Smartphone, smartwatch, smartTV... ¿SmartCard?

- Vulnerabilidades y fortalezas en NFC -

Seguridad de la información

Gorka Barturen
Rubén Sánchez
Gaizka Virumbrales

Universidad de Deusto
Ingeniería Informática

Copyright © Universidad de Deusto

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: 11

Fecha:
8 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

1. Introducción **1**
1.1. NFC 2
1.2. Usos 2

2. Seguridad en NFC **3**
2.1. Justificación 4
2.2. Amenazas 4
2.2.1. Eavesdropping 4
2.2.2. Skimming 5
2.2.3. Denial of Service 5
2.2.4. Modificación de datos 5
2.2.5. Inserción de datos 6
2.2.6. Man-in-the-middle 6

3. Ataques a sistemas NFC **7**
3.1. Smartphones android 7
3.2. PICCs 7

4. Conclusion **9**

A. Appendix A name **11**

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.

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.

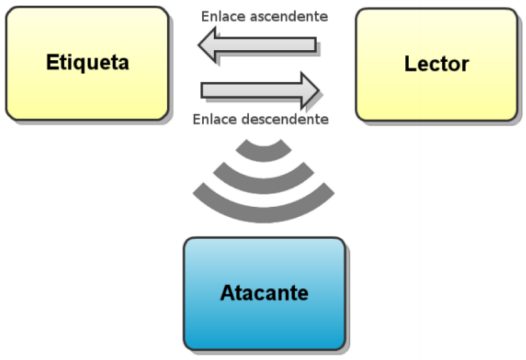
2.2. Amenazas

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.



2.2.2. Skimming

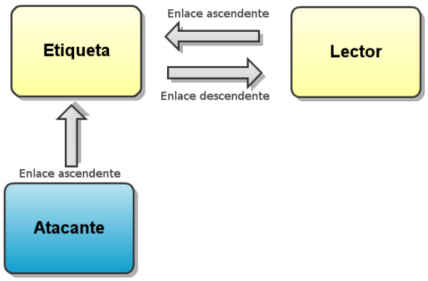
Esta es la vulnerabilidad que atacaremos nosotros en el proyecto, consiste en obtener toda la información del sistema de la víctima y replicarlo en donde el atacante quiera. En esencia, la clonación.

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.

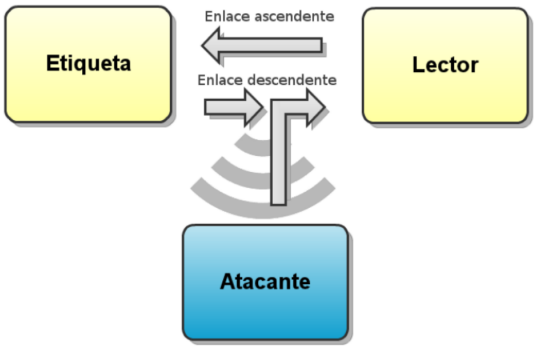
2.2.4. Modificación de datos

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.



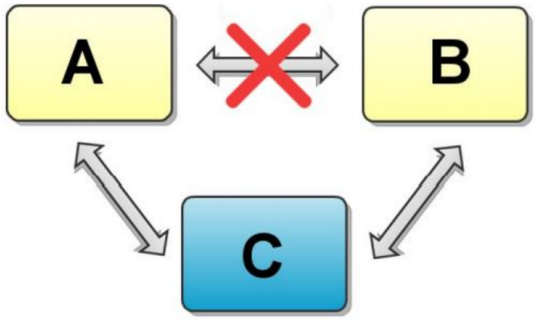
2.2.5. Inserción de datos

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

Ataques a sistemas NFC

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 PICCs preparados expresamente para ello.

3.1. Smartphones android

3.2. PICCs

En esta seccion hablaremos sobre los PICCs preparados para vulnerar las seguridades de NFC.

3.2.1. Explicación

3.2.2. Tipos

3.2.3. Usos

Capítulo 4

Conclusion

In case you have questions, comments, suggestions or have found a bug, please do not hesitate to contact me. You can find my contact details below.

Jesper Kjær Nielsen
jkn@es.aau.dk
http://kom.aau.dk/~jkn
Fredrik Bajers Vej 7
9220 Aalborg Ø

Apéndice A

Appendix A name

Here is the first appendix