Protocolo Near Field Communication: Vulnerabilidades, ataques y contramedidas

Dr. Ricardo J. Rodríguez

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...

CUD Zaragoza

Agenda

Agenda

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 $\sim$ \$5 – descuentos al por mayor!
  - Datos de tarjeta de crédito UE son más caros (\$5 $\sim$ \$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

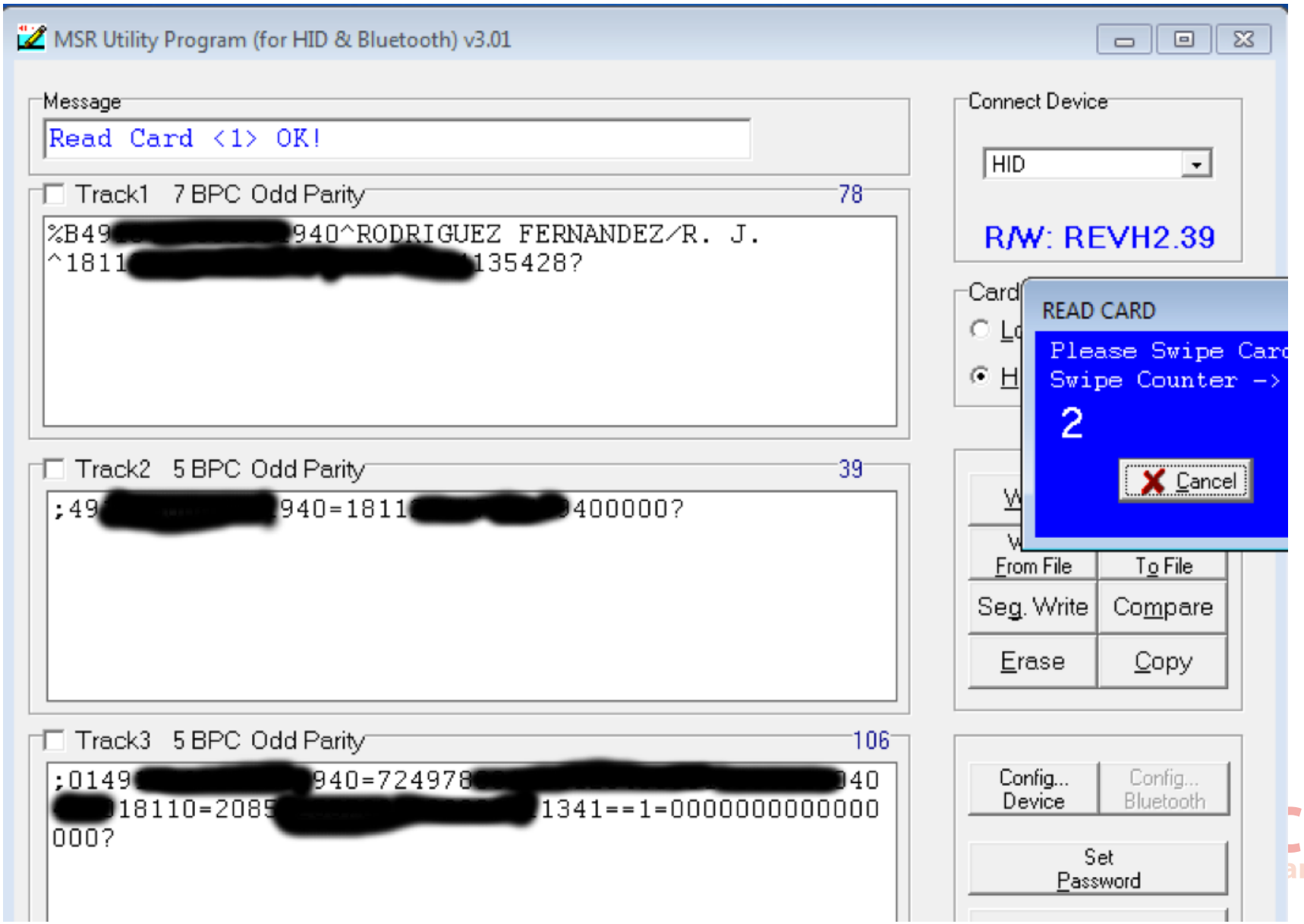
Tarjetas de banda magnética

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



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 autentificar 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

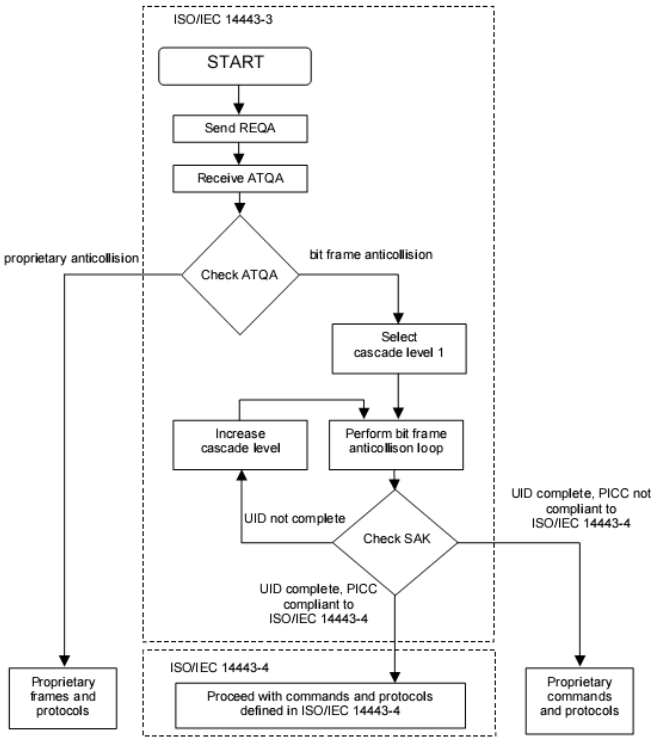
Introducción
Introducción a NFC

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

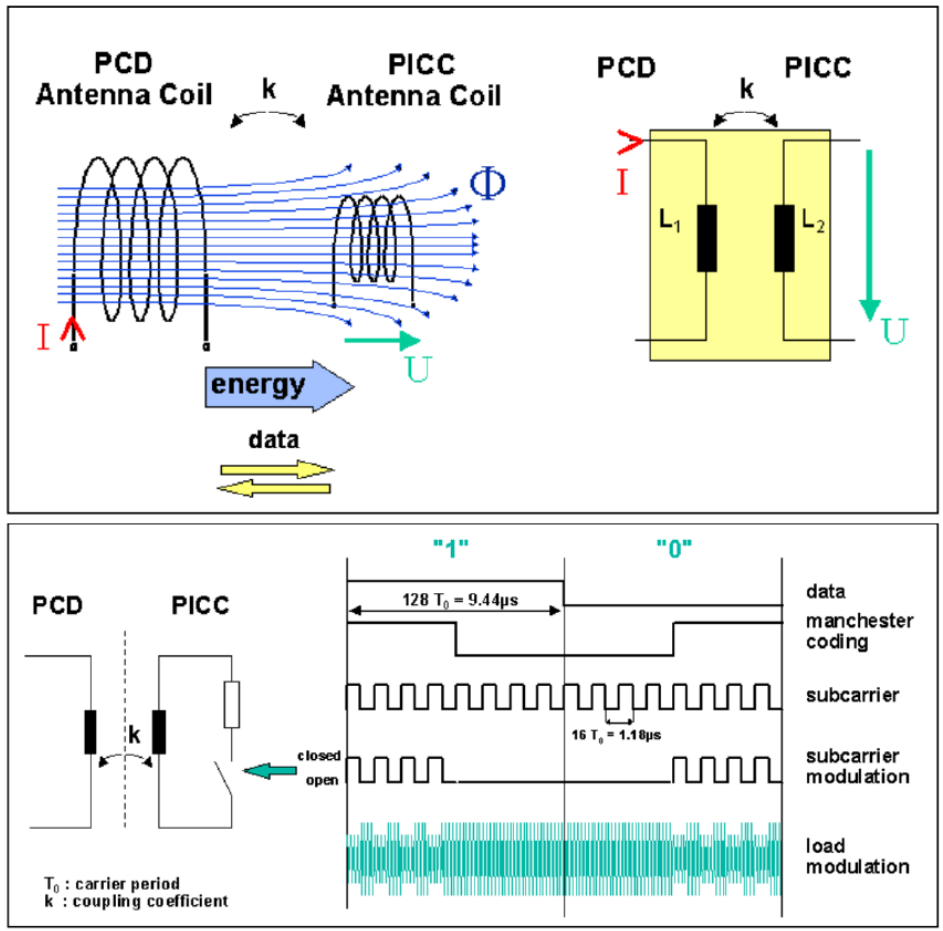
Introducción a NFC – estándares relacionados

ISO/IEC 7816

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

Introducción

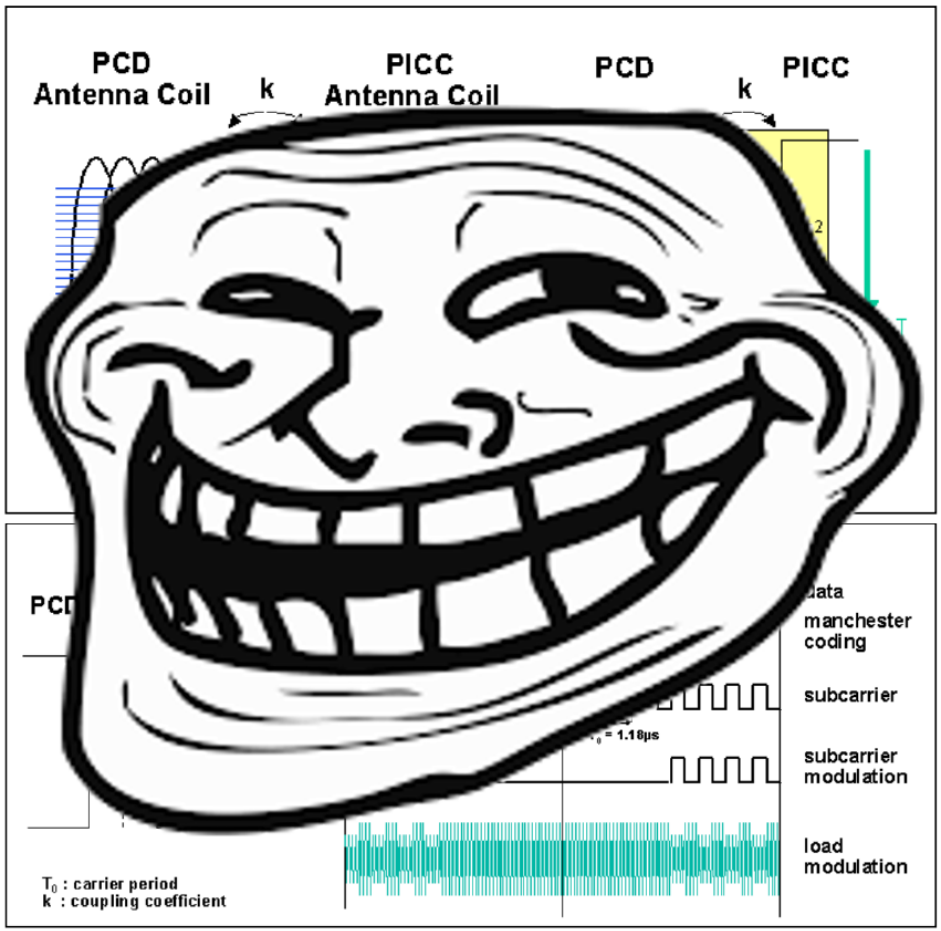
Introducción a NFC – ¡Vamos con la física!



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

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`)]

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 DNIe3.0, que lleva NFC. Si estáis interesados, el estudio está aquí: doi: 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

Identification

Time & Attendance

NFC

Loyalty & Memberships

Physical Access

Cashless Payment

Transit

Secure PC Log-On

Introducción

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

Introducción

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

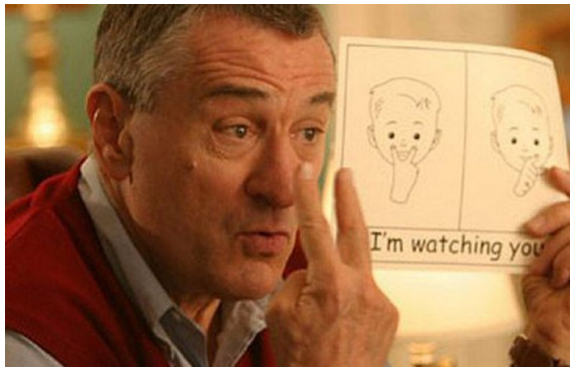
Potenciales riesgos de NFC

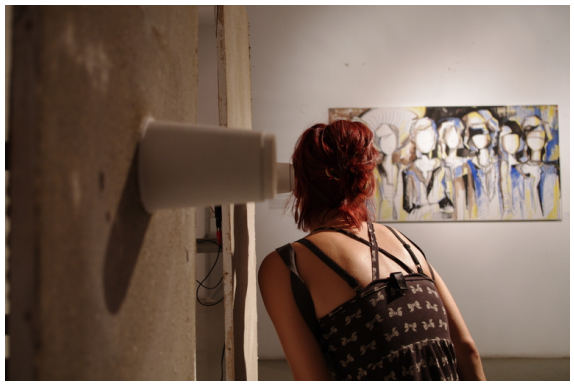
- ***Eavesdropping***
- **Modificación de los datos** (i.e., alteración, inserción, o destrucción)
- **Retransmisión**

Agenda

Riesgos de NFC

Eavesdropping



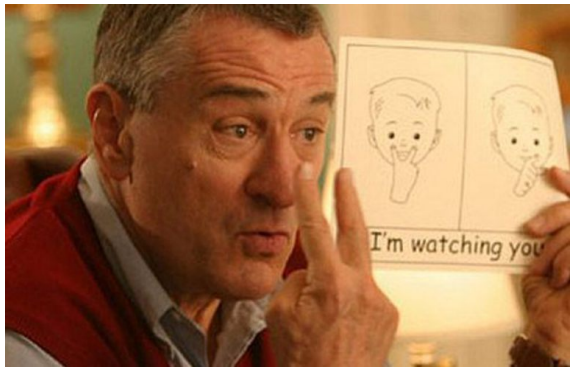


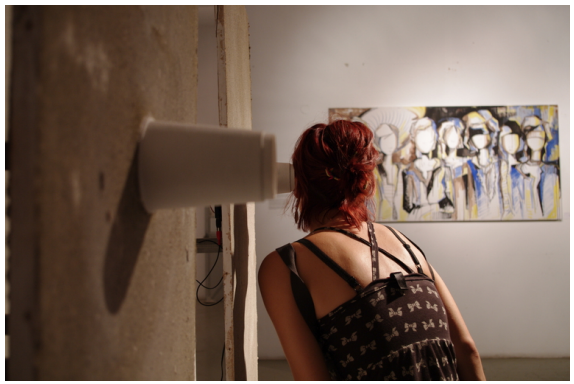
¿Qué información se transmite desde mi tarjeta?

(**¡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

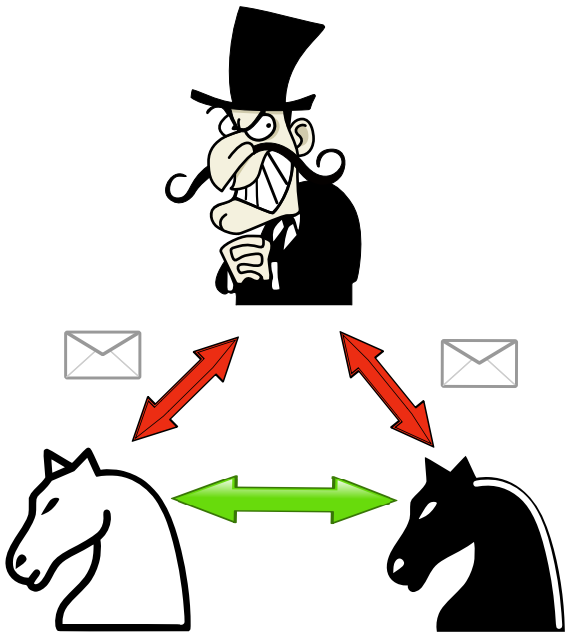
Riesgos de NFC

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)

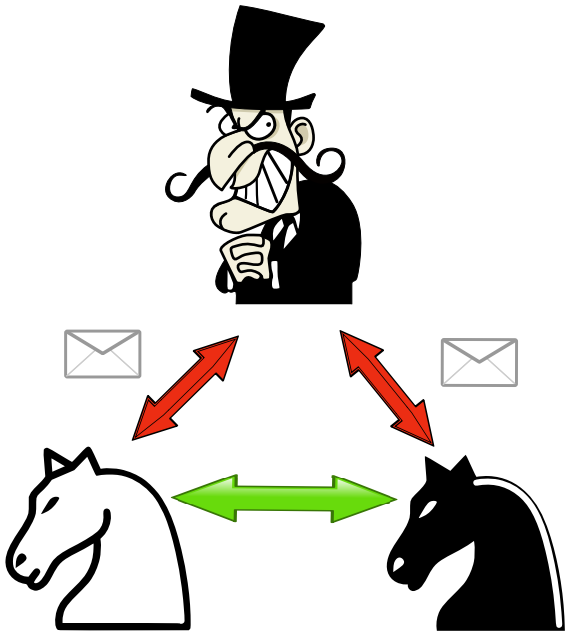
***Mafia frauds* – Y. Desmedt (SecuriCom'88)**

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

- **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)

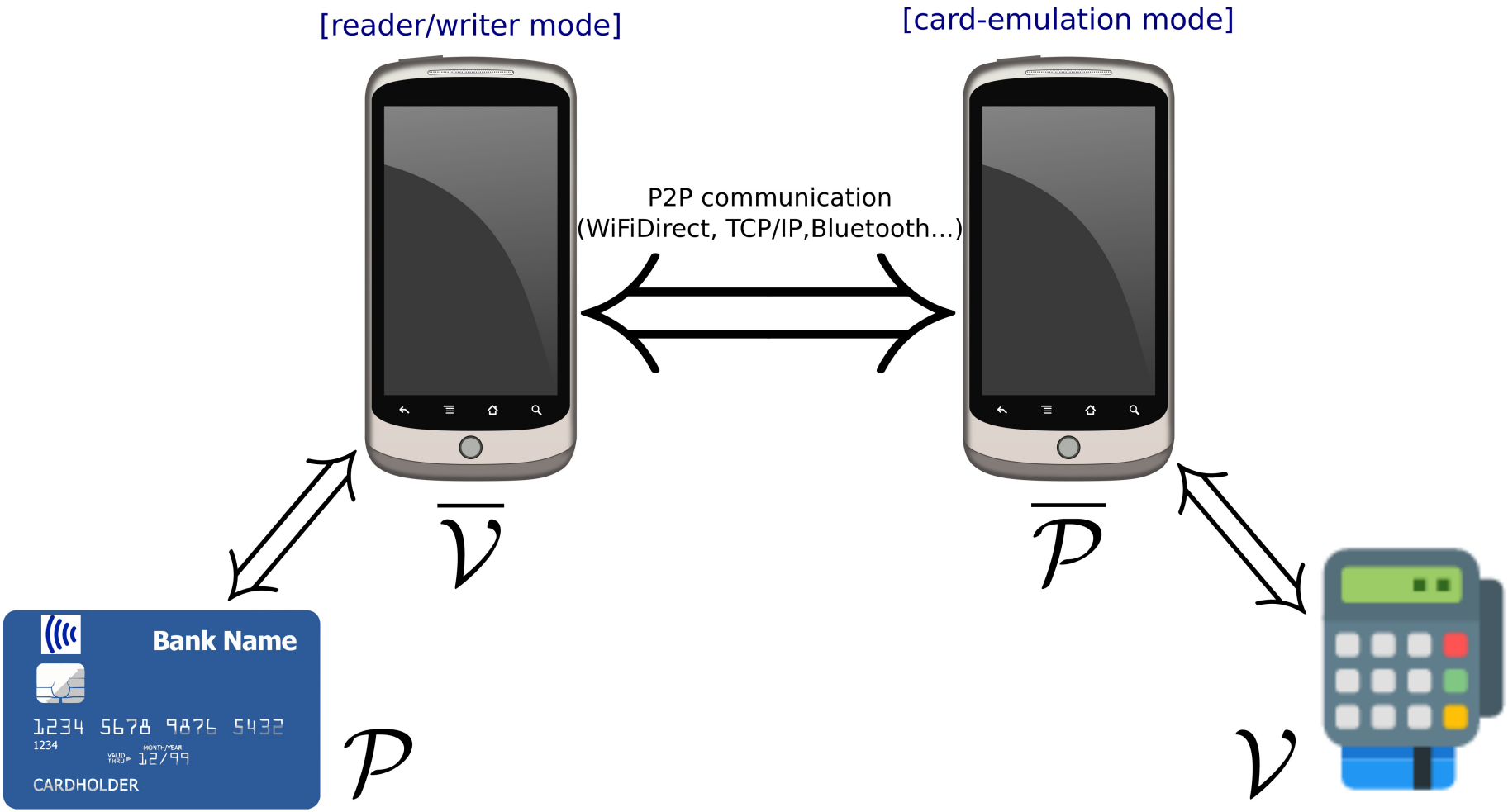
***Mafia frauds* – Y. Desmedt (SecuriCom'88)**

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

- **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

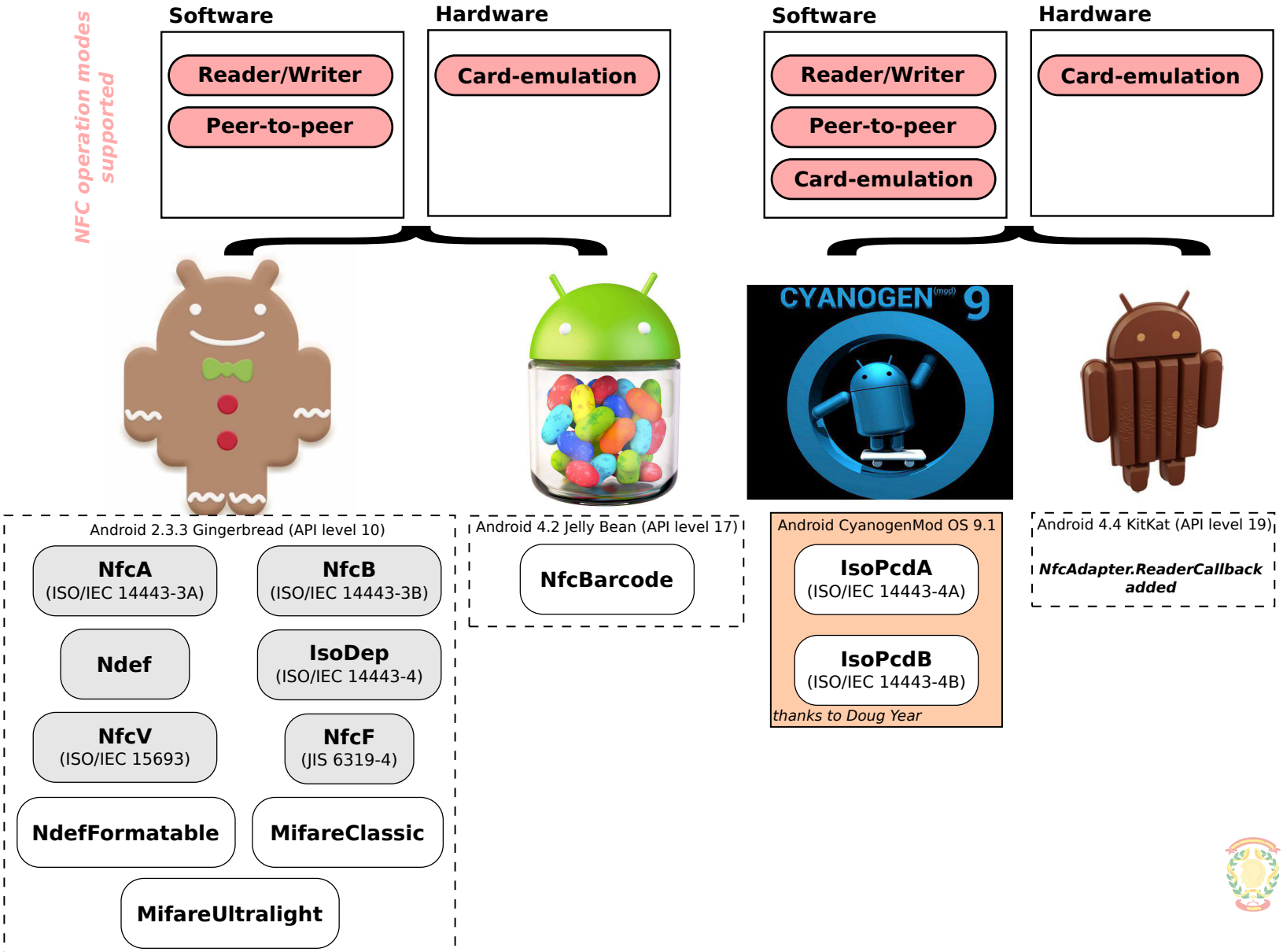
Riesgos de NFC

Ataques de retransmisión – ejemplo gráfico



Android y NFC: Una historia de am♥r

Breve resumen del soporte de NFC en Android



Android y NFC: Una historia de am♥r

¿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

CUD Zaragoza

Android y NFC: Una historia de am♥r

¿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 am♥r

¿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** $\leq 5s$

CUD Zaragoza

Riesgos de NFC

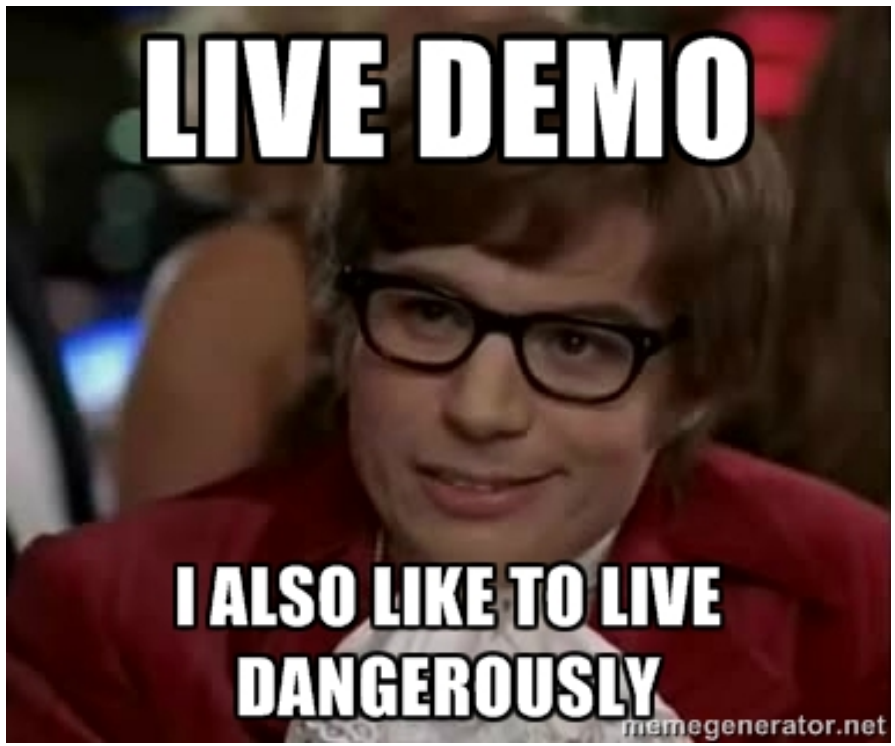
Experimento

- 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** ⌣̈

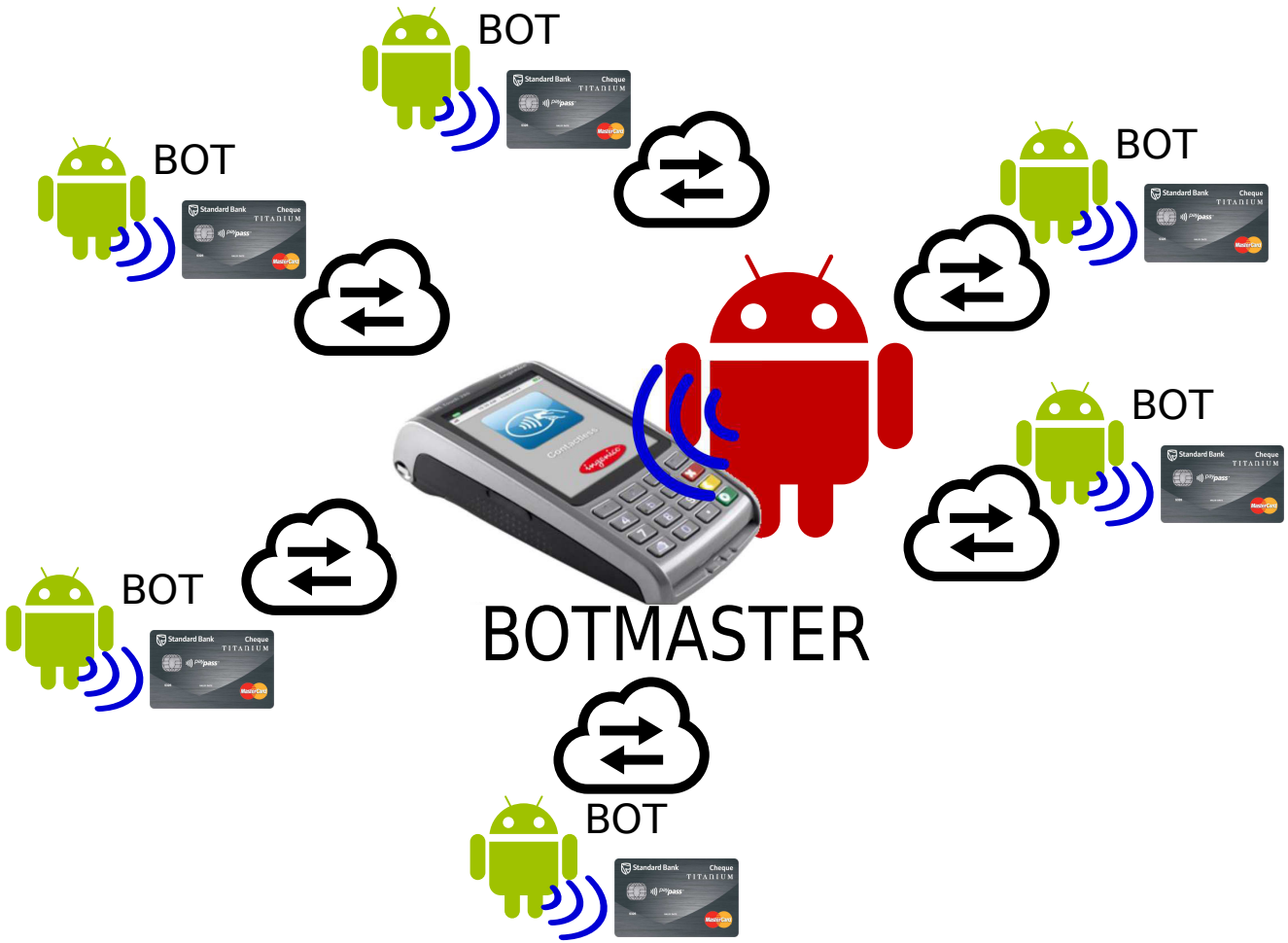


CUD Zaragoza

Riesgos de NFC

Ataques de retransmisión – posibles escenarios de amenazas

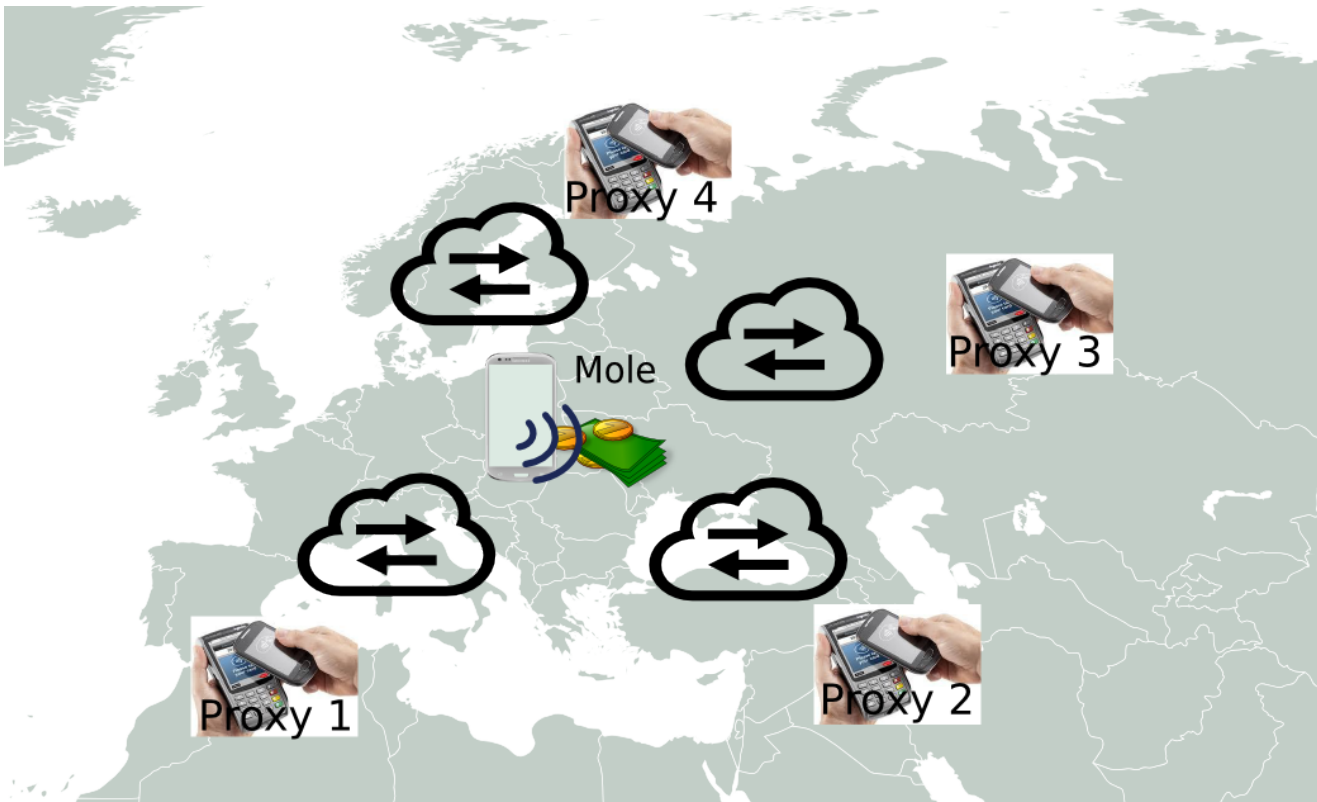
Fraude de Mafia distribuida



Riesgos de NFC

Ataques de retransmisión – posibles escenarios de amenazas

Ocultación de localización del fraude



Agenda

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 especifico 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

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**

CUD Zaragoza

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:

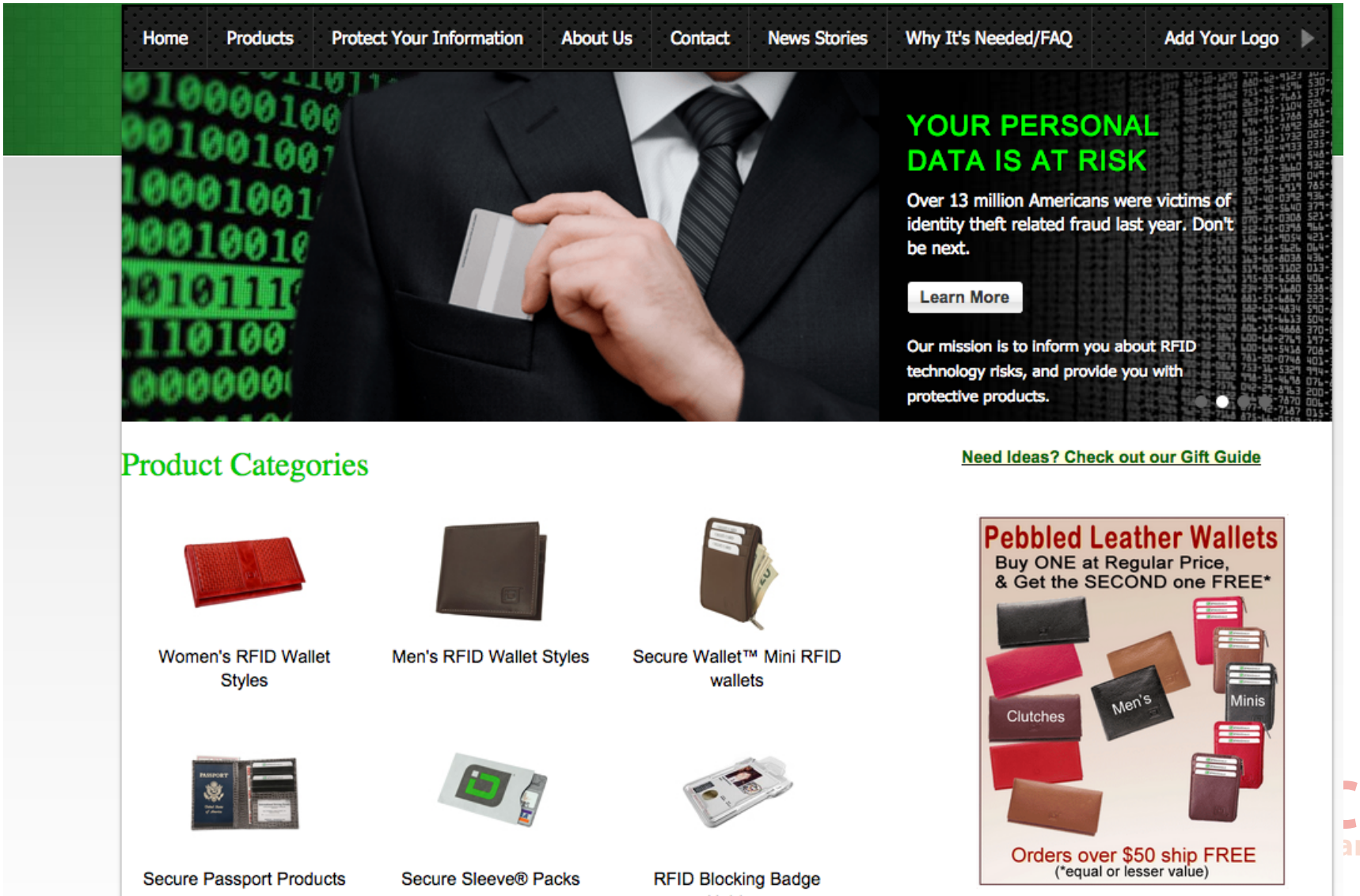
vigila tu cartera y cualquier tarjeta NFC que tengas!

¿Qué más puedo hacer para protegerme?

Conclusiones

Take-home message:

vigila tu cartera y cualquier tarjeta NFC que tengas!



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

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