

# Protocolo Near Field Communication: Vulnerabilidades, ataques y contramedidas

**Dr. Ricardo J. Rodríguez**

© All wrongs reversed

rjrodriguez@unizar.es \* @RicardoJRdez \* www.ricardojrodriguez.es



**Centro Universitario  
de la Defensa Zaragoza**

Centro Universitario de la Defensa  
Academia General Militar, Zaragoza, Spain

8 de mayo de 2018

**Ciclo: “Ciberseguridad y defensa en infraestructuras críticas”**  
Zaragoza

# \$whoami



- **Ph.D. en Informática** (Universidad de Zaragoza, 2013)
- **Profesor en Centro Universitario de la Defensa,**  
Academia General Militar (Zaragoza)
- Líneas de Investigación:
  - Análisis de rendimiento de sistemas complejos y críticos
  - Ingeniería dirigida por modelos (con aspectos de seguridad)
  - Análisis de programas binarios (análisis de malware)
  - Seguridad RFID/NFC
- Ponente en NcN, HackLU, RootedCON, STIC  
CCN-CERT, HIP, MalCON, HITB. . .

# Agenda

- 1 Introducción
- 2 Riesgos de NFC
- 3 Mecanismos de Seguridad
- 4 Conclusiones

# Agenda

- 1** Introducción
- 2 Riesgos de NFC
- 3 Mecanismos de Seguridad
- 4 Conclusiones

# Introducción

## Servicios financieros

- Proporcionan **servicios esenciales a la sociedad**
  - La tarjeta de crédito/débito se está convirtiendo en el método primario de pago
    - Algunos países están fomentando que sea el único método de pago
- **Caídas de servicio normalmente debidas a eventos intencionados**
  - Tendencia creciente de (ciber)ataques reportados

# Introducción

## Servicios financieros

- Proporcionan **servicios esenciales a la sociedad**
  - La tarjeta de crédito/débito se está convirtiendo en el método primario de pago
    - Algunos países están fomentando que sea el único método de pago
- **Caídas de servicio normalmente debidas a eventos intencionados**
  - Tendencia creciente de (ciber)ataques reportados

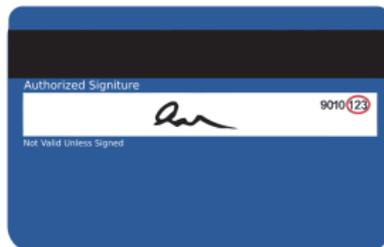
## Datos de tarjetas de crédito

- **Elemento muy deseado en el mercado negro**
  - Datos de tarjeta de crédito US: \$1.5 ~ \$5 – descuentos al por mayor!
  - Datos de tarjeta de crédito UE son más caros (\$5 ~ \$8)
  - Los precios pueden depender del tipo de tarjeta y de otra información (e.g., US fullz data +\$20)
- **Mínima información necesaria para hacer un pago**
  - Nombre del titular, fecha de expiración, número de la tarjeta



# Introducción

## Tarjetas de crédito/débito

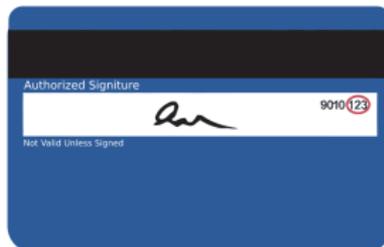
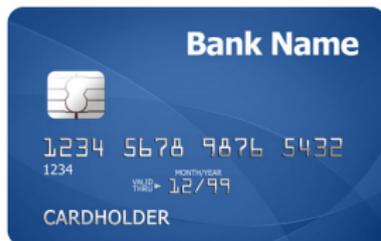


## Datos físicos

- Nombre
- Fecha de expiración: en formato “AA/MM” (o “MM/AA”)
- Número de la tarjeta / *Primary Account Number* (PAN)

# Introducción

## Tarjetas de crédito/débito



## Datos físicos

- Nombre
- Fecha de expiración: en formato "AA/MM" (o "MM/AA")
- Número de la tarjeta / *Primary Account Number* (PAN)
- *Card Verification Value* (CVV): valor de 3 a 4 dígitos (depende del fabricante de la tarjeta)
  - Prueba que se tiene acceso físico a la tarjeta

## ¿Cómo se puede acceder a la información de la tarjeta?

## ¿Cómo se puede acceder a la información de la tarjeta?

### Diferentes tecnologías

- Tarjetas de banda magnética
- Tarjetas Chip-and-PIN (también conocidas como EMV o de chip)
- Tarjetas sin contacto → **NFC**

# Introducción

## Tarjetas de banda magnética

### Algunos comentarios...

- Casi no se usa
- Tres *tracks* en la tarjeta, **contienen información mínima necesaria para completar un pago** (Track 1 y Track 2).
  - Track 3 puede contener otra información. Ejemplo: en tarjetas Ibercaja, contiene número de CC (eso es feo!)

# Introducción

## Tarjetas de banda magnética

The screenshot displays the MSR Utility Program interface. The main window shows three tracks of data from a magnetic stripe card. Track 1 (7 BPC Odd Parity) contains the name 'RODRIGUEZ FERNANDEZ/R. J.' and the number '135428?'. Track 2 (5 BPC Odd Parity) contains the number '940=1811' and '400000?'. Track 3 (5 BPC Odd Parity) contains the number '940=724978' and '18110=2085' followed by a long string of zeros. A 'READ CARD' dialog box is overlaid on the right, displaying the number '2' and a 'Cancel' button. The background interface includes a 'Connect Device' dropdown set to 'HID', a 'R/W: REVH2.39' indicator, and various operation buttons like 'Seg. Write', 'Compare', 'Erase', and 'Copy'.

MSR Utility Program (for HID & Bluetooth) v3.01

Message  
Read Card <1> OK!

Track1 7 BPC Odd Parity 78  
%B49 [redacted] 940^RODRIGUEZ FERNANDEZ/R. J.  
^1811 [redacted] 135428?

Track2 5 BPC Odd Parity 39  
:49 [redacted] 940=1811 [redacted] 400000?

Track3 5 BPC Odd Parity 106  
:0149 [redacted] 940=724978 [redacted] 40  
[redacted] 18110=2085 [redacted] 1341==1=00000000000000  
000?

Connect Device  
HID  
R/W: REVH2.39

Card  
 L  
 H

READ CARD  
Please Swipe Card  
Swipe Counter ->  
2  
Cancel

From File To File  
Seg. Write Compare  
Erase Copy  
Config... Device Config... Bluetooth  
Set Password

# Introducción

## Tarjetas de banda magnética

### Algunos comentarios...

- Casi no se usa
- Tres *tracks* en la tarjeta, **contienen información mínima necesaria para completar un pago** (Track 1 y Track 2).
  - Track 3 puede contener otra información. Ejemplo: en tarjetas Ibercaja, contiene número de CC (eso es feo!)
- **Muy insegura**
- **Ataques posibles:**
  - **Skimming** (Micro cámara + MSR; Micro cámara + pad skimming)
  - **Software malicioso específico:** POS RAM scrapping malware

# Introducción

## Tarjetas Chip-and-PIN

- **Objetivo: reducir el fraude de tarjetas**
- Estándar de 1993/1994, fechas de despliegue diferentes (e.g., 2003 en UK)
- **Toda transacción se autoriza mediante un PIN**
- Cambio de la responsabilidad ante fraude:
  - Del comerciante, si no se usa una tarjeta EMV
  - Del cliente, si se usa el PIN

# Introducción

## Tarjetas Chip-and-PIN

- **Objetivo: reducir el fraude de tarjetas**
- Estándar de 1993/1994, fechas de despliegue diferentes (e.g., 2003 en UK)
- **Toda transacción se autoriza mediante un PIN**
- Cambio de la responsabilidad ante fraude:
  - Del comerciante, si no se usa una tarjeta EMV
  - Del cliente, si se usa el PIN
- **Ataques posibles:**
  - **Skimming:** la información de la banda magnética también está en el chip
  - **Clonado de tarjetas SDA** (YES-cards)
    - SDA no permitido en tarjetas con transacciones offline
  - **DDA Man-in-the-middle**
  - **Ataque rollback:** forzar a autenticar con PIN en texto plano
  - **Ataque preplay**

# Introducción

## Tarjetas sin contacto (NFC)

### ¿Qué es NFC? – Near Field Communication

- **Tecnología para comunicación bidireccional de corto alcance sin contacto**
  - Hasta 10 cm (en teoría)
- Basada en estándares RFID, **espectro de 13.56 MHz**
- Diferentes tasas de transmisión (velocidad de transferencia de datos)



# Introducción

## Tarjetas sin contacto (NFC)

### ¿Qué es NFC? – Near Field Communication

- Tecnología para comunicación bidireccional de corto alcance sin contacto
  - Hasta 10 cm (en teoría)
- Basada en estándares RFID, **espectro de 13.56 MHz**
- Diferentes tasas de transmisión (velocidad de transferencia de datos)



**Seguridad basada en el principio de proximidad: restricciones físicas**

# Introducción

## Introducción a NFC

### Wow! *NFC sounds pretty hipster!*

#### ■ **Dos elementos principales:**

- **Proximity Coupling Device** (PCD, también llamado dispositivo con capacidad NFC) – lector
- **Proximity Integrated Circuit Cards** (PICC, también llamado NFC tags) – tarjetas

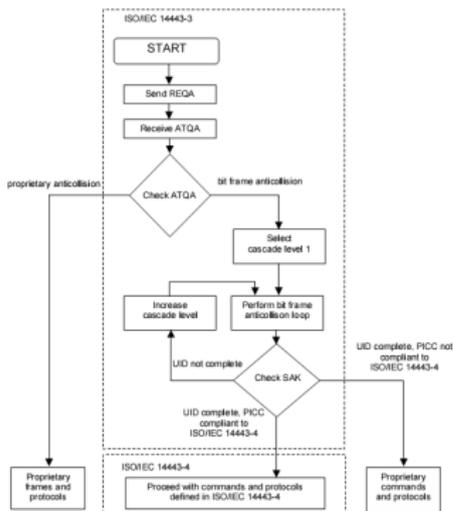
#### ■ **Tres modos de operación:**

- **Punto a punto:** comunicación directa entre las partes
- **Lectura/escritura:** comunicación con un tag NFC
- **Emulación de tarjeta:** un dispositivo NFC se comporta como una tarjeta

# Introducción

## Introducción a NFC – estándares relacionados

### Estándar ISO/IEC 14443



#### ■ Estándar internacional de 4 partes para tarjetas inteligentes sin contacto

- 1 Tamaño, características físicas, etc.
- 2 Fuente RF y esquemas de señalización (tipo A & B). **Half-duplex, 106 kbps**
- 3 Protocolo de inicialización y anti-colisión
- 4 Protocolo de transmisión de datos Data

#### ■ Tarjetas IsoDep cards: cumplen las cuatro partes del estándar

- Ejemplo: tarjetas de crédito *contactless*
- **NO** es un requisito. Ejemplo: MIFARE Classic (Tarjeta Bus, tarjeta Ciudadana)

- Cumple parte del ISO/IEC 14443-3
- **ISO/IEC 14443-4 propio + criptografía propia**
- **NO es segura.** Ataques: *replay*, “darkside”, anidado



# Introducción

## Introducción a NFC – estándares relacionados

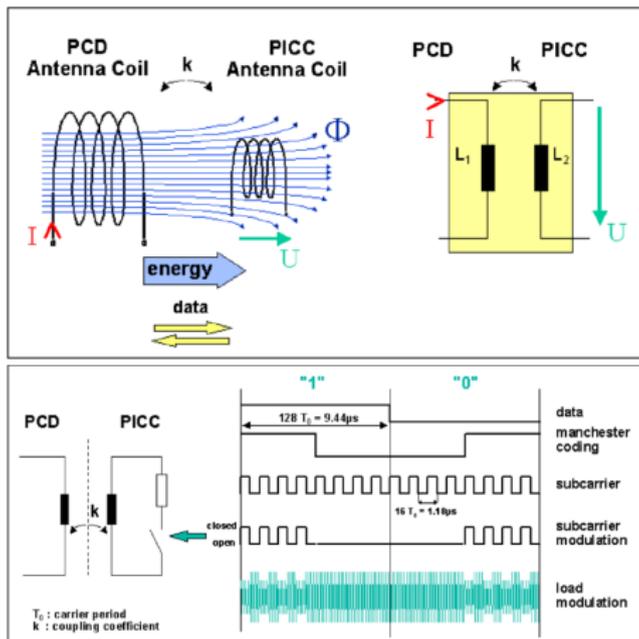


### ISO/IEC 7816

- Estándar internacional de 15 partes relacionado con circuitos integrados, especialmente tarjetas inteligentes
- **Application Protocol Data Units** (APDUs)

# Introducción

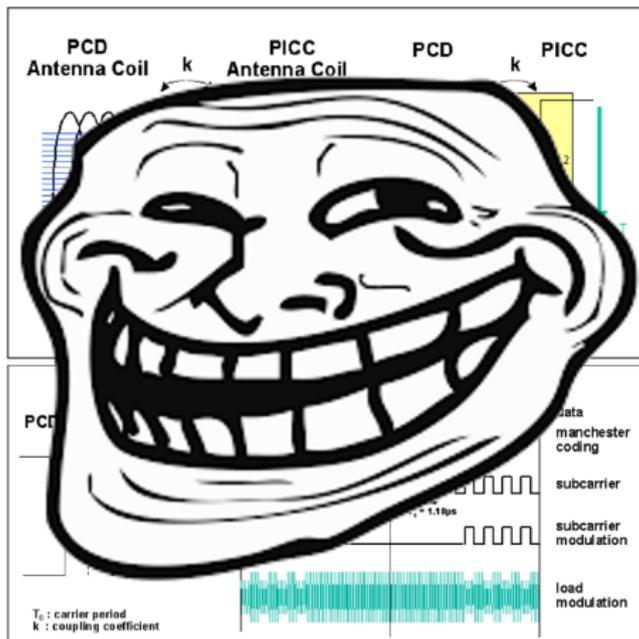
## Introducción a NFC – ¡Vamos con la física!



[Extraído de 13.56 MHz RFID Proximity Antennas ([http://www.nxp.com/documents/application\\_note/AN78010.pdf](http://www.nxp.com/documents/application_note/AN78010.pdf))]

# Introducción

## Introducción a NFC – ¡Vamos con la física!



[Extraído de *13.56 MHz RFID Proximity Antennas* ([http://www.nxp.com/documents/application\\_note/AN78010.pdf](http://www.nxp.com/documents/application_note/AN78010.pdf))]

# ISO/IEC 14443

## Ejemplos de tarjetas NFC

- MIFARE
- Calypso (sistema de ticketing electrónico)
- **Pasaportes biométricos**
- **Terjetas de pago EMV** (PayPass, payWave, ExpressPay)
- **Carnets de identificación españoles y alemanes**
  - Hace poco estuvimos investigando la seguridad del DNle3.0, que lleva NFC. Si estáis interesados, el estudio está aquí: [doi: 10.1049/iet-ifs.2017.0299](https://doi.org/10.1049/iet-ifs.2017.0299)
- ...

# Introducción

## ¿Por qué NFC?



- **NFC “junta” las tarjetas con los dispositivos móviles**
- **El sector de pago es el más interesado en esta tecnología**
  - Se esperan 500M de usuarios usando NFC para pagar en 2019
- **+300 dispositivos móviles disponibles en este momento** con capacidad NFC
  - See <http://www.nfcworld.com/nfc-phones-list/>
  - Muchos de ellos ejecutan **Android OS**

# Introducción



**Ticketing**



**Loyalty & Memberships**



**Cashless Payment**

**Identification**

**NFC**



**Transit**



**Time & Attendance**



**Physical Access**



**Secure PC Log-On**



# Introducción

Ok. . . Entonces, ¿es seguro, verdad? ¿¿Verdad??

Ok. . . Entonces, ¿es seguro, verdad? ¿¿Verdad??

## Potenciales riesgos de NFC

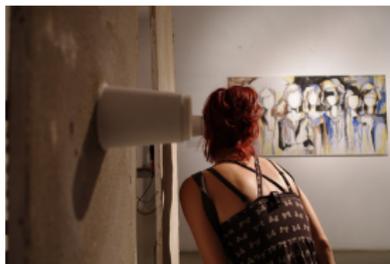
- ***Eavesdropping***
- **Modificación de los datos** (i.e., alteración, inserción, o destrucción)
- **Retransmisión**

# Agenda

- 1 Introducción
- 2 Riesgos de NFC**
- 3 Mecanismos de Seguridad
- 4 Conclusiones

# Riesgos de NFC

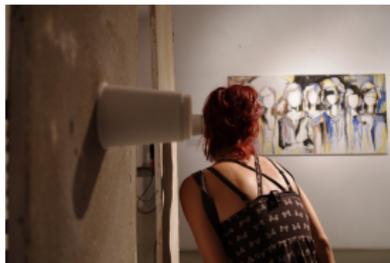
## Eavesdropping



**¿Qué información se transmite desde mi tarjeta?**  
**(¡y sin verificar quién es el lector, toma ya!)**

# Riesgos de NFC

## Eavesdropping



## ¿Qué información se transmite desde mi tarjeta? (¡y sin verificar quién es el lector, toma ya!)

- **Primary Account Number (PAN)**
- **Nombre**
- **Fecha de expiración**
- **Historial de últimas transacciones**
  - Recoge pagos NFC y de chip – **¡NFC no es más que una interfaz inalámbrica** al chip!

- **Usar comunicación segura es la única solución (cifrado)**

# NFC Eavesdropping

## Experimento



**Recuerda:** demo

*Hw usado:* móvil Android + tarjeta MasterCard NFC

# Riesgos de NFC

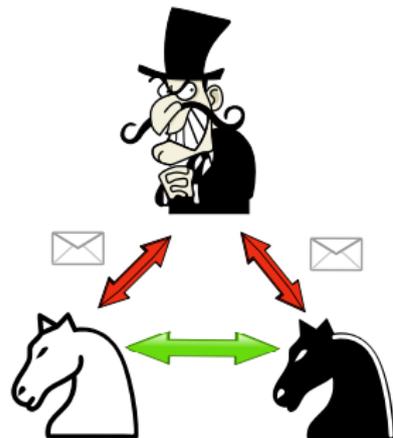
## Modificación de datos

- **Es posible la emisión ondas de radio en el mismo espectro**
  - **Conocimientos avanzados de RF + hw especializado**
  - Accesible a cualquier persona interesada (e.g., HackRF ~300€)
- **Haciendo los cálculos correctos podríamos...**
  - Alterar las ondas, inhabilitando la comunicación legítima
  - Bloquear el canal para denegar el servicio legítimo
  - Acoplar ondas para destruir las legítimas

# Riesgos de NFC

## Ataques de retransmisión

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



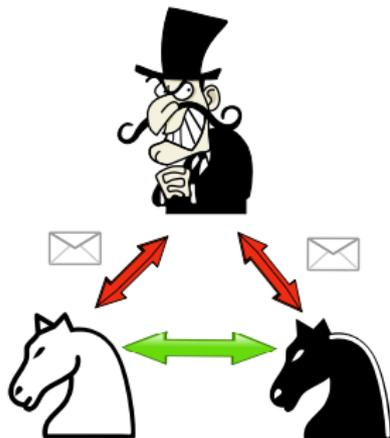
**Mafia frauds – Y. Desmedt (SecuriCom'88)**

$$\mathcal{P} \longrightarrow \overline{\mathcal{V}} \ll \text{enlace de comunicacion} \gg \overline{\mathcal{P}} \longrightarrow \mathcal{V}$$

- **Fraude en tiempo real donde dos actores fraudulentos cooperan ( $\overline{\mathcal{P}}$ ,  $\overline{\mathcal{V}}$ )**

# Riesgos de NFC

## Ataques de retransmisión



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

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

$$\mathcal{P} \longrightarrow \overline{\mathcal{V}} \ll \text{enlace de comunicacion} \gg \overline{\mathcal{P}} \longrightarrow \mathcal{V}$$

- **Fraude en tiempo real donde dos actores fraudulentos cooperan ( $\overline{\mathcal{P}}$ ,  $\overline{\mathcal{V}}$ )**

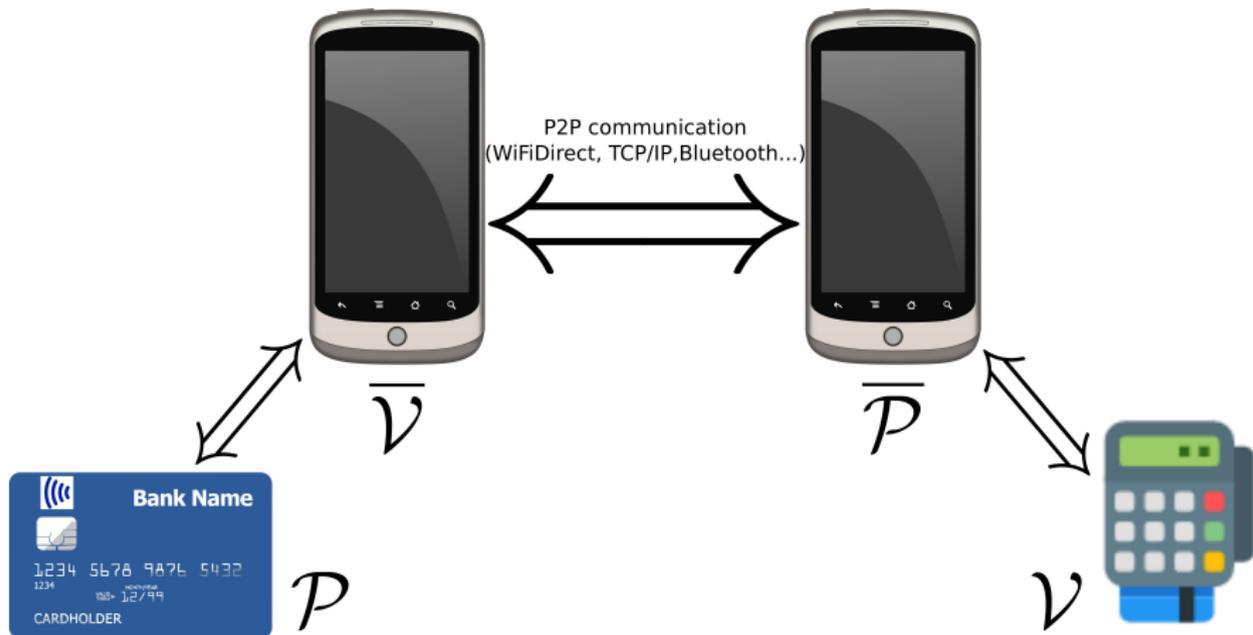
- **Partes honestas:** un TPV y una tarjeta de pago NFC
- **Partes deshonestas:** dos móviles Android con NFC

# Riesgos de NFC

## Ataques de retransmisión – ejemplo gráfico

[reader/writer mode]

[card-emulation mode]



# Android y NFC: Una historia de amor♥

## Breve resumen del soporte de NFC en Android

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 y NFC: Una historia de amor

¿Qué se puede hacer con un móvil Android con chip NFC?

## 1 Sólo se puede comunicar con tarjetas IsoDep

- Limitación impuesta por el chip NFC del móvil
- Cambio producido en los chips a partir del Nexus 4 (aproximadamente)
- **Solución:** **modificar el software que controla el chip** (difícil)

## 2 Dispositivo que se comunica con el TPV tiene que estar en modo HCE

- **La identificación de la aplicación que se emula se tiene que conocer de antemano.**  
Fácil: lista de aplicaciones conocidas en Wikipedia

# Android y NFC: Una historia de amor

¿Qué se puede hacer con un móvil Android con chip NFC?

## 1 Sólo se puede comunicar con tarjetas IsoDep

- Limitación impuesta por el chip NFC del móvil
- Cambio producido en los chips a partir del Nexus 4 (aproximadamente)
- **Solución:** *modificar el software que controla el chip* (difícil)

## 2 Dispositivo que se comunica con el TPV tiene que estar en modo HCE

- **La identificación de la aplicación que se emula se tiene que conocer de antemano.**  
Fácil: lista de aplicaciones conocidas en Wikipedia
- **Solución:** *sudo make me a sandwich* (i.e., tener los máximos permisos en el dispositivo Android)

## 3 Máximo retraso en el canal de retransmisión, por definición:

$FWT = 256 \cdot (16/f_c) \cdot 2^{FWI}, 0 \leq FWI \leq 14$ , donde  $f_c = 13.56$  MHz

# Android y NFC: Una historia de amor

¿Qué se puede hacer con un móvil Android con chip NFC?

## 1 Sólo se puede comunicar con tarjetas IsoDep

- Limitación impuesta por el chip NFC del móvil
- Cambio producido en los chips a partir del Nexus 4 (aproximadamente)
- **Solución:** **modificar el software que controla el chip** (difícil)

## 2 Dispositivo que se comunica con el TPV tiene que estar en modo HCE

- **La identificación de la aplicación que se emula se tiene que conocer de antemano.**  
Fácil: lista de aplicaciones conocidas en Wikipedia
- **Solución:** **sudo make me a sandwich** (i.e., tener los máximos permisos en el dispositivo Android)

## 3 Máximo retraso en el canal de retransmisión, por definición:

$FWT = 256 \cdot (16/f_c) \cdot 2^{FWI}$ ,  $0 \leq FWI \leq 14$ , donde  $f_c = 13.56$  MHz

- $FWT \in [500\mu s, 5s] \rightarrow$  **la retransmisión es posible si el retraso en el canal es  $\leq 5s$**

# Riesgos de NFC

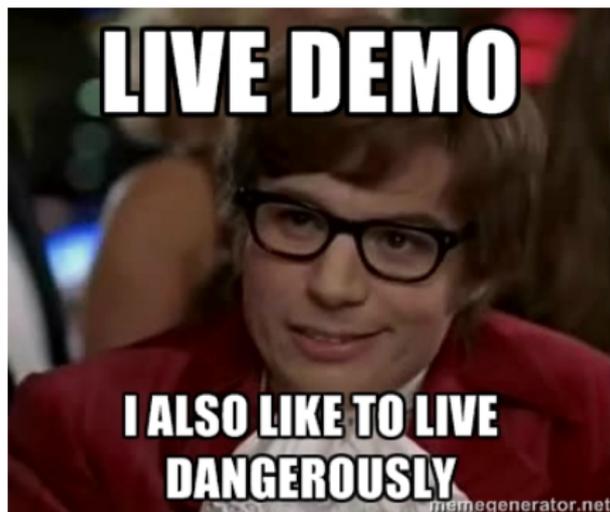
## Experimento

- Dispositivo TPV: **VeriFone VX 680 con GRPS + NFC**
- **Aplicación Android desarrollada**
- **Dos teléfonos Android de fábrica**
  - **Restricción adicional**: el que se comunica con la tarjeta necesita Android OS  $\geq$  4.4

# Riesgos de NFC

## Experimento

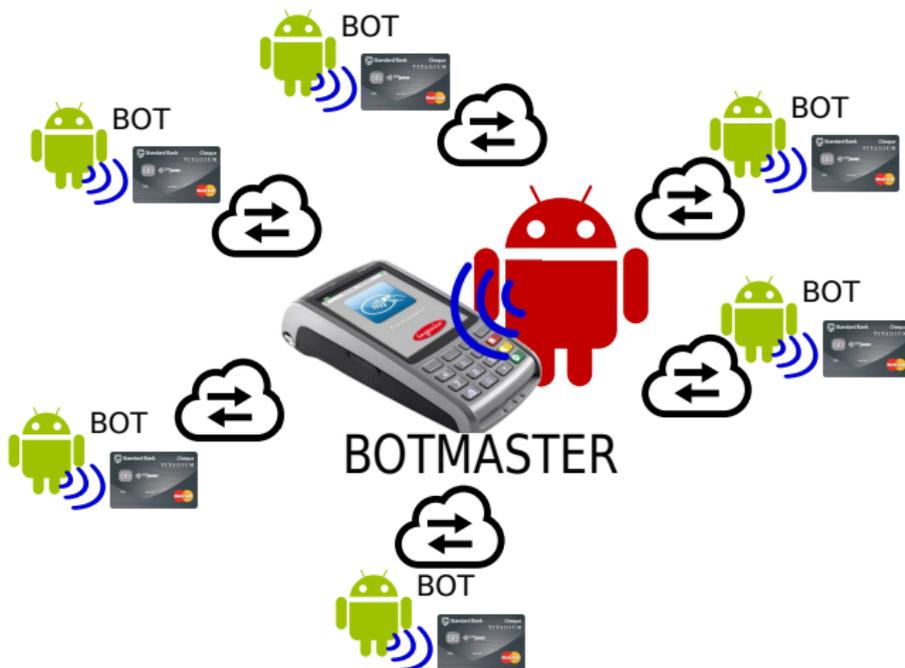
- Dispositivo TPV: **VeriFone VX 680 con GRPS + NFC**
- **Aplicación Android desarrollada**
- **Dos teléfonos Android de fábrica**
  - **Restricción adicional:** el que se comunica con la tarjeta necesita Android OS  $\geq$  4.4
  - **Truco muy bueno:** estando en Nueva York, pagué con mi tarjeta de débito NFC 1€ (como prueba de concepto) en un TPV de Madrid 😊



# Riesgos de NFC

## Ataques de retransmisión – posibles escenarios de amenazas

### FRAUDE DE MAFIA DISTRIBUIDA



# Riesgos de NFC

## Ataques de retransmisión – posibles escenarios de amenazas

### OCULTACIÓN DE LOCALIZACIÓN DEL FRAUDE



# Agenda

- 1 Introducción
- 2 Riesgos de NFC
- 3 Mecanismos de Seguridad**
- 4 Conclusiones

# Mecanismos de Seguridad

## Contra *eavesdropping*

- **Bloqueado de señales RFID**
- **Botón físico para activación de NFC** (implementado vía app)
- **Métodos de autenticación secundaria** (e.g., “escáner” de huellas en la tarjeta)

# Mecanismos de Seguridad

## Contra *eavesdropping*

- **Bloqueado de señales RFID**
- **Botón físico para activación de NFC** (implementado vía app)
- **Métodos de autenticación secundaria** (e.g., “escáner” de huellas en la tarjeta)

## Contra los ataques de retransmisión

- **Protocolos de acotación de distancia**
  - Acotar la posible distancia física entre los elementos de la comunicación NFC usando tipo específico de protocolo (con criptografía)
- **Restricciones de tiempo reales**
  - No se exigen en los sistemas NFC actuales
  - **El propio protocolo permite pedir extensiones de tiempo (wTX)**
- **Otras contramedidas lógicas**
  - Whitelisting/Blacklisting de AIDs en modo HCE → imposible

# Agenda

- 1 Introducción
- 2 Riesgos de NFC
- 3 Mecanismos de Seguridad
- 4 Conclusiones**

# Conclusiones

**Seguridad de NFC: basada en el principio de proximidad física**

# Conclusiones

**Seguridad de NFC: basada en el principio de proximidad física**

**La proximidad física NO es una restricción fiable**

# Conclusiones

## Seguridad de NFC: basada en el principio de proximidad física

La proximidad física NO es una restricción fiable

- Riesgos de NFC: ***eavesdropping*, modificación de datos, retransmisión**
- El número de dispositivos Android con NFC sigue aumentando
  - **Ataques de retransmisión son posibles incluso con móviles Android de fábrica**
  - **Abuso intencionado para interactuar con tarjetas NFC en su proximidad**

# Conclusiones

## Seguridad de NFC: basada en el principio de proximidad física

La proximidad física NO es una restricción fiable

- Riesgos de NFC: **eavesdropping, modificación de datos, retransmisión**
- El número de dispositivos Android con NFC sigue aumentando
  - **Ataques de retransmisión son posibles incluso con móviles Android de fábrica**
  - **Abuso intencionado para interactuar con tarjetas NFC en su proximidad**

Riesgos de las tarjetas de pago sin contacto EMV

**Riesgos de EMV threats + riesgos de NFC**

# Conclusiones

## Seguridad de NFC: basada en el principio de proximidad física

La proximidad física NO es una restricción fiable

- Riesgos de NFC: **eavesdropping, modificación de datos, retransmisión**
- El número de dispositivos Android con NFC sigue aumentando
  - **Ataques de retransmisión son posibles incluso con móviles Android de fábrica**
  - **Abuso intencionado para interactuar con tarjetas NFC en su proximidad**

Riesgos de las tarjetas de pago sin contacto EMV

Riesgos de EMV threats + riesgos de NFC

¡**Los carteristas virtuales** ya están apareciendo!



# Conclusiones

## ***Take-home message:***

vigila tu cartera y cualquier tarjeta NFC que tengas!

**¿Qué más puedo hacer para protegerme?**

# Conclusiones

## **Take-home message:**

vigila tu cartera y cualquier tarjeta NFC que tengas!

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

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

**YOUR PERSONAL DATA IS AT RISK**

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

[Learn More](#)

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

**Product Categories**

- 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

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

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

# Conclusiones

## **Take-home message:**

vigila tu cartera y cualquier tarjeta NFC que tengas!



# Conclusiones

## Trabajo futuro

- ~~Desarrollar una infraestructura zombie y ganar dinero~~
- Estudiar las restricciones de tiempo impuestas por Android en modo HCE

## Trabajo actual

- **Efecto de mensajes WTX/NAK** para extender el tiempo: no es posible
- **Extensión a otras tecnologías sin cables** (e.g., Bluetooth)
- **Implementación de otros ataques posibles** (e.g., denegación de servicio)

# Conclusiones

## Trabajo futuro

- ~~Desarrollar una infraestructura zombie y ganar dinero~~
- Estudiar las restricciones de tiempo impuestas por Android en modo HCE

## Trabajo actual

- **Efecto de mensajes WTX/NAK** para extender el tiempo: no es posible
- **Extensión a otras tecnologías sin cables** (e.g., Bluetooth)
- **Implementación de otros ataques posibles** (e.g., denegación de servicio)

**¡Encantados de colaborar con instituciones financieras para mejorar la seguridad de sus productos NFC!**



# Protocolo Near Field Communication: Vulnerabilidades, ataques y contramedidas

**Dr. Ricardo J. Rodríguez**

© All wrongs reversed

rjrodriguez@unizar.es \* @RicardoJRdez \* www.ricardojrodriguez.es



**Centro Universitario  
de la Defensa Zaragoza**

Centro Universitario de la Defensa  
Academia General Militar, Zaragoza, Spain

8 de mayo de 2018

**Ciclo: “Ciberseguridad y defensa en infraestructuras críticas”**  
Zaragoza