Informe de Amenazas CCN-CERT IA-05/16

Comunicación de campo cercano (*Near Field Communication* - NFC). Vulnerabilidades

Enero de 2016

El **Dr. Ricardo J. Rodríguez**, profesor de la Universidad de Zaragoza, ha participado en la elaboración y modificación del presente documento y sus anexos.
RedSys ha prestado su colaboración para la realización del presente informe y sus anexos.

ÍNDICE

1. SOBRE CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad, modificado por el RD 951/2015, de 23 de octubre.

De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre **sistemas clasificados** y sobre sistemas de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

2. RESUMEN EJECUTIVO

La comunicación de campo cercano o Near Field Communication (NFC), es una tecnología de comunicación inalámbrica bidireccional de corto alcance (teóricamente, hasta 10 centímetros) basada en diferentes protocolos de identificación por radio frecuencia (RFID[1], por su traducción en inglés). En concreto, los estándares en los que se basa NFC son el ISO-14443 [Ref. – 1] y el JIS X 6319-4 (también conocido como Sony FeLiCa) [Ref. – 2]. Este último estándar es principalmente usado en países de Asia, a diferencia del primero que es el más usado en EEUU y Europa.

NFC fue desarrollada por NXP Semiconductors (anteriormente denominada Philips Semiconductors) y Sony como una evolución que aúna las tecnologías RFID inductivas y las tarjetas inteligentes. Además de la estandarización en base a normativas como las que se indicaban anteriormente, otros protocolos, formatos de datos y aplicaciones de NFC han sido propuestos por NFC Forum[2] [Ref. – 3].

NFC opera en el espectro de alta frecuencia 13.56MHz y soporta diferentes ratios de transmisión de información: 106 kbps (en ISO-14443), 216 kbps (en Sony FeLiCa) y 424 kbps (en Sony FeLiCa). NFC difiere de otras tecnologías de RFID de alta frecuencia en varios aspectos: primero, la comunicación en NFC es bidireccional (frente a unidireccional); segundo, la distancia de comunicación es entorno a 10cm frente a 1 metro; y por último, NFC no permite la lectura simultánea de más de un elemento. NFC define tres modos de operación:

- **Punto a punto *(Peer-to-peer)***: en este modo, dos dispositivos NFC se comunican directamente uno con otro. Es el modo típicamente usado para el intercambio de tarjetas de visita, credenciales para el establecimiento de un enlace de red seguro, o intercambio de cualquier tipo de información. Se basa en el protocolo de comunicación estandarizado ISO/IEC 18092 [Ref. – 4].
- **Lector/escritor**: este modo permite a un dispositivo con capacidad NFC comunicarse con una tarjeta o *tag* NFC (es decir, cualquier chip que incorpore la tecnología NFC para su comunicación, con una estructura de memoria para almacenar información en un formato estándar). Este modo permite que los dispositivos NFC sean operables con otros *tags* RFID e infraestructuras de tarjetas inteligentes.
- **Emulación de tarjeta**: este modo permite la comunicación entre dos dispositivos NFC, actuando uno de ellos como una tarjeta inteligente con capacidad NFC. El dispositivo NFC puede emular desde ISO/IEC 14443 hasta JIS X 6319-4 (Sony FeLiCa). Esta emulación puede ser bien vía hardware, a través de un dispositivo dedicado llamado elemento

[1] *Radio Frequency IDentification (RFID)*

[2] *NFC Forum es una asociación de organizaciones industriales y sin ánimo de lucro con un especial interés en NFC, inicialmente creada por NXP Semiconductors, Sony y Nokia con el fin de promocionar el uso de la tecnología NFC. Actualmente ofrecen un programa de certificación en sus especificaciones para asegurar una interoperabilidad entre diferentes productos e implementaciones*.

seguro[3]; o bien vía software, donde la emulación se realiza desde una aplicación que se ejecuta dentro del sistema operativo del dispositivo[4].

NFC está presente en multitud de aplicaciones cotidianas. Por ejemplo, desde coger el autobús, metro, o tranvía en ciudades como Madrid, Málaga, o Zaragoza, hasta el acceso de personal o usuarios a polideportivos municipales, bibliotecas públicas, universidades o recintos controlados como aeropuertos. Otra de las posibles aplicaciones es el pago con tarjeta sin contacto[5].

En el caso de pago sin contacto, si la cantidad a pagar no supera un cierto máximo (en España fijado en 20€ -- varía en función del país y moneda), la transacción se realiza sin ningún método de verificación adicional. Si la cantidad a pagar supera esta cantidad, el propietario de la tarjeta ha de introducir el PIN[6] como mecanismo de verificación.

Según diferentes estudios de mercado [Ref. – 5] [Ref. – 6], este sector ha sido uno de los que más interés ha generado. Este gran interés puede estar motivado por ser NFC una tecnología que se está introduciendo en dispositivos móviles (actualmente, más de 300 dispositivos móviles cuentan con un chip NFC [Ref. – 7]), siendo así una opción de llevar las "tarjetas" a estos dispositivos [Ref. – 8]. De hecho, en España algunas entidades financieras están ofreciendo ya aplicaciones que hacen uso del chip NFC del teléfono como medio de pago, sustituyendo a la propia tarjeta de crédito/débito del usuario.

Sin embargo, la tecnología NFC es insegura tal y como se ha demostrado en multitud de trabajos científicos [Ref. – 9][Ref. – 10][Ref. – 11][Ref. – 12], en donde se han relatado tanto los problemas de seguridad inherentes a la tecnología como posibles soluciones. Estos problemas de seguridad son, básicamente, la escucha secreta o a escondidas[7], la alteración de la información transmitida, y los ataques de retransmisión[8]. En este informe se detallan estos problemas de seguridad, presentando a su vez las soluciones propuestas y su efectividad.

Este informe se estructura de la siguiente manera. En el apartado 3 se especifican de forma resumida los aspectos de interés de los estándares relacionados con la tecnología NFC. En el apartado 4 se detallan los problemas de seguridad de NFC, poniéndolos además en contexto mediante pruebas de concepto. En el apartado 5 se describen las posibles soluciones o contramedidas frente a estos problemas de seguridad. Por último, el apartado 6 esboza las principales conclusiones de este informe.

[3] *Secure element, en inglés*

[4] *Llamado host-card emulation (HCE), software card emulation o soft-SE*

[5] *Contactless cashless payment, en inglés*

[6] *Número personal de identificación (Personal Identification Number PIN)*

[7] Eavesdropping, en inglés

[8] *Relay attacks, en inglés*

3. CONCEPTOS PREVIOS

Las tarjetas inteligentes, o smartcards, contienen un microchip (llamado circuito integrado) al que se puede acceder mediante cualquier lector de tarjetas inteligentes. Estas tarjetas, también conocidas como tarjetas de chip, pueden disponer de una interfaz de acceso a los datos que contienen no basada en contacto. Así, se incorpora la tecnología NFC a las tarjetas inteligentes para poder acceder a su contenido sin necesidad de contacto. Estas tarjetas inteligentes con NFC incorporan, además del chip, una antena alrededor de la propia tarjeta. Esta antena es necesaria para la generación de corriente eléctrica por el principio de inducción. Estas tarjetas, también llamadas tags NFC, pueden ser activos o pasivos en función de si tiene aporte energético propio o no. Los tags pasivos se componen de un condensador, que almacena la energía que le proporciona el lector, y una resistencia (véase Figura 3-1).

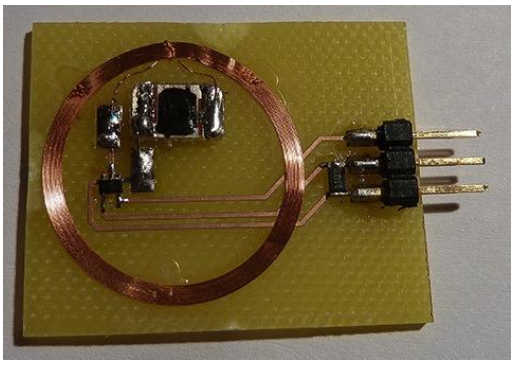


Figura 3-1. Ejemplo de tag NFC: circuito integrado y antena.

Como se ha comentado anteriormente, los tags NFC pasivos requieren que el aporte energético para funcionar sea proporcionado por el dispositivo NFC lector. Así, se produce un intercambio de energía entre ellos por el principio de inducción entre las espiras de la antena (véase la Figura 3-2).

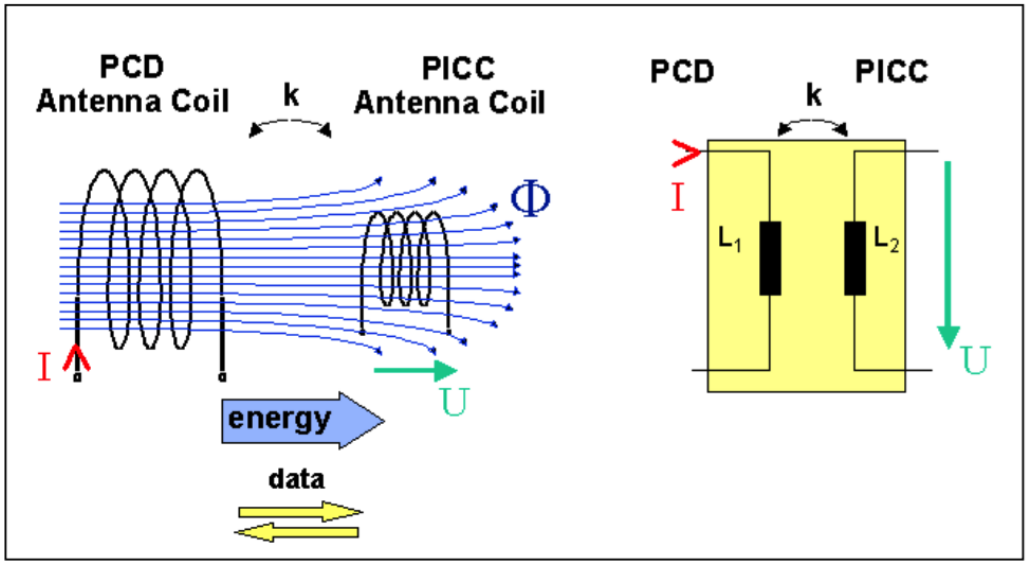


Figura 3-2. Principio de inducción entre el Proximity Coupling Device (PCD) y el Proximity Chip Card (PICC) (imagen extraída de http://www.nxp.com/documents/application_note/AN78010.pdf).

3.1 Estándares ISO/IEC 7816

El protocolo para comunicación con tarjetas inteligentes se define dentro de la serie de estándares ISO/IEC 7816 [Ref. – 13]. ISO/IEC 7816 está formado por quince partes, siendo las partes 3 y 4, relativas a la interfaz eléctrica, al protocolo de transporte de bajo nivel y al protocolo de aplicación, las destacables en este informe.

La parte 3 del estándar ISO/IEC 7816 (ISO/IEC 7816-3) define un protocolo maestro-esclavo de comunicación asíncrona en serie para el intercambio de información entre un lector y una tarjeta inteligente. Así, se define un procedimiento de inicialización entre estos dispositivos en el que la tarjeta, para responder al lector tras este procedimiento, le manda un ***Answer-to-Reset (ATR)***. Esta respuesta contiene información sobre características de la comunicación: velocidad soportada, protocolos aceptados, parámetros u otra información específica al producto particular.

La parte 4 del estándar, ISO/IEC 7816-4 [Ref. – 13], define el protocolo de aplicación para tarjetas inteligentes. Así pues, define la estructura de ficheros y los comandos para acceder a los mismos de manera segura. La estructura de ficheros que mantienen las tarjetas inteligentes viene definida por tres tipos de ficheros diferentes: fichero maestro ***(master file, MF)***, ficheros dedicados ***(dedicated files, DF)***, y ficheros elementales ***(elementary files, EF)***. La jerarquía entre ellos es como se muestra en la Figura 3-3.

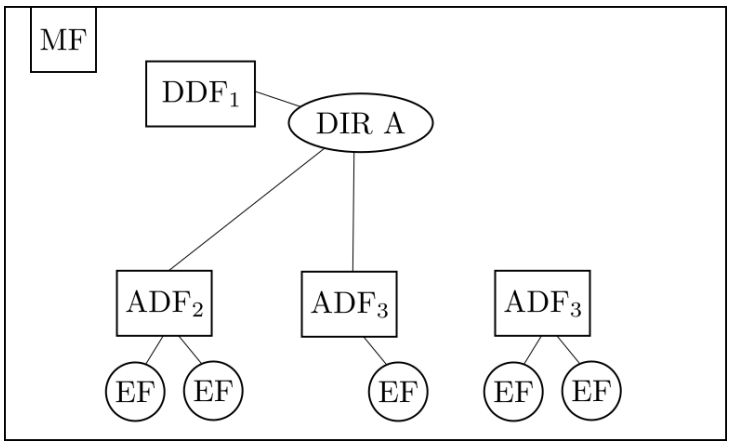


Figura 3-3. Ejemplo de organización de ficheros en una tarjeta inteligente.

Como se ha comentado anteriormente, la comunicación con las tarjetas inteligentes se realiza mediante comando-respuesta. En concreto, los paquetes que se envían reciben el nombre de ***(Application Protocol Data Unit, APDUs)***. Los paquetes comando se envían siempre desde el lector a la tarjeta, mientras que los paquetes respuesta se envían siempre de la tarjeta al lector.

Un comando APDU se divide entre la cabecera y el cuerpo. La cabecera tiene la siguiente estructura:

- **CLA (instruction class):** de tamaño 1 byte (8 bits), define el tipo de comando. Puede ser propietario o estándar.
- **INS (instruction code):** de tamaño 1 byte, define el comando específico a realizar (por ejemplo, "escribir información").
- **P1-P2:** de tamaño 2 bytes, define los parámetros concretos de la instrucción a realizar (por ejemplo, el desplazamiento dentro del contenido del fichero a escribir).

El cuerpo del comando APDU se divide, a su vez, en:

- **L_c**: de tamaño 0, 1 ó 3 bytes, define el número de bytes (N_c) de información del comando a realizar
- **Información**: de tamaño **N_c**, la información del comando concreta
- **L_e**: de tamaño 0, 1 ó 3 bytes, define el número máximo de bytes de respuesta esperados **(N_e).**

Una respuesta APDU se divide en un cuerpo y un trailer. El cuerpo contiene la respuesta al comando recibido, y puede ser de longitud menor o igual al **N_e** especificado por el comando. El ***trailer,*** de 2 bytes de tamaño ***(denominados SW1, SW2)***, especifica el estado de la instrucción ejecutada. Por ejemplo, un valor 0x9000 indica que el comando se ha ejecutado correctamente; o 0x61NN indica que el comando se ha ejecutado correctamente pero se espera más información.

3.2 Estándares ISO/IEC 14443

La comunicación con tarjetas inteligentes NFC se define en la serie de estándares ISO/IEC 14443 [Ref. – 1]. Este estándar, en concreto, define un sistema de RFID de proximidad basado en acoplamiento inductivo operando en la frecuencia 13.56MHz. Sobre este estándar, una tarjeta inteligente NFC puede usar el protocolo de aplicación de APDUs definido en el ISO/IEC 7816 [Ref. – 13], o definir un protocolo de aplicación propietario. En la Figura 3-4 se muestra una comparativa entre la pila de protocolo de ambos estándares.

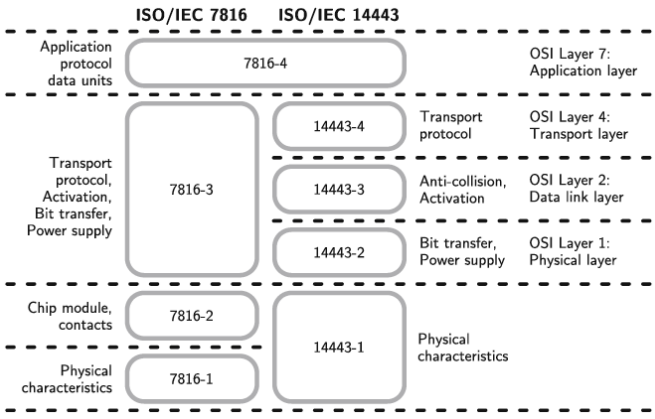


Figura 3-4. Comparativa entre las pilas de protocolo de ISO/IEC 7816 e ISO/IEC 14443 (extraída de [Ref. – 14]).

ISO/IEC 14443 se divide en cuatro partes, siendo las importantes a destacar la parte 3, que define la secuencia de activación y el protocolo de anticolisión; y la parte 4, que especifica un protocolo de transmisión *half-duplex* orientado a bloques. La parte 3, además, se divide en dos tipos (tipo A y tipo B), que difieren en el tipo de modulación y los esquemas de codificación de señal utilizados. Nótese que el protocolo de aplicación (definido en la parte 4) es el mismo para ambos tipos. ISO/IEC 14443 define una nueva terminología para referirse al lector, llamado ***Proximity Coupling Device (PCD)***, y a la tarjeta inteligente, llamada ***Proximity Integrated Circuit Card (PICC)***. Cabe destacar que no es obligatorio para una tarjeta el implementar todo el estándar ISO/IEC 14443. En el caso de que así sea, la tarjeta recibe el nombre de ***IsoDep*** (por ejemplo, las tarjetas de crédito/débito con capacidad NFC son tarjetas IsoDep).

El protocolo ISO/IEC 14443-3 es un protocolo de comunicación iniciado siempre por el lector. Así, el lector manda un comando a la tarjeta, que le devuelve una respuesta. Cada PICC se identifica por un valor (pseudo)único, almacenado dentro de la propia tarjeta y definido por el fabricante de la misma. Así, cuando el PCD está en modo ocioso, envía comandos REQUEST al medio esperando a la respuesta de alguna PICC para iniciar la comunicación. En concreto, el comando es REQA/REQB, en función de si implementa el protocolo ISO/IEC 14443-A o ISO/IEC 14443-B.

En el caso del tipo A, el comando REQA es respondido por todas las tarjetas que no están activadas por ATQA. Tras ello, el PCD comienza el protocolo de anti-colisión, que permite seleccionar de manera exclusiva una tarjeta para comunicarse con ella. El protocolo de anti-colisión enumera todas las tarjetas que han respondido en base a su número de identificación única, mediante un algoritmo de búsqueda binaria. El PICC seleccionado en la fase de anti-colisión informa al PCD, con su respuesta, de qué protocolo de transporte utiliza/soporta. La Figura 3-5 muestra un ejemplo de comunicación-respuesta entre un lector (PCD) y una tarjeta (PICC) según ISO/IEC 14443-3A. En el caso del tipo B, la selección realizada por el protocolo anti-colisión se basa en el algoritmo de slots ALOHA, y las respuestas a REQB son paquetes ATQB, que contienen información adicional respecto a ATQA.

El protocolo ISO/IEC 14443-4 define el procotolo de activación y transmisión para tarjetas inteligentes sin contacto. El protocolo de activación funciona como sigue: En el caso del tipo A, el lector (PCD) manda un comando RATS a la tarjeta (PICC), quien le responde con una respuesta ***Answer-To-Select (ATS***). Esta respuesta es similar a la respuesta ATR del protocolo ISO/IEC 7816, y contiene parámetros propios del protocolo y unos ciertos bytes para identificación de producto. En el caso del tipo B, esta información adicional ya ha sido intercambiada en la respuesta ATQB.

Tras la activación, se inicia el protocolo de transmisión que es igual para ambos tipos, como se detalló anteriormente. Por ejemplo, en el caso de las tarjetas de crédito/débito con NFC, tras esta activación se produce la consulta de todas las aplicaciones disponibles en el PICC, y la selección de la aplicación de ***MasterCard PayPass*** (mediante su ID específico usando el comando ***"SELECT AID"***) que va a atender las peticiones del PCD (siendo el PCD un terminal punto de venta, por ejemplo). Un ejemplo de esta comunicación se muestra en la Figura 3-6.

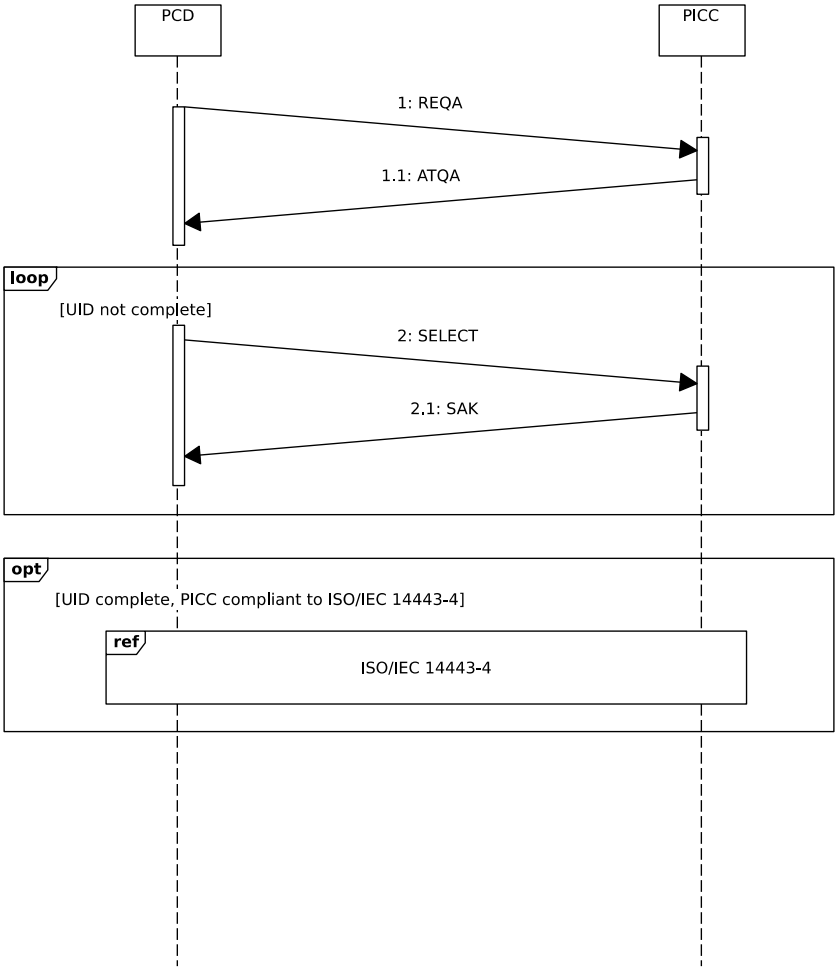


Figura 3-5. Comunicación-respuesta entre PCD y PICC según ISO/IEC 14443-3A.

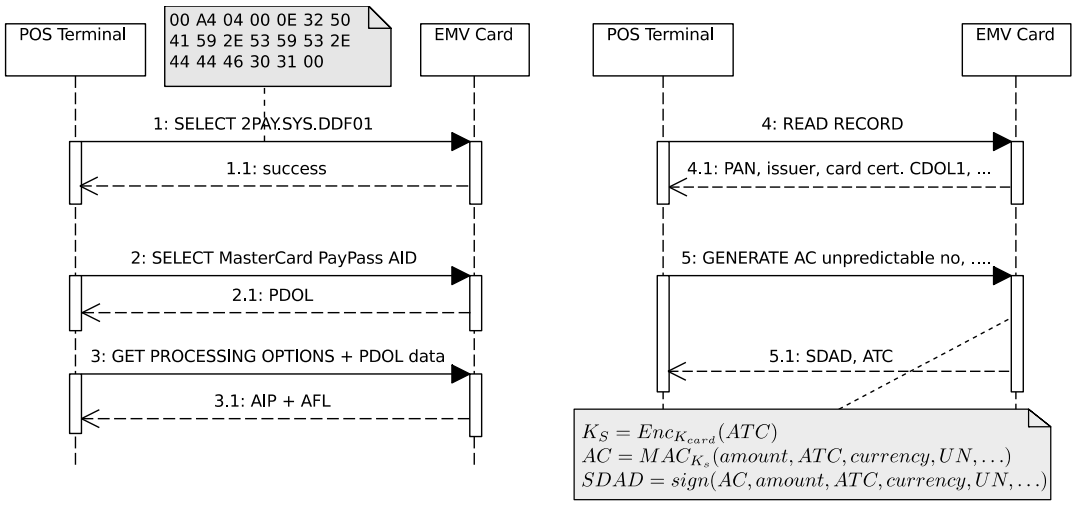


Figura 3-6. Selección de aplicación "MasterCard PayPass" en una tarjeta de crédito/débito con NFC.

Por último, el flujo de ejecución del protocolo ISO/IEC 14443-3A e ISO/IEC 14443-4 (opcional) se muestra en la Figura 3-7.

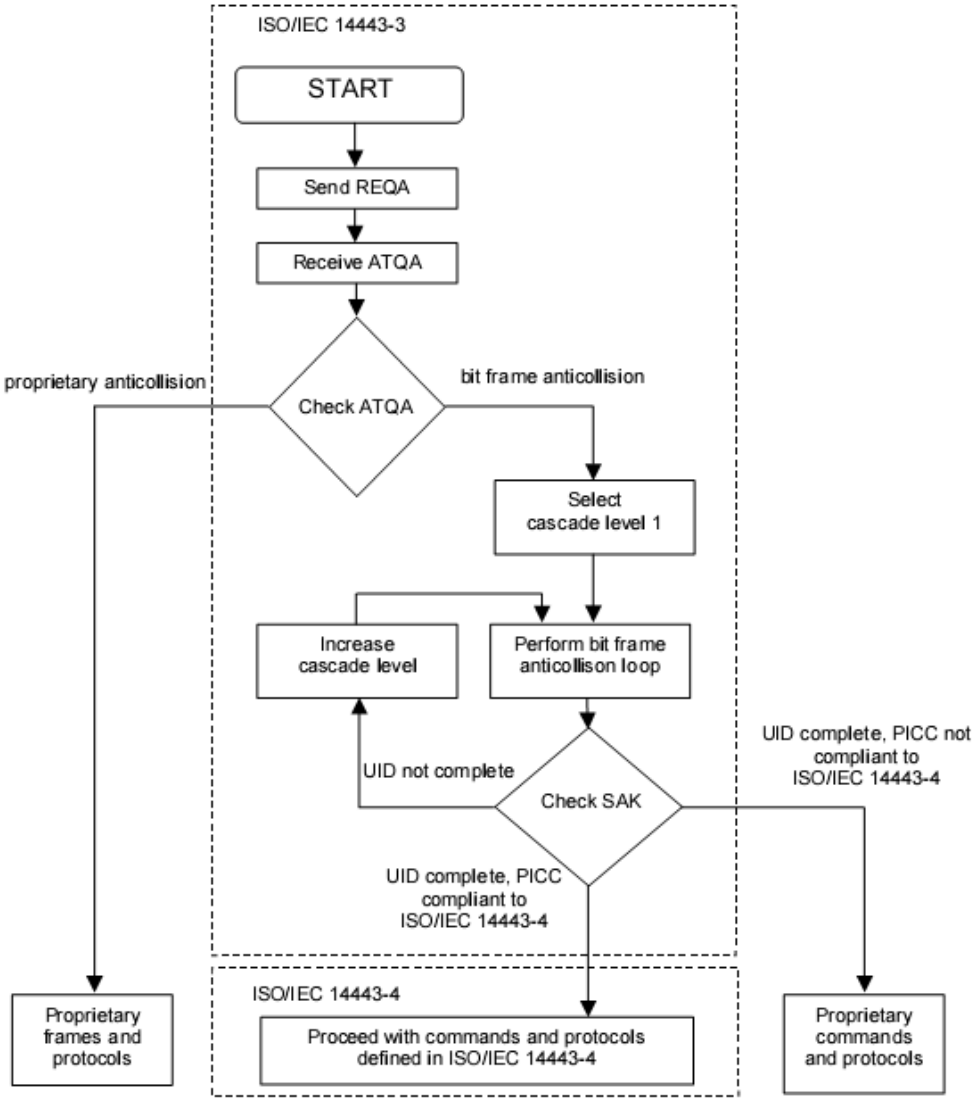


Figura 3-7. Flujo de ejecución del protocolo ISO/IEC 14443 (tipo A).

4. SEGURIDAD EN NFC

La tecnología NFC sufre de diferentes problemas de seguridad inherentes a su modo de funcionamiento, tal y como se ha demostrado en numerosos trabajos [Ref. – 9][Ref. – 10][Ref. – 11][Ref. – 12]. Estos problemas, como se resumió anteriormente, son la escucha secreta o a escondidas (**eavesdropping**, en inglés), la alteración de la información transmitida, y los ataques de retransmisión (***relay attacks***, en inglés). A continuación, se explica cada uno de estos problemas de seguridad en detalle mostrando ejemplos particulares de algunos de ellos.

4.1 Escucha secreta (*eavesdropping*)

Eavesdropping, un término inglés que se podría traducir como "escuchar secretamente o a escondidas", consiste en la capacidad de escuchar una conversación privada de terceros (cifrada o no) sin consentimiento [Ref. – 15].

Este problema de seguridad es inherente a cualquier comunicación que use ondas de radio para su transmisión. En este caso, la seguridad en NFC radica en que para poder "escuchar" la conversación entre un dispositivo lector NFC y una tarjeta o ***tag*** se ha de estar lo suficientemente cerca como para detectar los paquetes enviados por NFC. Legítimamente, **la distancia máxima** para poder comunicarse (o escuchar una comunicación) por NFC **son 10 centímetros**. Esta distancia máxima se extiende hasta 25 centímetros usando una antena de 40 centímetros de diámetro [Ref. – 16]. Sin embargo, existen estudios que demuestran cómo es posible la comunicación/escucha de tarjetas NFC a distancias mayores. Concretamente, se ha demostrado que es posible extender el rango de comunicación hasta una distancia de 100 centímetros en tarjetas NFC compatibles con ISO/IEC 14443-3A. Algunos ejemplos de tarjetas compatibles con esta tecnología son los pasaportes electrónicos, documentos de identidad electrónicos, tarjetas bancarias o tarjetas de acceso autorizado a instalaciones.

Como prueba de concepto, se van a realizar dos experimentos. En ambos experimentos se va a usar una tarjeta bancaria IsoDep tipo ISO/IEC 14443-3X y el lector/escritor RFID Proxmark3 (véase la Figura 4-1).

Figura 4-1. Elementos utilizados en el primer experimento.

En el primer experimento se va a utilizar un móvil Samsumg Galaxy Nexus ejecutando la aplicación "Credit Card Reader NFC (EMV)", disponible en Google Play (https://play.google.com/store/apps/details?id=com.github.devnied.emvnfccard&hl=en).

Esta aplicación permite leer el contenido de una tarjeta bancaria con capacidad NFC con un móvil Android que disponga de chip NFC.

Nótese que una tarjeta de crédito/débito con capacidad NFC permite leer al dispositivo lector la siguiente información sin verificar legítimamente: número de tarjeta

(impreso en el dorso, llamado ***Primary Account Number, PAN***), la fecha de expiración, titular de la tarjeta e histórico de transacciones realizadas con la tarjeta. Cabe destacar que este histórico incluye no sólo las transacciones realizadas mediante NFC, sino también las verificadas con el chip de la tarjeta. Por último, cabe destacar que los fabricantes de tarjeta están limitando al máximo la información que se filtra por NFC, evitando que las nuevas tarjetas emitan el titular y el histórico como mecanismo de privacidad.

A continuación, se muestra en la Figura 4-2 un extracto de la traza de la lectura realizada por dicha aplicación sobre la tarjeta mencionada, capturada por Proxmark3:

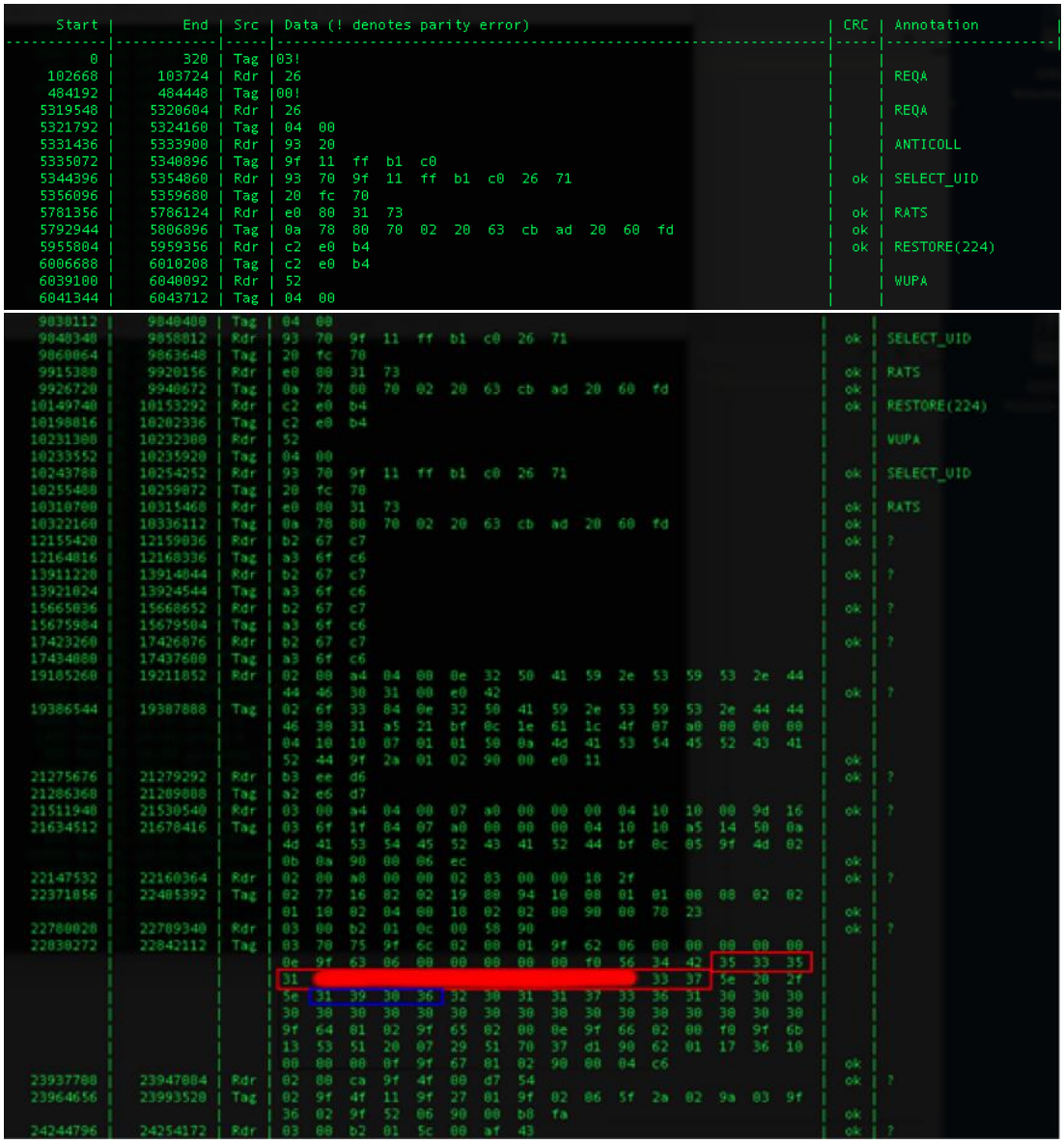


Figura 4-2. Extracto de traza de ejecución capturada con Proxmark3 (Aplicación Android "Credit Card Reader NFC (EMV)" comunicándose con tarjeta bancaria NFC).

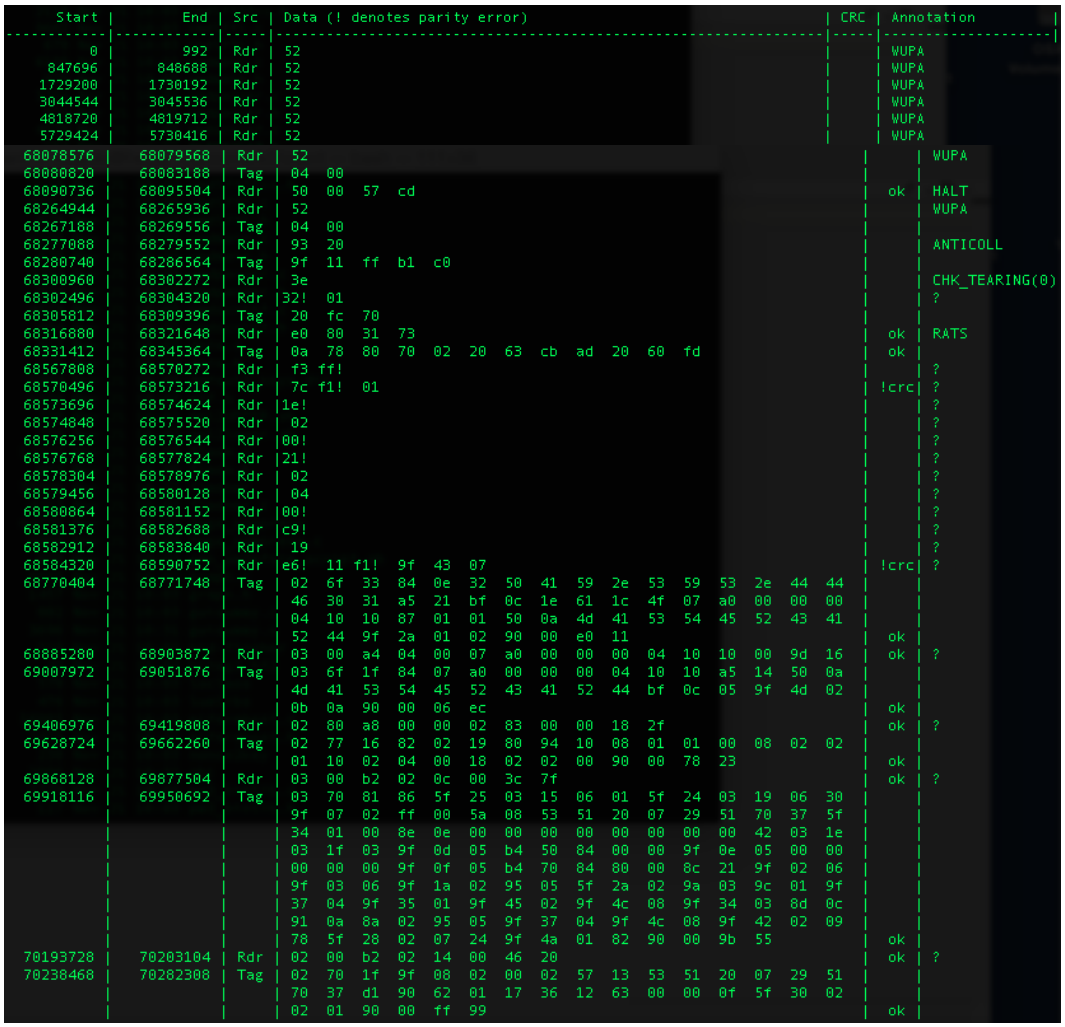
Figura 4-3. Elemento adicional utilizado en el segundo experimento: datáfono (también llamado Terminal Punto de Venta) VeriFone VX680.

Como se puede observar, los APDUs que se envían entre el dispositivo lector NFC (el móvil, en este caso) y la tarjeta no llevan ningún mecanismo de cifrado adicional, transmitiendo así la información totalmente en claro. Se ha destacado en la Figura 4-2 la parte relativa al número de tarjeta con un cuadrado rojo, y su fecha de expiración con un cuadrado azul.

En el segundo experimento se va a usar un datáfono con capacidad NFC, marca VeriFone y modelo VX680 (véase la Figura 4-3), junto con la misma tarjeta bancaria IsoDep usada en el experimento anterior. Se va a a proceder a simular un pago de 10€, capturando la traza de ejecución.

El extracto de la traza de ejecución se muestra en la Figura 4-4. Como se puede observar, todos los paquetes APDUs que se envían entre los dispositivos son interceptados. En concreto, estos APDUs siguen el protocolo de EMV-NFC definido para trabajar con tarjetas bancarias con capacidad NFC. La explicación de este protocolo y sus elementos no se detallan aquí, al considerarse fuera del ámbito del presente informe.

Obsérvese que un atacante podría explotar la comunicación con una tarjeta NFC mediante un TPV bajo su control para realizar cobros de menos de 20€ (recuérdese que menos de esta cantidad no se requiere identificación adicional), lo que supone un problema de seguridad intrínseco a la funcionalidad de micropagos mediante NFC. Del mismo modo, podrían realizarse cobros consecutivos sin identificación. Cabe destacar aquí que el número de transacciones NFC consecutivas sin identificación mediante PIN está también limitado, con lo que el fraude sufrido por el propietario de la tarjeta NFC sería (relativamente) moderado.



Start	End	Src	Data (! denotes parity error)	CRC	Annotation
0	992	Rdr	52		WUPA
847696	848688	Rdr	52		WUPA
1729200	1730192	Rdr	52		WUPA
3044544	3045536	Rdr	52		WUPA
4818720	4819712	Rdr	52		WUPA
5729424	5730416	Rdr	52		WUPA
68078576	68079568	Rdr	52		WUPA
68080820	68083188	Tag	04 00		
68090736	68095504	Rdr	50 00 57 cd	ok	HALT
68264944	68265936	Rdr	52		WUPA
68267188	68269556	Tag	04 00		
68277088	68279552	Rdr	93 20		ANTICOLL
68280740	68286564	Tag	9f 11 ff b1 c0		
68300960	68302272	Rdr	3e		CHK_TEARING(0)
68302496	68304320	Rdr	32! 01		?
68305812	68309396	Tag	20 fc 70		
68316880	68321648	Rdr	e0 80 31 73	ok	RATS
68331412	68345364	Tag	0a 78 80 70 02 20 63 cb ad 20 60 fd	ok	
68567808	68570272	Rdr	f3 ff!		?
68570496	68573216	Rdr	7c f1! 01	!crc	?
68573696	68574624	Rdr	1e!		?
68574848	68575520	Rdr	02		?
68576256	68576544	Rdr	00!		?
68576768	68577824	Rdr	21!		?
68578304	68578976	Rdr	02		?
68579456	68580128	Rdr	04		?
68580864	68581152	Rdr	00!		?
68581376	68582688	Rdr	c9!		?
68582912	68583840	Rdr	19		?
68584320	68590752	Rdr	e6! 11 f1! 9f 43 07	!crc	?
68770404	68771748	Tag	02 6f 33 84 0e 32 50 41 59 2e 53 59 53 2e 44 44		
			46 30 31 a5 21 bf 0c 1e 61 1c 4f 07 a0 00 00 00		
			04 10 10 87 01 01 50 0a 4d 41 53 54 45 52 43 41		
			52 44 9f 2a 01 02 90 00 e0 11	ok	
68885280	68903872	Rdr	03 00 a4 04 00 07 a0 00 00 00 04 10 10 00 9d 16	ok	?
69007972	69051876	Tag	03 6f 1f 84 07 a0 00 00 00 04 10 10 a5 14 50 0a		
			4d 41 53 54 45 52 43 41 52 44 bf 0c 05 9f 4d 02		
			0b 0a 90 00 06 ec	ok	
69406976	69419808	Rdr	02 80 a8 00 00 02 83 00 00 18 2f	ok	?
69628724	69662260	Tag	02 77 16 82 02 19 80 94 10 08 01 01 00 08 02 02		
			01 10 02 04 00 18 02 02 00 90 00 78 23	ok	
69868128	69877504	Rdr	03 00 b2 02 0c 00 3c 7f	ok	?
69918116	69950692	Tag	03 70 81 86 5f 25 03 15 06 01 5f 24 03 19 06 30		
			9f 07 02 ff 00 5a 08 53 51 20 07 29 51 70 37 5f		
			34 01 00 8e 0e 00 00 00 00 00 00 00 00 42 03 1e		
			03 1f 03 9f 0d 05 b4 50 84 00 00 9f 0e 05 00 00		
			00 00 00 9f 0f 05 b4 70 84 80 00 8c 21 9f 02 06		
			9f 03 06 9f 1a 02 95 05 5f 2a 02 9a 03 9c 01 9f		
			37 04 9f 35 01 9f 45 02 9f 4c 08 9f 34 03 8d 0c		
			91 0a 8a 02 95 05 9f 37 04 9f 4c 08 9f 42 02 09		
			78 5f 28 02 07 24 9f 4a 01 82 90 00 9b 55	ok	
70193728	70203104	Rdr	02 00 b2 02 14 00 46 20	ok	?
70238468	70282308	Tag	02 70 1f 9f 08 02 00 02 57 13 53 51 20 07 29 51		
			70 37 d1 90 62 01 17 36 12 63 00 00 0f 5f 30 02		
			02 01 90 00 ff 99	ok	

Figura 4-4. Extracto de la segunda traza de ejecución capturada con Proxmark3 (comunicación tarjeta de crédito/débito con capacidad NFC con Terminal Punto de Venta NFC).

4.2 Modificación de información

Dado que la información se transmite vía inalámbrica, es posible acceder y modificar la información que se está transmitiendo. Por modificación entiéndase inserción, destrucción o alteración de los APDUs que se están enviando.

En concreto, los posibles ataques que puede sufrir NFC respecto a la modificación de información son:

- **Denegación de servicio**: un atacante sería capaz de generar colisiones o respuestas erróneas durante el protocolo de anti-colisión que realiza el estándar ISO/IEC 14443, de tal modo que el lector intentará quedar vinculado a una ***tag*** no existente, consiguiendo así comprometer la disponibilidad del sistema.

- **Destrucción de la información**: un atacante puede emitir en determinada frecuencia para provocar efectos de superposición en la comunicación NFC, anulando así los paquetes APDUs legítimos que se transmiten por malformación de los mismos. Este tipo de ataques, conocidos como perturbación[9], atentan también contra la disponibilidad del sistema.
- **Modificación de la información**: un atacante puede usar la modulación de la señal para manipular un APDU. Nótese que este ataque es teóricamente posible, pero depende del mecanismo de codificación que se use en la modulación, además de que la información de un paquete APDU no puede ser arbitrariamente modificada, sino que tiene que seguir un cierto estándar. Este ataque compromete la integridad del sistema.
- **Inserción de información:** igualmente, un atacante puede generar APDUs durante una comunicación aceptada por el lector, suponiendo que el atacante es capaz de generar y enviar un APDU creado por él mismo antes de que responda el ***tag*** NFC (de otro modo, el mensaje generado por el atacante se consideraría malformado). Este ataque, como el anterior, afecta a la integridad del sistema.

4.3 Retransmisión

El ataque de retransmisión, o ataque de **relay**, supone que un atacante usa un canal de comunicación de retransmisión como un canal intermedio para incrementar el rango de comunicación. Así, se consigue que la comunicación entre un dispositivo lector NFC y una tarjeta NFC se realice a más distancia de la teóricamente posible. Este tipo de ataque requiere la cooperación de dos elementos, uno de ellos interactuando con el dispositivo lector (emulando ser la tarjeta) y otro con la tarjeta (emulando ser el dispositivo lector). Entre estos elementos se transmiten los APDUs que reciben del lector/tarjeta, y les envían la respuesta que recibe cada uno del otro elemento. Este tipo de ataque se denominó "***mafia fraud***" por Y. Desmedt en el 1988 [Ref. – 17].

Tal y como se ha demostrado en la literatura científica, los ataques de retransmisión a largas distancias son posibles [Ref. – 18][Ref. – 19][Ref. – 20]. El primer trabajo en este área [Ref. – 18] mostró que, usando hardware y software específico, se podía romper el principio de proximidad de NFC alcanzando distancias del orden de 115 cms. Esta distancia fue superada en [Ref. – 19], donde se muestra que un ataque de retransmisión en NFC a escala geográfica (del orden de cientos de kilómetros) es posible, teniendo además un retraso muy bajo en la retransmisión. En [Ref. – 20] también se realizó un ataque de retransmisión en NFC a escala geográfica, concretamente entre la ciudad de Nueva York y Madrid, realizando así un pago con una tarjeta de débito NFC ubicada en Nueva York en un datáfono ubicado en Madrid.

[9] *jamming, por su término en inglés*

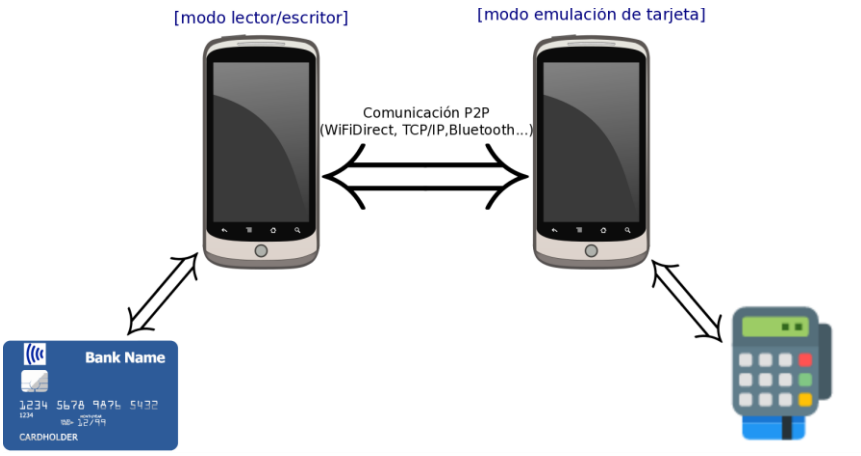


Figura 4-5. Escenario de ataque de retransmisión en NFC con dispositivos Android.

Los ataques de retransmisión en NFC se han estudiado extensivamente en la literatura [Ref. – 21][Ref. – 22][Ref. – 23][Ref. – 24][Ref. – 25][Ref. – 26][Ref. – 27][Ref. – 28][Ref. – 29]. Los primeros trabajos proponían el uso de hardware específico, o usaban dispositivos con capacidad NFC propios de la época (e.g., Nokia) atacando los elementos seguros de los dispositivos a través de interfaces Java o a través del propio dispositivo Android modificado para tener permisos de superusuario.

A partir de la versión 4.4 (***KitKat***) de Android, se incorporó la funcionalidad de emulación de tarjeta a nivel de usuario, con lo que es posible la realización de un ataque de retransmisión usando dos dispositivos Android con el sistema operativo por defecto, sin ninguna modificación adicional.

A continuación, se muestra una prueba de concepto de este ataque de retransmisión usando los siguientes elementos:

- Dos móviles Android, uno de ellos con versión 4.4 (en modo emulación de tarjeta) y otro con versión 4.3 (en modo lector/escritor).
- Datáfono con capacidad NFC.
- Tarjeta de crédito/débito con capacidad NFC.
- Aplicación desarrollada (menos de 2000 LOC[10]).

La configuración del experimento es la que se muestra la Figura 4-5: el dispositivo Android (versión 4.3) interactuará con la tarjeta NFC, mientras que el otro dispositivo (versión 4.4) interactúa con el datáfono. Así, realizando un pago de 0.01 céntimos de euro, la traza de comunicación completa entre el datáfono y la tarjeta que se ha realizado es la siguiente:

[10] *Líneas de código (Lines of CodeLOC)*

00A404000E325041592E5359532E444446303100
SELECT
6F30840E325041592E5359532E4444463031A51EBF0C1B61194F08A000000004101002500A4D41535445524341524487010190000
6f 30 -- File Control Information (FCI) Template
84 0e -- Dedicated File (DF) Name
32 50 41 59 2e 53 59 53 2e 44 44 46 30 31 (BINARY)
a5 1e -- File Control Information (FCI) Proprietary Template
bf 0c 1b -- File Control Information (FCI) Issuer Discretionary Data
61 19 -- Application Template
4f 08 -- Application Identifier (AID) - card
a0 00 00 00 04 10 10 02 (BINARY)
50 0a -- Application Label
4d 41 53 54 45 52 43 41 52 44 (=MASTERCARD)
87 01 -- Application Priority Indicator
01 (BINARY)
90 00 -- Issuer Public Key Certificate
(BINARY)

00A4040008A00000000410100200
SELECT
6F208408A000000004101002A514870101500A4D41535445524341524452F2D0263619000
6f 20 -- File Control Information (FCI) Template
84 08 -- Dedicated File (DF) Name
a0 00 00 00 04 10 10 02 (BINARY)
a5 14 -- File Control Information (FCI) Proprietary Template
87 01 -- Application Priority Indicator
01 (BINARY)
50 0a -- Application Label
4d 41 53 54 45 52 43 41 52 44 (=MASTERCARD)
5f 2d 02 -- Language PRef.erence
63 61 (=ca)
90 00 -- Issuer Public Key Certificate
(BINARY)

80A8000002830000
GET PROCESSING OPTIONS
771682021880941008010100100101001801020020010200900 0
77 16 -- Response Message Template Format 2
82 02 -- Application Interchange Profile
18 80 (BINARY)
94 10 -- Application File Locator (AFL)
08 01 01 00 10 01 01 00 18 01 02 00 20 01 02 00 (BINARY)
90 00 -- Issuer Public Key Certificate
(BINARY)

00B2011400
READ RECORD
7081935713<priv>5A08<priv>5F2403<priv>5F280207245F3401018C219F02069F03069F1A0295055F2A029A039C019F37049F35019F45029F4C089F34038D0C910A8A0295059F37049F4C088E0C000000000000000004203 1F039F07023D009F080200029F0D05B050AC80009F0E0500000000009F0F05B070AC98009F4A01829000
70 81 93 -- Record Template (EMV Proprietary)
57 13 -- Track 2 Equivalent Data
<priv>
(BINARY)
5a 08 -- Application Primary Account Number (PAN)
54 02 05 38 79 35 20 13 (NUMERIC)
5f 24 03 -- Application Expiration Date
<priv> (NUMERIC)
5f 28 02 -- Issuer Country Code
07 24 (NUMERIC)
5f 34 01 -- Application Primary Account Number (PAN) Sequence Number
01 (NUMERIC)
8c 21 -- Card Risk Management Data Object List 1 (CDOL1)
9f 02 06 -- Amount, Authorised (Numeric)
9f 03 06 -- Amount, Other (Numeric)

9f 1a 02 -- Terminal Country Code
95 05 -- Terminal Verification Results (TVR)
5f 2a 02 -- Transaction Currency Code
9a 03 -- Transaction Date
9c 01 -- Transaction Type
9f 37 04 -- Unpredictable Number
9f 35 01 -- Terminal Type
9f 45 02 -- Data Authentication Code
9f 4c 08 -- ICC Dynamic Number
9f 34 03 -- Cardholder Verification (CVM) Results
8d 0c -- Card Risk Management Data Object List 2 (CDOL2)
91 0a -- Issuer Authentication Data
8a 02 -- Authorisation Response Code
95 05 -- Terminal Verification Results (TVR)
9f 37 04 -- Unpredictable Number
9f 4c 08 -- ICC Dynamic Number
8e 0c -- Cardholder Verification Method (CVM) List
00 00 00 00 00 00 00 00 42 03 1f 03 (BINARY)
9f 07 02 -- Application Usage Control
3d 00 (BINARY)
9f 08 02 -- Application Version Number - card
00 02 (BINARY)
9f 0d 05 -- Issuer Action Code - Default
b0 50 ac 80 00 (BINARY)
9f 0e 05 -- Issuer Action Code - Denial
00 00 00 00 00 (BINARY)
9f 0f 05 -- Issuer Action Code - Online
b0 70 ac 98 00 (BINARY)
9f 4a 01 -- Static Data Authentication Tag List
82 (BINARY)
90 00 -- Issuer Public Key Certificate
(BINARY)

00B2011C00
READ RECORD
7081C28F01059F320301000192043DD025199081B03445…629000
70 81 c2 -- Record Template (EMV Proprietary)
8f 01 -- Certification Authority Public Key Index - card
05 (BINARY)
9f 32 03 -- Issuer Public Key Exponent
01 00 01 (BINARY)
92 04 -- Issuer Public Key Remainder
3d d0 25 19 (BINARY)
90 81 b0 -- Issuer Public Key Certificate
34 45 … 62 (BINARY)
90 00 -- Issuer Public Key Certificate
(BINARY)

00B2021C00
READ RECORD
7081B39381B03445…629000
70 81 b3 -- Record Template (EMV Proprietary)
93 81 b0 -- Signed Static Application Data
34 45 … 62 (BINARY)
90 00 -- Issuer Public Key Certificate
(BINARY)

00B2012400
READ RECORD
70339F47030100019F482A3E…6D9000
70 33 -- Record Template (EMV Proprietary)
9f 47 03 -- ICC Public Key Exponent
01 00 01 (BINARY)
9f 48 2a -- ICC Public Key Remainder
3e … 6d (BINARY)
90 00 -- Issuer Public Key Certificate

(BINARY)

00B2022400
READ RECORD
7081949F46819018…F59000
70 81 94 -- Record Template (EMV Proprietary)
9f 46 81 90 -- ICC Public Key Certificate
18 … f5 (BINARY)
90 00 -- Issuer Public Key Certificate
(BINARY)

80AE80002B0000000000010000000000007248000008000097815022400 37FB88BD2200000000000000000000001F030200
GENERATE APPLICATION CRYPTOGRAM
77299F2701XX9F3602XXXX9F2608XXXXXXXXXXXXXXXX9F1012XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX9000
77 29 -- Response Message Template Format 2
9f 27 01 -- Cryptogram Information Data
XX (BINARY)
9f 36 02 -- Application Transaction Counter (ATC)
XX XX (BINARY)
9f 26 08 -- Application Cryptogram
XX XX XX XX XX XX XX XX (BINARY)
9f 10 12 -- Issuer Application Data
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
(BINARY)
90 00 -- Issuer Public Key Certificate
(BINARY)

Se ha representado en negrita el comando APDU (enviado por el terminal a la tarjeta), y en cursiva la respuesta APDU (enviada por la tarjeta al terminal), además de detallar el contenido del mensaje. Nótese que esta traza es equivalente a la que se pudiera haber obtenido usando un dispositivo de escucha como el ***Proxmark3***, usado anteriormente. Por último, destacar que en la traza de comunicación se ha omitido información sensible de la tarjeta, susceptible de poder ser víctima de fraude. Un vídeo de la prueba de concepto desarrollada se puede encontrar en: http://webdiis.unizar.es/~ricardo/?p=598

Por último, cabe destacar que un ataque de retransmisión en NFC será siempre posible e independiente de la confidencialidad de los paquetes APDU si el canal de retransmisión que se use tiene una latencia baja. En concreto, este tiempo viene especificado por la fórmula de ***Frame Waiting Time (FWT)***, definida en ISO/IEC 14443-4 [Ref. – 1]: $\mathrm{FWT} = 256 \cdot (16/f_c) \cdot 2^{FWI}, 0 \leq \mathrm{FWI} \leq 14$, donde $f_c = 13.56$ MHz. Es decir, FWT varía entre **$500\mu s$ to $5s$**. Por lo tanto, **un ataque de retranmisión en NFC e ISO/IEC 14443-4 es posible cuando el retraso del canal de retranmisión es inferior a 5 segundos.**

5. CONTRAMEDIDAS

En esta sección se detallan aquellas contramedidas que se pueden aplicar en un sistema NFC para evitar los ataques presentados anteriormente.

Diversos experimentos, como los realizados aquí, muestran que un ataque de escucha secreta ***(eavesdropping)*** es posible hasta distancias de 30 ó 40 centímetros [Ref. – 16]. Esta limitación en distancia claramente supone una desventaja para un atacante, que tendría dificultad para ocultarse él mismo o su equipo de escucha. Sin embargo, en lugares donde hubiera mucha gente (e.g., horas punta en metros o cercanías) o comercios controlados por actores dañinos u organizaciones delictivas este tipo de ataque es posible. Para evitarlo, **se recomienda el uso de tarjeteros o carteras que bloqueen la comunicación RFID**, permitiendo esta únicamente cuando se extrae la tarjeta de su funda. Otras medidas físicas también se pueden aplicar, como tarjetas con botón de activación, activación desde un segundo dispositivo o aplicación móvil, o métodos de autentificación secundarios en la propia tarjeta (por ejemplo, incluyendo un escáner de huellas dactilares).

El uso de mecanismos de cifrado en la comunicación también puede evitar el problema de escucha secreta. Se recomienda no optar por esquemas criptográficos propietarios **(seguridad por oscuridad)** y acudir a esquemas criptográficos de eficacia reconocida, como ***RSA***, ***3DES,*** o cualquier otro (***CC-EAL4***[11]***)*** como mínimo. El uso de criptografía en una comunicación NFC desde luego ayudará a fortalecer la confidencialidad del sistema.

Existen numerosas propuestas [Ref. – 9] [Ref. – 22] [Ref. – 25] para evitar los ataques de retransmisión, como los protocolos de cota de distancia, restricciones temporales, o identificación de hardware específico. Los protocolos de cota de distancia tratan de establecer una cota superior a la distancia física entre dos entidades que se comunican usando el ***Round-Trip-Time (RTT)*** de los mensajes de desafío-respuesta criptográficos. Una buena implementación de estos protocolos pueden proveer un mecanismo de defensa adecuado contra los ataques de retransmisión. Sin embargo, en ciertos escenarios como por ejemplo aplicaciones móviles bancarias que realizan ellas mismas, una comunicación con los servidores de la entidad financiera a través de Internet **se introduce un retardo "permitido" en la comunicación**. Este hecho pone de manifiesto la dificultad de distinguir entre una transacción retransmitida legítima o ilegítima.

Imponer restricciones temporales en la comunicación para detectar retrasos puede ser un buen mecanismo de detección de canales de retransmisión. Sin embargo, el propio protocolo ISO/IEC 14443-4 dispone de comandos específicos para solicitar extensiones de tiempo en la comunicación (usados por aplicaciones NFC que necesitan instrucciones criptográficas de alta complejidad), lo que puede resultar problemático. Imponer estas restricciones puede ayudar a evitar escenarios de ataque donde el canal de retranmisión tiene una alta latencia.

[11] *Producto evaluado y certificado con un nivel 4 de confianza en la evaluación de los Criterios Comunes (Common Criteria Evaluation Assurance Level 4 CC-EAL4)*

Los dispositivos NFC emplean un identificador único generado aleatoriamente cuando se encuentran en modo emulación de tarjeta. Se podría, por tanto, realizar un filtrado de los identificadores permitidos en ciertos escenarios. Esta solución, sin embargo, no sería extrapolable a grandes sistemas como los sistemas de pago móvil NFC, donde el identificador único no es posible conocerlo con anterioridad.

Figura 5-1. Menú de ajustes del sistema operativo Android en donde se puede activar/desactivar NFC

También es posible, como contramedida desde el punto de vista del usuario, **deshabilitar la comunicación NFC en el dispositivo Android del usuario**. Nótese que esto no inhabilitaría la posibilidad de que un usuario instalara, por desconocimiento, una aplicación maliciosa con permiso de activación o desactivación de NFC. En concreto, esta aplicación requerirá los permisos *NFC* y ***WRITE_SECURE_SETTINGS***, así como usar refllexión para conseguir realizar con éxito la activación/desactivación de NFC. En la Figura 5-1 se muestra la opción del menú del sistema operativo Android en donde se puede activar/desactivar NFC. Esta opción se encuentra en "Ajustes", "Más…", "NFC".

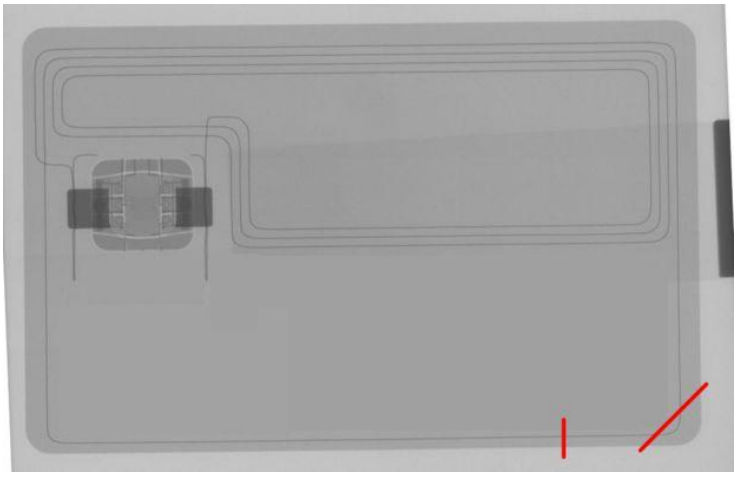


Figura 5-2. Ejemplo de radiografía de tarjeta con chip NFC, y dónde realizar los cortes (o perforaciones) para inhabilitar la comunicación NFC (extraído de http://www.instructables.com/id/Disabling-Contacless-Payment-on-Debit-Cards).

Como última contramedida que puede usar el usuario final, más drástica que todas las anteriores, es la destrucción de la antena de una tarjeta bancaria con chip NFC. Dado el funcionamiento inductivo de NFC, si se daña la antena el chip NFC no será capaz de recibir la energía suficiente como para poder realizar una comunicación NFC. Para ello, habría que primero localizar dónde se encuentra (por ejemplo, mediante un análisis de rayos X) y segundo, realizar una perforación en la tarjeta. Un ejemplos de radiografía de una tarjeta NFC, con el objetivo de localizar su antena, así como de dónde realizar un corte (o dónde perforar) se muestran en la Figura 5-2.

6. CONCLUSIONES

La comunicación de campo cercano o ***Near Field Communication (NFC),*** es una tecnología de comunicación inalámbrica bidireccional de corto alcance (hasta 10 centímetros) basada en diferentes protocolos de RFID. NFC fue desarrollada como una evolución que auna las tecnologías RFID inductivas y las tarjetas inteligentes. NFC opera en el espectro de alta frecuencia 13.56MHz y soporta diferentes ratios de tranmisión de información: 106, 216 y 424 kbps. La tecnología NFC tiene multitud de aplicaciones, como identificación de elementos, uso de transporte público, acceso a edificios controlados, o pagos bancarios con tarjeta (cantidades limitadas, según moneda y país, hasta un máximo sin requerir ningún tipo de identificación – por ejemplo, en España la cantidad máxima que se puede pagar mediante NFC sin petición de PIN son 20€).

Esta rápida penetración de la tecnología NFC en diferentes dominios pone de manifiesto el interés por la misma. Sin embargo, NFC se basa en un principio de comunicación en el campo cercano (rango limitado) que no se cumple, lo que deja la tecnología vulnerable ante posibles ataques a su confidencialidad, integridad y disponibilidad.

En concreto, los problemas de seguridad que sufre NFC son la escucha secreta o a escondidas (**eavesdropping,** en inglés), la alteración de la información transmitida, y los ataques de retransmisión (**relay attacks**, en inglés). Cabe destacar que las vulnerabilidades destacadas en este informe son inherentes a la propia tecnología NFC, con lo que cualquier sistema que se implemente sobre NFC heredará estos problemas.

En este documento se han detallado las vulnerabilidades, mostrando diversos escenarios de ataque como prueba de concepto. Del mismo modo, se han resumido las posibles soluciones frente a estos ataques. Por último, cabe recordar que la tecnología NFC está cada vez más presente en los dispositivos móviles, lo que evidencia que más tarde o más temprano empezarán a ser usados como vector de ataque.

7. CONTACTO

Se puede ampliar cualquier punto del informe, utilizando como vía preferente de comunicación el portal http://www.ccn-cert.cni.es

- Teléfono: +34 91372 59 74
- E-Mail: ccn-cert@cni.es

ANEXO A. REFERENCIAS

[Ref. – 1]	**ISO/IEC 14443-3: Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 3: Initialization and anticollision** Estándar ISO Abril 2011 http://www.iso.org/iso/catalogue_detail.htm?csnumber=50942
[Ref. – 2]	**JIS X 6319-4:2010: Specification of implementation for integrated circuit(s) cards -- Part 4: High speed proximity cards** Estándar JIS Octubre 2010 http://www.webstore.jsa.or.jp/webstore/PrevPdfServlet?dc=JIS&fn=pre_jis_x_06319_004_000_2010_e_ed10_i4.pdf
[Ref. – 3]	**NFC Forum** Página web de asociación industrial http://www.nfc-forum.org/
[Ref. – 4]	**ISO/IEC 18092:2013: Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1)** Estándar ISO Marzo 2013 http://www.iso.org/iso/catalogue_detail.htm?csnumber=56692
[Ref. – 5]	**FinExtra: "The year 2014 was a tipping point for NFC payments"** Nota de prensa Enero 2015 http://www.finextra.com/blogs/fullblog.aspx?blogid=10382
[Ref. – 6]	**Juniper Research Limited: "Apple Pay and HCE to Push NFC Payment Users to More Than 500 Million by 2019"** Nota de prensa Octubre 2014 http://www.marketwired.com/press-release/apple-pay-hce-push-nfc-payment-users-more-than-500-million-2019-juniper-research-finds-1961558.htm
[Ref. – 7]	**NFC World: "NFC phones: The definitive list"** Página web http://www.nfcworld.com/nfc-phones-list/
[Ref. – 8]	**Secure ID news: "NFC is the bridge from cards to the mobile"** Nota de prensa Enero 2015 http://www.secureidnews.com/news-item/nfc-is-the-bridge-from-cards-to-the-mobile/

[Ref. – 9]	**"Security in Near Field Communication (NFC) -- Strengths and Weaknesses" (E. Haselsteiner & K. Breitfuß)** Contribución de congreso RFID Security and Privacy (RFIDSec) 2006 http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf
[Ref. – 10]	**"NFC Devices: Security and Privacy" (G. Madlmayr, J. Langer, C. Kantner & J. Scharinger)** Contribución de congreso Availability, Reliability and Security (ARES) 2008 http://dx.doi.org/10.1109/ARES.2008.105
[Ref. – 11]	**"Practical Experiences with NFC Security on mobile Phones" (G. Van Damme & K. Wouters)** Contribución de congreso RFID Security and Privacy (RFIDSec) 2009 https://www.cosic.esat.kuleuven.be/publications/article-1288.pdf
[Ref. – 12]	**"NFC and Its Application to Mobile Payment: Overview and Comparison" (C. Oak)** Contribución de congreso Information Science and Digital Content Technology (ICIDT) 2012 http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6269257
[Ref. – 13]	**ISO/IEC 7816-4-2013: Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange** Estándar ISO 2013 http://www.iso.org/iso/catalogue_detail.htm?csnumber=54550
[Ref. – 14]	**"Security Issues in Mobile NFC Devices" (M. Roland)** Libro 2015 http://www.springer.com/gp/book/9783319154879
[Ref. – 15]	**Eavesdropping (Wikipedia)** Página web Enero 2016 https://en.wikipedia.org/wiki/Eavesdropping
[Ref. – 16]	**"An RFID Skimming Gate Using Higher Harmonics" (R. Habraken, P. Dolron, E. Poll, J. de Ruiter)** Contribución de congreso RFID: Security and Privacy (RFIDSec) Junio 2015 http://dx.doi.org/10.1007/978-3-319-24837-0_8

[Ref. – 17]	**"Major security problems with the "unforgeable" (Feige-)Fiat-Shamir proofs for identity and how to overcome them" (Y. Desmedt)** Contribución de congreso Computer and Communications Security and Protection (SecuriComm) 1988
[Ref. – 18]	**"Range Extension Attacks on Contactless Smart Cards" (Y. Oren, D. Schirman & A. Wool)** Contribución de congreso European Symposium on Research in Computer Security (ESORICS) 2013 http://dx.doi.org/10.1007/978-3-642-40203-6_36
[Ref. – 19]	**Long Distance Relay Attack (L. Sportiello & A. Ciardulli)** Contribución de congreso RFID: Security and Privacy (RFIDSec) 2013 http://dx.doi.org/10.1007/978-3-642-41332-2_5
[Ref. – 20]	**"Practical Experiences on NFC Relay Attacks with Android: Virtual Pickpocketing Revisited" (J. Vila & R. J. Rodríguez)** Contribución de congreso RFID: Security and Privacy (RFIDSec) Junio 2015 http://dx.doi.org/10.1007/978-3-319-24837-0_6
[Ref. – 21]	**"Picking Virtual Pockets using Relay Attacks on Contactless Smartcard" (Z. Kfir & A. Wool)** Contribución de congreso Security and Privacy for Emerging Areas in Communications Networks (SecureComm) 2005 http://dx.doi.org/10.1109/SECURECOMM.2005.32
[Ref. – 22]	**"Confidence in smart token proximity: Relay attacks revisited" (G. Hancke, K. Mayes & K. Markantonakis)** Artículo de revista científica Computers & Security 2009 http://dx.doi.org/10.1016/j.cose.2009.06.001
[Ref. – 23]	**"Practical NFC Peer-to-Peer Relay Attack Using Mobile Phones" (Francis, L.; Hancke, G.; Mayes, K. & Markantonakis, K.)** Contribución de congreso RFID: Security and Privacy (RFIDSec) 2010 http://dx.doi.org/10.1007/978-3-642-16822-2_4
[Ref. – 24]	**"Practical Attacks on NFC Enabled Cell Phones" (R. Verdult & F. Kooman)** Contribución de congreso Near Field Communication (NFC) 2011 http://dx.doi.org/10.1109/NFC.2011.16

[Ref. – 25]	**"Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones" (L. Francis, G. Hancke, K. Mayes & K. Markantonakis)** Contribución de congreso RFID and IoT Security (RFIDsec 2012 Asia) 2012
[Ref. – 26]	**"Practical Attack Scenarios on Secure Element-Enabled Mobile Devices" (M. Roland, J. Langer & J. Scharinger)** Contribución de congreso Near Field Communication (NFC) Marzo 2012 http://dx.doi.org/10.1109/NFC.2012.10
[Ref. – 27]	**"Relay Attacks on Secure Element-Enabled Mobile Devices" (M. Roland, J. Langer & J. Scharinger)** Contribución de congreso Information Security and Privacy Conference (IFIP SEC) 2012 http://dx.doi.org/10.1007/978-3-642-30436-1_1
[Ref. – 28]	**"Applying Relay Attacks to Google Wallet" (M. Roland, J. Langer & J. Scharinger)** Contribución de congreso Near Field Communication (NFC) Febrero 2013 http://dx.doi.org/10.1109/NFC.2013.6482441
[Ref. – 29]	**"On the Power of Active Relay Attacks using Custom-Made Proxies" (T. Korak & M. Hutter)** Contribución de congreso IEEE RFID Abril 2014 http://dx.doi.org/10.1109/RFID.2014.6810722