

VIII JORNADAS

STIC CCN-CERT

La defensa del patrimonio tecnológico
frente a los ciberataques

10 y 11 de diciembre de 2014



Ataques de relay en tarjetas EMV NFC con dispositivos Android





José Vila

EY

jose.vilabausili@es.ey.com



Dr. Ricardo J. Rodríguez

Universidad de León -- INCIBE

rj.rodriguez@unileon.es



Índice

1. Tecnología NFC
2. Tarjetas EMV NFC
3. Ataques de relay en NFC y Android
4. PoC: NFCLeech
5. Conclusiones

1.

Tecnología NFC

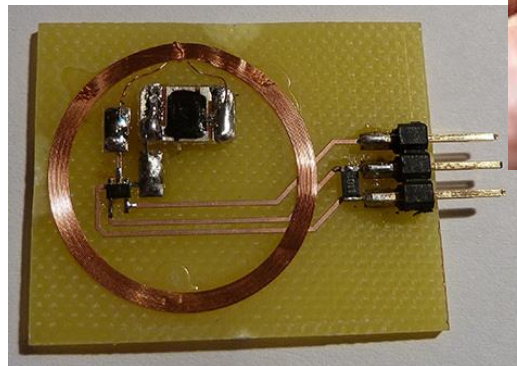
Marco teórico

1. Tecnología NFC: ¿qué es? (I)



- Near Field Communication
 - Estándar para establecer comunicación vía radio entre dispositivos
 - Tocándose, o en entornos cercanos
- Tecnología RFID
 - Radio-Frequency ID: permite identificar y hacer seguimiento sobre cosas/animales/personas usando ondas de radio
- Trabaja en la banda HF de 13.56MHz (ISO/IEC 18000-3)
- Distancia necesaria: 10cm (teóricamente, hasta 20cm)
- Ratios de transmisión: 106 – 424 kbit/s
- Participantes:
 - Iniciador: genera el campo de RF
 - Target
- Los dispositivos NFC pueden trabajar en dos modos:
 - Pasivo: el target necesita de un iniciador para poder comunicarse
 - Activo: ambos (iniciador, target) generan su campo de RF

1. Tecnología NFC: Actores involucrados (II)



• PCD

- Proximity Coupling Device
- Lector/Escritor
- Activo
- Contiene una antena, y genera el campo eléctrico
- Comunicación en la banda 13.56MHz (± 7 kHz)

• PICC

- Proximity Integrity Circuit Card
- Tag
- Pasivo o activo (depende de la fuente de alimentación). Los más usados: pasivos – más baratos
- Contiene:
 - Condensador interno
 - Resistencia

1. Tecnología NFC: Usos (III)



1. Tecnología NFC: Protocolos ISO (IV)

- ISO 14443
 - Identification cards – Contactless integrated circuit cards – Proximity cards
 - Protocolo que define cómo se interactúa con este tipo de tarjetas
 - Cuatro partes:
 - ISO/IEC 14443-1: Características físicas
 - ISO/IEC 14443-2: Potencia y señal de la radio frecuencia
 - ISO/IEC 14443-3: Algoritmos de inicialización y anti-colisión.
 - ISO/IEC 14443-4: Transmisión
- Tarjetas IsoDep: cumplen las cuatro partes
 - NO OBLIGATORIO. Ejemplo: MIFARE Classic
- ISO 7816-4
 - Organization, security and commands for interchange
 - Independencia de la tecnología física
 - APDU: Application Protocol Data Unit
 - Mensajes transmitidos sobre el canal half-dúplex

2.

Tarjetas EMV NFC

2. Tarjetas EMV contactless (I)

- Estándar de Europay, Mastercard y VISA standard para la interoperación de tarjetas, puntos de venta y cajeros
- Permite autenticar las transacciones de débito/crédito
- Comandos definidos en ISO/IEC 7816-3 and ISO/IEC 7816-4
 - Application block / unblock
 - Card block
 - External authenticate (7816-4)
 - Generate application cryptogram
 - Get data (7816-4)

(más en http://en.wikipedia.org/wiki/EMV#Application_selection)

**Una tarjeta EMV puede contener diferentes
“aplicaciones” (AID) en el chip**

Researchers Hack Visa EMV Flaw



A flaw in Visa's EMV-based contactless payment card system in the United Kingdom means that attackers could potentially use foreign currency transactions to commit **fraud**, according to researchers at Newcastle University. In particular, the foreign currency flaw could, in theory, be exploited by any attacker using an Android smart phone who was able to get close to a contactless card, which typically has a range of about two inches, the researchers say.

*Nov 3, 2014: <http://www.bankinfosecurity.com/android-attack-exploits-visa-emv-flaw-a-7516/op-1>



 MY ACCOUNT

CARDS

 **BUSINESS**

Personal > Visa Ser

[Back to Card Main](#) ➤

[All Card Benefits](#) ➤

CHECKOUT WITH EXPRESSPAY

GO FOR A SMOOTH RIDE AT THE REGISTER.



Pay for things in the time it takes to say "Express Pay". When you have the ExpressPay feature built in on your card, you can make everyday purchases like the Sunday paper or a soda without swiping your Card.

[See where](#) you can use ExpressPay.

GET IN AND OUT IN A FLASH

Just hold your card up to the special ExpressPay reader at the register your card out the door.

- There's no slip to sign.
- ExpressPay uses technology that helps make transactions safe and secure.
- You can continue to earn points or cash back for purchases made on eligible Cards.



You can continue to earn rewards or cash back when you make eligible purchases with ExpressPay. Please see [Terms and Conditions](#) for more details.

IT'S IN YOUR CARD

If the back of your Card has the ExpressPay logo, you're all set. Don't see one? Call the number on the back of your Card to get ExpressPay right away.

[Read the FAQs](#)

Don't have Blue yet? [Apply now](#)

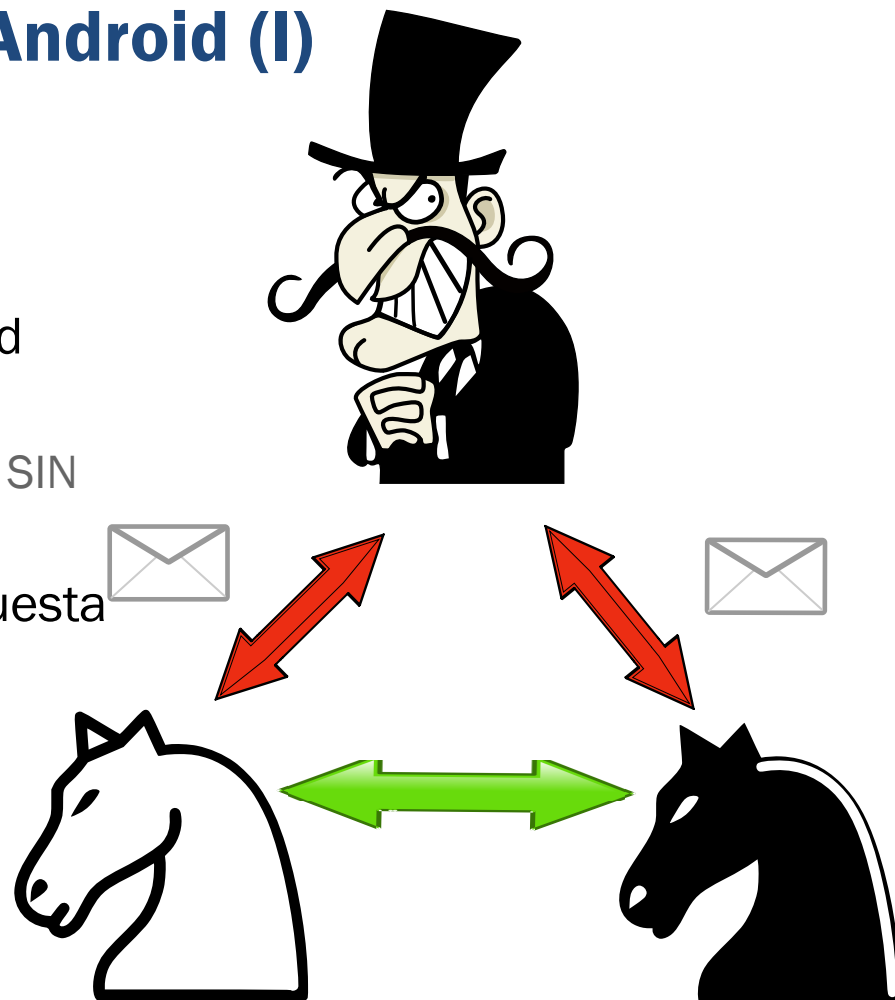


3.

Ataques relay en NFC y Android

3. Ataques relay en NFC y Android (I)

- ¿Qué es un ataque relay?
 - Relay = retransmisión
- John H. Conway, 1976: “On Numbers and Games”
 - Cómo vencer a dos maestros de ajedrez SIN conocer las reglas
- Aplicable en protocolos de desafío-respuesta
- Y... ¿son “buenos” estos ataques?
 - TRABAJAN EN NIVEL OSI 2
 - Medidas en capas superiores: inútiles

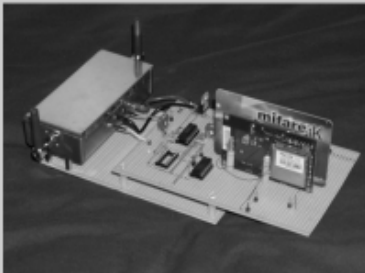


3. Ataques relay en NFC y Android (II)

- En la literatura: “Mafia frauds”
 - Definidos por Y. Desmedt en 1988
 - $P \rightarrow V' \ll \text{link de comunicación} \gg P' \rightarrow V$
 - Ataque cooperativo: P', V'
- En NFC, esto es...



3. Ataques relay en NFC y Android (III)

Feb. 2005	Sep. 2005	Jun. 2007	May. 2010
 Hardware ad-hoc ISO 14443-3	Hardware ad-hoc Lectura de tags a 50cm Solución: tarjeteros Jaula de Faraday	Relay con un TPV malicioso Funciona en transacciones con PIN	Review de ataques en NFC Presenta distintos escenarios Implementa ataque con dispositivo móvil + Beagle Board (libnfc)
Jun. 2010	Feb. 2012	Jun. 2012	Oct. 2013
Utiliza dispositivos móviles NFC P2P 	1er ataque relay NFC con disp. móviles Limitado a ISO 14443-4 Difícil instalación y distribución 	Soporte emulación software en Cyanogen Mod. NFC Proxy: relay ISO 14443-4 para Android	Android implementa HCE en KitKat (versión 4.4) Permite emulación software de tags IsoDep

3. Ataques relay en NFC y Android (IV)

¿Es posible usar un dispositivo Android genérico?

- NFCLeech: Prueba de concepto
 - Implementación en dispositivos Android SIN modificar (i.e., ¡no root necesario!)
 - No existen permisos especiales: sólo el uso de NFC
 - Arquitectura modular: soporta comunicación P2P vía Bluetooth, WiFi, GPRS
 - Timings:
 - Se empezó a trabajar en Enero de 2014, obteniéndose la PoC en Julio
- NO es la “primera” PoC: NFCSpy
 - Soportada por Google
 - Subida code.google.com el 21 de Febrero de 2014
 - Subida al Google Play en Abril de 2014
 - Usa un módulo Xposed para responder a cualquier AID (API hooking, necesario root)

4.

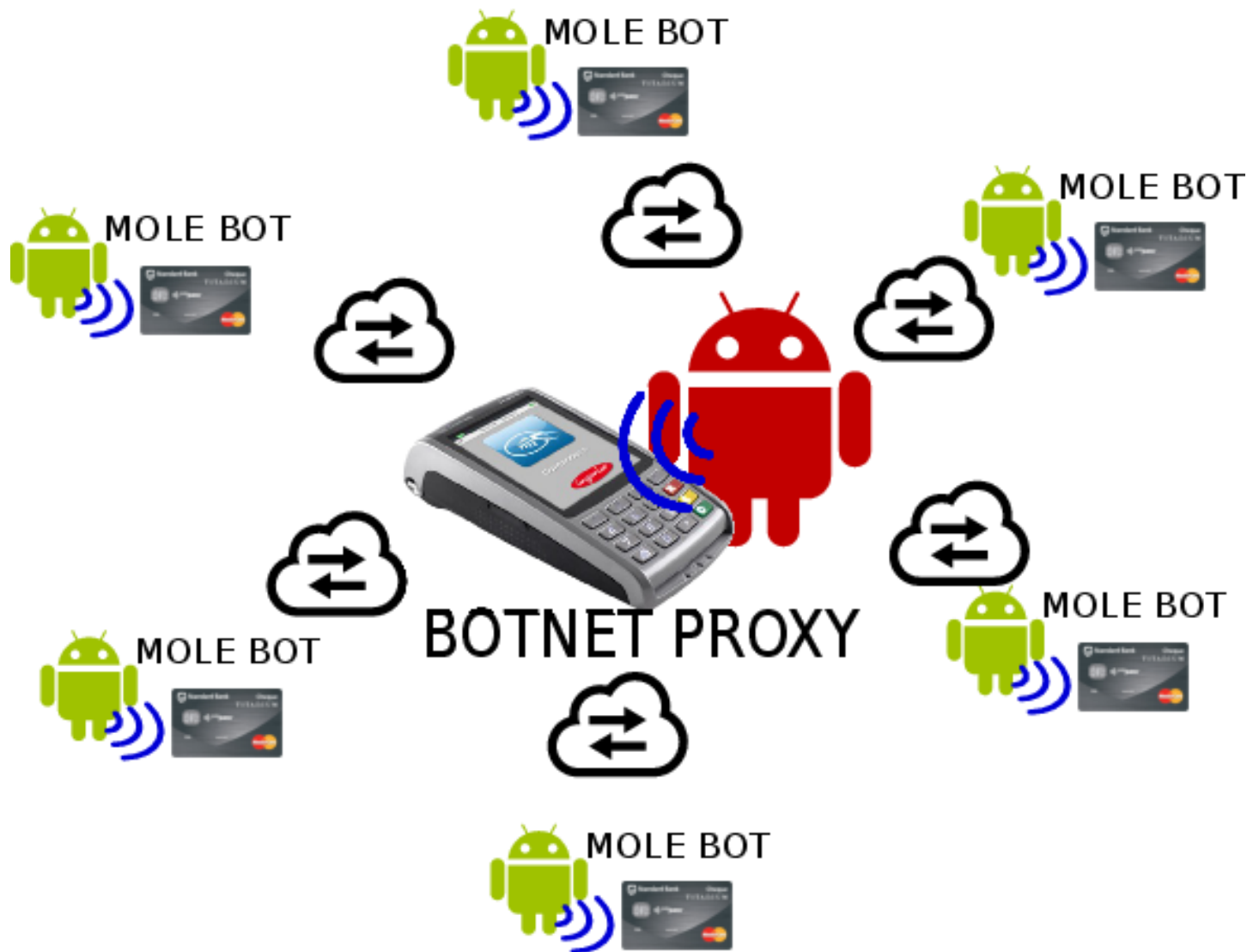
PoC NFCLeech

4. PoC NFCLeech (I)

DEMO TIME!



4. PoC NFCLeech (II): Escenarios de ataque



4. PoC NFCLeech (III): Escenarios de ataque



5.

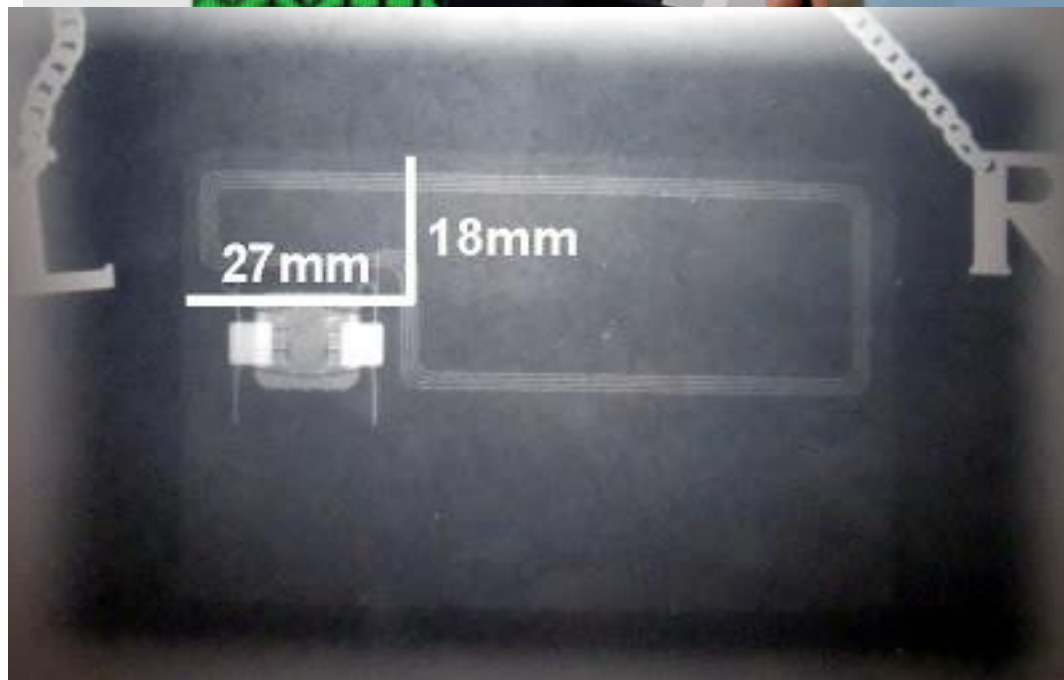
Conclusiones

Home

Products

Protect Your Information

010000100
00100100
10001001
00010010
00101110



Secure Passport Products

Secure Sleeve® Pack

Protect Yourself from Electronic Pi

5. Conclusiones (II)

- NFC: tecnología inalámbrica basada en RFID
 - Diferencia principal: Comunicación entre pares
- ¿NFC es seguro? Principio de comunicación próxima
 - Vulnerable a ataques de retransmisión (relay)
 - Ataques de capa 2...
- En un futuro, NFC se impondrá en el día a día
 - Tarjetas EMV contactless: pago con tarjetas de crédito/débito
- Soluciones:
 - Usar monedero “jaula de Faraday”
 - Troquelar la tarjeta 😊
 - Meterla al microondas *dicen* que también funciona...
 - Confiar en la ciencia:
 - Protocolos Distance-Bounding
 - Location and Time-based Access Control

Toca convivir con una tecnología insegura a sabiendas de su problemática (por ahora...)

Pero podemos...: https://www.youtube.com/watch?v=luL_C0cGe9A

➤ E-Mails

- ccn-cert@cni.es
- info@ccn-cert.cni.es
- ccn@cni.es
- sondas@ccn-cert.cni.es
- redsara@ccn-cert.cni.es
- carmen@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es



Síguenos en Linked in