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

Bibliografía

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