UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja.
Máster universitario en Seguridad Informática.

Metodología para la auditoría de seguridad en implementaciones de tecnología NFC con dispositivos pasivos.

Trabajo Fin de Máster.

presentado por: Mendoza Casado, Carlos.

Director/a: Sánchez Rubio, Manuel.

Ciudad: Burgos.
Fecha: 23 de septiembre de 2016.

Resumen

Los dispositivos NFC están siendo incorporados en nuestras vidas como una tecnología que nos brinda la posibilidad de realizar las tareas comunes de una manera más fácil y eficiente. Pero no somos conscientes de la existencia de fallos de seguridad en sistemas basados en NFC que podrían poner en riesgo tanto la integridad del sistema como nuestros propios datos personales. Esta metodología nace con el objetivo de revisar y construir sistemas más seguros para proteger nuestra privacidad y la continuidad de los negocios.

Palabras clave: NFC, auditoría, seguridad, riesgos, amenazas

Abstract

NFC devices are being adopted in our lives as a technology that brings us the possibility to do common task in a more easy and efficient way. But we aren't aware of existing security flaws in NFC based deployments that could be a high risk for both the integrity of the deployment and our own personal data. This methodology born with the objective to review and make more secure deployments to protect our privacy and business continuity.

Keywords: NFC, audit, security, risks, threats

Contenido

Índice de ilustraciones

Índice de tablas

Listado de acrónimos

AES, Advanced Encryption Standard, 17

BAC, Basic Access Control, 29

CC, Common Criteria (www.commoncriteriaportal.org), 17, 18

CCP, Close Coupling Cards, 14

CEO, Chief Executive Officer, 39

CISO, Chief Information Security Officer, 39

CTO, Chief Technology Officer, 39

DNIe, Documento Nacional de Identidad electrónico, 28

DoS, Denial of Service, 24

DPA, Differential Power Analysis, 29

ECMA, European Computer Manufacturers Association (www.ecma-international.org), 12

EMVCo, Europay MasterCard VISA Company, (www.emvco.com), 12

ICAO, International Civil Aviation Organization, 29

IEC, International Electrotechnical Commission (www.iec.org), 12

ISO, International Organization for Standardization (www.iso.org), 12

JIS, Japanese Industrial Standards, 12, 15

JISC, Japanese Industrial Standards Committee (www.jisc.go.jp), 15

MitM, Man in the Middle, 24

MRTD, Machine-Readable Travel Document, 29

NFC, Near Field Communications, 9

OTA, Over The Air, 18

P2P, Peer To Peer, 19

PCDs, Proximity Coupling Devices, 12

PICCs, Proximity Integrated Circuit Cards, 12

PKI, Public Key Infrastructure, 25

RFID, Radio Frequency Identification, 11

SD, Secure Digital, 18

SDA, Side Channel Attack, 29

SE, Secure Element, 18

TBD, To Be Done, 26

TPM, Trusted Platform Module, 30

VC, Vicinity Cards, 16

VCD, Vicinity Coupling Device, 13, 14

VICC, Vicinity Integrated Circuit Card, 14

WORM, Write Once Read Many, 26

1. Introducción

Los avances de la tecnología continuamente van inundando nuestras vidas de nuevos productos que la sociedad puede llegar a asimilar dependiendo de muchos factores, como, por ejemplo, el ofrecernos una forma de realizar las tareas cotidianas de forma más sencilla.

Uno de estos avances es el ofrecido por la tecnología inalámbrica NFC (Near Field Communications) que en castellano se traduce como “Comunicaciones de campo cercano”, que basa su funcionamiento en la comunicación de dos elementos a través de ondas de radio separados por una distancia corta de un máximo de 4 a 10 centímetros.

Esta tecnología está experimentando en los últimos años un gran auge y se está implementando en multitud de soluciones para realizar funciones como la de tarjeta monedero en máquinas de *vending*, monedero/abono en servicios de transporte, tarjetas de crédito o incluso para controlar el acceso a edificios o zonas restringidas.

Este auge conlleva una gran demanda de soluciones que, en muchos casos, están siendo implementadas sin tener en cuenta qué riesgos se añaden a las soluciones que incorpora esta tecnología, ya sea por desconocimiento del funcionamiento o por un mal diseño de base o en la selección de la tecnología concreta a usar. Es por eso, que cada vez aparecen más noticias en los medios de comunicación en las cuales la tecnología NFC es la protagonista, por ser, en la mayoría de los casos, mal implementada y la base para la realización de estafas, robos u otras acciones consideradas ilegales.

Este trabajo tiene como objetivo el desarrollo de una herramienta sencilla y lo más fácil posible de entender y aplicar para poder analizar una solución propuesta o ya implementada que utilice NFC como una de sus tecnologías aplicadas, de forma que se pueda concluir si dicha propuesta posee un nivel de seguridad adecuado en cuanto el uso del NFC que no ponga en peligro los objetivos de la solución.

Para conseguir el desarrollo de esta metodología, el contenido de este trabajo se ha dividido en los siguientes capítulos:

- La tecnología NFC. Estándares y aplicaciones: Se hará una breve introducción a la tecnología NFC, se estudiarán con detalle todas las normas y estándares más importantes que definen la tecnología y se explicará la terminología asociada a NFC que se usará en la redacción de este trabajo.
- Amenazas y vulnerabilidades de la tecnología NFC: En este punto se estudiarán las amenazas y vulnerabilidades que afectan a esta tecnología y a los dispositivos que la

integran, desde la trasmisión de ondas de radio a nivel físico hasta las implementaciones de las aplicaciones.

- Hipótesis de trabajo y objetivos concretos de la investigación: Aquí haremos una reflexión sobre lo visto en los dos capítulos anteriores y reflexionaremos sobre el porqué del desarrollo de esta metodología y los objetivos que buscamos con su aplicación.
- Desarrollo de la metodología: En este punto se detallará los pasos seguidos para desarrollar la metodología, se desarrollará la propia metodología y se explicará a fondo cómo se realizará su aplicación y cómo se mejorará en base a la experiencia de su aplicación y de su revisión por personal experto.
- Conclusiones: Terminaremos el trabajo con las conclusiones que hemos obtenido tras desarrollar la metodología, indicando qué objetivos se han conseguido de su aplicación y si estos han sido acordes con lo esperado.
- Líneas de trabajo futuro: El desarrollo de una metodología que se basa en algo tan cambiante como la tecnología, y concretamente, en una tecnología en pleno proceso de integración en nuestras vidas, siempre va a tener que estar actualizada. En este apartado explicaremos cuales podrían ser las líneas de mejora de la metodología a desarrollar en futuros trabajos.
- Referencias: Un listado completo de todas las referencias que han servido como fuente de conocimiento para la realización de este trabajo y que pueden servir a quien quiera continuar desarrollando esta metodología como apoyo en la profundización técnica de la tecnología y de las amenazas y vulnerabilidades que la rodean.

2. La tecnología NFC. Estándares y aplicaciones

2.1. Introducción

La tecnología NFC está basada en la tecnología RFID. La tecnología RFID básicamente se usa para la lectura de etiquetas, algo que está contemplado también en NFC, pero a nivel tecnológico se diferencia sobre todo en que RFID dispone de varias bandas de frecuencias para la transmisión de información, lo que ofrece diferentes rangos de distancias, desde unos pocos centímetros hasta llegar a los 100 metros (ISO/IEC 18000-7:2014).

Otra gran diferencia entre NFC y RFID es que en la tecnología NFC, la comunicación es bidireccional, mientras que en RFID es la tarjeta la que envía la información al lector. Esto permite que NFC se utilice actualmente para entornos que requieren una comunicación bidireccional.

Pero el objetivo de este trabajo es centrarse en la tecnología NFC, la cual está basada por una serie de normativas y estándares, aunque esta información se verá más en detalle en el apartado “2.3 Normas y estándares relacionados con NFC”.

2.2. Historia de la tecnología NFC

Para entender mejor los origines de la tecnología NFC, tendríamos que conocer también los orígenes del RFID, al igual que para profundizar en la propia tecnología sobre la que está soportada NFC, hay que hacer lo mismo, al menos, en la parte de la tecnología RFID en la que se basa.

Se puede decir que el primer uso de una tecnología que se podría considerar como RFID, fue realizada durante la Segunda Guerra Mundial.

En el año 1983, Charles *Walton* registró una patente en la que por primera vez se usaba el acrónimo RFID titulada “Portable radio frequency emitting identifier” (Estados Unidos Patente nº US 4384288 A, 1983).

A partir de ahí se fueron desarrollando varias aplicaciones y estándares en base a diferentes usos del RFID.

En el año 2004, Sony, Philips y Nokia fundaron el NFC Forum (NFC Forum, 2004), que desde entonces se ha dedicado a promover y difundir el uso de la tecnología NFC. En capítulos

posteriores veremos las aportaciones que ha realizado el NFC Forum en cuanto a estándares que son reconocidos y utilizados internacionalmente.

Actualmente la tecnología NFC se desarrolla y normaliza en base a la colaboración de distintos organismos reguladores, empresas privadas y organizaciones como el NFC Forum.

2.3. Normas y estándares relacionados con NFC

Para poder comprender cómo funciona la tecnología NFC, de forma que podamos profundizar en esta tecnología y así poder investigar sobre sus debilidades y amenazas, tendríamos que estudiar los principales estándares y normas que rodean esta tecnología y que son asumidos por la industria como parte de la especificación que han de seguir los productos que salen al mercado.

La tecnología NFC está definida por una serie de estándares realizados por entidades internacionales (*ISO* e *IEC)*, entidades reguladoras en áreas concretas (*JIS* y *ECMA)*, los definidos por organizaciones privadas (*NFC Forum* y *EMVCo)*, y los definidos por fabricantes, como los protocolos que soportan los productos *MiFARE* (NXP Semiconductors), *Felica* (Sony Global) o *EMV* (EMVCo).

A continuación, se enumeran y se describen brevemente los principales estándares y normas de diferentes entidades que definen la tecnología NFC y otras similares a tener en cuenta, entendiendo por similares en cuanto al uso de la frecuencia de 13,54 MHz y características muy parecidas en cuanto a la transmisión de datos.

- **ISO/IEC 14443** (Identification cards – Contactless integrated circuit cards – Proximity cards): Está dividida en cuatro partes:
    - Parte 1 – Características físicas (ISO/IEC 14443-1:2016, 2016): Especifica las características de las tarjetas de proximidad (*PICCs*) a nivel físico.
    - Parte 2 – Alimentación por radiofrecuencia e interfaz de señal (ISO/IEC 14443-2:2016, 2016): Especifica las características radioeléctricas para la comunicación bidireccional y la alimentación inalámbrica de los dispositivos pasivos entre los dispositivos de acoplamiento cercano (*PCDs*) y las tarjetas de proximidad (PICCs).
    - Parte 3 – Inicialización y anticolisión (ISO/IEC 14443-3:2016, 2016): Especifica los protocolos de inicialización de la comunicación entre los dispositivos, métodos de comunicación anti-colisión en caso de existir varias PICCs en el

campo de alcance, los mecanismos de búsqueda de tarjetas cuando entran en el alcance de PCDs.

- Parte 4 – Protocolo de transmisión (ISO/IEC 14443-4:2016, 2016): Especifica el protocolo de transmisión de bloques no simultaneo (*half-duplex*) teniendo en cuenta las características especiales por ser una comunicación inalámbrica. También define la parte del protocolo que se utiliza para la activación y desactivación de la comunicación.

- **ISO/IEC 18092** (ISO/IEC 18092:2013, 2013) (Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol NFCIP-1), también publicado por la ECMA (ECMA-340, 2013): define los modos de interfaz NFC y el protocolo NFCIP1 y los modos de comunicación activa y pasiva. También se especifica de forma concreta los tipos de modulación utilizados, codificación, velocidades de transferencia, formato de trama de la interfaz de radiofrecuencia y los esquemas de inicialización y condiciones requeridas para el control de colisiones durante la inicialización. También se define un protocolo de transporte incluyendo métodos de activación e intercambio de datos.
- **ISO/IEC 21481** (ISO/IEC 21481:2012, 2012) (Telecommunications and information exchange between systems -- Near Field Communication Interface and Protocol 2 NFCIP-2), también publicado por la ECMA (ECMA-352, 2013): El principal objetivo de este estándar es la integración de dispositivos que sean compatibles con varios tipos de tarjetas que usan la frecuencia de los 13,56MHz. Esto lo realiza especificando un mecanismo para la selección del modo de comunicación. Esto permite usar dispositivos que soporten los siguientes estándares con lectores que cumplan tanto con la norma ISO/IEC 21481 como con las siguientes:
  - ISO/IEC 18092 o ECMA-340: *NFC*.
  - ISO/IEC 14443: *PCD*.
  - ISO/IEC 15693: *VCD*.
- **ISO/IEC 18000** (Radio frequency identification for item management): Norma compuesta por 7 partes, de las que nos interesan las siguientes:
  - Parte 1 – Arquitectura de referencia y definición de los parámetros a ser estandarizados (ISO/IEC 18000-1:2008, 2008): Establece las definiciones base para las partes que conforman esta norma.
  - Parte 3 – Parámetros para las comunicaciones por aire en 13,56 MHz (ISO/IEC 18000-3:2010, 2010): Especifica los parámetros para la comunicación de interfaces aéreas usando la frecuencia de 13,56 MHz.

- **ISO/IEC 10536** (ISO/IEC 10536, 1996-2000): Fue el primer estándar de comunicación sin contacto en aparecer. Está basado en tarjetas *CCP*, las cuales necesitaban ser introducidas en un lector o colocarse justo encima para poder comunicarse. Actualmente ya no hay nadie que provea de tecnología conforme a este estándar, por lo que se puede decir que está abandonado.
- **ISO/IEC 15693** (Identification cards -- Contactless integrated circuit cards -- Vicinity cards): Esta serie de normas ISO está formada por tres partes en las que se define una tecnología parecida a NFC, pero en la que el rango de alcance de la tarjeta es de hasta un metro. A las tarjetas desarrolladas se las da el nombre de Vicinity Integrated Circuit Card (VICC) y a los lectores se les da el nombre de Vicinity Coupling Device (VCD).
- **ISO/IEC 7816-4** - Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange (ISO/IEC 7816-4:2013/Cor.1:2014, 2014) : Este estándar es el más utilizado por las tarjetas denominadas *smartcard*, ya que establece una capa a nivel de protocolo de aplicación a partir de la cual se pueden implementar aplicaciones de cualquier tipo. Este protocolo establece el nivel común a partir del cual las tarjetas pueden ser utilizadas tanto a nivel de NFC como a nivel físico (a través de conexiones físicas). Para entender esto mejor podemos verlo en la siguiente ilustración:

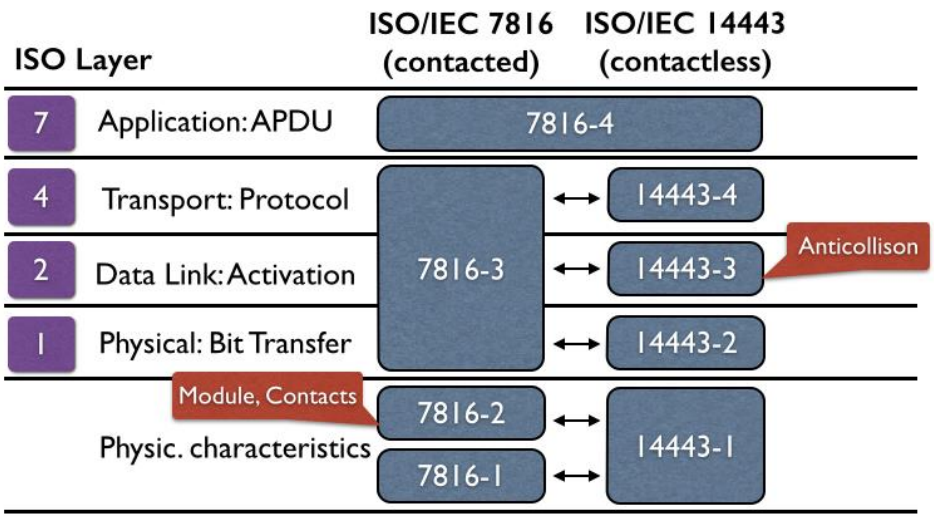

Ilustración 1. Contexto de capas en el modelo ISO/OSI sobre tarjetas SmartCard (Funke, 2013).

- **EMV Contactless** (EMV Contactless): Es un estándar de pago desarrollado por *EMVCo*, que es un consorcio que está controlado por las compañías *American Express*, *Discover*, *JCB*, *MasterCard*, *UnionPay* y *VISA* (EMVCo Members, 2016). También existen otros actores, como los socios tecnológicos (EMVCo Technical

Associates, 2016), que colaboran en el desarrollo del estándar mediante la implementación y pruebas que realizan. El estándar *EMV Contactless* se basa en el estándar EMV (EMV 4.3, 2011), y utiliza como base los estándares ISO/IEC 7816-4 e ISO/IEC 14443 (EMV FAQ: Card / Terminal General Questions). El estándar *EMV Contactless* está definido por el contenido de cuatro libros:

  - **Libro A** - Arquitectura y Requerimientos Generales (EMV Contactless: Book A: Architecture and General Requirements, 2016).
  - **Libro B** - Punto de entrada (EMV Contactless: Book B: Entry Point, 2016).
  - **Libros C** - Especificación del núcleo (EMV Contactless: Books C [C-1, C-2, C-3, C-4, C-5, C-6, C-7]: Kernel Specifications, 2016).
  - **Libro D** - Protocolo de comunicación sin Contacto (EMV Contactless: Book D: Contactless Communication Protocol, 2016).

- **JIS X 6319** (Especificación de implementación de tarjetas con circuito integrado), de la que nos interesa la parte 4 de esta norma (JIS X 6319-4:2016, 2016) (Tarjetas de proximidad de alta velocidad): Los estándares *JIS* son las normas oficiales de Japón y están definidas por el *JISC*. Esta norma define las características de forma física de las tarjetas, las características físicas de la transmisión de datos por el aire, los protocolos de inicialización y anticolisión y una especificación de comandos a nivel de aplicación.
- **FeliCa** (Sony Global - Felica - Technical Information, 2016)**:** Es una especificación desarrollada por Sony y orientada para el mercado japonés, definida por los estándares JIS X 6319-4, NFC Forum Tag 3 e ISO/IEC 18092, aunque incorporando comandos propietarios a nivel del protocolo de aplicación.
- **NFC Forum** (NFC Forum, 2004): Este organismo desarrolla varios estándares, en su mayoría alineados con las series de normas ISO/IEC 14443, ISO/IEC 18092, ISO/IEC 15693 y con la norma JIS X 6319-4. Entre los estándares que desarrollan podemos encontrar:

  - **NDEF** (NFC Data Exchange Format (NDEF) Technical Specification, 2006): Define un formato común de datos para los dispositivos y etiquetas NFC que deben cumplir si el fabricante quiere que éstos obtengan la certificación de cumplimiento que otorga NFC Forum. Este formato actualmente es un estándar a nivel internacional.
  - **Etiquetas** (NFC Forum: Tag Type Technical Specifications, 2016): Existen una serie de especificaciones según el tipo de etiqueta:

- **Etiqueta tipo 1**: Están basadas en el estándar ISO/IEC 14443 (solo en el tipo A). En estas etiquetas se pueden realizar operaciones tanto de lectura como de escritura, pudiendo configurarla el usuario como de solo lectura. La capacidad de almacenamiento soportada esta entre 96 y 2048 *bytes* dependiendo de la etiqueta.
- **Etiqueta tipo 2**: También están basadas en el estándar ISO/IEC 14443 (solo en el tipo A) y se pueden realizar operaciones de lectura y escritura, pudiendo ser configurados como de solo lectura por el usuario. La capacidad de almacenamiento soportada esta entre 48 y 2048 bytes dependiendo de la etiqueta.
- **Etiqueta tipo 3**: Estas etiquetas están basadas en el estándar JIS X 6319-4. Se pueden realizar operaciones de lectura o de lectura y escritura, pero, en este caso, viene configurado de fábrica. La capacidad disponible en estas tarjetas es variable hasta un máximo de 1 MB (megabytes).
- **Etiqueta tipo 4**: Esta tarjeta es compatible completamente con el estándar ISO/IEC 14443, por lo que soporta tanto el estándar ISO/IEC 14443-A como el ISO/IEC 14443-B. Las etiquetas se configuran en fábrica para que sean de solo lectura o de lectura y escritura. La capacidad de almacenamiento de estas etiquetas puede ser de hasta 32 KB (kilobytes).
- **Etiqueta tipo 5**: Estas etiquetas se basan en el estándar ISO/IEC 15693 (VC). NFC Fórum define cómo ha de interactuar un dispositivo NFC con una etiqueta de este tipo, pero no cómo se fabrica. Estas etiquetas son capaces de almacenar mensajes NDEF.

  - **NFC Logical Link Control Protocol - LLCP** (NFC Forum: Protocol Technical Specifications, 2016): Define un protocolo basado en la capa 2 del nivel OSI para soportar comunicaciones entre dos dispositivos P2P (peer to peer) a través de la interfaz NFC.

- **MiFARE** (MIFARE® ICs, 2016)**:** Ésta es la marca comercial del fabricante NXP Semiconductors. Es la compañía que lidera el mercado en venta de chips controladores de NFC con un 74% en el año 2002 y de chips para elementos seguros (SE) con un 54,7% en 2012 (Clark, 2013). Dentro de los productos que ofrece, éstos son parte de los más importantes:

  - **MiFARE Classic**: Es una de las tarjetas de almacenamiento de datos, que cumple con el estándar ISO/IEC 14443 A (niveles 1 a 3). Está disponible en

capacidades de 1 y 4 Kbytes. Los datos que almacenan se encuentran separados en bloques formados por varios sectores en los que se aplican permisos de acceso dependiendo de cuál de las dos claves que existen para cada bloque sea utilizada en la autenticación. Utilizan un protocolo propietario de NXP denominado CRIPTO-1, que es vulnerable a ataques. Existen dos modelos diferentes:

- MiFARE Classic (MIFARE® Classic): Son el primer modelo de tarjetas que salieron al mercado.
- MiFARE Classic EV1 (MIFARE® Classic EV1, 2014): La denominación EV1 en estas tarjetas indica la inclusión de mejoras en la tarjeta en cuanto a la durabilidad, un generador de números aleatorios más eficaz y la existencia de un mecanismo para comprobar que la tarjeta es original, entre otros. Es más segura que el modelo original, pero sigue incorporando el protocolo CRIPTO-1.

- **MiFARE PLUS** (MIFARE® Plus): Engloba una serie de tarjetas denominadas "S", "SE", "X" y "EV1". Las que tienen la denominación "S" y "X" disponen de la certificación CC EAL4+, y la que tiene la denominación "EV1" dispone de la certificación CC EAL5+. Una gran ventaja que aportan las series "X" y "EV1" es la función denominada *Proximity Check*, que incorpora un mecanismo para bloquear el ataque de *Relay*. La función de esta tarjeta es el almacenamiento de datos. Está diseñada para ser usada en las mismas aplicaciones que la versión MiFARE Classic original (sigue incorporando el protocolo CRIPTO-1, pero también incorpora uno mucho más seguro basado en AES).
- **MiFARE Ultralight**: Es una tarjeta muy similar al modelo MiFARE Classic en cuanto a la compatibilidad con el estándar ISO/IEC 14443 A, que también soporta los niveles 1 a 3. Se diferencia de la anterior en que el almacenamiento es inferior (entre 40 y 144 bytes). Su diseño está orientado al uso en aplicaciones de transporte público, como por ejemplo, una tarjeta con límite de viajes, o, incluso para aplicaciones de acceso a eventos. Existen varias variantes (normal, nano, EV1, C) que difieren en funciones como la posibilidad de habilitar una contraseña de acceso, el cifrado de los datos y el chequeo de la originalidad de la tarjeta.
- **MiFARE DESFire**: Se basa en una tarjeta que ofrece la posibilidad de incorporar más de una aplicación. Cumple completamente con los cuatro niveles de ISO/IEC 14443 A y es capaz de usar los comandos especificados

en la norma ISO/IEC 7816-4. Está disponible en capacidades de 2, 4 y 8 Kbytes. Tiene la certificación CC EAL4+.

  - MiFARE DESFire (clásica): Philips dejó de fabricar esta tarjeta por ser vulnerable a un ataque por el que se podían sacar sus claves (Oswald & Paar, Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World - Extended Version, 2011).
  - MiFARE DESFire EV1 (MIFARE® DESFire EV1, 2015): Está disponible en capacidades de 2, 4 y 8 Kbytes. Tiene la certificación CC EAL4+.
  - MiFARE DESFire EV2 (MIFARE DESFire EV2, 2014): Es una mejora sobre la anterior en el que aumenta el rendimiento, la seguridad y privacidad de los datos y el soporte de aplicaciones múltiples, como la virtualización de tarjetas. En este caso, está certificada por el CC con la calificación EAL5+.

- **MiFARE4Mobile** (Mifare4Mobile, 2015): Es un grupo industrial formado por empresas como *Gemalto*, *Giesecke & Devrient*, *NXP Semiconductors*, *Oberthur Technologies* y *STMicroelectronics* que desarrollan una tecnología que comercializan con el mismo nombre basada en la utilización de dispositivos móviles en vez de las tarjetas físicas para realizar las funciones de éstas. Su objetivo es proporcionar aplicaciones a través de OTA que serán instaladas en un elemento seguro del dispositivo (SE) que podría ser la tarjeta sim, una tarjeta SD en la que exista esta funcionalidad o un elemento integrado en el propio dispositivo. Esta funcionalidad está actualmente en producción utilizando dispositivos como los basados en el sistema operativo Android en los que se hace uso de la funcionalidad HCE (Host-based Card Emulation | Android Developers, 2016) y se puede usar, por ejemplo, para el pago en el sistema de transporte urbano de la ciudad de Albacete a través de la aplicación *PayBus* de la empresa *PrePay Technologies* (antiguamente conocida como *PaniniTech*) (Prepay Technologies, 2016).

2.4. Terminología de la tecnología NFC

En este capítulo veremos la terminología utilizada cuando se habla de NFC.

En primer lugar, deberemos identificar los tipos de dispositivos que existen dependiendo de cómo se comportan en el momento de establecerse la comunicación. En este caso existen dos tipos de dispositivo:

- **Dispositivos activos**: Son los dispositivos que emiten un campo electromagnético que, cuando se acerca un dispositivo pasivo, le transfiere la energía necesaria para que éste se active y puedan establecer una comunicación.
- **Dispositivos pasivos**: Estos dispositivos no tienen la capacidad de producir un campo magnético ni tienen una fuente de energía para poder activarse por sí solos, por lo que siempre necesitarán activarse y alimentarse mediante un campo electromagnético que estará generado por un dispositivo activo.

Cuando se inicia una conexión, se dirá que el dispositivo que inicia dicha conexión es el dispositivo iniciador (Initiator), y sobre el dispositivo al que se le requiere que inicie la conexión se dirá que es el dispositivo objetivo (target). Un dispositivo pasivo nunca pude ser el iniciador.

Cuando se produce la comunicación entre dos dispositivos activos, los dispositivos se comportan de manera diferente a cuando la comunicación es entre un dispositivo activo y pasivo, ya que el campo electromagnético solo es generado en los momentos en los que cada uno de los dispositivos envía información al otro.

Los dispositivos activos, a su vez, se pueden clasificar teniendo en cuenta los modos de comportamiento que pueden tener. En este caso, los clasificaremos en tres tipos de dispositivos:

- **Dispositivos emuladores de tarjetas**: permite a un dispositivo de tipo activo comportarse como si fuera una tarjeta pasiva. Esta funcionalidad está disponible en algunos dispositivos móviles, como teléfonos Android y permite que el dispositivo se pueda utilizar, por ejemplo, para la realización de pagos en comercios de manera similar a si usáramos una tarjeta de crédito con tecnología NFC.
- **Dispositivos de lectura/escritura**: Son los dispositivos que tienen como función la lectura y escritura en ciertos dispositivos pasivos, como las etiquetas NFC (NFC Forum: Tag Type Technical Specifications, 2016).
- **Dispositivos Peer to Peer** (P2P): Son los dispositivos que permiten comunicarse con otro dispositivo NFC activo para intercambiar información directamente.

La comunicación entre dispositivos NFC está diseñada para realizarse entre dos elementos de forma simultánea, pero se puede dar el caso en el que un dispositivo iniciador pueda habilitar varios dispositivos objetivos que estén dentro del alcance de su campo de radiofrecuencia. En este caso, el dispositivo iniciador podría hablar con varios dispositivos, pero solo con uno a la vez. Esto se puede conseguir por implementación del protocolo de anticolisión que recoge la norma ISO/IEC 14443-2. Lo que no se puede realizar es el envío

simultáneo de información a varios dispositivos, ya que no se contemplan comunicaciones de tipo broadcast (Haselsteiner & Breitfuß, 2006).

3. Amenazas y vulnerabilidades de la tecnología NFC

3.1. Introducción

Hay que entender que la tecnología NFC es un medio de comunicación, y que sobre dicho medio de comunicación se han desarrollado una serie de elementos basados en esta tecnología para la transmisión de datos. Por tanto, si nos ciñéramos estrictamente a estudiar las amenazas y vulnerabilidades de la tecnología NFC nos tendríamos que centrar en los aspectos físicos del medio de transmisión y los demás protocolos que se desarrollan, como los definidos en la serie de normas ISO/IEC 14443 (apartado 2 al 3) y la ISO/IEC 18092. Si bien ésta es una parte importante a tener en cuenta y, como tal, la vamos a analizar, hemos de tener en cuenta la serie de servicios que se ofrecen a través de NFC y en los que residen una parte importante de las amenazas y vulnerabilidades que, aún a día de hoy, están siendo explotadas y produciendo pérdidas a muchas compañías. Todos estos elementos han de analizarse para entender si pueden poner en peligro un sistema en el que se use NFC de tal forma que se pueda analizar cómo afrontar ese riesgo correctamente.

Por tanto, en este capítulo, hablaremos de amenazas y vulnerabilidades, no solo de la tecnología NFC en sí, sino también de los dispositivos que incorporan esta tecnología.

3.2. Dispositivos de auditoría y ataque a la tecnología NFC

En el mercado existen, a disposición de cualquiera, una serie de productos que permiten realizar acciones avanzadas dentro de la tecnología NFC que permiten poder auditar tanto la tecnología como las implementaciones que de ésta se han realizado. Además, debido al auge que está experimentando la tecnología NFC, cada vez es más la información que está disponible en Internet y que cualquiera puede consultar para ponerla en práctica.

De entre todos los dispositivos que existen actualmente, el más conocido es el *Proxmark III* (Proxmark.org), basado en un diseño realizado por *Jonathan Westhues* (Westhues, 2009), que actualmente se sigue desarrollando y está disponible para ser comprado fácilmente. Este dispositivo permite comportarse como un dispositivo activo o pasivo indistintamente, incluso permite realizar funciones de escucha de las comunicaciones posicionándolo cerca de los objetivos a escuchar. Dentro de las funciones de ser un dispositivo pasivo, permite la emulación de varios de los tags que se encuentran disponibles en el mercado, como las

tarjetas MiFARE Classic. Además, también puede ser usado no solo para NFC, sino también para otros estándares soportados por RFID, como algunos de los soportados en la frecuencia de los 125 kHz. Esto hace que sea el dispositivo más conocido a nivel mundial.

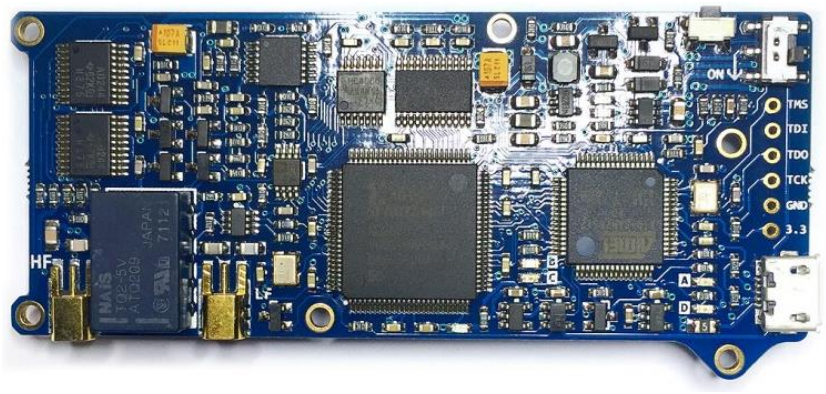

Ilustración 2. Imagen de dispositivo Proxmark III actual (Lab401, 2016)

Una desventaja de este dispositivo es que tiene que estar conectado a un ordenador para realizar algunas funciones y, dependiendo del uso que se le vaya a dar, puede considerarse que su precio sea alto. Por lo que otro dispositivo similar que podría sustituir al *Proxmark III* es la última versión del *ChameleonMini* (Kasper & Oswald, ChameleonMini, 2016). Como indican sus creadores, este dispositivo es compatible con la tecnología NFC y con la ISO/IEC 15693, por lo que también podría usarse para las *Vicinity Cards*. Permite comportarse tanto como un dispositivo NFC activo o como un dispositivo NFC pasivo, además de que también permite realizar escuchas colocándose cerca de los objetivos. Las grandes ventajas que aporta con respecto al Proxmark III es que no hace falta que esté conectado a un ordenador para funcionar (dispone de una batería reemplazable), es totalmente programable, su tamaño es prácticamente como el de una tarjeta normal y su precio es la mitad del precio del *Proxmark III*.

Ilustración 3. Modelo actual de tarjeta ChameleonMini Rev. G (Oswald & Kasper, ChameleonMini - A Versatile NFC Card Emulator, and more..., 2016).

Hay otros dispositivos que también se pueden usar para realizar auditorías y comprobaciones en las implementaciones ya realizadas, como teléfonos móviles que disponen de NFC o dispositivos de lectura/escritura externos que pueden ser conectados a cualquier PC e incluso a teléfonos móviles.

Para investigar a nivel de radiofrecuencia, también se pueden utilizar osciloscopios digitales modernos con captura y procesamiento de señales.

3.3. Amenazas y vulnerabilidades basadas en el ataque sobre el medio de transmisión de NFC

Como cualquier medio de transmisión que se base en comunicaciones inalámbricas a través de ondas de radio, existen una serie de amenazas que hay que tener en cuenta. Aunque podemos encontrar muchos documentos sobre estos tipos de amenazas, concretamente hay uno titulado “Security in Near Field Communication (NFC) – Strengths and Weaknesses” (Haselsteiner & Breitfuß, 2006), en el que se detalla, desde el punto de vista de la tecnología NFC, qué amenazas hemos de tener en consideración.

3.3.1. Escuchas de la transmisión

Esta amenaza es más conocida por el término anglosajón “*eavesdropping*”. Se basa en la posibilidad de escuchar la señal transmitida por los interlocutores para poder analizarla y extraer datos en claro de lo que han transmitido. Dispositivos como los vistos en el apartado “3.2 Dispositivos de auditoría y ataque a la tecnología NFC” pueden ser utilizados para esta función, aunque han de situarse a una distancia muy cercana a la de los interlocutores a escuchar. En un estudio realizado por investigadores de la Universidad de Surrey en Reino Unido (Thomas P. Diakos, 2013) sobre este tema, llegaron a la conclusión de que, si bien la distancia máxima a la que se podría realizar una escucha depende mayoritariamente de la fuerza de la señal del emisor, se puede conseguir realizar dicha lectura a un máximo de 20-90 centímetros.

La mejor manera para evitar estos casos es utilizar un cifrado seguro de los datos transmitidos, de tal forma que no puedan ser entendidos.

3.3.2. Denegación de servicio (DoS)

En este caso, se trata de intentar modificar los datos que se transmiten desde un dispositivo. Se puede conseguir transmitiendo frecuencias válidas en el espectro de los datos en el momento que queremos modificar la transmisión. De esta forma, el receptor de los datos no podrá recibir correctamente los datos del emisor, por lo que, sencillamente, no funcionaría el servicio.

La forma de evitar este ataque, sería detectando el envió de las señales de radiofrecuencia del dispositivo atacante en los dispositivos atacados, ya que, como el emisor estaría generando un campo con una potencia lo suficientemente fuerte para producir la denegación de servicio, este campo sería fácilmente detectable en los propios dispositivos atacados.

3.3.3. Modificación de los datos

A diferencia del anterior caso, en éste se trataría de manipular la señal de radio transmitida para que el receptor reciba la señal modificada, de tal forma que los datos que recibe puedan ser manipulados deliberadamente.

Para solucionar este problema, al igual que en las escuchas, lo mejor sería usar un cifrado de los datos, aunque también se podría usar el firmado de dichos datos si no nos importa que sean escuchados.

3.3.4. Adición de datos.

Esta amenaza se basa en que, cuando uno de los dispositivos está en pausa (puede ser mientras procesa la respuesta que va a transmitir), un tercero aprovecha ese periodo de tiempo para enviar los datos que desee añadir. Este ataque solo puede tener éxito siempre que dentro del periodo en el que se efectúa el envío de los datos a añadir, no se haya iniciado el envío de datos por parte de uno de los dispositivos atacados.

La forma de solucionarlo, sería igual que en el anterior caso, usando la firma de los datos transmitidos o incluso un cifrado completo de los datos para garantizar la confidencialidad.

3.3.5. Ataque de hombre en el medio (MitM) y de *Relay*

Este tipo de ataque, muy conocido en el mundo de la seguridad informática, se basa en la incorporación de un tercer elemento en el medio de una comunicación que hace de intermediario entre los elementos principales de la comunicación.

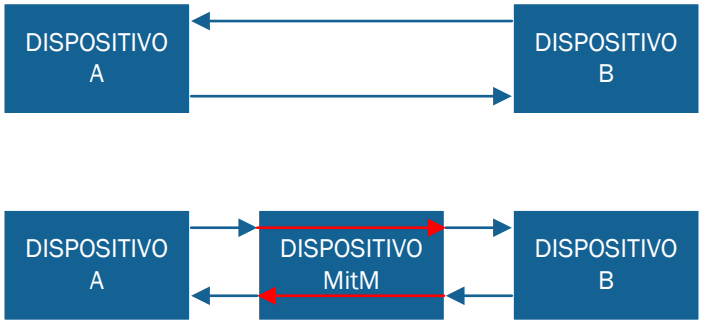

Ilustración 4. Ejemplo de ataque Man in the Middle clásico

De esta forma, no solo podremos escuchar la comunicación que se efectúa entre los dos interlocutores principales, sino que también podremos modificar dicha comunicación de una forma mucho más sencilla que en los apartados explicados anteriormente.

En el caso de NFC, para poder realizar este ataque serían necesarios dos dispositivos NFC activos o uno con dos antenas, ya que sería necesario que se establecieran dos campos de comunicación independientes y separados. Este ataque se denomina ataque de relé (relay attack).

Ilustración 5. Ejemplo de ataque de relé (relay attack) en NFC

Existen varios documentos de investigadores en los que este tipo de ataques se ha realizado con éxito en pruebas de laboratorio, como el indicado en el documento “Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones” (Francis, Hancke, Mayes, & Markantonakis, 2012) u otro, más actual, en el que el propio servicio que Google (Google, s.f.) ofrece para pagar mediante el uso del móvil, *Google Wallet* (Google Wallet, s.f.), es atacado exitosamente (Roland, Langer, & Scharinger, 2013).

Una posible solución a estos ataques es el uso del mecanismo *distance bounding* (delimitar distancias), basado en analizar el comportamiento que suele tener el dispositivo original en cuanto a las latencias de respuesta, pero se ha demostrado que esto no es eficiente en todos los casos.

La mejor solución sería utilizar una autenticación mutua segura mediante un secreto pre-compartido que tanto el dispositivo A como el B ya conozcan previamente, o lo más ideal, mediante una infraestructura de clave pública (PKI), de forma que los dispositivos NFC pasivos ya tuvieran un certificado previamente instalado de fábrica o se provisionara en el

momento de configurar la tarjeta por el proveedor del servicio. Para los lectores también sería recomendable que tuvieran otro certificado. Aunque esta solución no dejaría de tener problemas de seguridad si no se lograse, por ejemplo, que todos los dispositivos pudieran consultar la lista de revocación de certificados de la entidad certificadora o de qué forma un elemento como la tarjeta podría comprobar fehacientemente, por ejemplo, que los certificados no hayan caducado (Nithyanand, Tsudik, & Uzun, 2011).

3.4. Amenazas y vulnerabilidades basadas en dispositivos NFC pasivos

Como se ha comentado anteriormente, los dispositivos NFC pasivos son aquellos que necesitan ser alimentados por el otro interlocutor, que debe ser activo. En este apartado vamos a clasificar los principales tipos de dispositivos pasivos que existen basándonos en su funcionalidad y haciendo especial énfasis en las amenazas y vulnerabilidades que actualmente existen sobre estos.

**NOTA: Para realizar la metodología, aunque se enumeran los tipos de elementos más usados, se ha reducido el estudio de las amenazas y vulnerabilidades, ya que la cantidad de dispositivos que nos podemos encontrar en una implementación es bastante elevada. Al menos, el marco de aplicación de la metodología especificado en el apartado "5.3 Definición de un marco de aplicación de la metodología" está completo, por lo que se puede empezar a aplicar la metodología sin problemas. Estos apartados se señalizan con el acrónimo TBD en la tabla resumen.*

3.4.1. Dispositivos NFC pasivos cuya función principal es el almacenamiento de datos:

- Dispositivo Broadcom – Topaz (Compatible con NFC Forum Tag – Tipo 1) (NFC Forum Mandated Type 1 Tag Format, 2007): Son dispositivos para almacenar información en formato NDEF. Poseen funciones para escribir una vez y que solo se permita la lectura muchas veces (WORM). Su identificación se realiza mediante la lectura del UID, por lo que no es segura, así que puede ser emulada.
- Dispositivos de NXP MiFARE Classic (original y EV1): el primer dispositivo presenta varios vectores de ataques por el que se puede llegar a acceder a toda la información que contiene. El dispositivo MiFARE Classic EV1 es una revisión mejorada que soluciona muchas de las debilidades que presenta el primer dispositivo excepto una,

que se basa en que sigue usando el protocolo propietario CRYPTO1 para realizar cifrados de flujo. Estos ataques son sencillos de realizar (Meijer & Verdult, 2015) incluso con un simple teléfono móvil y una tarjeta *Proxmark III* (van Dijk, Sangers, & Davis, 2016).

- Dispositivos de NXP MiFARE Plus (original, S, SE, X y EV1): Estos dispositivos son vulnerables a un ataque al protocolo CRIPTO-1 siempre y cuando podamos obtener una de las claves de acceso (Meijer & Verdult, 2015).
- Dispositivos de NXP MiFARE Ultralight (original, Nano, EV1 y C) (Compatible con NFC Forum Tag – Tipo 2): La seguridad de estos dispositivos depende de la implementación y la aplicación en la que se usen. La manipulación de estas tarjetas es bastante alta, por lo que se deberían aplicar controles de su uso en algún proceso centralizado de BackOffice en la implementación.

En la siguiente tabla se muestra un resumen de las vulnerabilidades encontradas en estos dispositivos:

Dispositivo / Amenazas	Lectura no autorizada	Escritura no autorizada	Extracción de claves	Control tarjeta original débil	Clonado posible	Emulación posible	Escuchas efectivas	Relay Attack
Broadcom - Topaz (NFC Forum TAG. Tipo 1) ISO/IEC 14443A (parte 2)	N/A	NO	N/A	SI	TBD	TBD	TBD	**SI**
NXP - MiFARE Ultralight (original) (NFC Forum TAG. Tipo 2) ISO/IEC 14443A (partes 2-3) + protocolo propietario NXP	NP	TBD	TBD	SI	TBD	TBD	TBD	**SI**
NXP - MiFARE Ultralight Nano (NFC Forum TAG. Tipo 2) ISO/IEC 14443A (partes 2-3) + protocolo propietario NXP	N/A	N/A	N/A	SI	TBD	TBD	SI	**SI**
NXP - MiFARE Ultralight EV1 (NFC Forum TAG. Tipo 2) ISO/IEC 14443A (partes 2-3) + protocolo propietario NXP	TBD	TBD	TBD	SI	TBD	TBD	SI	**SI**
NXP - MiFARE Ultralight C (NFC Forum TAG. Tipo 2) ISO/IEC 14443A (partes 2-3) + protocolo propietario NXP	TBD	TBD	TBD	SI	TBD	TBD	NO	**SI**
NXP – MiFARE Classic ISO/IEC 14443A (partes 2-3) + protocolo propietario MiFARE	**SI**	**SI**	**SI**	**SI**	**SI**	**SI**	NO	**SI**
NXP – MiFARE Classic EV1 ISO/IEC 14443A (partes 2-3) + protocolo propietario MiFARE	**SI**[1]	**SI**[1]	**SI**[1]	**SI**	**Si**	**SI**	NO	**SI**

[1] Posible si se conoce la una de las claves de acceso (Meijer & Verdult, 2015)

Dispositivo / Amenazas	Lectura no autorizada	Escritura no autorizada	Extracción de claves	Control tarjeta original débil	Clonado posible	Emulación posible	Escuchas efectivas	Relay Attack
NXP – MiFARE Plus S ISO/IEC 14443 A	**SI**[1]	**SI**[1]	**SI**[1]	NO	NO	NO?	NO	**SI**
NXP – MiFARE Plus SE ISO/IEC 14443 A	**SI**[1]	**SI**[1]	**SI**[1]	NO	NO	NO?	NO	**SI**
NXP – MiFARE Plus X ISO/IEC 14443 A	**SI**[1]	**SI**[1]	**SI**[1]	NO	NO	NO?	NO	NO
NXP – MiFARE Plus EV1 ISO/IEC 14443 A + ISO/IEC 7816-4	**SI**[1]**?**	**SI**[1]**?**	**SI**[1]**?**	NO	NO	NO?	NO	NO

Tabla 1. Listado de amenazas y vulnerabilidades de dispositivos NFC pasivos de almacenamiento de datos.

3.4.1. Dispositivos NFC pasivos cuya función principal no es el almacenamiento de datos, aunque lo incluyan.

En este apartado estudiaremos los dispositivos que se denominan SmartCards, cuya función principal no sea la de almacenar datos, sino que estén configurados para la ejecución de aplicaciones. Parte de estos dispositivos podrían emular tarjetas de almacenamiento de datos, como sería el caso del dispositivo MiFARE DESfire EV2, que podría emular tarjeta MiFARE Classic.

Estos elementos se caracterizan por ofrecer una total compatibilidad con el Estándar ISO/IEC 14443 (excepto los que no tengan la forma física de una tarjeta normalizada por la parte 1 de este estándar) y tienen soporte también para el protocolo de aplicaciones especificado en el estándar ISO/IEC 7816-4. Esta compatibilidad permite la existencia de tarjetas que pueden ser utilizadas a través de NFC o a través de los contactos físicos que poseen en la tarjeta.

El nivel de seguridad ofrecido por estas tarjetas se basaría más en la implementación realizada de las aplicaciones contenidas internamente, y no por el diseño de la tarjeta en sí. Aunque es posible que éstas puedan verse afectadas por el ataque de *Relay* si no se diseñan con un mecanismo que lo detecte.

Sobre estas tarjetas, prácticamente no existe literatura que encuentre problemas en su diseño, ya que dichos problemas es más fácil encontrarlos en la implementación que se realiza con ella.

Si tuviéramos que analizar un dispositivo de este tipo y quisiéramos elegir el más extendido en España, tendríamos que hablar del DNIe en su versión 3.0. Este dispositivo es un ejemplo

de tarjeta que cumple el estándar ISO/IEC 14443 (tipo B). Por encima de la capa 4 de la ISO/IEC 14443, se sitúa el estándar ISO/IEC 7816-4, y, a su vez, por encima de esa capa, se ofrecen dos aplicaciones:

- ePassport (MRTD): Esta aplicación está estandarizada por el ICAO (ICAO - Doc 9303 - Sevent Edition, 2015). Una de las funcionalidades del MRTD es que, mediante una autenticación con información que aparece impresa en el documento que se realiza con un mecanismo denominado BAC, se pueden acceder a ciertos datos personales del titular del documento. Existe un procedimiento documentado sobre un ataque al mecanismo de autenticación BAC, basado en la escucha de la comunicación entre un terminal de lectura y el propio documento y el posterior ataque por fuerza bruta (Liu, Kasper, Lemke-Rust, & Paar, 2007). Este ataque, que realmente demuestra un fallo de seguridad muy grave por el ataque a la confidencialidad de los datos del portador, es poco útil, ya que el único sitio donde realmente se leen estos documentos es en los controles de aduanas y estos sitios siempre están llenos de policías … ¿Quién se atreve a poner una antena a menos de un metro de los dispositivos de lectura?
- PKCS#15 Signature Application: Es la aplicación en la que residen la cadena de certificados públicos del DNI y los dos certificados privados que se asignan a cada persona, uno cuya función principal es la de autorizar, y otro cuya función principal es la de firmar. Esta aplicación esta implementada en base al estándar ISO/IEC 7816-15 (ISO/IEC 7816-15:2016, 2016) *Identification cards -- Integrated circuit cards -- Part 15: Cryptographic information application*.

Otro dispositivo que se englobaría dentro de los que llamamos SmartCards, sería el del fabricante NXP – MiFARE DESFire (original, EV1 y EV2). Es compatible con NFC Forum Tag – Tipo 4. Se ha documentado la extracción de claves de la tarjeta original mediante un ataque de canal lateral (Oswald & Paar, Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World - Extended Version, 2011) y mediante un ataque usando un análisis diferencial de energía (DPA) que también se basa en un ataque de canal lateral (SDA). Debido a esto, NXP dejó de comercializar la tarjeta clásica en el año 2011 (Update on MIFARE DESFire (MF3ICD40), 2011). Sobre las versiones clásica y EV1 hay un estudio que ha logrado emular, al menos parcialmente, el funcionamiento de la tarjeta en base al uso de un microcontrolador programable (Kasper, von Maurich, Oswald, & Paar, 2010). Sobre la versión EV2, que ya ha sido anunciada por el fabricante, no hay ninguna referencia en artículos de investigación (ni siquiera en todo internet) y tampoco se encuentran sitios en Internet donde comprarla, por lo que es posible que el fabricante todavía no la haya puesto a la venta.

Esta tabla representa un resumen de los dispositivos que hemos analizado junto a las vulnerabilidades que los comprometen:

Dispositivo / Amenazas	Lectura no autorizada	Escritura no autorizada	Extracción de claves	Control tarjeta original débil	Clonado posible	Emulación posible	Escuchas efectivas	Relay Attack
NXP – MiFARE DESFire (NFC Forum TAG. Tipo 4) ISO/IEC 14443A + ISO/IEC 7816-4	**SI**	**SI**	**SI**	SI	NO?	SI	NO	**SI**
NXP – MiFARE DESFire EV1 (NFC Forum TAG. Tipo 4) ISO/IEC 14443A + ISO/IEC 7816-4	NO	NO	NO	SI	NO	SI	NO	**SI**
NXP – MiFARE DESFire EV2 (NFC Forum TAG. Tipo 4) ISO/IEC 14443A + ISO/IEC 7816-4	NO	NO	NO	NO	NO	NO	NO	NO
DNIe version 3.0 ISO/IEC 14443 B + ISO/IEC 7816-4 + Aplicacion MRTD + Aplicación PKCS15#	NO	NO	NO	NO	NO	NO	NO	NO

Tabla 2. Listado de amenazas y vulnerabilidades de algunos Dispositivos SmartCard con múltiples aplicaciones.

3.5. Amenazas y vulnerabilidades basadas en dispositivos NFC activos

En todas las implementaciones NFC los dispositivos activos juegan un papel fundamental en el éxito de la explotación de dicha implementación. Estos dispositivos se suelen proteger de tal forma que no se puedan manipular, robar o romper. Tan importante es la integridad física de estos dispositivos como su integridad lógica. Es necesario proteger dichos dispositivos, de tal forma, que se garantice la integridad tanto del propio dispositivo NFC como de los elementos que están asociados a él. Por ejemplo, un terminal de pago para tarjetas de crédito, si fuese manipulado se podría utilizar para extraer datos de las tarjetas de los usuarios o para realizar cargos ilícitos. Otro ejemplo sería el de un terminal de alquiler de bicicletas, en el que se han dado casos de sabotajes a través del acceso a ellos de forma remota para instalar software no autorizado que compromete su integridad (Periódico El Mundo, 2014).

Pero hay que tener en cuenta que, un posible robo de los terminales, podría comprometer las posibles claves que contuviera el sistema, por lo que se deben usar mecanismos que garanticen la confidencialidad, como por ejemplo, el cifrado del almacenamiento interno de dichos sistemas mediante el uso de elementos seguros como, por ejemplo, un TPM (Ramírez, 2013).

Otra opción sería que dichos dispositivos no tengan ninguna información crítica en ellos, sino que establezcan una comunicación directa con un servicio externo y que toda la comunicación entre el dispositivo activo y dicho servicio central se realice de manera cifrada. Un sistema de este estilo, por ejemplo, se usaba para realizar ciertas acciones sobre el DNIe, como el cambio del PIN, (DGPGC, 2014), en el que se establecía un canal seguro entre la propia tarjeta del DNIe y los servidores que gestionan realmente el cambio del PIN, aunque este procedimiento ya no se ofrece de forma telemática.

3.6. Amenazas y vulnerabilidades basadas en la lógica de la implementación de la solución

Muchas de las soluciones que se desarrollan actualmente se realizan desde un punto de vista muy alejado de la seguridad. Aunque se disponga de una buena planificación para la realización de un proyecto, la realidad indica que suelen darse muchos problemas durante su desarrollo, como cambios en las especificaciones cuando se está en una etapa muy avanzada del desarrollo o que se retrase el desarrollo y los plazos de entrega provoquen que se haga hincapié en que todo funcione “ya”, de la forma que sea. También es muy común que no se tenga en cuenta la seguridad del sistema, por lo que el diseño ya se realiza con defectos de seguridad desde el principio.

Aunque podríamos enumerar muchos más motivos, lo cierto es que, al final, es fácil encontrar implementaciones con defectos en su lógica que, una persona con experiencia, podría llegar a detectar y explotar en cuestión de minutos.

Los sistemas actuales que usan NFC no se quedan cortos ante este problema, pudiendo encontrar vulnerabilidades debidas a un mal diseño en, por ejemplo, sistemas de tarjetas monedero para *vending*, transporte de pasajeros y controles de acceso.

En algunos casos son errores que, tras la auditoría de un experto, salen a la luz, pero todavía hay desarrollos en los que las personas involucradas utilizan código fuente de ejemplos que contienen las APIs de programación que, incluyen contraseñas por defecto, y son desplegados en producción sin haberse preocupado por cambiar dichas contraseñas (Courtois, 2009).

3.7. Amenazas y vulnerabilidades basadas en la fuga de información interna.

Es importante tener en cuenta que cuando se va a realizar un despliegue de dispositivos con tecnología NFC, se suele hacer protegiéndolos con algún tipo de mecanismo para que los dispositivos no se vean comprometidos. Estos mecanismos pueden basar su protección en algo tan sencillo como una contraseña, que puede ser única para todos los dispositivos, o en un certificado, que sería mucho más robusto.

Es importante que esa información pueda ser consultada exclusivamente por las personas que lo requieran para su trabajo y solamente en los momentos que necesiten dicha información, por lo que deberá almacenarse de forma que se asegure que no pueda ser accedida por terceros, ya sea mediante listas de acceso, cifrándola o aplicando tanto cifrado como listas de acceso.

En caso de que el mecanismo utilizado para proteger los dispositivos NFC pasivos sea una clave o contraseña única, deberían tomarse medidas adicionales, como el cifrado del contenido interno. Esto incorporaría un factor doble de seguridad, ofreciendo integridad y confidencialidad de la información contenida.

También se podría implementar una contraseña que fuera diferente en todos los dispositivos. Esto se podría realizar calculándola mediante un algoritmo en el que se usase una clave única y un dato dinámico del interior del dispositivo (UID o bloque/sector que nunca modificaríamos). Este algoritmo y las funciones de seguridad que apliquemos también deberán ser protegidas de personas que no necesiten conocer lo que hacen esos algoritmos ni cómo lo hacen.

Para que los códigos de acceso de las tarjetas o los algoritmos que se usan para calcularlos no caigan en manos ajenas, se deberían realizar auditorías que verifiquen que la seguridad donde se almacenan dichos datos sea correcta. Se debería evitar que esas contraseñas caigan en manos de terceros, incluso cuando abrimos casos de soporte con una empresa de confianza, nos deberemos asegurar que los archivos que enviamos no incluyan dichas contraseñas.

Si, por ejemplo, se desvelase la contraseña maestra de una tarjeta como la MiFARE DESFire EV1, y ésta fuera usada en toda una infraestructura, los daños que de un mal uso de ella se pudieran hacer, podría ocasionar que una empresa quebrara si no se tomasen medidas de forma rápida y ágil.

De todas formas, las contramedidas expuestas en este apartado, que en principio pueden parecer excesivas, han de valorarse si se deben y/o pueden implementar basándose en el escenario final, teniendo en cuenta el alcance de la instalación y sus objetivos. Es decir, podría tener sentido ponerlas en práctica para una aplicación en la que ciertos dispositivos se usen como monederos o para pagar servicios de transporte, ya que estos dispositivos serían distribuidas entre los usuarios finales y estarían en su posesión permanentemente. Si algún usuario tuviera acceso a las claves, como tendría la tarjeta en su posesión, podrían acceder y modificar la información que contienen, comprometiendo la integridad de la solución.

4. Hipótesis de trabajo y objetivos concretos de la investigación

4.1. Objetivo general

Hemos visto como el uso de la tecnología NFC está creciendo debido al apoyo de la industria y a la gran aceptación entre los usuarios. También hemos repasado brevemente las amenazas y las vulnerabilidades asociadas actualmente a esta tecnología y como algunas de ellas se están explotando con éxito. Hemos de recordar que la seguridad es algo imposible de conseguir al 100%, pero que el nivel de seguridad que debemos de conseguir ha de ser acorde a los objetivos de la solución implantada o que hay que implantar.

Debido a la situación de las implementaciones actuales, y viendo que en muchos casos el nivel de seguridad es muy deficiente debido a motivos como el desconocimiento, el objetivo de crear una metodología es que tanto las implementaciones existentes como las que se vayan a desarrollar puedan ser evaluadas para poder saber si implementan un nivel de seguridad suficiente.

4.2. Objetivos específicos

La metodología ha de ser diseñada para poder evaluar una solución en cualquiera de sus fases, ya sea la fase de diseño, desarrollo, piloto o producción. Por lo tanto, deberemos establecer unos objetivos específicos sobre qué es lo que esperamos conseguir con la aplicación de la metodología:

- Analizar la solución (estudio inicial):
    - Objetivo del uso de la tecnología NFC.
    - Aplicación del uso que se va a dar a la tecnología NFC.
    - Calcular el alcance de la aplicación, en cuanto a estimación de usuarios finales, ámbitos de aplicación, etc…
    - Dispositivos NFC que van a utilizarse.
    - Dispositivos no NFC que van a dar soporte a los dispositivos NFC.
    - Procesos y algoritmos que van a interactuar entre los dispositivos NFC y los dispositivos que los soportan, así como con los datos que se utilicen en la solución y donde se almacenan estos (lógica de la aplicación/implantación)

- Realizar un informe donde:
    - Se detecten las fortalezas y debilidades que se han encontrado. Esto se ha de realizar enumerando los riesgos detectados y valorándolos de forma objetiva (Informe técnico).
    - Se resuma de forma clara y con un lenguaje entendible, los riesgos encontrados en la solución (Informe ejecutivo).
- Opcionalmente, cada aplicación de la metodología servirá para mejorar la propia metodología mediante la aplicación de los procesos diseñados específicamente para esta tarea.
- El objetivo para la organización que aplique esta metodología sería:
    - Determinar el nivel de riesgo de la solución y valorar como se ha de gestionar. Este paso lo debería realizar la empresa, si fuera procedente, mediante un proceso de gestión de riesgos.
    - Gestionar dichos riesgos según se vayan a asumir los riesgos.
    - Volver a aplicar la metodología (actualizada) cada año.

4.3. Metodología del trabajo

Debido a los cambios que se producen en todas las tecnologías, es importante que la metodología se mantenga actualizada teniendo en cuenta la aparición de nuevas necesidades o usos, tanto por la modificación o incorporación de estándares que cubren la tecnología NFC como por la adición de nuevas mejoras e innovaciones en dicha tecnología, u otros aspectos que se deban tener en cuenta, como la aparición de nuevas amenazas y vulnerabilidades.

Esto hace necesario que esta metodología se revise utilizando una metodología similar a un plan de mejora continua, en la que los cambios producidos por estándares, normas, amenazas, vulnerabilidades u otros de diversa consideración que hayan de tenerse en cuenta, hagan necesario que la metodología tenga que revisarse para ser adaptarse.

Inicialmente, se realizará un desarrollo de una metodología teniendo en cuenta el estudio del arte realizado en cuanto los aspectos técnicos de la tecnología NFC, las amenazas y vulnerabilidades que la acompañan y los objetivos generales y específicos que se esperan de su aplicación.

Una vez realizada la metodología, ésta se debe poner en práctica y/o se deberán realizar unas encuestas sobre su aplicación a personal experto en la materia. La realización de estas acciones tendrá como entregable un informe de mejora de la metodología, en el que se

recogerán los aspectos que habría que mejorar, según el punto de vista de los roles que la aplican. Este informe deberá ser tratado por las personas encargadas de realizar la metodología para estudiarlo y, si corresponde, aplicar las mejoras que correspondan.

Periódicamente y como máximo cada año, deberán repetirse los procesos de Estudio de la tecnología y de sus amenazas y vulnerabilidades, de tal forma que, en caso de ser necesario, se revísela metodología para adaptarse a los cambios detectados.

Después de realizar los anteriores procesos, tendríamos una nueva versión de la metodología.

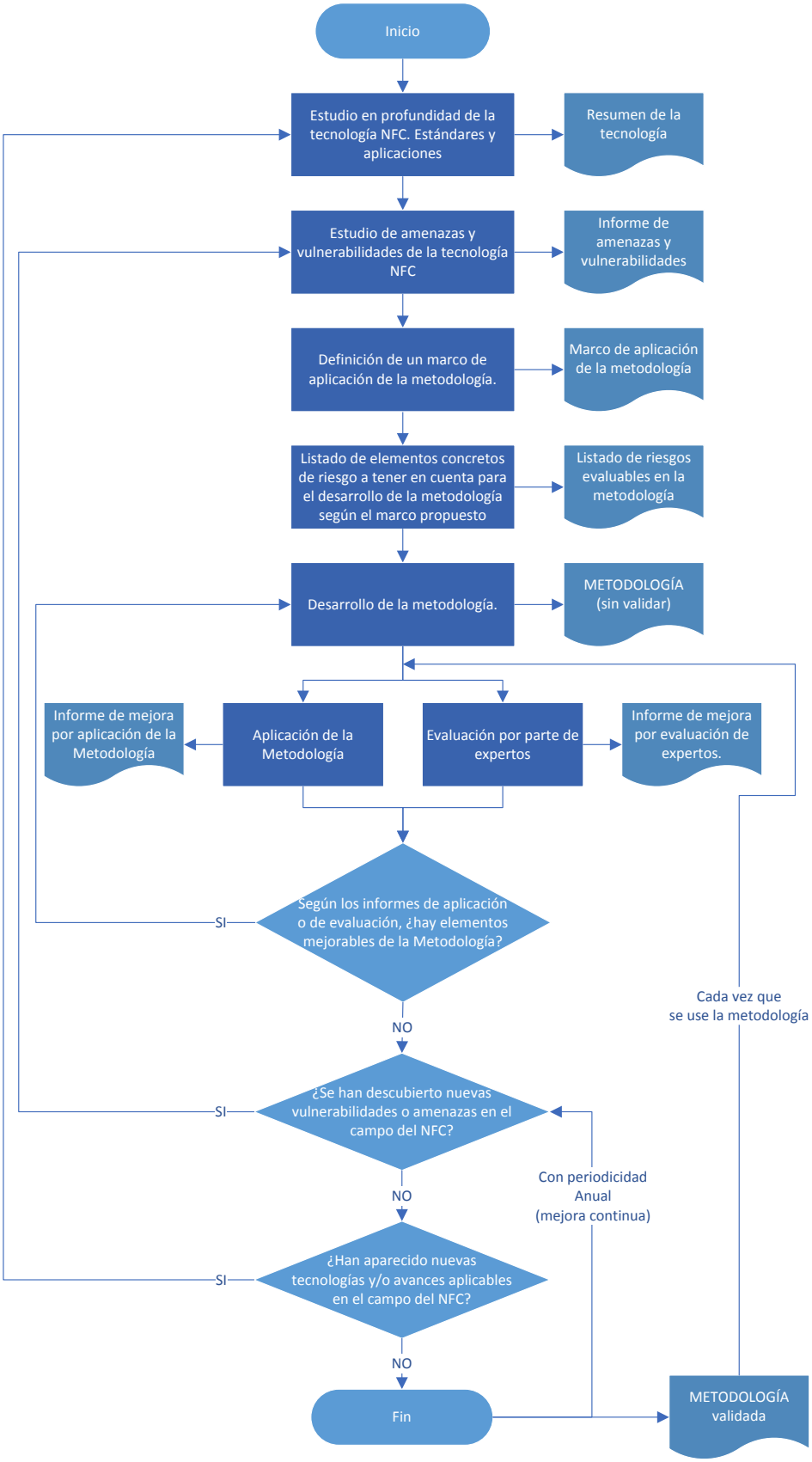

Ilustración 6. Procesos, entregables y decisiones para el desarrollo de la metodología.

Para poder dar por válida una nueva versión de cada metodología debería ser aplicada un número de veces suficiente que demuestre su validez o debería ser examinada por una serie de personas expertas o un grupo formado por éstas.

Sería importante que cada vez que se aplique la metodología se realice el informe correspondiente para poder evaluar si es necesario modificar la metodología y se haga llegar a dicho grupo de personas o grupo de expertos para que lo analice.

5. Desarrollo de la metodología

Los apartados anteriores han servido para conocer el funcionamiento de la tecnología NFC, las amenazas y las vulnerabilidades que se pueden asociar y los objetivos que queremos conseguir con la metodología.

Para poder desarrollar una primera versión válida de la metodología, empezaremos por acotar el marco de trabajo lo necesario como para abarcar un gran número de amenazas y vulnerabilidades que podríamos encontrarnos, y para que sea lo suficientemente manejable como para poder probar si la metodología es efectiva y fácil de aplicar.

Para realizar el desarrollo de esta metodología, en los siguientes apartados de este capítulo:

- identificaremos los roles necesarios para que pueda ser llevada a cabo,
- planificaremos la ejecución de la metodología en fases para poder planificar mejor las tareas asociadas,
- definiremos un marco de aplicación que, aunque sea limitado en esta primera versión, cubra muchos de los aspectos importantes de la tecnología NFC,
- identificaremos los requisitos para poder aplicarla en base a todo lo anterior,
- desarrollaremos los pasos de la metodología y
- haremos una evaluación para medir su eficacia aplicándola a una solución del mundo real de tamaño medio.

5.1. Roles necesarios para la ejecución de la metodología

El diseño de la metodología se va a basar en un análisis de riesgos simplificado y orientado a los aspectos que hemos de analizar para poder verificar que la implementación de la tecnología NFC se hace en base a unos riesgos adecuados. Hemos de partir del hecho de que la seguridad total es imposible, y que el máximo nivel de seguridad tampoco es el adecuado para todas las implementaciones, ya que un nivel de seguridad que se acerque al 100% aumentaría el coste de los proyectos y no siempre va a ser necesaria. Es por ello que, una vez aplicada la metodología y con los informes en la mano, se debe decidir si el nivel de seguridad que aporta la solución es adecuado a lo que se necesita. Esta tarea, que no estaría dentro de la competencia de la metodología, dependería de un responsable de la empra que podría ser el CTO, el CEO, el CISO, jefe de proyecto o una figura similar. De las decisiones

que salgan del análisis que se realice se tomarán o no las medidas correctivas oportunas sobre la solución para mejorar la seguridad.

En cuanto a la ejecución de la metodología, sí que van a ser necesarios varios roles. El primero sería el propio responsable de llevarla a cabo, que podría ser alguien externo a la organización o incluso alguien interno de la empresa o hasta del propio proyecto. En principio no tendría que haber ningún requisito especial, aunque si que sería recomendable que tuviera ciertos conocimientos técnicos sobre NFC de tal forma que las realizaciones de los informes sean coherentes con la realidad.

Otro de los roles que han de colaborar son jefes del proyecto, desarrolladores, ingenieros de sistemas y otros roles que colaboren en la realización del proyecto o hayan colaborado en su día. Estos roles son importantes porque son los que tendrán un conocimiento profundo de la solución de tal forma que las respuestas a las preguntas sean acordes a la realidad. Es importante indicar a los roles que, si algo no lo saben con seguridad, que no lo contesten o que investiguen cual es la respuesta correcta. También es muy importante transmitirles que han de ser imparciales y objetivos en sus respuestas.

5.2. Fases de la ejecución de la metodología

La ejecución de la metodología se ha de realizar en tres fases. El objetivo de dividir la ejecución de la metodología es organizar la fase en tareas similares y asignar los recursos necesarios que harán falta y que serían los siguientes:

- **FASE 1 - Obtención de información**: En esta fase hará falta contar con la colaboración de los roles que han definido o están definiendo la solución y que conocen la aplicación con gran profundidad. Las acciones que se realizarán en esta fase serán:
    - Identificar la aplicación o aplicaciones que se quiere dar a la tecnología NFC dentro de la solución.
    - Identificar los tipos de localizaciones en los que habrá dispositivos NFC activos no de usuario.
    - Identificar los tipos de roles que van a ser usuarios de la aplicación y si estos van a ser internos o externos, así como los dispositivos NFC que van a usar.
    - Identificar los tipos de roles y sus funciones en cada fase del proyecto (Ej: desarrollo, piloto, producción) y que van a realizar tareas internas como las de soporte y administración de la aplicación.

  - Identificar los elementos hardware y software que gestionan la infraestructura NFC.
  - Completar los cuestionarios necesarios sobre los elementos identificados anteriormente.

- **FASE 2 – Realización de informes técnico y ejecutivo**: Para esta tarea se realizará un análisis de la información obtenida en la fase 1, identificando las amenazas y vulnerabilidades que se hayan podido detectar y calculando el riesgo que aportan en cada caso. Una vez realizados estos informes, el informe técnico deberá ser entregado y revisado por el responsable del proyecto, y el informe ejecutivo deberá ser entregado y revisado por el responsable de la empresa (CEO, CTO, CISO, …). Es posible que haya que modificar los informes, si una vez revisados por los responsables de la empresa se detecta que hay información que no se corresponde con la realidad.
- **FASE 3 – Realización de informe para mejora de la metodología (opcional)**: Tanto por parte del auditor, como por parte de los responsables de la empresa, en caso de ser necesario, deberán realizar un escrito de las partes que podrían ser mejoradas en la metodología, de tal forma que pueda ser tenida en cuenta para mejorarla. También se podrían tener en cuenta los comentarios realizados en los cuestionarios de la primera fase, ya que también podrían aportar mejoras para la metodología. Esta fase podría ser opcional, pero sería muy recomendable que se ejecutara para que el conocimiento adquirido durante su ejecución pueda ser aplicado a futuras ejecuciones.

5.3. Definición de un marco de aplicación de la metodología

Como indica el título de esta metodología, uno de los límites que definen el marco de aplicación de la metodología es que en la solución en el que se aplique solo se utilicen dispositivos pasivos en la parte del usuario final, de tal forma que no vamos a contemplar que el usuario utilice dispositivos activos como teléfonos móviles.

Otra restricción que vamos a poner para poder desarrollar la metodología de una manera más sencilla, es que el dispositivo pasivo sea una tarjeta MiFARE Classic o MiFARE Classic EV1. Esta restricción solo tiene la función de simplificar el desarrollo de la metodología y la ventaja de que estaremos aplicando una de las tarjetas con mayor despliegue en soluciones que se encuentran en producción en el mundo real y que contienen una serie de debilidades que sirven para poner a prueba muchos de los aspectos de la metodología.

Como esta es una metodología abierta a cualquier tipo de mejoras y avances en la tecnología NFC, se podrían incluir cualquier tipo de tarjetas pasivas siempre que se realice un análisis exhaustivo de las amenazas y vulnerabilidades que las puedan afectar. Incluso una vez que la metodología haya adquirido un nivel de madurez alto, se podría plantear la inclusión de dispositivos activos en la parte del usuario.

Por lo tanto, el ámbito ideal que debería definir el marco de aplicación, tendría que contemplar la aplicación en cualquier solución que utilice NFC, como, por ejemplo, sistemas de transporte público, sistemas de control de acceso a edificios y sistemas de pago en máquinas de *vending,* realización de acciones automáticas tras lectura de etiquetas, control de activos, domótica, …

5.3.1. Listado de elementos concretos de riesgo a tener en cuenta para el desarrollo de la metodología según el marco propuesto

Los elementos que vamos a analizar en este apartado son los definidos por el marco de aplicación de la metodología. Estos elementos se consultarán después de haber realizado la primera fase para conocer en detalle las amenazas y vulnerabilidades que podrían aportar a la solución.

- Tarjeta NXP MiFARE Classic (original): Esta tarjeta incorpora muchas vulnerabilidades en su implementación que pueden poner en peligro la integridad y confidencialidad de los datos que contiene internamente, ya que el acceso a dichos datos está protegido por contraseña y existen ataques por los que se pueden obtener dichas contraseñas en cuestión de segundos. Otra amenaza posible es la originalidad de la tarjeta, ya que existen diferentes maneras de duplicar la tarjeta de forma que no se pueda detectar, como la emulación o la clonación. Por lo tanto, éstos serían los riesgos que incorporaría el uso de dichas tarjetas:
    - Control de acceso: CRIPTO1 (Riesgo: ALTO): Se usan contraseñas que son recuperables mediante ataque.
    - Datos contenidos (Riesgo: ALTO): Al poder calcular las contraseñas, se podría acceder a todos los datos de la tarjeta e incluso modificarlos.
    - Unicidad de la tarjeta: UID de 7 bytes (Riesgo: ALTO): Posibilidad de clonar y emular la tarjeta.

- Tarjeta NXP MiFARE Classic EV1: Esta tarjeta incorpora menos vulnerabilidades que la anterior, pero al seguir usando el protocolo CRIPTO1, es vulnerable a ataques por los que podemos acceder a sus datos. Estos serían los riesgos del uso de la tarjeta:
    - Control de acceso: CRIPTO1 (Riesgo: MEDIO/ALTO): Aún sin poder calcular las contraseñas es posible acceder y modificar el contenido de la tarjeta.
    - Datos contenidos (Riesgo: MEDIO/ALTO): Posibilidad de acceder y modificar el contenido interno.
    - Unicidad de la tarjeta: Se puede realizar de dos formas:
        - Comprobación de UID compatible con modelo anterior (Riesgo: ALTO).
        - Comprobación de firma electrónica de la tarjeta: (Riesgo: MUY BAJO).

Según se vaya ampliando el marco de aplicación, se deberán ir introduciendo en este apartado los elementos analizados en el apartado “3.4 Amenazas y vulnerabilidades basadas en dispositivos NFC pasivos”.

Para el análisis de los demás elementos de riesgo nos tendremos que guiar por todo el apartado “3 Amenazas y vulnerabilidades de la tecnología NFC”.

5.4. Identificación de requisitos para aplicar la metodología

En este apartado indicaremos los requisitos necesarios mínimos para poder aplicar la metodología correctamente. Hay que tener en cuenta que estos requisitos tienen que estar alineados con el marco de aplicación de la metodología, por lo que podrían ir cambiando en sucesivas versiones de la metodología:

- Requisitos técnicos de la solución:
    - Se ha de utilizar la tecnología NFC como medio para conseguir una o varias funcionalidades dentro de la solución.
    - Si un elemento, como el dispositivo NFC de un usuario, es compartido por aplicaciones diferentes de empresas diferentes, se deberá aplicar la metodología dos veces, una por cada aplicación.
    - Los elementos que usarán los usuarios, serán elementos NFC pasivos y deberán de ser uno o varios de los siguientes (si hubiera otros requerirá de un estudio de vulnerabilidades y amenazas, en caso de que no se hubiera realizado anteriormente, y de una valoración de los riesgos del dispositivo que deberán detallarse en el apartado “5.3.1 Listado de elementos concretos de

riesgo a tener en cuenta para el desarrollo de la metodología según el marco *propuesto*":

- MiFARE Classic (versión original).
- MiFARE Classic EV1.

- Requisitos de recursos humanos:
  - Se necesita la colaboración del jefe de proyecto y/o de las personas que conozcan en profundidad la solución sobre la que se soportan todos los dispositivos NFC.
  - Se necesita una persona como responsable de aplicar la metodología. Para las primeras aplicaciones de la metodología sería necesario que tenga una serie de requisitos que, tras realizar los procesos de mejora, deberían reducirse según vaya madurando esta metodología. El uso de personal no cualificado, podría poner en peligro los procesos de mejora de la metodología por lo que partiremos de los siguientes requisitos:
    - Conocimientos técnicos de la tecnología NFC: Medio.
    - Conocimientos técnicos de auditorías de seguridad: Medio/Alto
    - Conocimientos prácticos de análisis de riesgos: Bajo/Medio.
  - En caso de tener que realizar cambios a la metodología, se deben realizar por una persona con grandes conocimientos o un grupo formado por varias personas de este tipo. El éxito de la maduración de la metodología depende de la experiencia, conocimientos y coherencia de quien modifique la metodología. Debido a esto se requerirá siempre una persona o equipo que contenga las siguientes cualidades:
    - Conocimientos técnicos en la tecnología NFC: Alto/Experto.
    - Conocimientos técnicos de auditorías de seguridad: Alto.
    - Conocimientos prácticos de análisis de riesgos: Medio/Alto.
    - Experiencia profesional en el campo de la seguridad: Alto (senior).

5.5. Descripción de la metodología

En este apartado se desarrollarán los pasos concretos que se han de seguir cuando se aplique la metodología.

Se ha optado por un desarrollo en tres fases, de las cuales, las dos primeras serán las necesarias para obtener los objetivos en cuanto a la valoración de los riesgos de la solución

sobre la que se aplique, y la tercera (opcional en su ejecución) será para integrar su aplicación en los procesos de mejora continua de la propia metodología.

Como la fase 3 incluye aplicar una serie de preguntas adicionales en los cuestionarios de la fase 1, estas preguntas han de omitirse si no se va a realizar la fase 3. Estas preguntas se pueden identificar por señalizarse con la etiqueta entre corchetes *[Opcional para mejora de metodología]*. La realización de esta tercera fase, en los momentos iniciales del desarrollo de la metodología o cuando se publique una nueva versión, es muy importante, ya que para que la metodología madure, ésta se ha de retroalimentar con los comentarios de los roles que colaboran durante las fases dos y tres. Para la mejora en cuanto a la adaptación a novedades tecnológicas en el marco de NFC y a las amenazas y vulnerabilidades que aparezcan, ya se incorpora un procedimiento que se ha de ejecutar al menos cada año para que la metodología se mantenga adaptada a la situación de cada momento.

El siguiente diagrama muestra los procesos, los entregables y la decisión de si realizar la FASE 3. Este diagrama servirá de aclaración del proceso de aplicación de la metodología en caso de que hiciera falta.

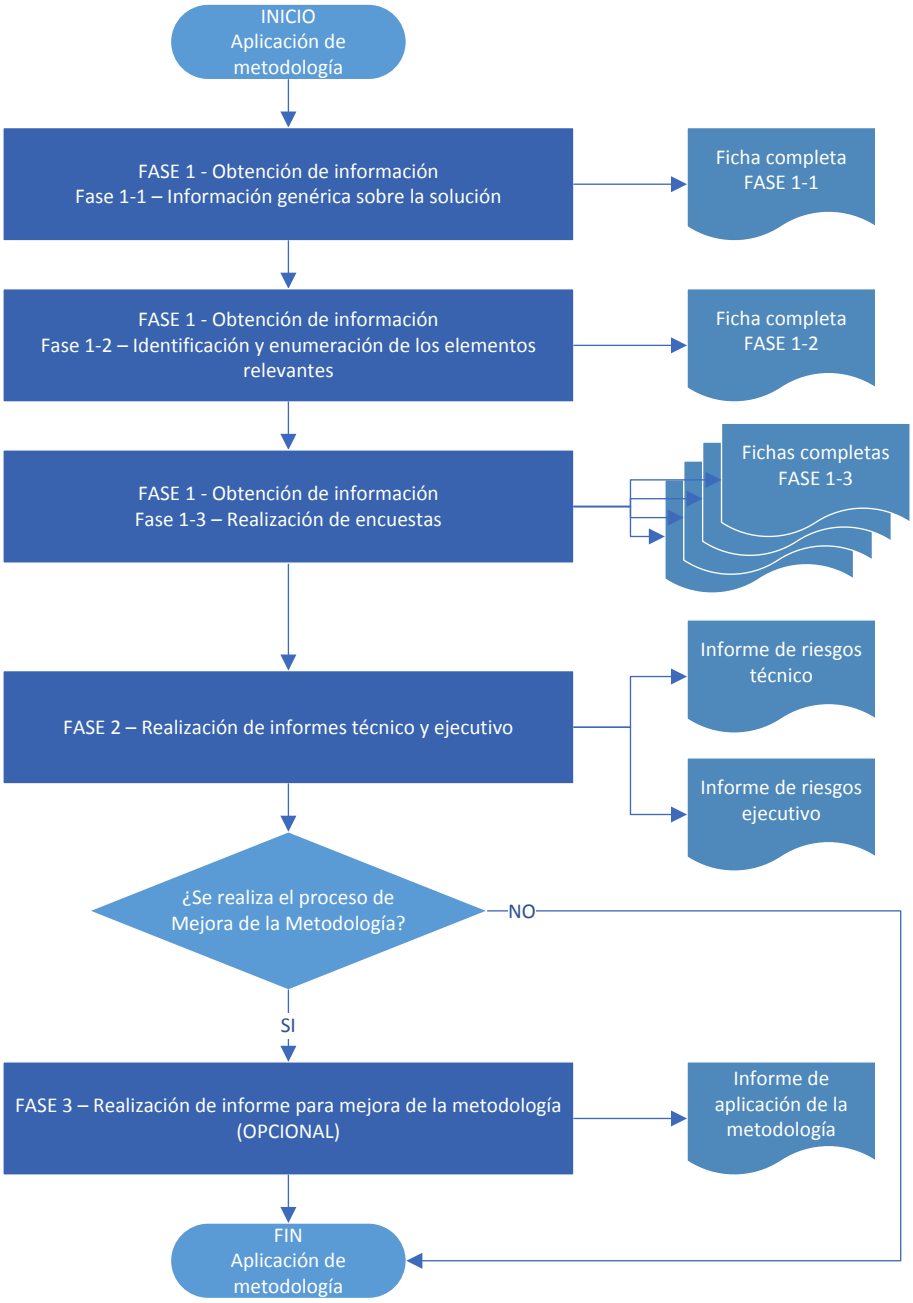

Ilustración 7. Diagrama de procesos, entregables y decisiones para la aplicación de la metodología.

Una vez explicadas las fases que existen y la importancia de la realización de la fase 3, en los siguientes apartados se definen las tareas a realizar en cada fase.

5.5.1. Fase 1 – Obtención de información.

En esta primera fase se deberá recoger toda la información necesaria para poder realizar los informes de seguridad. Esta parte es muy importante y es necesario que se haga de forma concisa, correcta y completa.

Para ejecutar esta fase la vamos a dividir en tres sub-fases, de forma que se pueda adaptar a las diferentes soluciones en las que se pueda aplicar dependiendo de su tamaño.

5.5.1.1. Fase 1-1 – Información genérica sobre la solución

Lo primero que tenemos que solicitar es una serie de información básica sobre la solución en la que vamos a aplicar la metodología. Si la solución está en fase de diseño o desarrollo, las preguntas que se refieren al alcance y que dependan del nivel de implantación/aceptación que pueda haber tenido la solución, deberán responderse con una estimación a uno o dos años de haber implantado en producción dicha solución.

Estas serían las preguntas en las que nos basaremos para solicitar la información necesaria en esta fase:

- ¿Cuál o cuáles son las aplicaciones concretas por las que se usa NFC y qué tipos de operación se realizan?
  Ejemplo: Tarjeta monedero (carga, compra, devolución), tarjeta transporte (carga, cancelación de billete, cancelación de billete por transbordo gratuito), control de accesos (identificación y autenticación de usuario), …

Aplicación	Funciones
<espacio para contestar>	<espacio para contestar>

- Por cada aplicación, ¿Cuántos terminales de lectura existen aproximadamente? ¿Cuántos usuarios totales están dados de alta aproximadamente? ¿Cuál es la estimación de crecimiento de terminales y usuarios para dentro de cuatro años?

<espacio para contestar>

- Por cada aplicación, ¿Cuántos usuarios existen aproximadamente? ¿Cuál es la estimación de crecimiento a cuatro años?

<espacio para contestar>

- ¿Cuál es el alcance o ámbito geográfico de la solución? ¿Cuál es la estimación de crecimiento en cuanto al ámbito geográfico para dentro de cuatro años.?

<espacio para contestar>

- ¿Cuál es el alcance o ámbito geográfico de la implementación? ¿Cuál es la estimación de crecimiento a cuatro años?

<espacio para contestar>

5.5.1.2. Fase 1-2 – Identificación y enumeración de los elementos relevantes

Se debe realizar un listado de todos los elementos relevantes que se han de analizar.

Si el tamaño de la solución NFC es muy grande, como, por ejemplo, un sistema de transporte urbano de una gran ciudad, sería recomendable que este listado pudiera solicitarse a los responsables de los proyectos dándoles el tiempo necesario para poder realizarlo de forma que no se les olvide ningún elemento.

En casos de soluciones pequeñas, como, por ejemplo, un control de acceso en un edificio de tamaño pequeño, sería una tarea mucho más fácil de realizar que podría no requerir más de una hora.

Como la tecnología NFC se puede utilizar para muchas finalidades, no podemos definir en la metodología que elementos concretos hay que enumerar, pero sí que podemos definir una serie tipos de elementos que van a ser relevantes y que van a cubrir la mayoría de los casos. Éstos serían los tipos de elementos a enumerar:

- TIPO A: Identificar y enumerar los tipos de localizaciones en los que existirán dispositivos de lectura/escritura NFC (dispositivos activos) que interactuarán con los usuarios.
  Ejemplo: Tótems públicos (validar usuario, consultar saldo), comercios con terminal de recarga (recarga de tarjetas), autobuses (cancelar billete), …

Localización	Funciones
<espacio para contestar>	<espacio para contestar>

- TIPO B: Identificar y enumerar la marca y modelo de los diferentes dispositivos NFC que van a ser usados por el conjunto de los usuarios de la aplicación (dispositivos pasivos).
  Ejemplo: MiFARE Classic (original), MiFARE DESFire EV2, DNIe 3.0, Pasaporte.

<espacio para contestar>

- TIPO C: Identificar y enumerar los tipos de roles de usuarios que van a usar la aplicación, identificando si son externos (ámbito público) o internos (ámbito privado o de la empresa).
  Ejemplo para gestión de alquiler de bicis: Clientes (externos), Personal mantenimiento bicis (interno), Probadores en producción (interno).

Rol de usuario	Ámbito (Elegir: interno o externo)

<espacio para contestar>	<espacio para contestar>

- TIPO D: Identificar y enumerar los tipos de roles del personal y la fase o fases en las que participaran en la solución (diseño, desarrollo, piloto o producción). Incluir solo los que van a estar implicados en tareas técnicas asociadas al proyecto (desarrolladores, implantadores, ingenieros, técnicos de soporte, …).
  Ejemplo: Desarrolladores (desarrollo, pre-producción), Probadores (pre-producción, producción), Jefe proyecto (diseño, desarrollo, pre-produción, producción, soporte), arquitectos del sistema (diseño, desarrollo), técnicos (producción), instaladores de sistemas (producción).

Rol de personal	Fases de participación.
<espacio para contestar>	<espacio para contestar>

- TIPO E: Especificar si existen los siguientes elementos en la lógica de la aplicación:
  - ☐ Base de datos centralizada.
  - ☐ Recuperación y almacenamiento de datos de registro originados por el uso de tarjetas de usuario.
  - ☐ Procesos de BackOffice (consolidación de usos y comprobaciones).
  - ☐ Procesos de auditorías internas de seguridad.
  - ☐ Procesos de auditorías externas de seguridad.
  - ☐ Se dispone de un diagrama claro de los flujos de información entre los lectores NFC (dispositivos activos) y el núcleo de la aplicación (BBDD, Core APP, APIs, …).
  - ☐ [Opcional para mejora de metodología] Indicar otros elementos relevantes de la lógica de la aplicación que no se hayan tenido en cuenta:

    <espacio para contestar>

- TIPO Z [Opcional para mejora de metodología]: Otros elementos relevantes: En caso de que exista algún elemento relevante que no se pueda clasificar en los anteriores, se deberán especificar en este apartado para su posible inclusión en futuras mejoras de la metodología.

<espacio para contestar>

5.5.1.1. Fase 1-3 – Realización de encuestas

En este apartado y para cada elemento enumerado o identificado en el apartado “5.5.1.2 Fase 1-2 – Identificación y enumeración de los elementos relevantes”, se rellenará un cuestionario del que se obtendrá información más detallada sobre dicho elemento y que servirá para poder

identificar y evaluar los riesgos de forma detallada. Muchas de estas preguntas se han diseñado para tener en cuenta las amenazas y vulnerabilidades que se han desarrollado en el apartado “3 Amenazas y vulnerabilidades de la tecnología NFC”, de forma que se evalúe si aportan riesgos a la solución.

El diseño de las preguntas debe ser objetivo y escueto, de tal forma que se puedan contestar siempre con un “SI”, un “NO” o con un no procede “NP”. Aparte de la contestación, se dejará un espacio para añadir posibles comentarios y aclaraciones sobre las respuestas, pero este campo será tan solo para anotaciones personales del responsable de la realización de la auditoría o para la toma de notas que puedan derivar en una mejora de la metodología.

Estas serían las preguntas en las que nos basaremos para solicitar la información necesaria en esta fase:

- **TIPO A: Localizaciones con lectores NFC (dispositivos activos).** Realizar las siguientes preguntas para cada localización.
    - ¿Estas ubicaciones están vigiladas o custodiadas por un sistema de video vigilancia o por la cercanía de personal interno de la empresa?
    - Si se encuentra en un lugar público o fácilmente accesible a todo el mundo, ¿Cuenta con un diseño anti-vandalismo?
    - En caso de ser comprometida esta ubicación por robo de elementos internos, ¿contiene datos críticos que podrían poner en riesgo la solución o parte de ella? Y además ¿esos datos se almacenan sin protección suficiente de forma que podrían ser extraídos de forma entendible?
    - En caso de responder SI a la pregunta anterior ¿Existe algún procedimiento para que, en caso de que esos datos sean extraídos por un tercero, se pueda evitar que esa información ponga en peligro la integridad de la solución?
    - ¿Están estos dispositivos conectados con algún sistema centralizado de control?
    - En caso de estar conectados con un sistema centralizado de control, ¿se envían las trazas o registros completos de cada uso que hacen los usuarios al sistema central?
    - En caso de responder que SI a la anterior pregunta, ¿el envío se hace en el momento que se utiliza o en menos de 24 horas?
    - En caso de que los dispositivos no estén conectados al sistema central, ¿Se realiza algún volcado manual de los datos de registros para cargarlos en el sistema?

- **TIPO B: Dispositivos pasivos.** Realizar las siguientes preguntas para cada dispositivo.
    - ¿Los dispositivos que se utilizan están pre configurados por la empresa o por el fabricante?
    - ¿Se utilizan dispositivos originales del fabricante obtenidas por vías oficiales o distribuidores de confianza?
    - Cuando el usuario utiliza el dispositivo, ¿se autentica el propio dispositivo para garantizar que es realmente el dispositivo del usuario (unicidad)?
    - Cuando el usuario utiliza el dispositivo, ¿se comprueba en algún momento (no superior a las 24 horas) que los datos consultados de la tarjeta durante su uso son correctos y no han sido modificados?
    - En caso de responder que SI a la pregunta anterior, si dicha comprobación detecta un error en la integridad del dispositivo, ¿se genera un evento de seguridad que más adelante (en menos de 24 horas) será verificado por un operador?
    - La información crítica almacenada en el dispositivo, ¿está protegida utilizando los medios de protección más robustos que soporta el dispositivo?
    - La información crítica almacenada en el dispositivo, ¿está protegida utilizando un cifrado de datos externo a los mecanismos de seguridad del dispositivo?
    - En caso de responder que SI a la pregunta anterior, ¿se gestionan dichos eventos de forma manual o se realizan informes sobre todos los ocurridos?
    - ¿Se ha realizado alguna vez una auditoría por un experto sobre este dispositivo de usuario para comprobar la robustez de su configuración?
    - En caso de responder que SI a la pregunta anterior, ¿Dicho test tuvo como resultado que el dispositivo está configurado de forma robusta?
- **TIPO C: Roles de usuario finales.** Realizar las siguientes preguntas para cada rol de usuario.
    - ¿Se identifica al usuario final y se le asocia al dispositivo NFC que se le entrega?
    - En caso de responder “SI” a la anterior pregunta, ¿Se puede deshabilitar el uso de la tarjeta del usuario si fuera necesario?
    - ¿El dueño del dispositivo NFC es el usuario?
    - ¿El usuario firma algún contrato o escrito con condiciones de uso o compromiso de buen uso y dicho contrato ha sido revisado por el responsable legal?
    - ¿Este usuario utiliza el dispositivo NFC como parte de un factor de doble autenticación?

- **TIPO D: Roles de personal interno.** Realizar las siguientes preguntas para cada rol de usuario interno.
    - ¿Existe un contrato específico o genérico para acordar con el usuario cláusulas de confidencialidad sobre la información que manejan en el trabajo? Y, además, ¿Dicho contrato ha sido validado por algún servicio jurídico para asegurarnos de su legalidad?
    - En caso de responder que SI a la anterior pregunta, ¿Todos los usuarios pertenecientes a este rol han firmado dicho contrato?
    - La información más crítica que protege los dispositivos NFC y los procesos más importantes, ¿puede ser accedida estrictamente por las personas que la necesitan para el desempeño de sus trabajos?
    - Cuando alguien accede a esa información, ¿se crean los correspondientes registros de auditoría?
- **TIPO E: Elementos lógicos y procesos.**
    - ☐ Base de datos centralizada
        - ¿Se almacena toda la información relativa al uso de dispositivos NFC de forma centralizada?
        - ¿Dicha información se actualiza con todos los datos de registro al menos cada 24 horas?
        - ¿Se realizan copias de seguridad diarias de los datos contenidos en esta base de datos siguiendo recomendaciones de buenas prácticas en la gestión de bases de datos?
    - ☐ Recuperación y almacenamiento de datos de registro de uso de tarjetas de usuario.
        - ¿Se recuperan de forma centralizada todas las transacciones válidas que se realizan en los dispositivos NFC activos al menos cada 24 horas?
        - ¿Se recuperan de forma centralizada todas las transacciones no válidas que se realizan en los dispositivos NFC activos al menos cada 24 horas?
        - ¿Se realizan informes de todas las transacciones realizadas para poder detectar comportamientos anómalos?
    - ☐ Procesos de BackOffice (consolidación de usos y comprobaciones)

- En caso de que un usuario presente un dispositivo ajeno al servicio, ¿se genera un evento de seguridad por esa acción?
- Todas las acciones dadas por válidas, ¿se consolidan para comprobar que todas siguen una lógica correcta, de forma que se garantice la integridad del sistema?
- En caso de detectar usos que comprometan la integridad del sistema, ¿está contemplada la funcionalidad de permitir la aplicación de listas blancas de dispositivos NFC de usuario?
- En caso de detectar usos que comprometan la integridad del sistema, ¿está contemplada la funcionalidad de permitir la aplicación de listas blancas de dispositivos NFC de usuario?
- Los procesos de consolidación, ¿son capaces de comprobar la integridad del sistema al 100%? Es decir, ¿Se puede garantizar que todas las transacciones realizadas por los usuarios son totalmente válidas?

- ☐ Procesos de auditorías internas de seguridad.

  - ¿Se realizan auditorías de seguridad sobre la solución completa de forma interna?
  - En caso de responder que SI a la pregunta anterior, ¿dicha auditoría se tiene en cuenta para garantizar la seguridad de la solución?

- ☐ Procesos de auditorías externas de seguridad.

  - ¿Se realizan auditorías de seguridad sobre la solución completa de forma externa?
  - En caso de responder que SI a la pregunta anterior, ¿dicha auditoría se tiene en cuenta para garantizar la seguridad de la solución?

- ☐ Se dispone de un diagrama claro de los flujos de información entre los lectores NFC (dispositivos activos) y el núcleo de la aplicación (BBDD, Core APP, APIs, …).

  - ¿Se han validado dichos flujos de información con personal experto de seguridad en el desarrollo de software seguro para todos los diferentes usos que se dan a los dispositivos NFC de los usuarios?
  - En caso de responder que SI a la pregunta anterior, ¿se han detectado problemas que pueden poner en peligro la integridad, o la confidencialidad de algún componente de la solución?

        - En caso de responder que SI a la pregunta anterior, ¿se han tomado medidas para paliar dichos peligros de seguridad?
    - ☐ [Opcional para mejora de metodología] Indicar otros elementos relevantes de la lógica de la aplicación que no se hayan tenido en cuenta.

- TIPO Z [Opcional para mejora de metodología]: Especificar otros elementos relevantes no tenidos en cuenta en los apartados anteriores.

5.5.2. Fase 2 - Realización de informes técnico y ejecutivo

En esta fase, se deberán de analizar los datos obtenidos durante toda la ejecución de la fase 1 para realizar dos informes, uno dirigido a los responsables de la solución (informe técnico) y otro dirigido al responsable de la empresa (CEO), (CTO), (CISO) o el que corresponda.

En las fases iniciales de la elaboración de estos informes, la redacción de estos informes deberá ser realizada por una persona con conocimientos técnicos avanzados de la tecnología NFC y en la realización de auditorías.

Una de las mejoras que se han de realizar, es la creación de plantillas de informe, basadas en la experiencia de haber aplicado la metodología al menos unas 10 veces o hasta que se vea que su madurez permita realizar una plantilla que sea útil.

5.5.2.1. Realización del informe técnico.

Como hemos indicado en el anterior apartado, al ser esta una metodología que se ha aplicado pocas veces, todavía no es coherente la realización de una plantilla para que la realización del informe técnico sea sencilla para alguien que no tiene experiencia ni conocimientos técnicos avanzados, ya que no tenemos información suficientes para desarrollarla correctamente.

Lo que sí que podemos definir es la estructura que debería tener dicho informe y que debería ser la base para su redacción, por lo que el informe debería indicar:

- Datos generales:
    - Empresa en la que se aplica la metodología
    - Datos de contacto del destinatario del informe.
    - Ámbito de aplicación.
    - Fechas de realización.
    - Datos de contacto de la persona que aplica la metodología.

- Datos de contacto de las personas que colaboran en la toma de datos

- Resumen técnico de amenazas y vulnerabilidades detectadas, indicando los principales riesgos y su cuantificación.
- Resumen detallado de las amenazas y vulnerabilidades detectadas: Se deberá realizar un listado completo de todas las amenazas y vulnerabilidades detectadas, ofreciendo detalles adicionales sobre dichas amenazas y vulnerabilidades que pudieran ayudar a entenderlas más a fondo al destinatario del informe.

5.5.2.2. Realización del informe ejecutivo.

La redacción del informe ejecutivo será un documento con una extensión máxima preferible de no más de una cara de un folio. Se trata de realizar un documento con lenguaje no técnico, que será dirigido a un perfil directivo de la empresa que podría no tener conocimientos de seguridad. Es por ese motivo por lo que el informe deberá ser breve, claro y plasmar con la mayor exactitud posible el estado de los riesgos detectados en base al uso de la tecnología NFC.

Al igual que para el informe técnico, en la realización de los informes durante las primeras aplicaciones de la metodología, el informe no se realizará en base a una plantilla que simplifique la creación de dicho informe, por lo que nos basaremos en seguir una estructura parecida a la del informe anterior:

- Datos generales:
  - Empresa en la que se aplica la metodología
  - Datos de contacto del destinatario del informe.
  - Ámbito de aplicación.
  - Fechas de realización.
  - Datos de contacto de la persona que aplica la metodología.
  - Datos de contacto de las personas que colaboran en la toma de datos.
  - Datos de contacto del responsable técnico de la solución.
- Resumen del estado de las amenazas y riesgos detectados, teniendo en cuenta que dicho resumen va a ser leído por una persona que podría no tener conocimientos técnicos en la materia. La persona que redacte este informe deberá usar terminología sencilla, entendible por todos los públicos. Este resumen deberá ser breve y conciso. Deberá transmitir a quien lo lea una visión general del estado de seguridad en cuanto a cómo se aplica la tecnología NFC en la solución y que riesgos existen, de forma que,

si hiciera falta tomar una decisión a nivel ejecutivo, este informe pueda servir de base para ello.

5.5.3. Fase 3 - Realización de informe para mejora de la metodología

Esta fase solo se realizará si se deciden aplicar los procedimientos de mejora de la metodología. Se deberá iniciar cuando se hayan realizado los informes técnico y ejecutivo, y una vez que estos hayan sido revisados por la empresa.

A partir de este momento, la persona encargada de aplicar la metodología deberá realizar un informe que será tan sencillo como realizar un listado de incidentes ocurridos durante la aplicación de las fases 1 y 2 en las que se incluyan anomalías o debilidades en los procesos, casos no contemplados, o cualquier otro evento, como los informados en las casillas contempladas en los cuestionarios de la FASE 1.

Para cada incidente se deberá especificar:

- Situación en la que se ha detectado el incidente (Ejemplo: Fase 1-2).
- Descripción breve del incidente: (Ejemplo: No se contempla…).
- Detalle del incidente: (Ejemplo: La empresa dispone de <*elemento_no_contemplado_en_metodología*> y es algo que se debería tener en cuenta, ya que es un elemento relevante para el uso que da del NFC).

Una vez realizado dicho informe, deberá ser entregado a las personas o grupo encargado de revisar la metodología para que puedan realizar mejoras si así lo consideran.

5.6. Evaluación de la metodología

La evaluación de la metodología se ha incorporado como un proceso interno de la propia metodología.

El objetivo de dicha evaluación es mantener la metodología actualizada y permitir que madure progresivamente mediante:

- la adaptación a nuevas tecnologías y avances en el campo del NFC,
- la adaptación a las vulnerabilidades y amenazas que vayan surgiendo,
- la ampliación del marco de aplicación de la metodología, ya sea mediante la inclusión de más dispositivos pasivos NFC o mediante la inclusión de los dispositivos NFC

activos como parte de los dispositivos de los usuarios finales (con tecnologías como HCE y similares que están actualmente en auge),

- la mejora del diseño y estructura de la metodología en base a la retroalimentación de su aplicación y
- la mejora de los procesos y fases de aplicación de la metodología.

Para la consecución de dichos objetivos de mejora se han definido varios procesos:

- Revisión periódica de la tecnología NFC (sus estándares y aplicaciones) y de las amenazas y vulnerabilidades que se aplican. Este proceso se deberá realizar con una periodicidad máxima de un año.
- Revisión de la metodología por:
    - La evaluación de su aplicación en un entorno real.
    - La evaluación por parte de expertos deberán estudiarla a fondo.

5.6.1. Evaluación de la aplicación de la metodología

En el anexo IV (Ejecución de la metodología para su evaluación), se aportan los documentos resultantes de la aplicación de la metodología en un sistema de gestión de transporte público de una ciudad, incluyendo:

- Las fichas con los cuestionarios realizados.
- El informe técnico realizado
- El informe ejecutivo realizado.
- El informe de mejora por la aplicación de la metodología.

**NOTA: Los datos que contiene el informe de mejora por la aplicación de la metodología en este caso han sido utilizados para la adaptación y mejora de la metodología expuesta en los diferentes apartados contenidos en el capítulo "5 Desarrollo de la metodología".*

5.6.2. Evaluación por parte de expertos

Otra forma de mejorar la metodología será mediante la evaluación realizada por expertos.

En este caso, los expertos deberán leer este trabajo completamente, e incluso profundizar si hiciera falta en los apartados "2 La tecnología NFC. Estándares y aplicaciones" y "3 Amenazas y vulnerabilidades de la tecnología NFC".

Una lectura por los capítulos siguientes (el “4 Hipótesis de trabajo y objetivos concretos de la investigación” y el “5 Desarrollo de la metodología”), les servirá para entender las bases sobre la creación de la metodología y cómo se ha realizado su desarrollo.

Una vez realizada la lectura del texto completo, deberían redactar un informe con formato libre en el que expresen qué cambios creen que serían recomendables aplicar a la metodología e incluso sobre todos los capítulos que contiene este documento.

Otra opción es que, a través de este documento, en su formato editable, incorporasen comentarios directamente en los lugares adecuados para expresar sus opiniones y las mejoras que incorporarían.

6. Conclusiones

Tras la aplicación de la metodología, se han podido comprobar muchos aspectos importantes que han confirmado, no solo que la solución tenía muchos riesgos de nivel muy alto, sino que también existían usuarios que estaban explotando dichos riesgos activamente.

Se han identificado riesgos originados por vulnerabilidades en la utilización de la tarjeta MiFARE Classic, que originaban que ciertos usuarios las modificaran arbitrariamente de forma que les resultaba fácil manipular los datos que en ella contenían para, por ejemplo, modificar la cantidad de saldo de la tarjeta.

Se ha verificado que no existía ningún control en la lógica de la aplicación para detectar el uso de estas tarjetas modificadas arbitrariamente.

En cuanto a los dispositivos NFC activos, no se ha encontrado ningún problema reseñable, ya que éstos, o se encuentran siempre bajo la supervisión de un responsable o están debidamente protegidos con un nivel aceptable contra vandalismo y con un nivel aceptable contra el robo. Como punto negativo, sería fácil la obtención de algunas de las claves si alguien robara algunos de estos dispositivos y los analizase.

Actualmente la empresa ha incorporado algunos mecanismos de comprobación de las tarjetas como la inclusión de listas negras, aunque solo sea para detectar a parte de las personas que estaban usando las tarjetas modificadas.

La empresa, actualmente está evaluando como mejorar la seguridad del servicio, estudiando las medidas que puede aplicar, el grado de seguridad que dichas medidas incorporarían y el coste que tendría cada una de las medidas para poder llegar a una solución robusta que no ponga en peligro la integridad del sistema, ya sea por la modificación de las tarjetas de los usuarios (que es necesario cambiar en su totalidad) como por el acceso indebido a los diferentes dispositivos NFC activos.

Esta primera evaluación de la metodología ha demostrado ser eficaz en este entorno, pero sería necesario aplicarla en otros para poder seguir mejorándola.

7. Líneas de trabajo futuro

La metodología recogida en este trabajo se ha realizado mediante la incorporación del estado actual de varios elementos que varían con el paso del tiempo. Cualquier trabajo futuro sobre esta metodología debería incluir la revisión de dichos elementos para que la metodología sea lo más eficaz posible en la consecución de sus objetivos. Los elementos que hay que actualizar son los definidos en los siguientes capítulos:

- 2 La tecnología NFC. Estándares y aplicaciones: Los siguientes sub-apartados:
    - 2.3 Normas y estándares relacionados con NFC.
    - 2.4 Terminología de la tecnología NFC.
- "3 Amenazas y vulnerabilidades de la tecnología NFC": Este capítulo, además de mantenerse actualizado, se debería ampliar con el análisis de más dispositivos NFC, de forma que se pueda ampliar el marco de aplicación de la metodología.

Otro aspecto importante, sería la incorporación de los dispositivos NFC activos como parte de los dispositivos de los usuarios. Esta opción no se ha incorporado en esta metodología para poder realizar un diseño inicial más sencillo y más fácil de mejorar inicialmente.

Por otra parte, un tema que no se ha tratado en esta metodología, es la mejora de la usabilidad en el momento de su aplicación, de forma que el perfil del usuario que hace falta para aplicar la metodología pueda ser un usuario con escasos conocimientos técnicos. Para ello, una línea de trabajo importante sería realizar un rediseño de las instrucciones de las fases 1 y 2 para conseguir este objetivo.

Podría ser conveniente también incorporar preguntas para los perfiles de aplicación más comunes. Esto podría permitir controlar los elementos que comparten todas las aplicaciones de ese tipo. Por ejemplo, para una aplicación de transporte urbano, se podrían hacer las preguntas:

- ¿Se controla que cuando el usuario realiza una cancelación del billete a precio especial (como podría ser en el caso de un transbordo), realmente tiene derecho a dicho precio especial?

Aunque este aspecto hiciera más extenso el desarrollo de la metodología, la efectividad de su aplicación aumentaría.

Y, por último, otra de las mejoras que se podrían hacer, y que podrían ir englobadas en el aumento de su usabilidad, es la posibilidad de aplicar la metodología mediante una aplicación, de tal forma que parte de los procesos a realizar de forma manual, se realizasen automáticamente. Esto incluiría:

- Requerir automáticamente las fichas que se han de rellenar en la realización de encuestas.
- Simplicidad a la hora de evaluar los elementos de riesgos concretos con tan solo elegir los dispositivos de usuario que se utilizan.
- Posibilidad de incorporar fichas con cuestionarios específicos a las aplicaciones más comunes sin que el usuario note que la metodología sea más difícil y extensa de realizar en su aplicación.
- Realización de borradores de informes técnicos y ejecutivos automáticos.
- Envío de los incidentes sobre la mejora de la metodología automáticamente a las personas encargadas de modificarla.
- Posibilidad de actualizar la metodología de forma centralizada para todas las entidades que la usen, por lo que siempre se aplicará la última versión disponible.
- Posibilidad de ofrecer este servicio a terceros bajo algún modelo de pago por uso o acceso.

8. Referencias

Clark, S. (13 de junio de 2013). *ABI reports NFC chip market shares*. Recuperado el 19 de septiembre de 2016, de http://www.nfcworld.com/2013/06/12/324581/abi-reports-nfc-chip-market-shares/

Courtois, N. T. (2009). The Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes, Anywhere, Anytime. *The 5th Workshop on RFID Security.* Leuven, Belgium. Obtenido de http://discovery.ucl.ac.uk/id/eprint/196096

DGPGC. (04 de julio de 2014). *DNI electrónico - Guía de Referencia Básica.* Recuperado el 20 de septiembre de 2016, de http://www.dnielectronico.es/PDFs/Guia_de_referencia_basica_v1_4.pdf

ECMA-340. (junio de 2013). *Near Field Communication Interface and Protocol 1 (NFCIP-1)*. Obtenido de http://www.ecma-international.org/publications/standards/Ecma-340.htm

ECMA-352. (junio de 2013). *Near Field Communication Interface and Protocol 2 (NFCIP-2)*. Obtenido de http://www.ecma-international.org/publications/standards/Ecma-352.htm

EMV 4.3. (noviembre de 2011). Recuperado el 19 de septiembre de 2016, de https://www.emvco.com/specifications.aspx?id=223

EMV Contactless. (s.f.). Recuperado el 16 de 09 de 2016, de https://www.emvco.com/specifications.aspx?id=21

EMV Contactless: Book A: Architecture and General Requirements. (abril de 2016). Recuperado el 19 de septiembre de 2016, de https://www.emvco.com/download_agreement.aspx?id=1230

EMV Contactless: Book B: Entry Point. (agosto de 2016). Recuperado el 19 de septiembre de 2016, de https://www.emvco.com/download_agreement.aspx?id=1276

EMV Contactless: Book D: Contactless Communication Protocol. (marzo de 2016). Recuperado el 19 de septiembre de 2016, de https://www.emvco.com/download_agreement.aspx?id=1208

EMV Contactless: Books C [C-1, C-2, C-3, C-4, C-5, C-6, C-7]: Kernel Specifications. (mayo de 2016). Recuperado el 19 de 09 de 2016, de https://www.emvco.com/specifications.aspx?id=21

EMV FAQ: Card / Terminal General Questions. (s.f.). Recuperado el 16 de septiembre de 2016, de https://www.emvco.com/faq.aspx?id=41#1

EMVCo. (s.f.). Recuperado el 11 de septiembre de 2016, de www.emvco.com

EMVCo Members. (16 de 09 de 2016). Obtenido de https://www.emvco.com/about_emvco.aspx?id=156

EMVCo Technical Associates. (16 de septiembre de 2016). Obtenido de https://www.emvco.com/about_emvco.aspx?id=184

Francis, L., Hancke, G., Mayes, K., & Markantonakis, K. (2012). Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones. En N.-W. Lo, & Y. Li, *Radio Frequency Identification System Security* (pág. 108). IOS Press. doi:10.3233/978-1-61499-143-4-21

Funke, H. (noviembre de 2013). *Standards of Smart Cards in ISO Layer Model.* Obtenido de http://blog.protocolbench.org/2013/11/standards-smart-cards-iso-layer-model/

Google. (s.f.). *Acerca de Google*. Recuperado el 20 de septiembre de 2016, de https://www.google.com/about/

Google Wallet. (s.f.). Recuperado el 21 de septiembre de 2016, de http://wallet.google.com

Haselsteiner, E., & Breitfuß, K. (2006). Security in Near Field Communication (NFC). Strengths and weaknesses. *Workshop on RFID Security*, (pág. 11). Graz, Austria.

Host-based Card Emulation | Android Developers. (20 de septiembre de 2016). Obtenido de https://developer.android.com/guide/topics/connectivity/nfc/hce.html

ICAO - Doc 9303 - Sevent Edition. (2015). Recuperado el 21 de septiembre de 2016, de http://www.icao.int/publications/pages/publication.aspx?docnum=9303

ISO/IEC 10536. (1996-2000). *Identification cards -- Contactless integrated circuit(s) cards*. Obtenido de http://www.iso.org/iso/home/search.htm?qt=10536&sort=rel&type=simple&published=on

ISO/IEC 14443-1:2016. (15 de marzo de 2016). *Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics*. Obtenido de http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=70170

ISO/IEC 14443-2:2016. (17 de julio de 2016). *Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 2: Radio frequency power and signal interface*. Obtenido de http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66288

ISO/IEC 14443-3:2016. (1 de junio de 2016). *Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anticollision*. Obtenido de http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=70171

ISO/IEC 14443-4:2016. (1 de junio de 2016). *Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 4: Transmission protocol*. Obtenido de http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=70172

ISO/IEC 15693. (s.f.). *Identification cards -- Contactless integrated circuit cards -- Vicinity cards*.

ISO/IEC 18000-1:2008. (1 de julio de 2008). *Information technology -- Radio frequency identification for item management -- Part 1: Reference architecture and definition of parameters to be standardized*. Obtenido de http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46145

ISO/IEC 18000-3:2010. (s.f.). *Information technology -- Radio frequency identification for item management -- Part 3: Parameters for air interface communications at 13,56 MHz*. Obtenido de http://www.iso.org/iso/catalogue_detail.htm?csnumber=53424

ISO/IEC 18000-3:2010. (11 de noviembre de 2010). *Information technology -- Radio frequency identification for item management -- Part 3: Parameters for air interface communications at 13,56 MHz*. Obtenido de http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53424

ISO/IEC 18000-7:2014. (s.f.). *Information technology — Radio frequency identification for item management — Part 7: Parameters for active air interface communications at 433 MHz*. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:18000:-7:en

ISO/IEC 18092:2013. (15 de marzo de 2013). *Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1)*. Obtenido de http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56692

ISO/IEC 21481:2012. (1 de julio de 2012). Recuperado el 20 de 09 de 2016, de http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56855

ISO/IEC 7816-15:2016. (15 de mayo de 2016). Recuperado el 21 de septiembre de 2016, de http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=65250

ISO/IEC 7816-4:2013/Cor.1:2014. (15 de agosto de 2014). Recuperado el 20 de septiembre de 2016, de Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=65200

JIS X 6319-4:2016. (3 de marzo de 2016). *Specification of implementation for integrated circuit(s) cards-Part 4: High speed proximity cards*. Obtenido de Specification of implementation for integrated circuit(s) cards-Part 4: High speed proximity cards.

Kasper, T., & Oswald, D. (20 de septiembre de 2016). *ChameleonMini*. Obtenido de http://kasper-oswald.de/gb/chameleonmini/

Kasper, T., von Maurich, I., Oswald, D., & Paar, C. (2010). Cloning Cryptographic RFID Cards for 25$. *5th Benelux Workshop on Information and System Security, WisSec 2010*, (pág. 15). Nijmegen, the Netherlands. Obtenido de http://proxmark.nl/files/Documents/13.56%20MHz%20-%20MIFARE%20DESFire/Cloning_Cryptographic_RFID_Cards_for_25USD-WISSEC_2010.pdf

Lab401. (20 de septiembre de 2016). *Proxmark III RDV*. Obtenido de https://lab401.com/proxmark/8-proxmark-3-rdv.html

Liu, Y., Kasper, T., Lemke-Rust, K., & Paar, C. (29 de enero de 2007). E-Passport: Cracking Basic Access Control Keys with COPACOBANA. *SHARCS 2007*, (pág. 18). Vienna,

Austria. Recuperado el 22 de septiembre de 2016, de http://hgi.ruhr-uni-bochum.de/media/crypto/veroeffentlichungen/2011/01/29/epasscrack_otm07.pdf

Meijer, C., & Verdult, R. (2015). Ciphertext-only Cryptanalysis on Hardened Mifare Classic Cards. *22nd ACM Conference on Computer and Communications Security (CCS 2015)* (págs. 18-30). Denver, EEUU: ACM.

MIFARE DESFire EV2. (marzo de 2014). Recuperado el 16 de septiembre de 2016, de https://www.mifare.net/wp-content/uploads/2015/05/MIFARE-DESFire-EV2-Leaflet.pdf

MIFARE DESFire EV2. (4 de diciembre de 2014). Recuperado el 16 de septiembre de 2016, de https://www.mifare.net/wp-content/uploads/2015/05/MIFARE-DESFire-EV2-Leaflet.pdf

MIFARE® Classic. (s.f.). Recuperado el 19 de septiembre de 2016, de http://www.nxp.com/products/identification-and-security/mifare-ics/mifare-classic/mifare-classic-1k-mainstream-contactless-smart-card-ic-for-fast-and-easy-solution-development:MF1S5030DA3?

MIFARE® Classic EV1. (marzo de 2014). Recuperado el 19 de septiembre de 2016, de https://www.mifare.net/wp-content/uploads/2015/03/MIFARE_Classic_EV1.pdf

MIFARE® DESFire EV1. (febrero de 2015). Recuperado el 2016 de septiembre de 2016, de https://www.mifare.net/wp-content/uploads/2015/04/MIFARE-DESFire-EV1-Registered.pdf

MIFARE® DESFire EV1. (28 de octubre de 2015). Recuperado el 2016 de septiembre de 2016, de https://www.mifare.net/wp-content/uploads/2015/04/MIFARE-DESFire-EV1-Registered.pdf

MIFARE® ICs. (17 de septiembre de 2016). Obtenido de http://www.nxp.com/products/identification-and-security/mifare-ics:MC_53422?

MIFARE® Plus. (s.f.). Recuperado el 20 de septiembre de 2016, de http://www.nxp.com/products/identification-and-security/mifare-ics/mifare-plus:MC_57609

Mifare4Mobile. (2015). Recuperado el 09 de septiembre de 2016, de https://www.mifare4mobile.org/

NFC Data Exchange Format (NDEF) Technical Specification. (24 de julio de 2006). Obtenido de http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/data-exchange-format-technical-specification/

NFC Forum. (2004). Recuperado el 20 de septiembre de 2016, de http://nfc-forum.org/

NFC Forum Mandated Type 1 Tag Format. (02 de junio de 2007). Recuperado el 21 de septiembre de 2016, de http://www.acs.com.hk/download-manual/6071/TDS_TOPAZ.pdf

NFC Forum: Protocol Technical Specifications. (16 de 09 de 2016). Obtenido de http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/protocol-technical-specifications/

NFC Forum: Tag Type Technical Specifications. (16 de 09 de 2016). Obtenido de http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/tag-type-technical-specifications/

Nithyanand, R., Tsudik, G., & Uzun, E. (2011). *User-aided Reader Revocation in PKI-Based.* doi:10.3233/JCS-2011-0435

NXP Semiconductors. (6 de septiembre de 2016). MiFare ICs. Obtenido de http://www.nxp.com/products/identification-and-security/mifare-ics:MC_53422

Oswald, D., & Kasper, T. (26 de julio de 2016). *ChameleonMini - A Versatile NFC Card Emulator, and more...* Recuperado el 20 de septiembre de 2016, de https://www.kickstarter.com/projects/1980078555/chameleonmini-a-versatile-nfc-card-emulator-and-mo/posts/1638980

Oswald, D., & Paar, C. (2011). Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World - Extended Version. *Cryptographic Hardware and Embedded Systems CHES*, (pág. 19). Nara, Japan. Obtenido de http://emsec.rub.de/media/crypto/veroeffentlichungen/2011/10/10/desfire_2011_extended_1.pdf

Periódico El Mundo. (30 de junio de 2014). *BiciMAD: cuelan un vídeo obsceno en las pantallas del servicio de alquiler de bicicletas de Madrid*. Recuperado el 21 de septiembre de 2016, de http://www.elmundo.es/madrid/2014/06/30/53b10674ca4741415d8b456e.html

Prepay Technologies. (julio de 2016). *PayBus.* Recuperado el 20 de 09 de 2016, de http://www.prepay.es/paybus/

Proxmark.org. (s.f.). Recuperado el 20 de septiembre de 2016, de http://www.proxmark.org/proxmark

Ramírez, R. (29 de abril de 2013). *Cifrado de discos: proteger tu privacidad de forma sencilla y efectiva.* Recuperado el 20 de septiembre de 2016, de http://www.criptored.upm.es/crypt4you/temas/privacidad-proteccion/leccion2/leccion2.html

Roland, M., Langer, J., & Scharinger, J. (2013). Applying Relay Attacks to Google Wallet. *Near Field Communication (NFC), 2013 5th International Workshop* (pág. 6). Zurich, Switzerland: IEEE. doi:10.1109/NFC.2013.6482441

Sony Global - Felica - Technical Information. (16 de septiembre de 2016). Obtenido de https://www.sony.net/Products/felica/business/tech-support/index.html

Sony Global. (6 de septiembre de 2016). Obtenido de http://www.sony.net/Products/felica/

Thomas P. Diakos, J. A. (11 de septiembre de 2013). Eavesdropping near-field contactless payments: a quantitative analysis. *The Journal of Engineering*, 7. doi:10.1049/joe.2013.0087

Update on MIFARE DESFire (MF3ICD40). (28 de septiembre de 2011). Recuperado el 20 de septiembre de 2016, de https://www.mifare.net/update-on-mifare-desfire-mf3icd40/

van Dijk, R., Sangers, L., & Davis, A. (7 de febrero de 2016). Portable RFID Bumping Device.

Walton, C. A. (1983). *Estados Unidos Patente nº US 4384288 A.* Recuperado el 16 de septiembre de 2016, de http://www.google.com/patents/US4384288

Westhues, J. (2009). *A Test Instrument for HF/LF RFID*. Recuperado el 20 de septiembre de 2016, de http://cq.cx/proxmark3.pl

Anexo I – Ficha con cuestionario de FASE 1-1

- ¿Cuál o cuáles son las aplicaciones concretas por las que se usa NFC y que tipos de operación se realizan?

  Ejemplo: Tarjeta monedero (carga, compra, devolución), tarjeta transporte (carga, cancelación de billete, cancelación de billete por transbordo gratuito), control de accesos (identificación y autenticación de usuario), …

Aplicación	Funciones

- Por cada aplicación y aproximadamente, ¿Cuántos terminales de lectura existen? ¿Cuál es la estimación de crecimiento a cuatro años?

- Por cada aplicación y aproximadamente, ¿Cuántos usuarios existen? ¿Cuál es la estimación de crecimiento a cuatro años?

- ¿Cuál es el alcance o ámbito geográfico de la implementación? ¿Cuál es la estimación de crecimiento a cuatro años?

Anexo II – Ficha con cuestionario de FASE 1-2

Enumerar los siguientes elementos de forma concisa:

- TIPO A: Identificar y enumerar los tipos de localizaciones en los que existirán dispositivos de lectura/escritura NFC (dispositivos activos) que interactuarán con los usuarios.

  Ejemplo: Tótems públicos (validar usuario, consultar saldo), comercios con terminal de recarga (recarga de tarjetas), autobuses (cancelar billete), …

Localización	Funciones

- TIPO B: Identificar y enumerar la marca y modelo de los diferentes dispositivos NFC que van a ser usados por el conjunto de los usuarios de la aplicación (dispositivos pasivos).

  Ejemplo: MiFARE Classic (original), MiFARE DESFire EV2, DNIe 3.0, Pasaporte.

- TIPO C: Identificar y enumerar los tipos de roles de usuarios que van a usar la aplicación, identificando si son externos (ámbito público) o internos (ámbito privado o de la empresa).

  Ejemplo para gestión de alquiler de bicis: Clientes (externos), Personal mantenimiento bicis (interno), Probadores en producción (interno).

Rol de usuario	Ámbito (Elegir: interno o externo)

- TIPO D: Identificar y enumerar los tipos de roles del personal y la fase o fases en las que participaran en la solución (diseño, desarrollo, piloto o producción). Incluir solo los que van a estar implicados en tareas técnicas asociadas a la solución (desarrolladores, implantadores, ingenieros, técnicos de soporte, …).

  Ejemplo: Desarrolladores (desarrollo, pre-producción), Probadores (pre-producción, producción), Jefe proyecto (diseño, desarrollo, pre-produción, producción, soporte), arquitectos del sistema (diseño, desarrollo), técnicos (producción), instaladores de sistemas (producción).

Rol de personal	Fases de participación.

- TIPO E: Especificar si existen los siguientes elementos en la lógica de la aplicación:
  - ☐ Base de datos centralizada
  - ☐ Recuperación y almacenamiento de datos de registro de uso de tarjetas de usuario.
  - ☐ Procesos de BackOffice (consolidación de usos y comprobaciones)
  - ☐ Procesos de auditorías internas de seguridad.
  - ☐ Procesos de auditorías externas de seguridad.
  - ☐ Se dispone de un diagrama claro de los flujos de información lectores y tarjetas NFC (dispositivos activos y pasivos)
  - ☐ Se dispone de un diagrama claro de los flujos de información entre los lectores NFC (dispositivos activos) y el núcleo de la aplicación (BBDD, Core APP, APIs, …).
  - ☐ [Opcional para mejora de metodología] Indicar otros elementos relevantes de la lógica de la aplicación que no se hayan tenido en cuenta:

- TIPO Z [Opcional para mejora de metodología]: Otros elementos relevantes: En caso de que exista algún elemento relevante que no se pueda clasificar en los anteriores, se deberán especificar en este apartado para su posible inclusión en futuras mejoras de la metodología.

Anexo III – Fichas con cuestionarios de FASE 1-3

INSTRUCCIONES: Contestar las siguientes preguntas para cada elemento TIPO. Es importante que cada pregunta sea contestada objetivamente con un SI, un NO o un "No Procede" (NP). El apartado comentarios tan solo se utilizará para comentarios que sirvan de aclaración posterior a la persona que ejecuta la metodología o para un proceso posterior de mejora de la metodología.

CUESTIONARIO TIPO A (Fase 1-3)

Tipos de localizaciones de elementos NFC Activos (lectores) y función o funciones de los lectores.

Localización concreta	Funciones

Pregunta	Respuesta (SI/NO/NP)
¿Estas ubicaciones están vigiladas o custodiadas por un sistema de video vigilancia o por la cercanía de personal interno de la empresa? Comentarios:	
Si se encuentra en un lugar público o fácilmente accesible a todo el mundo, ¿Cuenta con un diseño anti-vandalismo? Comentarios:	
En caso de ser comprometida esta ubicación por robo de elementos internos, ¿contiene datos críticos que podrían poner en riesgo la solución o parte de ella? Y además ¿esos datos se almacenan sin protección suficiente de forma que podrían ser extraídos de forma entendible? Comentarios:	
En caso de responder SI a la pregunta anterior ¿Existe algún procedimiento para que, en caso de que esos datos sean extraídos por un tercero, se pueda evitar que esa información ponga en peligro la integridad de la solución? Comentarios:	
¿Están estos dispositivos conectados con algún sistema centralizado de control? Comentarios:	

Pregunta	Respuesta (SI/NO/NP)
En caso de estar conectados con un sistema centralizado de control, ¿se envían las trazas o registros completos de cada uso que hacen los usuarios al sistema central? Comentarios:	
En caso de responder que SI a la anterior pregunta, ¿el envío se hace en el momento que se utiliza o en menos de 24 horas? Comentarios:	
En caso de que los dispositivos no estén conectados al sistema central, ¿Se realiza algún volcado manual de los datos de registros para cargarlos en el sistema? Comentarios:	

CUESTIONARIO TIPO B (Fase 1-3)

Tipos de dispositivos NFC pasivos utilizados por los usuarios.

Dispositivo NFC:	

Pregunta	Respuesta (SI/NO/NP)
¿Los dispositivos que se utilizan están pre configurados por la empresa o por el fabricante? Comentarios:	
¿Se utilizan dispositivos originales del fabricante obtenidas por vías oficiales o distribuidores de confianza? Comentarios:	
Cuando el usuario utiliza el dispositivo, ¿se autentica el propio dispositivo para garantizar que es realmente el dispositivo del usuario (unicidad)? Comentarios:	
Cuando el usuario utiliza el dispositivo, ¿se comprueba en algún momento (no superior a las 24 horas) que los datos consultados de la tarjeta durante su uso son correctos y no han sido modificados? Comentarios:	

Pregunta	Respuesta (SI/NO/NP)
En caso de responder que SI a la pregunta anterior, si dicha comprobación detecta un error en la integridad del dispositivo, ¿se genera un evento de seguridad que más adelante (en menos de 24 horas) será verificado por un operador? Comentarios:	
La información crítica almacenada en el dispositivo, ¿está protegida utilizando los medios de protección más robustos que soporta el dispositivo? Comentarios:	
La información crítica almacenada en el dispositivo, ¿está protegida utilizando un cifrado de datos externo a los mecanismos de seguridad del dispositivo? Comentarios:	
En caso de responder que SI a la pregunta anterior, ¿se gestionan dichos eventos de forma manual o se realizan informes sobre todos los ocurridos? Comentarios:	
¿Se ha realizado alguna vez una auditoría por un experto sobre este dispositivo de usuario para comprobar la robustez de su configuración? Comentarios:	
En caso de responder que SI a la pregunta anterior, ¿Dicho test tuvo como resultado que el dispositivo está configurado de forma robusta? Comentarios:	

CUESTIONARIO TIPO C (Fase 1-3)

Listado de roles de usuarios y si son externos (ámbito público) o internos (ámbito de la empresa).

Rol de usuario	Ámbito (interno o externo)

Pregunta	Respuesta (SI/NO/NP)
¿Se identifica al usuario final y se le asocia al dispositivo NFC que se le entrega? Comentarios:	
En caso de responder “SI” a la anterior pregunta, ¿Se puede deshabilitar el uso de la tarjeta del usuario si fuera necesario? Comentarios:	
¿El dueño del dispositivo NFC es el usuario? Comentarios:	
¿El usuario firma algún contrato o escrito con condiciones de uso o compromiso de buen uso y dicho contrato ha sido revisado por el responsable legal? Comentarios:	
¿Este usuario utiliza el dispositivo NFC como parte de un factor de doble autenticación? Comentarios:	

CUESTIONARIO TIPO D (Fase 1-3)

Roles de personal interno, fases del proyecto en el que participan.

> Ejemplo: Desarrolladores (desarrollo, pre-producción), Probadores (pre-producción, producción), Jefe proyecto (desarrollo, pre-produción, producción, soporte), técnicos (producción), instaladores de sistemas (producción).

Rol de persona	Fases de participación.

Pregunta	Respuesta (SI/NO/NP)
¿Existe un contrato específico o genérico para acordar con el usuario cláusulas de confidencialidad sobre la información que manejan en el trabajo? Y, además, ¿Dicho contrato ha sido validado por algún servicio jurídico para asegurarnos de su legalidad? Comentarios:	

Pregunta	Respuesta (SI/NO/NP)
En caso de responder que SI a la anterior pregunta, ¿Todos los usuarios pertenecientes a este rol han firmado dicho contrato? Comentarios:	
La información más crítica que protege los dispositivos NFC y los procesos más importantes, ¿puede ser accedida estrictamente por las personas que la necesitan para el desempeño de sus trabajos? Comentarios:	
Cuando alguien accede a esa información, ¿se crean los correspondientes registros de auditoría? Comentarios:	

CUESTIONARIO TIPO E (Fase 1-3)

Lógica de aplicación. Realizar los cuestionarios que procedan:

- ☐ Base de datos centralizada

Pregunta	Respuesta (SI/NO/NP)
¿Se almacena toda la información relativa al uso de dispositivos NFC de forma centralizada? Comentarios:	
¿Dicha información se actualiza con todos los datos de registro al menos cada 24 horas? Comentarios:	
¿Se realizan copias de seguridad diarias de los datos contenidos en esta base de datos siguiendo recomendaciones de buenas prácticas en la gestión de bases de datos? Comentarios:	

- ☐ Recuperación y almacenamiento de datos de registro de uso de tarjetas de usuario.

Pregunta	Respuesta (SI/NO/NP)
¿Se recuperan de forma centralizada todas las transacciones válidas que se realizan en los dispositivos NFC activos al menos cada 24 horas? Comentarios:	
¿Se recuperan de forma centralizada todas las transacciones no válidas que se realizan en los dispositivos NFC activos al menos cada 24 horas? Comentarios:	
¿Se realizan informes de todas las transacciones realizadas para poder detectar comportamientos anómalos? Comentarios:	

- ☐ Procesos de BackOffice (consolidación de usos y comprobaciones)

Pregunta	Respuesta (SI/NO/NP)
En caso de que un usuario presente un dispositivo ajeno al servicio, ¿se genera un evento de seguridad por esa acción? Comentarios:	
Todas las acciones dadas por válidas, ¿se consolidan para comprobar que todas siguen una lógica correcta, de forma que se garantice la integridad del sistema? Comentarios:	
En caso de detectar usos que comprometan la integridad del sistema, ¿está contemplada la funcionalidad de permitir la aplicación de listas blancas de dispositivos NFC de usuario? Comentarios:	
En caso de detectar usos que comprometan la integridad del sistema, ¿está contemplada la funcionalidad de permitir la aplicación de listas blancas de dispositivos NFC de usuario? Comentarios:	
Los procesos de consolidación, ¿son capaces de comprobar la integridad del sistema al 100%? Es decir, ¿Se puede garantizar que todas las transacciones realizadas por los usuarios son totalmente válidas? Comentarios:	

- ☐ Procesos de auditorías internas de seguridad.

Pregunta	Respuesta (SI/NO/NP)
¿Se realizan auditorías de seguridad sobre la solución completa de forma interna? Comentarios:	
En caso de responder que SI a la pregunta anterior, ¿dicha auditoría se tiene en cuenta para garantizar la seguridad de la solución? Comentarios:	

- ☐ Procesos de auditorías externas de seguridad.

Pregunta	Respuesta (SI/NO/NP)
¿Se realizan auditorías de seguridad sobre la solución completa de forma externa? Comentarios:	
En caso de responder que SI a la pregunta anterior, ¿dicha auditoría se tiene en cuenta para garantizar la seguridad de la solución? Comentarios:	

- ☐ Se dispone de un diagrama claro de los flujos de información entre los lectores NFC (dispositivos activos) y el núcleo de la aplicación (BBDD, Core APP, APIs, …).

Pregunta	Respuesta (SI/NO/NP)
¿Se han validado dichos flujos de información con personal experto de seguridad en el desarrollo de software seguro para todos los diferentes usos que se dan a los dispositivos NFC de los usuarios? Comentarios:	
En caso de responder que SI a la pregunta anterior, ¿se han detectado problemas que pueden poner en peligro la integridad, o la confidencialidad de algún componente de la solución? Comentarios:	
En caso de responder que SI a la pregunta anterior, ¿se han tomado medidas para paliar dichos peligros de seguridad? Comentarios:	

- ☐ [Opcional para mejora de metodología] Indicar otros elementos relevantes de la lógica de la aplicación que no se hayan tenido en cuenta:

- TIPO Z [Opcional para mejora de metodología]: Especificar otros elementos relevantes no tenidos en cuenta en los apartados anteriores.

Anexo IV – Puesta en práctica de la metodología para su evaluación

Ficha con cuestionario de FASE 1-1

En esta versión del documento no se ha podido incluir esta información por la firma de un acuerdo de confidencialidad.

Ficha con cuestionario de FASE 1-2

En esta versión del documento no se ha podido incluir esta información por la firma de un acuerdo de confidencialidad.

Fichas con cuestionarios de FASE 1-3

En esta versión del documento no se ha podido incluir esta información por la firma de un acuerdo de confidencialidad.

Informe técnico

En esta versión del documento no se ha podido incluir esta información por la firma de un acuerdo de confidencialidad.

Informe ejecutivo

En esta versión del documento no se ha podido incluir esta información por la firma de un acuerdo de confidencialidad.

Informe de mejora por aplicación de la metodología

En esta versión del documento no se ha podido incluir esta información por la firma de un acuerdo de confidencialidad.