Smartphone, smartwatch, smartTV... ¿SmartCard?

- Vulnerabilidades y fortalezas en NFC -

Seguridad de la información

Gorka Barturen
Rubén Sánchez
Gaizka Virumbrales

Universidad de Deusto
Ingeniería Informática

En este proyecto hemos utilizado la herramienta de programación Android Studio, ApkTool para decompilar aplicaciones de la Play Store. También nos hemos adentrado un poco en el uso de ofuscadores como ProGuard.

Ingeniería Informática
Universidad de Deusto
http://ingenieria.deusto.es

Título:
Seguridad en NFC

Tema:
Seguridad de la Información

Proyecto:
Proyecto de asignatura

Número de grupo:
2

Participantes:
Gorka Barturen
Rubén Sánchez
Gaizka Virumbrales

Supervisor:
Pablo García Bringas

Copias: 1

Número de páginas: 17

Fecha:
12 de junio de 2016

Abstract:

En este proyecto estudiaremos las fortalezas y las debilidades de las NFC, como usarlas de un forma segura y como conseguir privatizar su información interna. Además intentaremos copiar una tarjeta mediante un programa que hemos creado nosotros mismos.

Índice general

Capítulo 1

Introducción

En este capítulo trataremos temas introductorios sobre la tecnología NFC, como su definición, formas de funcionar o usos. Servirá para tener una idea sobre como funciona esta tecnología y para tratar futuros temas de la seguridad y vulnerabilidades.

1.1. NFC

NFC significa *Near Field Communication*. Se trata de una tecnología inalámbrica que deriva de las tarjetas RFID, utilizadas en sistemas de transporte o de seguridad de algún establecimiento.

NFC es una plataforma abierta pensada desde el inicio para el teléfono o dispositivos móviles. Tanto su tasa de velocidad (424kbit/s) como su alcance (20m) son muy bajos, ¿Por qué se utiliza esta tecnología entonces?

Su punto fuerte esta en la velocidad de la comunicación, que es casi instantánea y no necesita de un emparejamiento previo. Además, el uso es transparente para los usuarios y los equipos con NFC son capaces de enviar y recibir al mismo tiempo.

Las tecnologías NFC tienen dos formas de funcionar:

- **Activo:** ambos equipos con chip NFC generan un campo electromagnético e intercambian datos.
- **Pasivo:** solo hay un dispositivo activo y el otro aprovecha ese campo para intercambiar la información.

1.2. Usos

La premisa básica a la que se acoge el uso de la tecnología NFC es aquella situación en la que es necesario un intercambio de datos de forma inalámbrica. Lo usos que más futuro tienen son la identificación, la recogida e intercambio de información y sobre todo, el pago.

- **Identificación:** acceso a lugares donde es preciso identificarse podría llevarse a cabo mediante el teléfono o con una tarjeta con NFC.
- **Recogida/intercambio de datos:** marcar un lugar en un mapa, recibir información de un evento o establecimiento es inmediato.
- **Pago:** pagar con tarjetas *contactless* o con el teléfono móvil convierte esta tarea en algo realmente cómodo.

Sin embargo, la comodidad es un gran enemigo de la seguridad.

1.2.1. Transferir fotos, vídeo o música

Aunque existen otras alternativas a la hora de pasar contenidos multimedia de un dispositivo móvil a otro (Bump es una de las más interesantes de los últimos

tiempos), NFC es (o al menos era originalmente) una forma muy interesante de dar acceso a esta capacidad.

De hecho, los chips NFC que comienzan a integrarse en algunos portátiles como el HP Envy 14 Spectre o en cámaras de fotos como las Panasonic Lumix DMC-ZS30 y DMC-TS5 que se comercializarán a partir de este mes permiten utilizar estos chips para transferir fotos, vídeos y música con este estándar, aunque probablemente lo combinen con Bluetooth y WiFi Direct para poder aumentar las velocidades de transferencia.

1.2.2. Identificación y control del coche

En el pasado CES se pudo ver un Porsche Carrera con un chip NFC integrado y con un pequeño ordenador basado en el sistema operativo de tiempo real QNX que disponía de una cuna para situar el smartphone con conectividad NFC. Al hacerlo el teléfono empezaba a recargarse, pero además se establecía la conexión para poder reproducir la música del móvil a través de los altavoces del coche, o realizar llamadas utilizando la agenda de contactos del smartphone.

Otra de las posibilidades consistiría en usar el móvil como una llave de acceso al coche, lo que permitiría convertir a los smartphones como sistemas redundantes (la llave convencional no se eliminaría) para poder acceder al interior del coche e incluso para poder encender el motor y desplazarnos con él. Orange y Opel ya lanzaron un sistema preliminar en este sentido que demuestra que esta es otra de las posibilidades de futuro reales de la tecnología NFC.

1.2.3. Cajeros automáticos 2.0

Otra alternativa en el ámbito de la identificación está en la capacidad de usar esta tecnología para comenzar una sesión en un cajero automático con la que poder sacar dinero. Al acercar nuestro terminal a la pantalla de un cajero con NFC, se realizaría la negociación inicial de la conexión para identificarnos y pedirnos nuestro correspondiente PIN.

Esta alternativa de nuevo se situaría como un sistema redundante que evitaría tener que utilizar la tarjeta de débito o crédito, y haría a menudo más cómoda la operación de acceder y utilizar un cajero automático.

1.2.4. Compras más allá de los códigos QR

Los códigos QR siguen teniendo validez para facilitar algunos procesos de compra, pero el hecho de tener que .^{es}canear"los códigos para luego acceder a las opciones que nos brinda ese código QR resulta algo incómodo comparado con la capacidad que tiene la tecnología NFC de transmitir esos datos automáticamente en cuanto acercásemos nuestro terminal a una etiqueta NFC con la información de ese producto.

Así, al realizar esa transferencia de información podríamos localizar determinados artículos en una tienda, pedir la ayuda de un asistente, o tratar de aprovechar cupones y ofertas si están disponibles en el sistema al realizar el pago.

1.2.5. Identificación en eventos

En el propio Mobile World Congress de Barcelona hemos visto como las posibilidades de identificación de la tecnología NFC son idóneas para mejorar los procesos de registro y control de acceso a todo tipo de eventos. Las llamadas NFC Badge eran acreditaciones con un chip NFC que permitían a los que las portaban poder acceder al recinto de la feria directamente y sin tener que mostrar repetidamente la acreditación física convencional.

Ese mismo sistema es el que poco a poco se va implantando –o se podría implantar al menos como opción– en otros eventos de todo tipo, tales como eventos deportivos, conciertos, acceso a hospitales y, por supuesto, acceso a oficinas de trabajo en las que además esa capacidad se combinaría con los sistemas de control de las jornadas laborales que muchas empresas utilizan.

1.2.6. Pagos móviles

La última posibilidad es sin duda de la que más se habla: los sistemas de pago móviles que hacen uso de la tecnología NFC llevan tiempo en desarrollo y pruebas, y de hecho hay implantaciones funcionando desde hace tiempo.

El servicio Google Wallet es probablemente el mejor ejemplo de esa ambición por proporcionar métodos de pago móviles de forma inalámbrica. En Estados Unidos la tecnología va por buen camino –200.000 comercios con sistemas de pago inalámbricos lo demuestran– pero de momento ese desarrollo no ha sido exportado a otros países. Los sistemas alternativos de Apple (Passbook) y de Samsung (el recién presentado Wallet, aunque menos ambicioso que el servicio de Google) persiguen el mismo objetivo, aunque su aplicación práctica real aún está por demostrarse.

Sin embargo, NFC sí es la base de muchos proyectos de grandes empresas financieras tales como Visa o Mastercard, y quizás en este 2013 comencemos a ver con cierta frecuencia a usuarios que pagan el transporte público (o el taxi) con su móvil vía NFC. En España ya hay ejemplos prácticos como el de La Caixa o Banesto y su implantación del sistema de pago contactless, con tarjetas de crédito que llevan implantadas el chip NFC y que permiten realizar pagos inalámbricos, más cómodos y que demuestran que esta tecnología puede ser una alternativa válida de futuro.

1.2.7. Etiquetas NFC

Las etiquetas (a menudo adhesivas) NFC permiten demostrar de nuevo las posibilidades de la tecnología al actuar como disparadores condicionales que permiten activar ciertos procesos en nuestro dispositivo móvil.

El escenario clásico sería el de tener una etiqueta en alguna pared (o varias) de nuestra casa para que al acercar el teléfono este habilitase la conectividad WiFi y Bluetooth, y que tuviéramos otra en la mesilla de noche que hiciera que al situar el smartphone al lado éste entrase en modo silencioso y se activase el despertador.

Un ejemplo de implementación práctica la tenemos en los Xperia SmartTags, que precisamente adaptan el perfil del teléfono según la etiqueta (a 14,90 euros cada un pack de cuatro, eso sí) a la que acerquemos el smartphone. Podríamos tener una etiqueta en el coche que activase el navegador GPS, y otras como las que hemos citado en casa para activar esos distintos perfiles. Lo mismo ocurre con las Samsung TecTiles, otro sinónimo de estas ingeniosas etiquetas inteligentes que tienen como objetivo hacernos la vida un poquito más fácil.

Capítulo 2

Seguridad en NFC

En este capítulo trataremos temas relacionados con la seguridad en las tarjetas NFC. Analizaremos vulnerabilidades y los métodos más comunes y eficaces para securizar los equipos NFC.

2.1. Justificación

Como hemos visto en el apartado anterior de usos, muchos de estos sistemas son utilizados como monedero, por lo tanto, corromper el sistema significaría acceder al dinero del portador del dispositivo.

En sistemas de identificación, falsificar la identidad de un directivo de la empresa, podría conceder al hacker permisos indeseados para los intereses de la empresa. Por lo tanto, debido al tipo de información que tienen estos equipos, garantizar la seguridad es una prioridad.

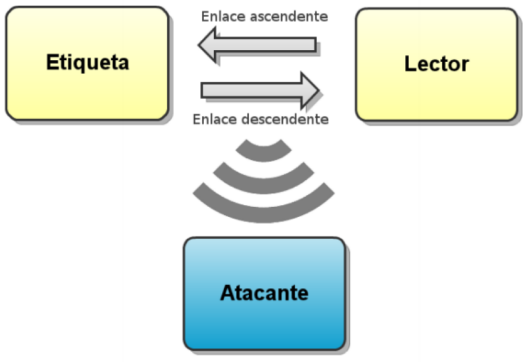
2.2. Amenazas

Las amenazas más comunes de los sistemas NFC son:

- Eavesdropping (Escucha)
- Skimming (Clonado)
- DoS (Denial of Service)
- Modificación de datos
- Inserción de datos
- Man-in-the-middle

2.2.1. Eavesdropping

La técnica de eavesdropping consiste en estar escuchando las conexiones de la víctima y el receptor sin llegar a hacer nada con los paquetes.



El espiar (snooping) y el observar los paquetes en la red (sniffing) son términos comunes para el eavesdropping.

El eavesdropping es el escuchar una conversación, espiar, husmear. La información recolectada por eavesdropping se puede utilizar para planear otros ataques a la red.

Un ejemplo de los datos susceptibles al eavesdropping, son las secuencias utilizadas en las comunidades SNMP versión 1, ya que se envían en texto claro. Un intruso podría hacer eavesdropping en los intercambios de información de SNMP, y recopilar datos valiosos de la configuración del equipo de la red.

Otro ejemplo, es la captura de nombres de usuario y contraseñas, números de la tarjeta de crédito o información personal sensible, cuando cruzan una red.

Un método común para realizar eavesdropping en comunicaciones, es capturar paquetes TCP/IP o de otros protocolos y descifrar el contenido usando un analizador de protocolos o una utilidad similar.

2.2.2. Skimming

Esta es la vulnerabilidad que atacaremos nosotros en el proyecto, consiste en obtener toda la información del sistema de la víctima y replicarlo en donde el atacante quiera. En esencia, la clonación.

Los escenarios comunes en los que se realiza skimming es en restaurantes, bares, gasolineras o en cajeros electrónicos donde un cómplice del criminal está en posesión de la tarjeta de crédito de la víctima o en un lugar en el que se ha instalado un dispositivo que puede copiar la información.

En el caso de un cajero automático, el autor del fraude pone un disposan a menudo en combinación con una microcámara que graba el código PIN (Código de seguridad) del usuario.

Es difícil que el titular de la tarjeta detecte el skimming, pero es bastante fácil de detectar para el emisor de la tarjeta con una muestra lo suficientemente grande.

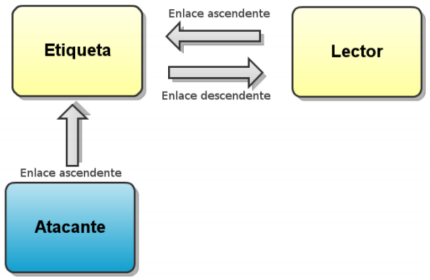
Por lo general, alguien en un cajero automático o en un local comercial utiliza un pequeño dispositivo para copiar y robar datos de la banda magnética de una tarjeta de crédito o de débito. Esa información se coloca sobre una tarjeta falsificada y se utiliza para hacer compras fraudulentas.

2.2.3. Denial of Service

Como en muchas otras disciplinas, en el campo de las NFC también es posible hacerle a la víctima una denegación de servicio saturando el sistema y llenándolo de ruido.

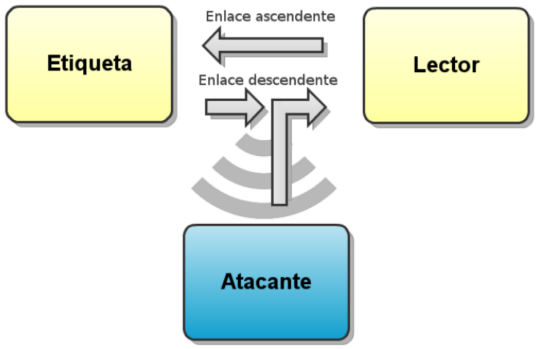
2.2.4. Modificación de datos

Este ataque consiste en modificar alguno -o todos- de los datos con los que actualmente cuenta la tarjeta. Esto puede utilizarse para el beneficio del sistema, por ejemplo recargar alguna tarjeta monedero, o para corromperla, insertando un chorro de unos.



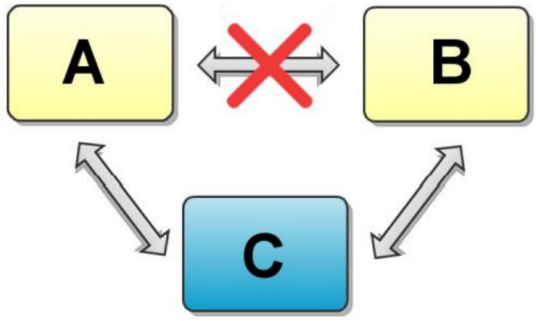
2.2.5. Inserción de datos

La inserción de datos se basa en sustituir el mensaje que la víctima manda por la que el atacante desee.



2.2.6. Man-in-the-middle

En el proceso de man-in-the-middle se basa en interceptar los mensajes y después mandarlo modificados o igual que como la víctima los intercepta.



Capítulo 3

Nuestra aproximación a la vulnerabilidad

En este capitulo trataremos la aproximación de nuestros ataques a los sistemas NFC por el método de skimming. Son diversas las posibilidades para realizar estos ataques pero nosotros optamos por dos, los smartphones Android y microcontroladores preparados expresamente para ello.

3.1. Smartphones Android

Los teléfonos Android con su tecnología NFC, son sin duda un muy buena plataforma para explotar las debilidades que hemos comentado. Nosotros hemos utilizado un *Samsung Galaxy S6* para realizar todas las pruebas.

3.1.1. Aplicación Android

Ante la imposibilidad de desofuscar una aplicación ya creada y modificarla a nuestro antojo, decidimos tomar el camino de crear nuestra propia aplicación. Nos servimos de AndroidStudio y de la API de Android para crearla.
Nuestro objetivo era ser capaces de guardar los diferentes tags de las tarjetas NFC en el móvil y ser capaces de reproducirlo a nuestro antojo.
La funcionalidad de nuestra aplicación es bastante simple, lee la tarjeta NFC, la guarda en una base de datos y escribir el ID a una tarjeta en blanco.
La aplicación consta de una interfaz en la que hay un botón. En cuanto se lee la tarjeta, se almacena en la base de datos y se muestra el código hexadecimal y decimal. Para escribir, la aplicación detecta automáticamente una tarjeta en blanco que se le aproxima y muestra como botones todos los tags en la base de datos. Al seleccionar uno de los botones, se termina el proceso de clonado.

3.1.2. Problemas

Android no soporta la emulación de tarjetas ni la programación a bajo nivel del NFC. Por lo tanto, nos decantamos porque la aplicación escribiera a una tarjeta NFC el contenido de la tarjeta objetivo. Sin embargo, no contamos con una tarjeta en blanco para hacer demostraciones físicas, pero la funcionalidad esta implantada.

3.2. Microcontroladores

En esta sección hablaremos sobre como abordar las vulnerabilidades de NFC con microcontroladores preparados para ello.

3.2.1. Opción PROXMARK III

Esta placa permite realizar sniffing de varias tecnologías NFC.

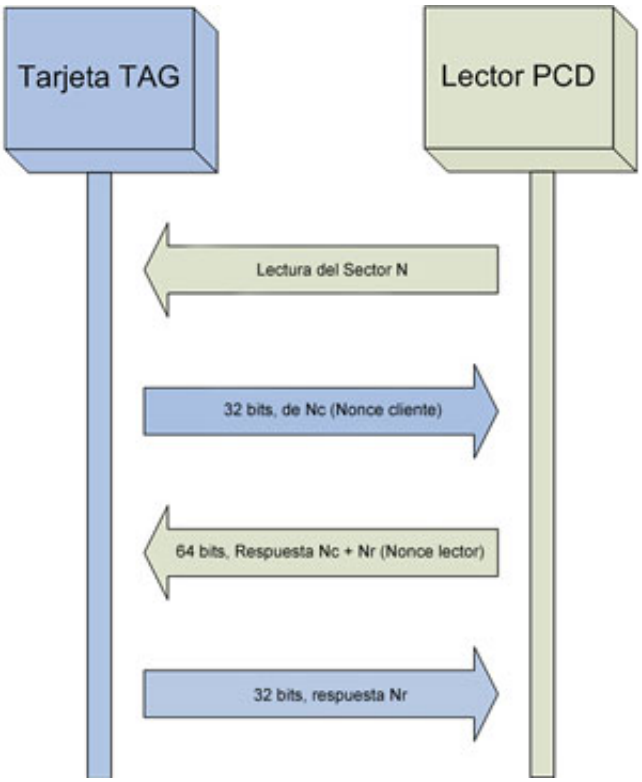


Figura 3.1: Proceso de handshake de las tarjetas Mifare

Al comenzar lector le comunica a la tarjeta que quiere realizar una operación sobre un sector de datos determinado N. El tag o tarjeta en ese momento remite un número aleatorio Nc (Nonce del cliente) de 32 bits a modo de reto, para que sea cifrado con la clave privada compartida previamente. Como respuesta, el lector remite el reto cifrado y un número aleatorio Nr (Nonce del lector) para que el tag lo cifre con la clave privada, generando una trama de 64 bits. En última instancia la tarjeta le envía al lector su reto cifrado. En este momento ambos tienen la certeza de que los dispositivos son legítimos. Destacar que los dos últimos intercambios se realizan ya de forma cifrada, permaneciendo en claro tan solo el envío de la petición de lectura y Nc.

Posteriormente necesitaríamos una tarjeta Mifare y un lector NFC conectado a un ordenador con el que posteriormente podremos ver los tags de la tarjeta. Colocando el sniffer entre la tarjeta y el lector podríamos proceder a realizar una lectura del sector 4, obteniendo la siguiente traza de bytes.

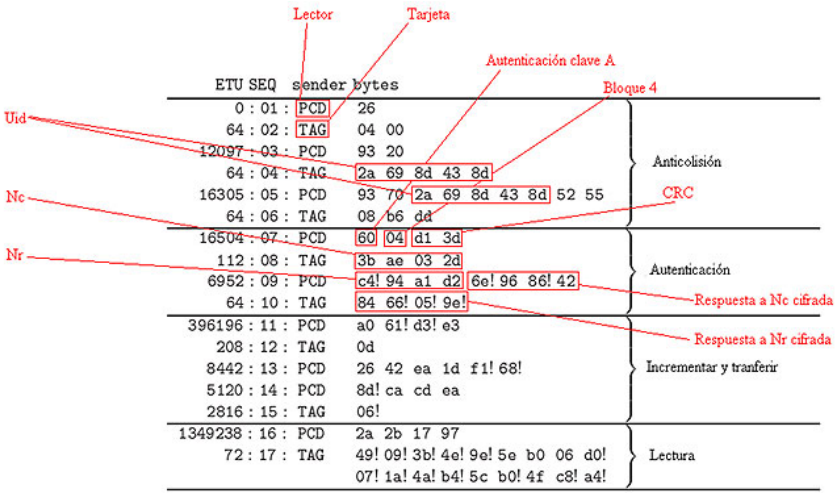


Figura 3.2: Lectura de la tarjeta Mifare

Con la información que hemos capturado podremos intervenir la clave privada del sector mediante una aplicacion llamada *CRAPTO1*.

Con esta clave privada ya podremos leer/modificar el contenido de los bloques de datos que componen el sector 01. Podríamos por ejemplo incrementar el valor del monedero electrónico, si el valor reside dentro de la tarjeta. Lo mas habitual es encontrarse el reste de sectores protegidos con la misma pk, lo que habilitaría un clonado completo de la tarjeta.

3.2.2. Conclusión

Los microcontroladores son una solución mas viable que las aplicaciones que se puedan crear para Android ya que los microcontroladores se hacen expresamente para esto y en cambio en Android tienes que ceñirte a la API que este te ofrece. En cambio, los microcontroladores requieren conocimientos de electrónica avanzados a parte de saber como programarlos.

Capítulo 4

Conclusión

Sin duda, la tecnología NFC ha avanzado en los últimos años y se está empezando a hacer más y más común el uso de estos sistemas para pagos o autentificaciones. Sin embargo, y como pasa en muchos otros sectores, la seguridad no parece ser un punto importante hasta que pase alguna desgracia. La seguridad que se esta implantando en estos sistemas es bastante mediocre para el tipo de información que manejan. Esto resulta en que sea relativamente fácil hackear la tarjeta de acceso de un directivo o obtener toda la información de las tarjetas de crédito de los asistentes a una conferencia. Si la seguridad sigue sin ser una prioridad, veremos en un futuro bastante cercano como algún hacker se ha aprovechado de esto.