UNIVERSIDAD DE GRANADA

TRABAJO FIN DE MÁSTER

MÁSTER PROPIO EN CIBERSEGURIDAD

Revisión y mejora de técnicas de hacking para dispositivos NFC

Autor
José Luis París Reyes

Directores
Gabriel Maciá Fernández

Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación

—

Granada, Julio de 2023

Revisión y mejora de técnicas de hacking para dispositivos NFC

José Luis París Reyes

Palabras clave: palabra_clave1, palabra_clave2, palabra_clave3, ...

Resumen

Poner aquí el resumen.

Project Title

First name, Family name (student)

Keywords: Keyword1, Keyword2, Keyword3, ...

Abstract

Write here the abstract in English.

Yo, **Nombre Apellido1 Apellido2**, alumno del **Máster Propio en Ciberseguridad** de la **Universidad de Granada**, con DNI XXXXXXXXX, autorizo la ubicación de la siguiente copia de mi *Trabajo Fin de Máster* en la biblioteca del centro para que pueda ser consultada por las personas que lo deseen.

Fdo: Nombre Apellido1 Apellido2

Granada a X de mes de 201 .

D. **Nombre Apellido1 Apellido2 (tutor1)**, Profesor del Departamento YYYY de la Universidad de Granada.

D. **Nombre Apellido1 Apellido2 (tutor2)**, Profesor del Departamento YYYY de la Universidad de Granada.

Informan:

Que el presente trabajo, titulado ***Título del proyecto***, ha sido realizado bajo su supervisión por **Nombre Apellido1 Apellido2 (alumno)**, y autorizamos la defensa de dicho trabajo ante el tribunal que corresponda.

Y para que conste, expiden y firman el presente informe en Granada a X de mes de 201 .

Los directores:

Nombre Apellido1 Apellido2 (tutor1) **Nombre Apellido1 Apellido2 (tutor2)**

Agradecimientos *(opcional)*

Poner aquí agradecimientos...

Índice general

Índice de figuras

Índice de cuadros

Listings

Capítulo 1

Introducción

1.1. Motivación

La evolución de la tecnología ha propiciado un gran avance para el ser humano y su calidad de vida, desde los primeros circuitos electrónicos y tarjetas perforadas en los años 60 y 70, hasta el supercomputador más sofisticado en la actualidad, capaz de hacer cálculos de gran complejidad en un tiempo inapreciable, identificación de patrones en ADN o predicción de fenómenos metereológicos, entre otras cosas.

Toda esta tecnología se compone a grandes rasgos de un hardware y un software que le permite funcionar correctamente y satisfacer las necesidades de los usuarios. Dicha evolución ha propiciado la sofisticación de estos dos componentes, provocando que se vuelvan lo suficientemente complejos como para que no se puedan tener en cuenta todas las casuísticas por las que pueden fallar.

El problema se vuelve aún mayor cuando esta tecnología, que permite almacenar, transmitir y procesar información y que está al alcance de cualquiera en forma de un dispositivo portable, es vulnerable, provocando que un usuario con intenciones malintencionadas obtenga información que no debería o adquiera el poder de realizar acciones suplantando la identidad de otra persona.

Además, la popularización de la tecnología *NFC* que aparece en 2006 ha agravado esta situación, permitiendo establecer una comunicación inalámbrica de corto alcance y alta frecuencia para el intercambio de datos entre dispositivos [1]. Es decir, esta tecnología se encuentra en todas partes, desde los pagos con tarjetas de crédito o débito hasta la sincronización entre dispositivos móviles o la transferencia de información entre ellos.

Es por ello que en este trabajo se revisarán las técnicas actuales que existen contra esa tecnología, se trabajará en posibles mejoras y se hará una realización práctica de las mismas en un laboratorio. La finalidad se basa en mostrar el peligro que supone la vulneración de su seguridad y lo importante que es la continua mejora en la protección de esta tecnología.

1.2. Contexto

1.3. Metodología

1.4. Estructura

Capítulo 2

Especificación de requisitos

En el siguiente capítulo se detallará la planificación temporal que ha seguido el proyecto, así como los recursos utilizados y el presupuesto necesario para lograrlo.

2.1. Planificación temporal

2.1.1. Estado del arte del trabajo

2.1.2. Análisis

2.1.3. Diseño e implementación

2.1.4. Pruebas

2.1.5. Redacción del documento de memoria

2.2. Recursos

Para la realización del trabajo se han necesitado de 3 tipos de recursos, los cuales han estado presentes durante toda la realización del trabajo: humanos, hardware y software.

2.2.1. Recursos humanos

Principalmente está compuesto por las personas involucradas en el desarrollo de la investigación. En este caso se trata de dos figuras:

- **José Luis París Reyes**, alumno del Máster en Formación Permanente en Ciberseguridad por la Escuela de Postgrado de la Universidad de Granada en colaboración con la propia universidad, al que corresponde la autoría de este mismo documento.

- **D. Gabriel Maciá Fernández**, profesor perteneciente al departamento de Teoría de la Señal, Telemática y Comunicaciones, como tutor del proyecto, cuya funcionalidad principal ha sido la de dirigir al estudiante para la investigación y estructura del mismo.

2.2.2. Recursos hardware

La realización de la investigación ha requerido de diferentes dispositivos hardware que se detallan a continuación:

- **Ordenador de sobremesa personal**, en el que se han ejecutado todas las pruebas respectivas al trabajo, así como clonación de información y ataques a diferentes tipos de tarjetas. Este ha sido el dispositivo de mayor prestaciones del que ha dispuesto el estudiante y el que ha otorgado mayor comodidad, por lo que la mayoría de pruebas se han realizado sobre el mismo. Las características principales son:
  - **Procesador:** Ryzen 5 5600X - 3700GHz - 6 Núcleos / 12 Hilos
  - **Tarjeta Gráfica:** Nvidia RTX 3070 Ti
  - **Memoria RAM:** 4x8GB DDR4 - 3200 MHz
- **Ordenador portátil personal**, aunque no ha sido usado con mucha frecuencia porque se ha utilizado principalmente si el estudiante ha necesitado desplazarse a otro lugar de residencia o a una reunión con el tutor. Las características principales no serán detalladas porque su función principal ha sido la continuación en la redacción del trabajo, por lo que sus prestaciones no han influido en la ejecución de las pruebas.
- **Conexión de fibra óptica a internet**, en todo momento se ha dispuesto de una conexión de alta velocidad a internet de 1Gbps. La función principal ha sido la de consulta bibliográfica, descarga y subida de ficheros desde el laboratorio de trabajo.
- **Lector de tarjetas RFID Proxmark3 Easy**, se trata del lector de tarjetas que se ha usado para realizar todas las pruebas del proyecto. **NO SÉ SI DEBERÍA INSERTAR LINK DE COMPRA**
- **Surtido de tarjetas RFID**, diferentes tarjetas que se han adquirido para la realización de diferentes ataques o clonación de datos en función de la frecuencia o tipo de las mismas. **NO SÉ SI DEBERÍA INSERTAR LINK DE COMPRA**

2.2.3. Recursos software

Aquel software del que se ha hecho uso y que será ampliado con mayor detalle en el capítulo 3.

- **Sistema Operativo Linux**, ambos dispositivos (ordenador de sobremesa y ordenador portátil) hacen uso de una distribución de Linux basada en Arch Linux, en este caso se trata de la distribución Manjaro. Sobre este sistema operativo se han realizado todas las pruebas y se han instalado los diferentes programas.
- **Lenguajes de programación**, principalmente han sido lenguajes de scripting como *Python* o *Bash* para la automatización y ejecución de pruebas.
- **Software para Proxmark3 Easy**, se trata del software que permite ajustar el firmware usado en la placa lectora de tarjetas.

2.3. Presupuesto

Tras haber detallado los recursos necesarios para el proyecto, así como la planificación temporal, se puede calcular el presupuesto de su desarrollo (ver Cuadro X.X).

Cuadro 2.1: Presupuesto del proyecto

Recurso	Coste	Tiempo	Coste total
Trabajo realizado por el autor	15€	-	X€
Trabajo realizado por el tutor	30€	-	X€
Alquiler de ordenador de sobremesa personal	5€	-	X€
Alquiler de ordenador portátil personal	3€	-	X€
Conexión de alta velocidad a internet	30€	-	X€
Lector de tarjeats RFID Proxmark3 Easy	50€	-	50€
Surtido de tarjetas RFID	15€	-	15€
Sistema Operativo Linux	0€	-	0€
Lenguaje de programación	0€	-	0€
Software para Proxmark3 Easy	0€	-	0€
Total			X€

El coste del hardware es aproximado y se ha calculado en base a un alquiler por hora, a excepción del lector de tarjetas y el surtido de las mismas, ya

que el coste es bajo y se puede asumir como compra en lugar de alquier. Este coste puede variar debido a las prestaciones que el usuario precise. Además, tras haber completado la ejecución de pruebas y recopilación de datos, no sería necesaria una posterior utilización del equipo.

El autor ha realizado una media de X horas al día durante X días para el desarrollo y finalización de la investigación, a un precio estimado de 15€ por hora. Puesto que no se tenía experiencia previa en la ejecución de técnicas de *hacking* con tecnología *NFC*, se ha requerido más tiempo del esperado para la obtención de resultados y conclusiones del que hubiese necesitado un profesional en ese sector.

Capítulo 3

Estado del arte

Tras haber presentado el proyecto, su motivación y estructura, así como los recursos que necesitará para desarrollarse y adjuntado el presupuesto aproximado de los mismos, se procede a detallar con un putno de vista más técnico, las técnicas y programas que se usarán para la realización de la investigación.

3.1. RFID

No se puede comenzar a trabajar con tecnología *NFC* sin conocer su tecnología predecesora, esta es *RFID (Radio Frequency Identification)*, que surge por primera vez [**?**]

Bibliografía

[1] Historia de la informática - NFC. https://histinf.blogs.upv.es/2012/11/21/nfc/.