Ataques de relay en NFC con dispositivos Android

Curso 2013/2014
Septiembre de 2014

Proyecto de Fin de Carrera de Ingeniería Informática

Universidad Zaragoza

José Vila Bausili

Director: Ricardo J. Rodríguez Fernández

Ponente: José Javier Merseguer Hernáiz

Timeline

- Motivación y objetivos.
- Conocimientos previos.
- Análisis de NFC en Android.
- NFC Leech: diseño, implementación y demo.
- Escenarios de ataque.
- Conclusiones y trabajo futuro.

1. Motivación y objetivos

- Motivación y objetivos.
- Conocimientos previos.
- Análisis de NFC en Android.
- NFC Leech: diseño, implementación y demo.
- Escenarios de ataque.
- Conclusiones y trabajo futuro.

1.1. Motivación

Crecimiento de la tecnología *contactless*:

- Gestión de stock.
- Sistemas de autenticación: acceso, llaves de coches...
- Pago: transporte público, máquinas expendedoras...

Recientemente el pago electrónico con tarjetas de crédito y móviles.

1.2. Objetivos

- Estudio de ataques de relay en NFC.
- Análisis de la arquitectura NFC en Android.
- Desarrollo de una aplicación móvil Android para llevar a cabo el ataque.

2. Conocimientos previos.

- Motivación y objetivos.
- Conocimientos previos.
- Análisis de NFC en Android.
- NFC Leech: diseño, implementación y demo.
- Escenarios de ataque.
- Conclusiones y trabajo futuro.

2.1. NFC y la familia ISO 14443

ISO/IEC 14443-1: Describe las características físicas.

ISO/IEC 14443-2: Describe la potencia y señal de la radio frecuencia.

ISO/IEC 14443-3: Detalla los algoritmos de inicialización y anti-colisión.

ISO/IEC 14443-4: Protocolo de transmisión.

2.2. APDU (ISO 7816-4) y EMV

Command APDU						
Header (required)				Body (optional)		
CLA	INS	P1	P2	Lc	Data Field	Le

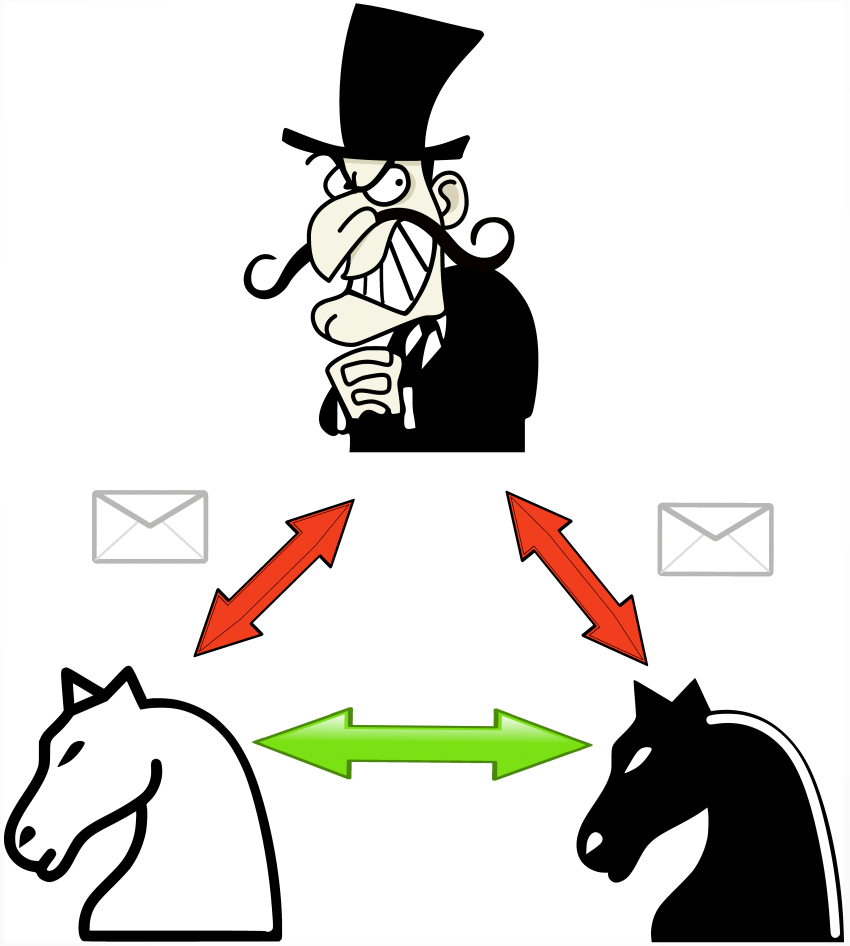
- Estándar global: Europay, Mastercard & VISA.

- Autentifica transacciones de tarjetas de crédito o débito.

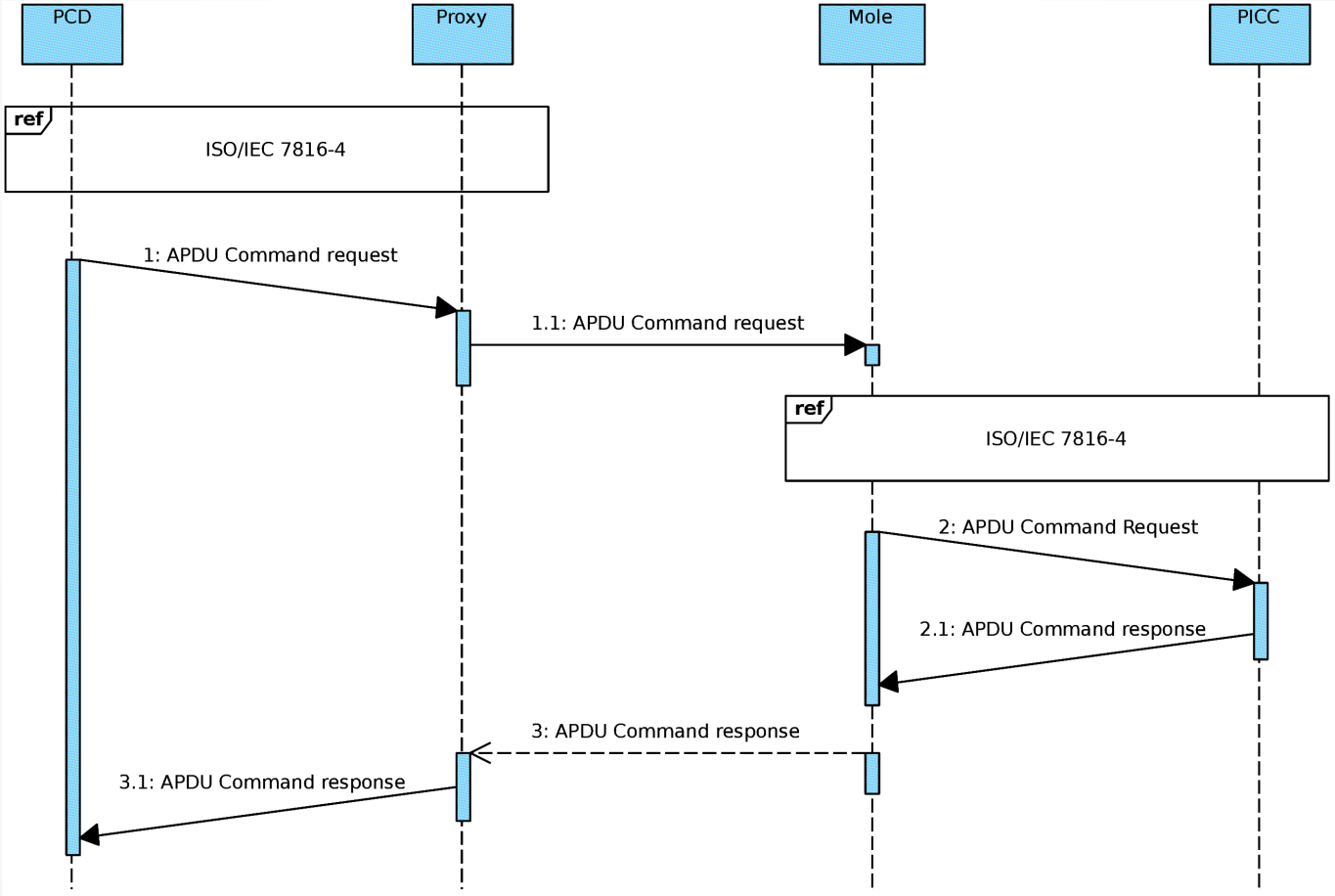
- Entre ICs, TPVs y ATM.

- Utiliza comandos APDU (select, get, check...)

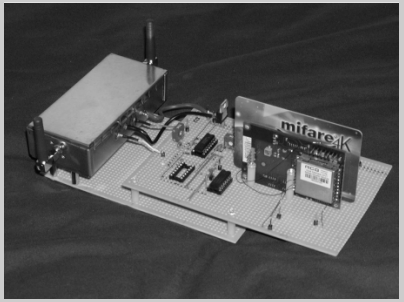
2.3. Ataques de relay

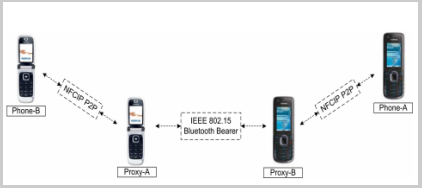
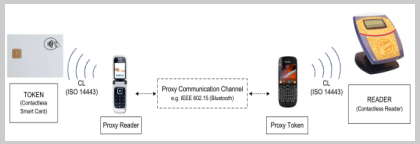


2.3. Ataques de relay



2.3. Ataques de relay

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. Análisis de NFC en Android

- Motivación y objetivos.
- Conocimientos previos.
- Análisis de NFC en Android.
- NFC Leech: diseño, implementación y demo.
- Escenarios de ataque.
- Conclusiones y trabajo futuro.

3.1. API NFC en Android

Dos modos de trabajo:

- Escritura/lectura: Mole
- Emulación software (o HCE): Proxy

Análisis de la implementación a través de:

- el código fuente (AOSP)
- la documentación
- y la depuración de librerías

3.2. API NFC en Android

N.	Descripción	Lenguaje(s)	Dependencia	OpenSource
1	Paquete `com.android.nfc` `https://android.googlesource.com/platform/packages/apps/Nfc/`	Java, JNI y C++	Ninguna	Sí
2	Librería del sistema: `libnfc-nxp` o `libnc-nci` `https://android.googlesource.com/platform/external/libnfc-nci/`	C/C++	Fabricante	Sí
3	Kernel de Linux `https://android.googlesource.com/kernel/msm.git/+/master/drivers/nfc/`	C	Hardware y fabricante	Sí
4	Firmware Directorio `/system/vendor/firmware` del dispositivo.	Binario	Hardware y fabricante	No

3.3. Alternativas: BCM vs. NXP

Chip Broadcom BCM20793

- ✔ LG Nexus 4
- ✔ Implementación NCI nuevo estándar del NFC Forum
- ✔ Soporte AOSP para HCE
- ✖ Soporte de tarjetas Mifare

Chip NXP PN544

- ✔ Soporte de tarjetas Mifare
- ✔ Emulación softare en CyanogenMod +10
- ✖ Falta de soporte HCE en algunas ROMs

3.3. Alternativas: BCM vs. NXP

Chip Broadcom BCM20793

- ✔ LG Nexus 4
- ✔ Implementación NCI nuevo estándar del NFC Forum
- ✔ Soporte AOSP para HCE
- ✖ Soporte de tarjetas Mifare

Chip NXP PN544

- ✔ Soporte de tarjetas Mifare
- ✔ Emulación softare en CyanogenMod +10
- ✖ Falta de soporte HCE en algunas ROMs

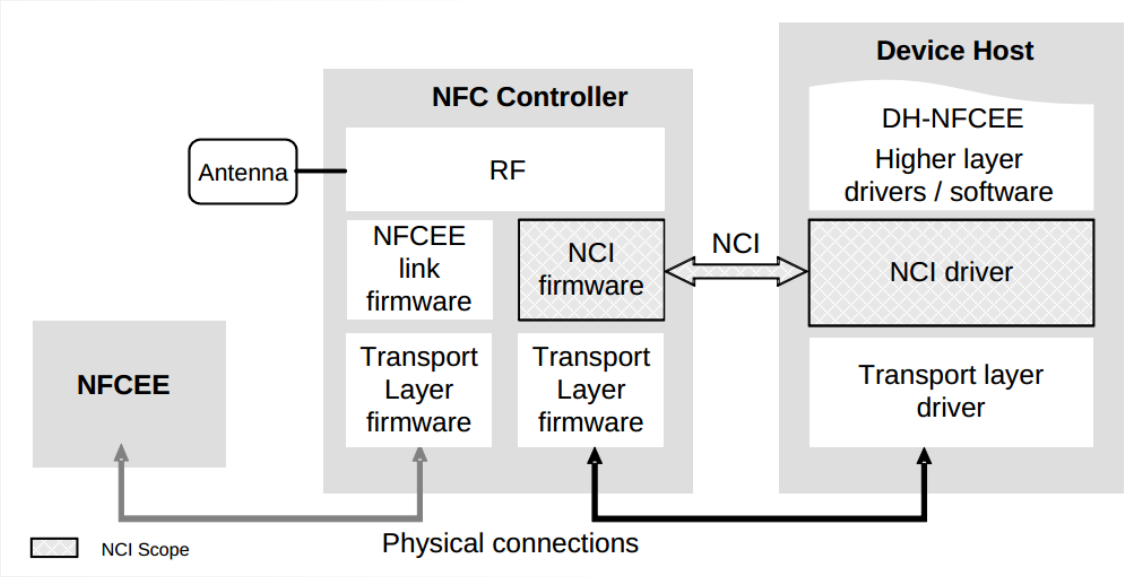
El estándar NCI dará más flexibilidad a los fabricantes de dipositivos y mayor rápidez de desarrollo a los fabricantes de chips.

3.3. NFC Interface Controller

NFCC: NFC Controller (parte del System on Chip)

DH: Device Host (dispositivo móvil o host)

NFCEE: NFC Execution Environment (normalmente en un Secure Element)



Mensajes de control: comandos, respuestas y notificaciones

Mensajes de datos: información dirigida al NFC Endpoint (o tag remoto)

Módulos NCI. Una interfaz RF define cómo el DH se va a comunicar con un Endpoint o cómo el *payload*, o contenido, de un mensaje de datos NCI encaja en el *payload* del respectivo mensaje del protocolo RF.

3.4. Limitaciones

- No es posible enviar órdenes *raw* directamente sobre ISO 14443-3.

- Android sólo es capaz de recibir a nivel software APDUs ISO 7816-4.

- Los APDU sólo son enrutados previo comando `SELECT`.

- Cualquier canal de *relay* incluye un retraso en la comunicación: el protocolo establece un *timeout* máximo (menor latencia, mayor distancia).

A pesar de todo los dispositivos Android con soporte NFC y una versión mayor que 4.4 pueden llevar a cabo un ataque de relay a nivel de APDU, simplemente con una aplicación móvil.

4. NFC Leech: diseño, implementación y demo

- Motivación y objetivos.
- Conocimientos previos.
- Análisis de NFC en Android.
- NFC Leech: diseño, implementación y demo.
- Escenarios de ataque.
- Conclusiones y trabajo futuro.

4.2. Requisitos y diseño

RF1: Utilizar un dispositivo genérico sin necesidad de software o hardware modificado.

RF2: Debe ser una aplicación modular:

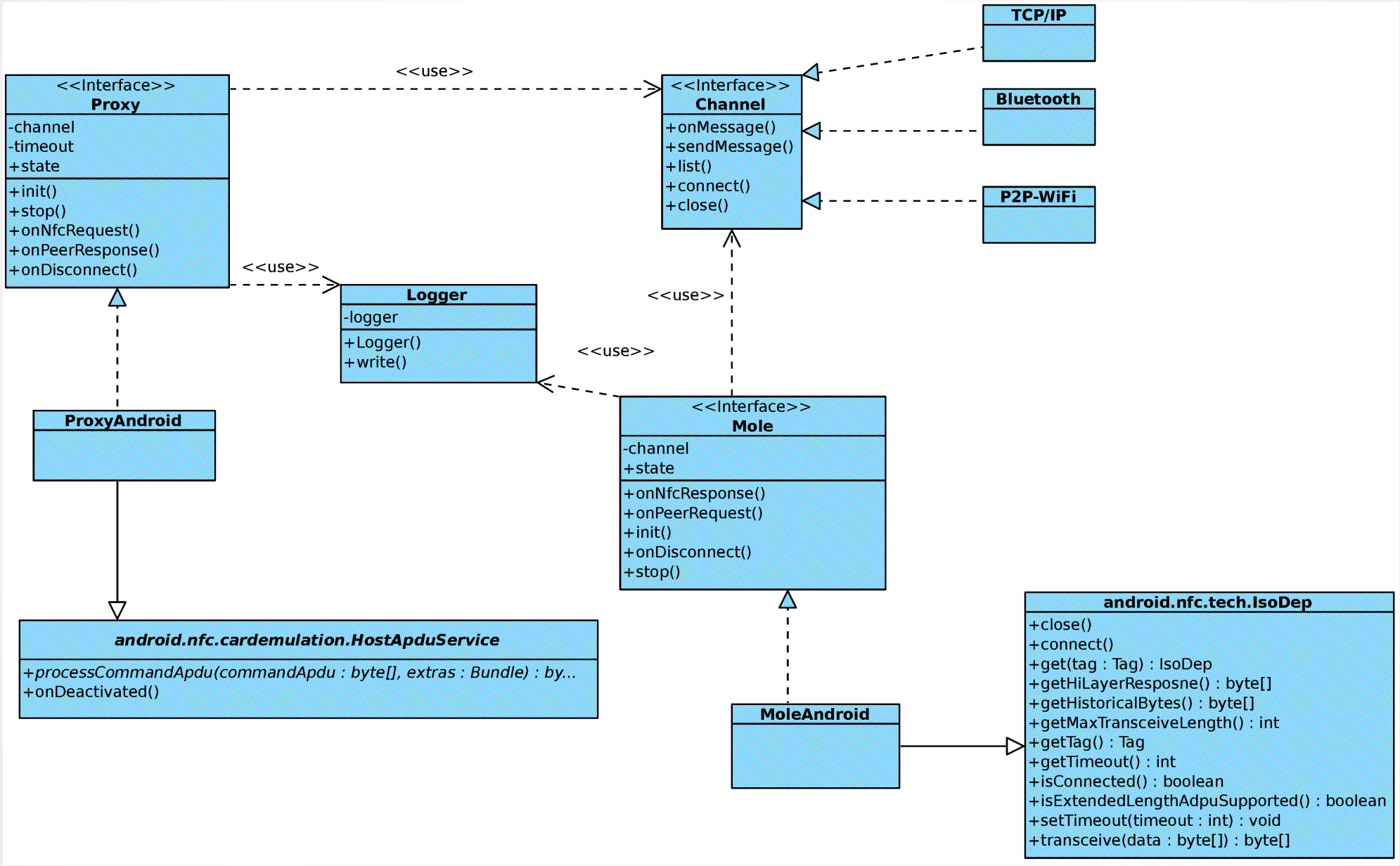
- capaz de utilizar distintos canales de comunicación.

- fácilmente integrable con otros dispositivos.

RF3: El usuario debe poder visualizar todo el proceso y ver los mensajes recibidos y enviados durante la comunicación.

RF4: La aplicación debe funcionar en una transacción de pago con tarjetas de crédito.

4.3. Requisitos y diseño



4.4. Implementación

Canal de retransmisión

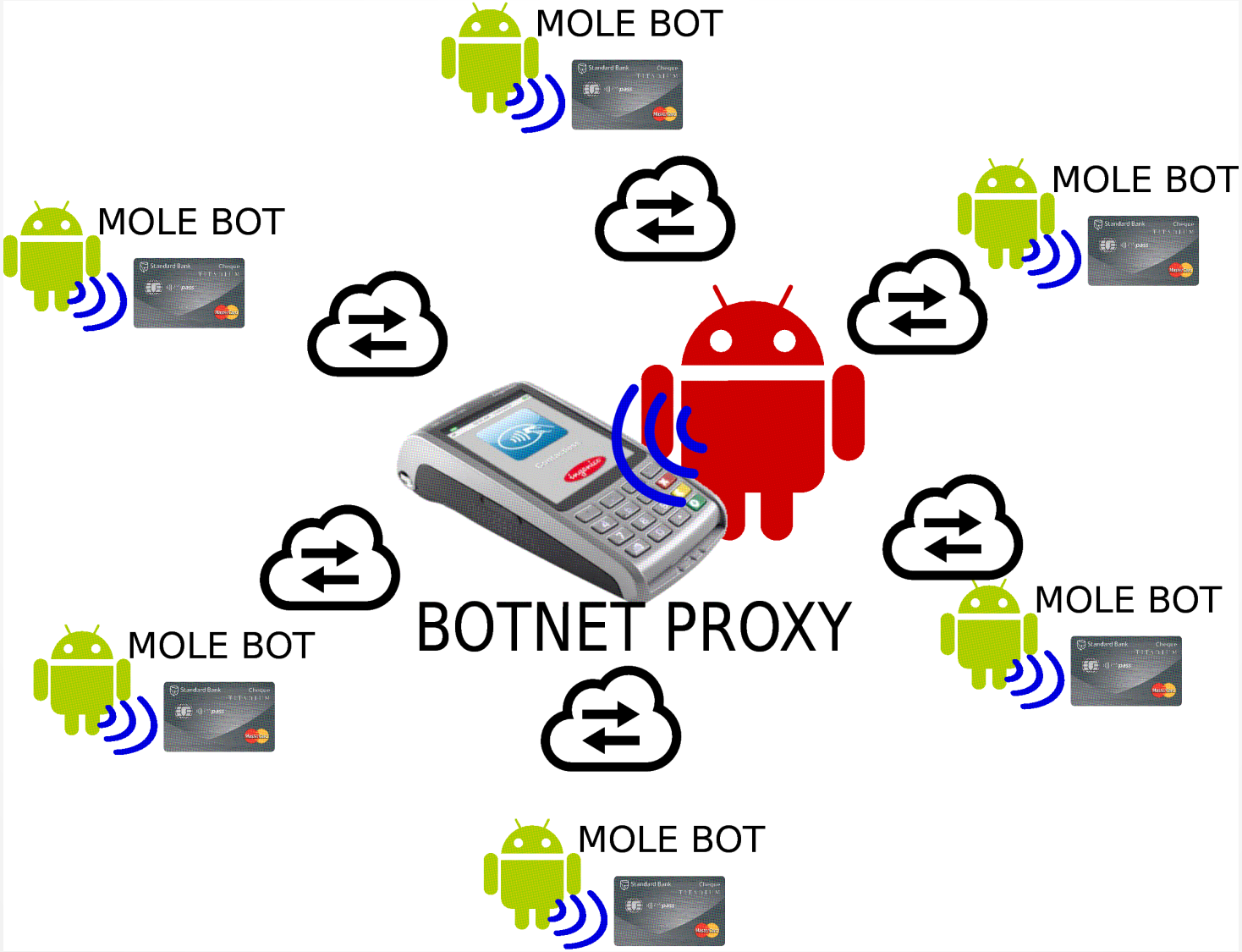
- **WiFiDirect**
  - Permite establecer una comunicación inalámbrica entre 2 dispositivos sin necesidad de configuración (hasta 50m)
  - Android ofrece una API basada en callbacks bien documentadas.
- **TCP/IP**
  - Utiliza un canal ya establecido para conectar con una IP y puerto.
  - Permite comunicaciones de cualquier distancia.
- **Bluetooth**
  - Al igual que WiFiDirect fácil comunicación entre 2 dispositivos.
  - Soporte BLE en Android 4.3, menor consumo de batería.

4.5. Demo

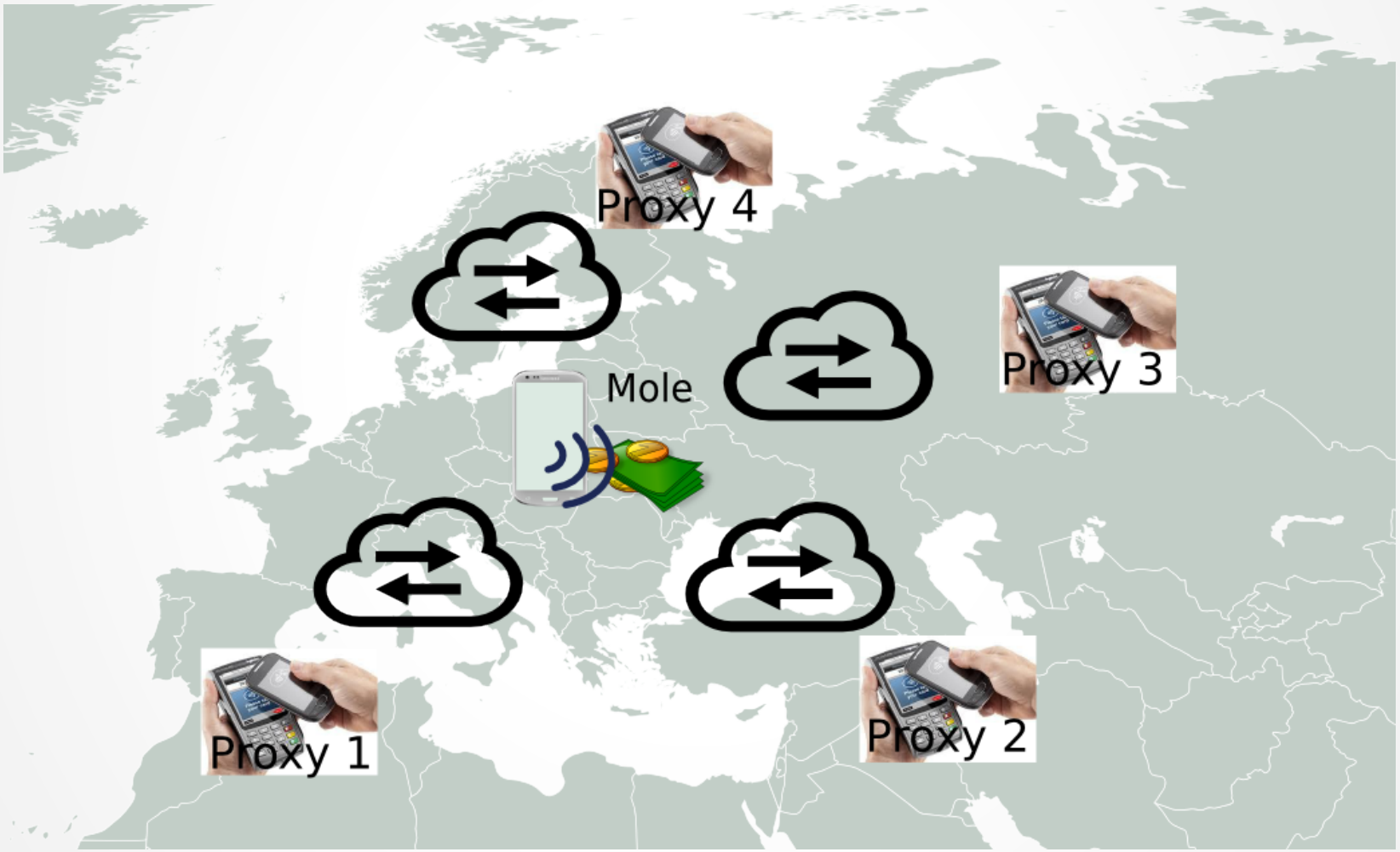
5. Escenarios de ataque

- Motivación y objetivos.
- Conocimientos previos.
- Análisis de NFC en Android.
- NFC Leech: diseño, implementación y demo.
- Escenarios de ataque.
- Conclusiones y trabajo futuro.

5.1. Botnet de tarjetas



5.2. Anti-rastreo



6. Conclusiones y trabajo futuro

- Motivación y objetivos.
- Conocimientos previos.
- Análisis de NFC en Android.
- NFC Leech: diseño, implementación y demo.
- Escenarios de ataque.
- Conclusiones y trabajo futuro.

6.1. Conclusiones

- Análisis de la implementación NFC en un dispositivo Android.
- Limitaciones y restricciones de dicha implementación.
- **NFC Leech:** aplicación para llevar a cabo un ataque de relay NFC en una transacción con tarjetas de crédito.

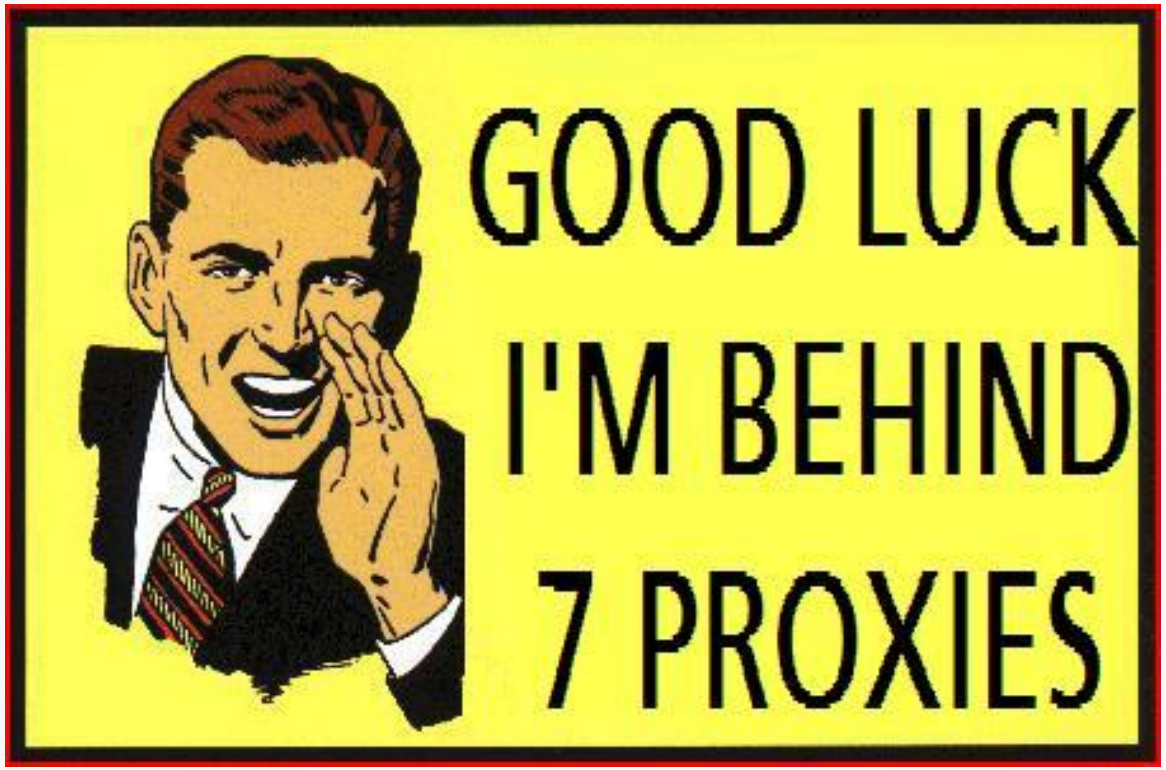
Crecimiento de las tecnologías NFC y el pago sin contacto.

En los próximos meses es posible que veamos alguno de los escenarios aquí presentados hecho realidad.

6.2. Trabajo futuro

- Estudio de la configuración NCI para extender las capacidades NFC.
- Ingeniería inversa y modificación del firmware.
- Librería Java para relay NFC.
- Procesamiento de mensajes APDU.
- Análisis de seguridad de los monederos digitales.
- Estudio de vectores de explotación y software malicioso.

¡Gracias!



Horas de trabajo