attack Implementation (II)

Threat Scenarios – Scenario 1

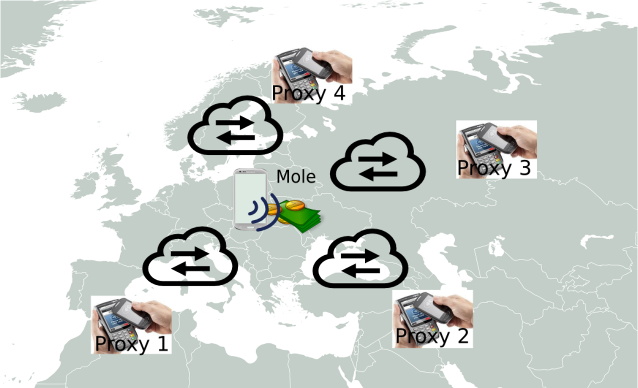
Distributed Mafia Fraud



Relay Attack Implementation (III)

Threat Scenarios – Scenario 2

Hiding Fraud Locations



Part IV – Solutions, Conclusions, and References

9 Mechanisms Against NFC Security Threats

10 Related Work

11 Conclusions

Mechanisms Against NFC Security Threats

Against eavesdropping

- RFID blocking covers
- Physical button/switch activation
- Secondary authentication methods (e.g., on-card fingerprint scanners)

Mechanisms Against NFC Security Threats

Against eavesdropping

- RFID blocking covers
- Physical button/switch activation
- Secondary authentication methods (e.g., on-card fingerprint scanners)

Against relay attacks

- 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

Related Work (I)

On EMV cards attacks

- Singleton, T.; *Credit Card Crimewave: What to Do?*. **Journal of Corporate Accounting & Finance**, 2014, 25, 7–11
- Bond, M. et al.; *Be Prepared: The EMV Preplay Attack*. In **IEEE Security & Privacy**, 2015, 13, 56–64
- Murdoch, S. et al.; *Chip and PIN is Broken*. In **IEEE Symposium on Security and Privacy**, 2010, 433–446
- Bond, M. et al.; *Chip and Skim: Cloning EMV Cards with the Pre-play Attack*. In **IEEE Symposium on Security and Privacy**, 2014, 49–64
- Anderson, R. & Murdoch, S. J.; *EMV: Why Payment Systems Fail*. In **Commun. ACM**, ACM, 2014, 57, 24–28
- de Ruiter, J. & Poll, E.; *Formal Analysis of the EMV Protocol Suite*. In **Theory of Security and Applications**, Springer Berlin Heidelberg, 2012, 6993, 113–129
- Adida, B. et al.; *Phish and Chips*. In **Proceedings of the 14th Int. Workshop on Security Protocols**, Springer, 2009, 5087, 40–48

Related Work (II)

On Point-of-Sales

- Gomzin, S.; *Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions*. John Wiley & Sons Inc., 2014
- Rantos, K. & Markantonakis, K.; *Analysis of Potential Vulnerabilities in Payment Terminals Secure Smart Embedded Devices*. In **Platforms and Applications**, Springer New York, 2014, 311–333
- Frisby, W. et al.; *Security Analysis of Smartphone Point-of-sale Systems*. In **Proceedings of the 6th USENIX Conference on Offensive Technologies**, USENIX Association, 2012, 1–12

Related Work (III)

On contactless payment cards

- Haselsteiner, E. & Breitfuß, K.; *Security in Near Field Communication (NFC) – Strengths and Weaknesses*. In **Proceedings of the Workshop on RFID Security and Privacy (RFIDSec)**, 2006
- Emms, M. et al.; *Risks of Offline Verify PIN on Contactless Cards*. In **Financial Cryptography and Data Security**, Springer Berlin Heidelberg, 2013, 7859, 313–321
- Chothia, T. et al.; *Relay Cost Bounding for Contactless EMV Payments*. In **Proceedings of the 19th International Conference on Financial Cryptography and Data Security** (FC), 2015
- Sanders, R.; *From EMV to NFC: the contactless trail?*. **Card Technology Today**, 2008, 20, 12-13

Related Work (IV): 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)

2015 Passive relay with Android OTS devices (Vila & Rodríguez)

Android apps available (SF and Google Play)

2012 `nfcproxy` (Cyanogen Mod, card-emulation support)

2014 `nfcspy` (catch-all AID module from XPosed framework)

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

- 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

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

EMV contactless payments threats

- EMV threats

Virtual pickpocketing attack may appear before long!

Universidad Zaragoza
1542

Conclusions (I)

Security of NFC is based on the physical proximity concern

Definitely, physical proximity is not a reliable constraint

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

EMV contactless payments threats

- EMV threats
- NFC threats

Virtual pickpocketing attack may appear before long!

Conclusions (I)

Security of NFC is based on the physical proximity concern

Definitely, physical proximity is not a reliable constraint

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

EMV contactless payments threats

- EMV threats
- NFC threats

Virtual pickpocketing attack may appear before long!

Conclusions (I)

Security of NFC is based on the physical proximity concern

Definitely, physical proximity is not a reliable constraint

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

EMV contactless payments threats

- EMV threats
- NFC threats

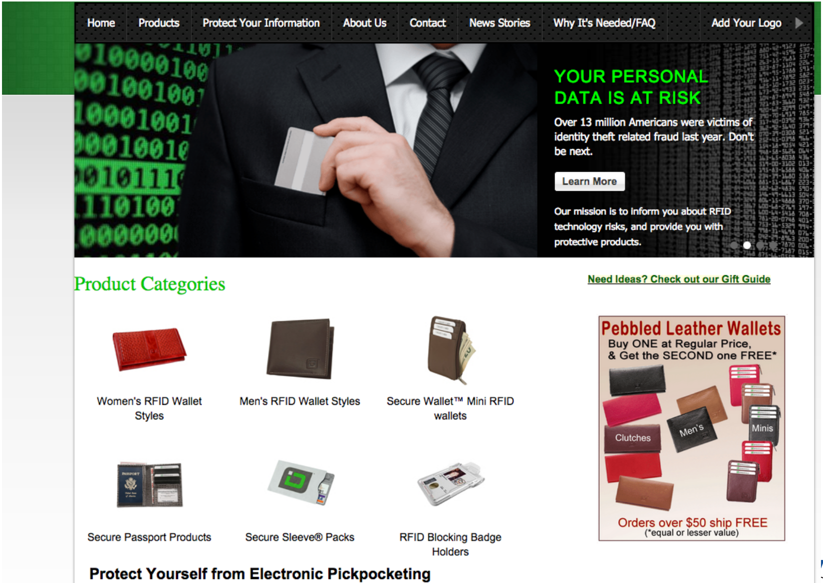
Virtual pickpocketing attack may appear before long!

Take-home message: watch your wallet and any NFC-capable cards on your own

Conclusions (II)

What can I do?

Conclusions (II)



YOUR PERSONAL DATA IS AT RISK

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

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

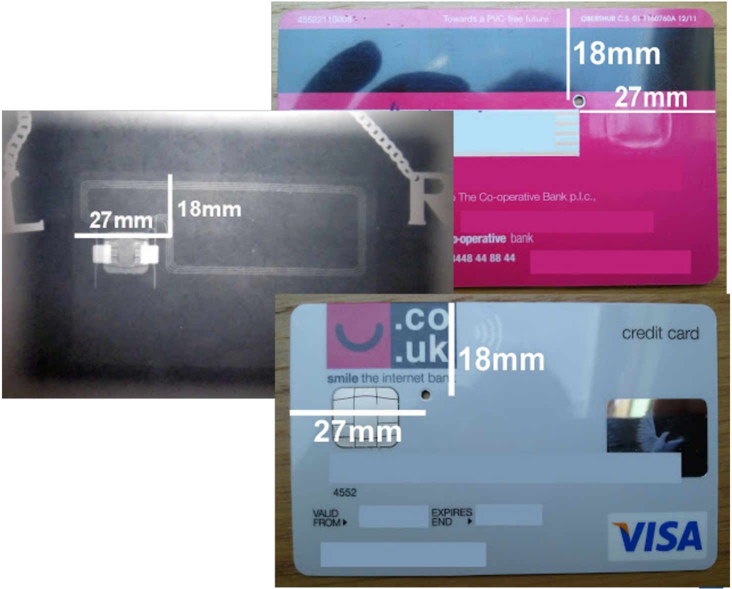
Pebbled Leather Wallets

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

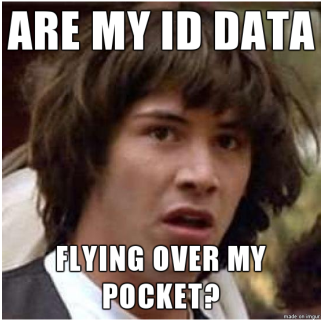
Orders over $50 ship FREE
(*equal or lesser value)

Protect Yourself from Electronic Pickpocketing

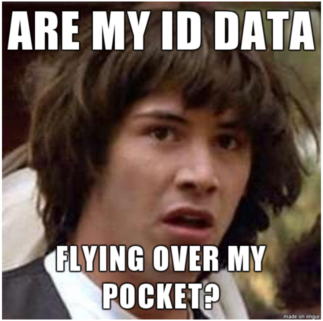
Conclusions (II)



Bonus Track: DNI v3.0 (I)

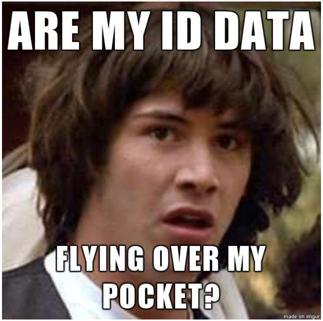


Bonus Track: DNI v3.0 (I)



Yeps, it is!*

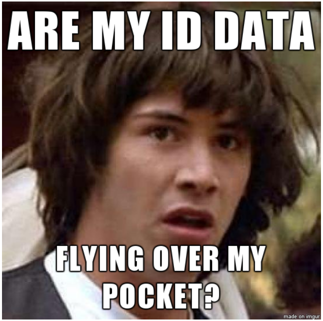
Bonus Track: DNI v3.0 (I)



Yeps, it is!*

- Basic Access Control: $f(MRZ)$
- MRZ (Machine Readable Zone) code:
  - Document number: 3 chars + 6 numbers
  - Date of birth: 6 numbers
  - Expiration date: 6 numbers

Bonus Track: DNI v3.0 (I)



Yeps, it is!*

- Basic Access Control: $f(MRZ)$
- MRZ (Machine Readable Zone) code:
  - Document number: 3 chars + 6 numbers
  - Date of birth: 6 numbers
  - Expiration date: 6 numbers

Bonus Track: DNI v3.0 (II)

Potential problems ahead…

- Attacks on identity (important for the Government)
  - Forgery
  - Impersonation
  - …
- Attacks on confidentiality (important for the people)
  - Privacy
  - Anonymity
  - …

Contactless Payment Cards: Vulnerabilities, Attacks, and Solutions

Dr. Ricardo J. Rodríguez

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

Universidad Zaragoza 1542

Department of Computer Science and Systems Engineering
University of Zaragoza, Spain

November 28, 2015

CyberCamp 2015
Madrid (Spain)