Nuevos retos de seguridad en dispositivos NFC

Dr. Juan Mir
Responsable de Infraestructuras de Seguridad Informática
GMV Soluciones Globales Internet S.A.U.
Email: jmir@gmv.com

***Resumen*—Las comunicaciones NFC (Near Field Communication) actualmente son "trending topic" en el mundo de la tecnología. Los dispositivos móviles de última generación empiezan a incorporar de serie la tecnología NFC, que permite comunicaciones inalámbricas de corto alcance.**

Esto abre un gran abanico a todo tipo de aplicaciones en todos los sectores, aplicaciones que se volverán más usables e intuitivas para los usuarios, y que, conjuntamente con la disponibilidad de conectividad por Internet en los móviles, se podrán ofrecer servicios no vistos hasta ahora.

La explosión de aplicaciones NFC en los próximos años está asegurada, pero también sus ataques con altas repercusiones, lo que ofrece nuevos retos tecnológicos a proteger con recursos limitados (capacidad computacional, consumo eléctrico, memoria y almacenamiento limitados). En este artículo presentamos la tecnología NFC y recogemos tanto las principales amenazas como algunas primeras soluciones, pero hay un gran camino a recorrer.

I. Introducción

En los últimos años, la tecnología de tarjetas sin contacto ha ido madurando y han sido adoptadas por los principales sectores. Paralelamente, los nuevos teléfonos móviles con las ofertas adicionales de servicios de Internet y multimedia han entrado con éxito en los estilos de vida de las personas. Esto hace que la tecnología de tarjetas sin contacto pueda ampliar su ámbito de aplicación mediante la adición de las funcionalidades del teléfono móvil, pero para hacerlo hace falta una comunicación entre ambos dispositivos, y aquí surge la tecnología NFC (Near Field Communication). La tecnología NFC permite hacer interacciones entre los dispositivos de manera muy simple e intuitiva.

II. Tecnología NFC

Desarrollada a partir de la unión de Phiplips y Sony en el 2002 [1], la tecnología NFC es una tecnología basada en el RFID (Radio Frequency Identification) que permite la comunicación inalámbrica entre dispositivos que no estén a una distancia superior a 10 centímetros, a una velocidad moderada y de forma activa o pasiva (en este segundo caso el dispositivo receptor no dispone de fuente de alimentación).

La tecnología NFC ha sido consolidada gracias al NFC Fórum [2] en estándares claramente definidos como el NFC-Interface Protocolo 1 (que recoge el ISO/IEC 18.092, el ECMA-340 y el ETSI 102 190) [3], y luego por NFC-Interface Protocolo 2 (que recoge el ISO/IEC 21481 y el ECMA-352) [4]. Además, también ofrece compatibilidad con los estándares de tarjetas sin contacto ISO/IEC 14443 tipo A y tipo B [5], y el ISO/IEC 15693 (Standard Vacinity Card) [6].

Pero, a parte de tener protocolos estandarizados, hace falta seguridad en las comunicaciones NFC y en las aplicaciones móviles, y este es un terreno por explorar lleno de grandes retos.

Prueba de ello son las noticias de vulnerabilidades que se están publicando en este 2012 sobre las soluciones de pago que utilizan NFC y dispositivos móviles [11].

El estándar también define los modelos de comunicación física. Los dispositivos NFC pueden comunicarse de forma pasiva o de forma activa. Generalmente se utiliza la modalidad pasiva, donde en la comunicación RFID uno de los dispositivos actúa como un lector (iniciador) y el otro como una etiqueta pasiva (de destino o "passive tag"). El dispositivo lector debe tener una fuente de alimentación y generar un campo de inducción magnética que alcance la etiqueta. La etiqueta, utilizando la energía por inducción, modula el campo generado dando una respuesta. Cuando las comunicaciones son en forma activa ambos dispositivos disponen de una fuente de alimentación interna y cada uno genera su propio campo de forma alterna para generar la comunicación (después de comunicar cierran siempre el campo para esperar la respuesta del otro dispositivo). Este modelo permite velocidades que pueden llegar hasta 6,78 Mbit/s.

II-A. Tipos de comunicación

El protocolo 2 de comunicaciones NFC (NFCIP-2) integra el NFCIP-1 y a los estándares de tarjetas sin contacto que ya existían previamente, el ISO/IEC 14443 tipo A y tipo B [5], que es el utilizado por las tarjetas de proximidad sin contacto, como la NXP Mifare[12], y el ISO/IEC 15693 [6] que es el utilizado para las tarjetas Vacinity que permiten una comunicación a mayor distancia (de hasta 1 o 1,5 metros). Los dispositivos que cumplan el NFCIP-2, deberían ser compatibles con aquellos dispositivos que comuniquen a 13,56 MHz. A parte, este estándar recoge los mecanismos para detectar y seleccionar un tipo de comunicación entre los dispositivos a conectarse, remarcando tres soluciones:

- **Card Emulation Mode**: Donde el dispositivo NFC actúa como una tarjeta NFC sin contacto pasiva, emulando una smart card. Como dispositivo pasivo no debe generar ningún campo de radio frecuencia.
- **Reader/Writer Mode**: El dispositivo NFC actúa como un lector de tarjetas activo, por lo que generará un campo de RF para comunicarse con otros dispositivos como tarjetas sin contacto, etiquetas RFID (tags) o otros dispositivos RFC.

- **Peer to Peer Mode**: Dos dispositivos NFC se comunicaran entre ellos, ya sea de forma activa o pasiva. Sujetos al modelo de maestro/esclavo, el iniciador o maestro inicia la transferencia de datos mientras que el objetivo o receptor esclavo espera para dar la respuesta.

II-B. Especificaciones

Tag types
El foro NFC ha especificado cuatro tipos de tags llamados "type 1, 2, 3, y 4" conforme a las diferentes normas existentes, de tarjetas sin contacto, como la norma ISO 14443, ISO 14443B y JIS X 6319-4 (FeliCa). Las especificaciones contienen la información técnica necesaria para los fabricantes de dispositivos NFC para implementar la funcionalidad necesaria para interactuar con las diferentes etiquetas, así como para los proveedores de etiquetas NFC para poder crear etiquetas compatibles.

NDEF Message
La especificación técnica del formato de intercambio de datos NFC (NDEF) especifica el formato de los mensajes intercambiados entre los dispositivos o etiquetas NFC. La especificación cubre únicamente el formato de datos y asume un protocolo subyacente de transporte fiable y por lo tanto no cubre los detalles de comunicación. Los mensajes que se intercambian son los llamados mensajes NDEF y contiene uno o más registros NDEF.

Registros NDEF
Un registro NDEF contiene la información descrita por un tipo. El nombre del tipo puede ser de diferentes formatos, tales como los medios de comunicación de tipo (MIME, RFC2046), un URI, un URN o un tipo de RTD (Record Type Definition) especificado como:

- **NFC Text RTD** Un formato compacto para la inclusión de texto plano con soporte para diferentes idiomas.
- **NFC URI RTD** Un formato compacto para la inclusión de identificadores unificados de recursos (URI) en las etiquetas. Prefijos típicos, tales como nombres de protocolo se abrevian con el fin de ahorrar espacio.
- **NFC Generic Control RTD** Define una manera de solicitar una acción específica para llevar a cabo en un dispositivo NFC. Por ejemplo, podría indicar si una URL se debe abrir o si se debe guardar para ser utilizada más adelante como un marcador, etc.
- **NFC Smart Poster RTD** El registro del cartel inteligente es un contenedor de un Registro de URI y los metadatos asociados, tales como un título en la forma de un registro de texto, un registro de un icono, un tamaño de registro, un registro y un registro de tipo de acción recomendada a realizar con una URI.

Tarjetas/etiquetas/tags	Capacidad
Mifare Ultralight	48 bytes
Innovision Topaz	96 bytes
Innovision Jewel	96 bytes
Mifare Ultralight C	192 bytes
Mifare Mini	320 bytes
Sony FeliCa (RC-S890 IC-token)	496 bytes
Mifare 1k	720 bytes
Sony FeliCa (RC-S885 card)	2464 bytes
Sony FeliCa (RC-S860 card)	2464 bytes
Mifare 4k	3480 bytes
Mifare Plus	3480 bytes
Mifare DESFire	2k, 4k bytes
Sony FeliCa (RC-S880 card)	6400 bytes
Mifare DESFire EV1	2k, 4k, 8k bytes

Tabla 1. Conjunto de targetas y etiquetas, y su capacidad.

Dispositivos móviles NFC
Actualmente se dispone de una gama aceptable de dispositivos móviles en el mercado, y en las principales tecnologías, a excepción de Apple (iPhone) que se rumorea que saldrá en breve. A continuación recogemos una pequeña tabla.

SO	**Modelo**
Android	Nexus S1 Google Nexus S 4G2 Galaxy Nexus by Samsung3 Samsung Galaxy S II (no todas las versiones)4 Samsung Galaxy Note (no todas las versiones) Galaxy Nexus5 HTC Amaze 4G Turkcell T20.6 Sony Xperia S HTC One X Panasonic Eluga
Ovi store/S40	J2ME Nokia 6212 Classic7 Nokia 6131 NFC8 Nokia 3220 + NFC Shell11 Nokia 5140(i) + NFC Shell12
Ovi store/S60	J2ME Nokia 603 Nokia 610 14 Nokia 700 Nokia 701 Nokia C7
BlackBerry	Blackberry Bold 9790 BlackBerry Bold 9900/9930 BlackBerry Torch 9810/986021 22 Blackberry Curve 9350/9360/9370/9380
Windows Mobile 6.0	Benq T8011
Windows Phone 7	Nokia Lumia 610 NFC 23

Tabla 2. Dispositivos móviles con NFC

Desgraciadamente, no todas las soluciones utilizan el mismo chip (como es el caso de Japón donde todos los dispositivos trabajan con Felica), por lo que la interoperabilidad es un punto pendiente a ser analizado.

III. Componentes y seguridad en los dispositivos móviles

El listado de teléfonos móviles disponibles con NFC no para de crecer, y es el foco principal de desarrollo de la industria. Dejando de lado los detalles generales de las características de telefonía de cada dispositivo, para analizar los aspectos de seguridad para NFC nos hemos de centrar en los tres componentes principales:

- **Entorno de ejecución de las aplicaciones** (Aplicación Execution Environment - AEE): Es el área donde el teléfono móvil ofrece a las aplicaciones capacidades de almacenamiento de datos y de procesamiento junto con otros servicios básicos de telefonía móvil.
- **Entorno de ejecución de confianza** (Trusted Execution Environment - TEE): El TEE se encuentra generalmente dentro de un elemento de seguridad (SE) y es el que proporciona un entorno de ejecución, almacenamiento y gestión de aplicaciones seguro. Un SE es en esencia una tarjeta inteligente que soporta Java Card 2.2.1 [7] (Java Card plataforma abierta [8]), Plataforma Global 2.1.1 [9]. La SE se aplican con mayor frecuencia como un módulo integrado en el móvil, ya sea un módulo soldado en el propio teléfono, como un componente integrado en la tarjeta SIM (U) (Universal/ Subscriber Identity Module) [10], o como un token (micro-sd) seguro de memoria que se pueda incorporar en el teléfono. Un desarrollo reciente ha sido el concepto de un "soft-SE", ubicado en el área del teléfono de aplicaciones móviles. El "soft-SE.^{es}tá abierto para el desarrollo, en contraste con los anteriores módulos de SE que han de ser desbloqueados para su uso. Por ejemplo, utilizando una "aplicación de desbloqueo"suministrada por el fabricante del teléfono. Ahora bien, una vez desbloqueada la SE, se debe considerar como no fiable, ya que se puede utilizar para cualquier otro fin.
- **Controlador NFC** : La controladora NFC gestiona las transmisiones físicas y recibe los datos a través del interfaz RF. La emulación de tarjeta, el modo reader/writer y el modo peer-to-peer permiten la comunicación entre la controladora y la AEE /TEE en función al modo de operación. Los modos reader y peer-to-peer normalmente son controlados a través de aplicaciones desde la AEE. En el caso de emulación de tarjeta, las comunicaciones se controlan desde las aplicaciones en el TEE, es decir, en el entorno de ejecución dentro de una SE.

IV. Amenazas de seguridad en dispositivos NFC

La tecnología NFC ofrece muchas posibilidades y todo un conjunto de futuras aplicaciones que en breve estarán entre nosotros. Esto es algo que los atacantes obviamente aprovecharán, por lo que los aspectos de seguridad de las soluciones NFC deben ser considerados desde varios puntos de vista. Asegurar el enlace de comunicación sólo es el primer paso, y después vendrán los retos de proteger los propios dispositivos o la búsqueda de mecanismos de identificación de los usuarios.

En esta sección ofrecemos una breve descripción de las principales amenazas que debe tenerse en cuenta al implementar cualquier solución de NFC y algunas primeras propuestas de solución, con sus pros y sus contras.

IV-A. Escuchas no autorizadas

Debido a que las comunicaciones no van cifradas a nivel de enlace, un atacante puede ser capaz de escuchar a observar el contenido de la comunicación NFC si no existe ningún cifrado en capas superiores. Una de las ventajas de la tecnología NFC es la corta distancia de alcance, por lo que los dispositivos de comunicación deben estar normalmente a una distancia de 10 centímetros o menor. Pero la verdadera pregunta es: a qué distancia puede estar un atacante para captar los datos? Y la respuesta depende de un gran número de factores, llegando a ser desde 1 a 10 metros [13]. Aunque el hecho de que un atacante pueda ser capaz de capturar el contenido de la comunicación no implica que la solución NFC sea una mala opción para la transferencia de información confidencial.

Otro aspecto que preocupa es la privacidad. Las etiquetas y/o tarjetas sin contacto generalmente disponen de un identificador único generado por el fabricante. Explotando esta identificación se puede realizar un seguimiento de las personas y sus acciones mediante la lectura de sus pasaportes u otros dispositivos NFC sin contacto cada vez que pase por delante de un lector oculto. Por ejemplo, si realizan algunas compras en un supermercado con productos con etiquetas NFC, se puede observar que productos lleva el cliente en sus bolsas.

IV-B. Corrupción de datos

Un atacante puede intentar corromper los datos de comunicación interfiriéndola. En [13] se indica que este ataque se puede detectar desde el dispositivo NFC, pero igualmente se puede ejecutar como un ataque de denegación de servicio (DoS) para no permitir que el usuario pueda utilizar el dispositivo NFC (ya sea tanto para recuperar información de otro dispositivo NFC, como para entregarla).

IV-C. Modificación de datos

La falta de seguridad de capa de enlace (o la seguridad en otras capas) hace posible que un atacante pueda intentar modificar los datos. ¿Qué dificultad hay en la modulación de una señal para realizar un ataque? [13].

Cuando un dispositivo NFC en el modo de lector/iniciador está leyendo un dispositivo pasivo, la posibilidad de haber modificado previamente los datos de la etiqueta seria otro tipo de ataque. Un mecanismo de prevenir este ataque puede consistir en que la etiqueta contuviera algún mecanismo que no permitiera realizar modificaciones en los datos si no se está en disposición de una clave. Otro mecanismo puede consistir en hacer que la etiqueta sea sólo de lectura ya des la

fabricación de la misma. Pero en la práctica, estas soluciones no funcionan, ya que las etiquetas pueden ser eliminadas y/o reemplazadas con etiquetas nuevas con un contenido diferente. Incluso si la etiqueta se colocara en un lugar más seguro (por ejemplo, detrás de vidrio) para que no pueda ser eliminada, se podría pegar una etiqueta nueva encima. La etiqueta vieja podría quedar apantallada detrás de una cap delgada de papel de aluminio [14].

Una propuesta en [15] consiste en utilizar firmas digitales sobre el contenido de las etiquetas NFC. La firma digital ofrece integridad de los datos y una manera de verificar si el contenido proviene de una fuente de confianza o no. La firma dice que el contenido cubierto por la firma original ha sido creado por el titular de la clave privada correspondiente a una clave pública en particular. Si esta clave pública está destinada a un usuario de un certificado firmado por una fuente de confianza, entonces podemos afirmar que el contenido solo lo ha podido firmar el titular de la clave privada y por tanto podemos obtener el no repudio. Así, con la simple operación de añadir una firma, se puede confiar en la fuente del contenido.

IV-D. ***Clonación***

Una nueva tarjeta se puede crear con el mismo contenido que la original. No obstante, las etiquetas o tarjetas más caras pueden disponer de mecanismos adicionales de prevención de lectura de los contenidos, y por tanto serán más difíciles de leer y por tanto de realizar una clonación exacta. Para aquellas etiquetas o tarjetas que no ofrezcan estos mecanismos, o se conozca algún ataque que las vulnere (como por ejemplo la Mifare Classic) se puede aplicar en un servidor un listado de tarjetas negras o clonadas que deberían ser verificadas [13].

Obviamente, un atacante tiene mayor interés en clonar una tarjeta que una simple etiqueta, pero se debe ser cuidadoso en no depositar demasiada confianza en las etiquetas. Juels, en [17], expone un ejemplo acerca de la recuperación de algunos bienes robados y dice que las etiquetas RFID también se pueden utilizar como mecanismo de confianza asociándose al portador de los mismos. Esta creencia en la autenticidad de la etiqueta es, en cierta medida, una ilusión ya que las etiquetas podrían haber sido clonadas.

Mulliner también explica un ejemplo donde las etiquetas se utilizan para identificar a las máquinas expendedoras y permite que los clientes paguen utilizando el teléfono móvil. En este escenario se sugiere que un atacante podría clonar la etiqueta de una máquina y ponerla en la otra. Después, el atacante puede volver a la primera máquina y esperar a que alguien utilice la etiqueta que clonó para pagar. De esta manera, el pago iría a la primera máquina y el atacante puede obtener el producto pagado por otro [14].

IV-E. ***Phishing***

Mediante la sustitución de una etiqueta/tag en un cartel publicitario (smart poster) se puede engañar a los usuarios y forzar la visita de sitios web con el mismo aspecto, pero malicioso. Un ejemplo sería el uso de un cartel para adquirir un billete de autobús mediante el envío de un SMS, y el número de teléfono puede ser cambiado por un número de una tarifa superior en su lugar. Es probable que los usuarios con prisas no se fijen en el detalle y soliciten los billetes de clases superiores. Además, los errores o deficiencias en la interfaz gráfica del móvil del usuario también pueden ser utilizados para inducir a los usuarios a un error. Esta situación puede ser incluso de mayor gravedad si la interfaz gráfica del usuario se mezcla con la información del usuario y con la información aportada por la etiqueta [14]. Un ataque muy simple es crear un cartel inteligente, con un título que muestra una dirección URL buena, pero por debajo suministra un código malicioso.

Si en un supermercado se utilizan etiquetas de NFC/RFID, los ladrones pueden cambiar la etiqueta de un producto por otro similar pero más económico [18].

Otras etiquetas se pueden utilizar para realizar la configuración WiFi (para la impresora o el acceso a Internet, etc) o para disponer de los parámetros de configuración y claves (es decir, WPA2) almacenados en una etiqueta. Si el contenido de la etiqueta ha sido modificado o han substituido la etiqueta por otra maliciosa, los visitantes no podrán disponer de conexión o se podrían estar conectando a un punto de acceso malicioso (AP), creyendo que están conectados en la red correcta.

En este último escenario, todo el tráfico que circule, como la navegación por la web, y que no utilice el nivel más alto de seguridad extremo a extremo (es decir, SSL o TLS), entonces las comunicaciones pueden ser fácilmente interceptadas.

IV-F. ***Retransmisión***

Un ataque de retransmisión puede tener serias implicaciones de seguridad. El atacante es capaz de pasar por alto la capa de seguridad de aplicación retransmitiendo por otra va las comunicaciones. Por ejemplo, un atacante puede eludir un protocolo de autenticación simplemente relanzando (por otro canal) el desafío a otro dispositivo que le proporcionará la respuesta correcta, permitiendo entonces retransmitir la respuesta al verificador. Esto permite "impersonar" un dispositivo remoto o realitar el temible "Man in the middle". En [20] se propone para contrarestar este ataque un control del tiempo de proceso aceptable o bien el uso de mecanismos de geolocalizacin del dispositivo para confirmar que no haya una retransmisin remota.

V. VALORACIÓN DE LAS SOLUCIONES

A parte del esfuerzo de encontrar una solución factible a las posibles amenazas, debemos tener presente que al trabajar con dispositivos NFC nos encontramos con muchas dificultades añadidas (recursos computacionales limitados, capacidad de almacenamiento reducida, consumo eléctrico limitado, etc). Todo esto aporta un segundo grado de dificultad a las soluciones y limita las posibles acciones preventivas o de protección en las etiquetas o en los dispositivos NFC en general. Por ello, se recomienda que toda solución haga una evaluación exhaustiva en términos de:

- **Tiempo de proceso**: Se debe medir el retardo adicional que supone para el usuario la solución de seguridad en

el dispositivo NFC. Por ejemplo, en una solución donde se utilice la firma digital para proteger los contenidos, el tiempo de procesamiento es uno para realizar la verificación y otro para cuando se realiza la firma. En el caso de verificación, el tiempo se calcula a partir de que el análisis se inicia hasta que las operaciones de verificación terminan y el usuario puede ver el resultado. Si el proceso de verificación fuera costoso, el usuario puede sentirse frustrado con en el sistema. El "tomar mucho tiempo de proceso" depende de la experiencia del usuario en la situación dada y en el tipo de aplicación. Esto normalmente se deber valorar mediante estudios con usuarios reales y sobre la afectación sobre todo el tiempo de proceso para ofrecer el servicio.
Normalmente se considera que 0,1 es una acción instantánea, mientras 1,0 segundo es el límite para mantener un flujo aceptable y 10 segundos es el límite para mantener centrada la atención del usuario [19].

- **Uso de memoria**: Otro aspecto a valorar es el uso de la memoria, así como de la memoria interna que se requiere en dispositivo móvil durante la ejecución para llevar a cabo las operaciones. Hasta ahora la mayor estructura de datos que se podía utilizar era la de un mensaje NDEF y el tamaño normalmente estaba limitado por los tipos de etiquetas, y se suponía que los dispositivos móviles tenían mayor memoria, pero con los nuevos modelos estos parámetros deberán ser revisados.
- **Tamaño del código**: Desgraciadamente, existen una gran variedad de sistemas operativos móviles con sus respectivas versiones. Esto normalmente se traduce en el desarrollo de varios códigos adhoc. Además, en algunos modelos nos encontramos que no es posible la compartición de librerías, y esto significa un incremento en el tamaño del código de la solución.

Es recomendable que las mediciones tomadas sean tanto en el emulador del dispositivo, como directamente en los propios dispositivos móviles. Los resultados se deben imprimir en alguna salida estándar para el emulador o en un archivo local en el caso de los dispositivos móviles.

VI. Conclusiones

La tecnología NFC abre las puertas a todo de aplicaciones en los dispositivos móviles en los próximos años. Es una tecnología de comunicación inalámbrica novedosa, intuitiva y de fácil uso, que requiere una alta proximidad entre los dispositivos a comunicar. El NFC está estandarizado entre los fabricantes, que buscan la interoperabilidad incluso con dispositivos RFID previos que funcionen en 13,56 MHz.

Los dispositivos NFC van desde simples etiquetas o tags muy económicos (que se pueden emplear en todos los sectores) con mínima capacidad de almacenamiento y sin procesamiento, hasta los dispositivos móviles de última generación. Las comunicaciones pueden ser realizadas de forma pasiva (el elemento receptor utiliza el campo de inducción del iniciador) o bien activas (cada elemento emite sus propias señales).

Esta tecnología inicialmente no dispone de herramientas de seguridad propias y las comunicaciones se transmiten en claro en el aire. Todo ello hace que existan muchas vulnerabilidades y sea un campo abonado para los ataques, así como para encontrar o proponer nuevas soluciones de seguridad que tendrán las dificultades de encontrarse un entorno complejo y variado. El éxito en los próximos años será encontrar soluciones de protección implementables que requieran el mínimo tiempo de proceso, al mismo tiempo que optimicen los recursos disponibles.

Referencias

[1] Sony, Philips, "Philips and Sony announce strategic cooperation to define next generation near field radio-frequency communications", en *h*ttp://www.sony.net/SonyInfo/News/Press_Archive/200209/02-0905E/ , Sep. 2002.

[2] "NFC Forum web page", en *h*ttp://www.nfc-forum.org/home/, 2012.

[3] International Organisation for Standardisation. "ISO/IEC 18092-4, Information technology -Telecommunications and information exchange between systems - *N*ear Field Communication Interface and Protocol (NFCIP-1)", 2004.

[4] International Organisation for Standardisation. "ISO/IEC 21481, Information technology -Telecommunications and information exchange between systems - *N*ear Field Communication Interface and Protocol (NFCIP-2)", 2005.

[5] International Organisation for Standardisation. "ISO/IEC 14443-1, Identification cards *C*ontactless integrated circuit(s) cards - Proximity cards -", 2008.

[6] International Organisation for Standardisation. "ISO/IEC 15693-1, Identification cards *C*ontactless integrated circuit(s) cards Vicinity cards -", 2000.

[7] Oracle/Sun Microsystems. "Java Card Platform Specifica-tion v2.2.1. Online: *h*ttp://java.sun.com/products/javacard/specs.html"

[8] NXP. "Java Card Open Platform. Online: *h*ttp://www.nxp.com"

[9] Global Platform. "Card Specification v2.1.1. Online: *h*ttp://www.globalplatform.org"

[10] Third Generation Partnership Project. "Characteristics of the Uni-versal Subscriber Identity Module (USIM) application (Release 7), TS 31.102 V7.10.0 Online: *h*ttp://www.3gpp.org/", 2007-09.

[11] Barclays contactless card users exposed to fraud, "*h*ttp://news.techworld.com/security/3346840/barclays-contactless-card-users-exposed-to-fraud", Google Wallet Security: PIN Exposure Vulnerability , "*h*ttps://zvelo.com/blog/entry/google-wallet-security-pin-exposure-vulnerability", Feb, 2012.

[12] MIFARE contactless smart card from NXP, en *h*ttp://www.mifare.net/".

[13] Ernst Haselsteiner and Klemens Breitfu, "Security in near field communication (NFC), en Workshop on RFID Security, RFIDSec 06. *P*hilips Semiconductors", July 2006.

[14] Collin Mulliner, "Attacking NFC mobile phones, Pre-sentation slides from talk at the 25th Chaos Communication Congress. *h*ttp://mulliner.org/nfc/feed", (25C3) Berlin, Germany, Dec 2008.

[15] Markus Kilas, "Digital Signatures on NFC Tags, at Ericsson, *K*TH - Royal Institute of Technology", Stockholm Sweden, ICT/ECS-2009-20, 2009.

[16] Wouter Teepe, "Making the best of Mifare Classic. *h*ttp://www.sos.cs.ru.nl/applications/rfid/2008-thebest.pdf", (25C3) Berlin, Oct 2008.

[17] A. Juels, "Rfid security and privacy: a research survey. Selected Areas in Communications *I*EEE Journal ", 24(2):381394, Feb. 2006.

[18] M.R. Rieback, B. Crispo, and A.S. Tanenbaum, "The evolution of RFID security. Pervasive Computing *I*EEE", IEEE, 5(1):6269, Jan.-March 2006.

[19] Jakob Nielsen, "Usability Engineering, *M*organ Kaufmann Publishers Inc.", San Francisco, CA, USA, 1995.

[20] L. Francis, G.P. Hancke, K.E. Mayes and K. Markantonakis., "Practical NFC Peer-to-Peer Relay Attack using Mobile Phones., *I*nformation Security Group", In Proceedings of the 6th Workshop on RFID Security (RFID-Sec10), LNCS, Springer-Verlag, June 2010.