UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

Plan de Investigación de fin de carrera titulado:

"ANÁLISIS DE BIOHACKING, CASO DE ESTUDIO: IMPLANTES DE MICROCHIP PARA HUMANOS CON TECNOLOGÍA NFC"

Realizado por:

BYRON FABIAN AGUINSACA HURTADO

Director del proyecto:

ING. LUIS FABIÁN HURTADO VARGAS, MGS.

Como requisito para la obtención del título de:

MASTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD DE REDES Y COMUNICACIÓN

DECLARACION JURAMENTADA

Yo, BYRON FABIAN AGUINSACA HURTADO, con cédula de identidad N°1104062383, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

_____

Byron Fabian Aguinsaca Hurtado

C.C.: 1104062383

DECLARATORIA

El presente trabajo de investigación titulado:

“ANÁLISIS DE BIOHACKING, CASO DE ESTUDIO: IMPLANTES DE MICROCHIP PARA HUMANOS CON TECNOLOGÍA NFC”

Realizado por:

BYRON FABIAN AGUINSACA HURTADO

Como requisito para la obtención del Título de:

MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD DE REDES Y COMUNICACIÓN

Ha sido dirigido por el profesor

ING. LUIS FABIÁN HURTADO VARGAS, MGS.

Quien considera que constituye un trabajo original de su autor

_____

Luis Hurtado

DIRECTOR

PROFESORES INFORMANTES

ING. DIEGO RIOFRIO, PhD.
ING. CHRISTIAN PAZMIÑO, MsC.

Después de revisar el trabajo presentado,
lo ha calificado como apto para su defensa oral ante
el tribunal examinador

_____	_____
ING. DIEGO RIOFRIO, PhD.	ING. CHRISTIAN PAZMIÑO, MsC.

Quito, 09 de septiembre del 2019

DEDICATORIA

El presente trabajo realizado para culminar uno de mis sueños profesionales, que inició hace cinco años atrás al llegar a esta ciudad, se lo dedico:

A Dios, por brindarme sus bendiciones en el transcurso de mi carrera estudiantil en la Universidad, guiándome en cada decisión tomada, para conseguir mis objetivos propuestos.

A mis abuelitos, Carmen, Ángel y Jorge, quienes desde el cielo siempre me cuidan las espaldas; y a mi abuelita Amada, quien desde la tierra me brinda su sabiduría, aconsejándome sobre las cosas buenas que tiene la vida y como vivir en armonía.

A mis padres, Ermel y Lidia, quienes siempre me han brindado su apoyo incondicional para cumplir las metas trazadas en mi vida. Los amo mucho y en el lugar en que me encuentre, los llevo siempre conmigo en mi corazón.

A mis hermanos, Yesenia y Vinicio, quienes me han animado e incentivado a ser mejor cada día con su ejemplo. A pesar de las diferencias que cada uno tenemos, siempre existe el amor infinito de hermanos.

A mis cuñados, Galo y Katy, quienes desde que pasaron a formar parte de mi familia, han sabido extenderme sus brazos para acogerme como un hermano.

A mis sobrinos, Josselyn, Jostyn, Mateo y Salome, quienes con sus diabluras y locuras siempre alegraran mi vida; y a mi sobrino Junior, quien desde el cielo brinda protección a toda la familia.

A ellos les dedico mis alegrías, mis triunfos, esta tesis.

AGRADECIMIENTOS

Existen tantas personas a las que me gustaría agradecer su apoyo, amistad, amor y ánimo en las diferentes etapas de mi vida. A algunas las veo diariamente, otras por la distancia de vez en cuando; y unas que me ha tocado verlas partir.

A mis padres y hermanos, por ser el motor y la fuerza principal de mi vida, por estar incondicionalmente, brindándome sus consejos y amor.

A mis amigos, Diana, Klever, Felipe, Mayra, Doris, Jessica, Verito, Pedro, Javier, Diego, Hugo y Liz; por formar parte importante de mi vida y ser un apoyo incondicional, en cada decisión tomada en el transcurso de mi estadía en la ciudad de Quito.

A los docentes de la Maestría en Tecnologías de la Información con mención en Seguridad de Redes, quienes me compartieron sus conocimientos y experiencias profesionales.

Finalmente, a todos mis compañeros de la carrera, juntos logramos un objetivo común y en el transcurso consolidamos una amistad tanto personal como profesional.

RESUMEN

En el presente trabajo se realiza el análisis de uno de los dispositivos de biohacking, como caso particular de estudio, los denominados implantes de microchips para humanos con tecnología NFC, considerando que estas innovaciones tecnológicas al contener información, pueden estar sujetas a ataques maliciosos

Para ejecutar la investigación, se estudió la arquitectura de la tecnología NFC, conjuntamente con el análisis de las vulnerabilidades existentes en un implante de microchip de la serie xNT, mediante técnicas de *Ethical hacking*.

En el desarrollo del análisis se establecieron dos escenarios de prueba para simular un sistema de funcionamiento real del implante, para lo cual se ejecutó un ataque mediante la técnica de clonación, a través de aplicaciones y herramientas especializadas. El ataque se efectuó en dos fases: en primera instancia, se clonó el UID del implante para burlar un control de acceso, y en la segunda, se duplicó la información almacenada en el microchip para automatizar la ejecución de tareas en un *Smartphone*.

A partir de los resultados obtenidos se determinaron las vulnerabilidades que tienen los implantes de la serie xNT. Con la información recabada se plantean mejores condiciones de seguridad a estos implantes, mediante estrategias que aumenten la seguridad de la información y reduzcan de manera significativa el riesgo del uso de esta tecnología.

Palabras claves: biohacking, microchip, ethical hacking, vulnerabilidades, clonación, seguridad de la información.

ABSTRACT

The present research is based on the analysis of one of the biohacking device as a particular case of study. These are known as the data of microchip implants for humans with NFC technology, considering that these technological innovations, as they contain information, may be subject to malicious attacks

In order to carry out this investigation, the NFC architecture was studied in conjunction with the analysis of the existing vulnerabilities in a microchip implant of xNT series by applying Ethical hacking techniques.

On the development of the analysis, two test scenarios were established to simulate a real functioning system of the implant, and thus an attack was executed with the cloning technique, through specialized applications and tools. The attack was carried out in two phases: First, the UID from the implant was cloned for circumventing the access control while in the second instance, the information stored in the microchip was duplicated to automate the tasks execution in a Smartphone

Based on the results obtained, the vulnerabilities of implant with xNT series were determined. The information gathered, pose better security conditions for these implants, through strategies that increase information security and significantly reduce the risk of using this technology

Key words: biohacking, microchip, ethical hacking, vulnerabilities, cloning, information security.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

CAPÍTULO I

INTRODUCCIÓN

1.1 EL PROBLEMA DE INVESTIGACIÓN

1.1.1 Diagnóstico del problema

Biohacking es la búsqueda del ser humano por mejorar las capacidades físicas de su cuerpo y de su mente, mediante la integración de la tecnología a su sistema biológico. Varios científicos, investigan y elaboran prototipos que permiten esas mejoras. Estos grupos de investigadores y aficionados, que incorporan modificaciones de su cuerpo, son los llamados biohackers (Fundación Telefónica, 2017).

Según Coenen (2017), no existe un límite de modificaciones que un ser humano se puede realizar, varios prototipos ya han sido probados, modificando ciertos aspectos del cuerpo, logrando mejorar las capacidades del usuario. Pero estas mejoras dejan una brecha abierta en relación a la información que almacenan, no garantizan su seguridad, existiendo la posibilidad de un ataque a un sistema biohacking.

A nivel de Latinoamérica, son pocos los países que han mostrado interés en el tema de biohacking, entre ellos se destacan Brasil y Chile. Se espera que en el Ecuador el tema de biohacking tomé impulso y las empresas tecnológicas empiecen a usar estos dispositivos en el desarrollo de sus proyectos. El país debe estar preparado, tanto para los beneficios, como para los riesgos que pueda tener el uso de esta tendencia tecnológica.

1.1.2 Pronóstico

Uno de los dispositivos que actualmente se comercializa a nivel mundial, es un microchip con tecnología NFC, el cual se implanta en las manos de los biohackers. Este puede ser utilizado de diferentes formas: como llaves de ingreso a distintas localidades, para activar equipos electrónicos

(laptops, vehículos o *Smartphone*), para ejecutar tareas en teléfonos inteligentes o como memoria de almacenamiento de información (Sanchez, 2014).

Los microchips almacenan información de interés del usuario y tienen un identificador único (UID), esto hace que sea necesario considerar las siguientes interrogantes: ¿Es seguro tener información almacenada en el microchip e implantarla en la mano?, ¿La tecnología NFC garantiza seguridad de esa información?, ¿Es posible obtener la información y el UID del implante?

1.1.3 Control del pronóstico

En varios documentos, se detallan análisis de vulnerabilidades a dispositivos electrónicos, algunos ejemplos son: los marcapasos, los *Smartphone* y los *Smartwatch*. Los cuales han sido vulnerados por hackers informáticos o hasta por aficionados, quienes lo realizan para obtener un beneficio personal o a su vez para probar la seguridad del dispositivo (Tori, 2018; Rojas & Ferney, 2015). Inclusive existen casos en los cuales las empresas fabricantes, solicitan a un experto informático verificar la seguridad del equipo.

Según Giusto (2018), la información que se encuentra en estos dispositivos no está segura, más aún si el usuario, no toma medidas de precaución ante las amenazas a las que se encuentra expuesto. Para mejorar la seguridad de la información, se debe concientizar a los usuarios acerca del hábito de ser precavidos.

De lo expuesto anteriormente, se puede decir que la información almacenada en los implantes de microchip está sujeta a ataques maliciosos. Además, es importante mencionar que hay gran cantidad de información respecto a las aplicaciones que tiene el implante; pero en cambio, poca información respecto a sus vulnerabilidades.

1.1.4 Formulación del Problema

El desconocimiento de las debilidades y falencias que tiene un sistema de biohacking, específicamente, los implantes de microchip con tecnología NFC en humanos, admite la

posibilidad de que la información almacenada o su UID, sean vulnerables a ataques que afecten la integridad, confidencialidad y disponibilidad de la información.

1.2 OBJETIVOS

1.2.1 Objetivo General

Analizar las vulnerabilidades existentes en un implante de microchip con tecnología NFC para humanos, mediante técnicas de *ethical hacking*, que permitan la identificación del riesgo al cual se encuentra expuesto la persona que utiliza el microchip.

1.2.2 Objetivos Específicos

- Identificar los componentes de un implante de microchip con tecnología NFC, a través del estudio de cada uno de sus elementos, determinando la estructura general que tiene un implante.
- Definir una técnica de *ethical hacking*, mediante el análisis de las técnicas existentes para la tecnología NFC, identificando las vulnerabilidades en los implantes de microchip para personas.
- Emplear la técnica de clonación en implantes de microchip para personas, por medio de aplicaciones o herramientas especializadas, mostrando el peligro al cual se encuentra expuesto los usuarios.
- Contrastar futuras condiciones de seguridad a implantes de microchips de la serie xNT, a través de distintas estrategias, aumentando la seguridad de la información y reduciendo el riesgo de uso de esta tecnología.

1.3 JUSTIFICACIÓN

Actualmente con el desarrollo tecnológico, se habla de una nueva etapa en la aplicación de la tecnología al campo de la biología humana, el ritmo de innovación con el cual se han realizado los avances tecnológicos, predice un camino de evolución para los biohackers (Diéguez, 2013).

Todas las personas utilizan de forma directa o indirecta, algún tipo de dispositivo que les ayuda a realizar determinadas actividades. De manera directa, al estar asociado a alguna función biológica del ser humano; y de manera indirecta, al utilizarlo cuando es necesario; siendo la actividad ejecutada o la información manejada por el dispositivo, vulnerable (Sanchez, 2014).

Basándose en lo anterior, es necesario realizar un análisis de vulnerabilidades, a un implante de microchip con tecnología NFC, mediante la aplicación de una técnica de *ethical hacking*, que identifique esas debilidades y mitigue el riesgo del uso de esta tecnología. El autor Tori (2018), define a *ethical hacking* como la explotación de las vulnerabilidades existentes en un sistema de interés, mediante técnicas de intrusión y con los resultados obtenidos se pueden tomar medidas preventivas.

La aplicación de una técnica de *ethical hacking* a implantes de microchips, permitirá establecer un método de ataque a estos dispositivos. Ésta puede ser usada como base por otros investigadores en otros dispositivos; o plantear experimentos, con artefactos del mismo estilo en otras versiones.

Con los resultados obtenidos en esta investigación, se espera realizar un aporte a la comunidad científica, contribuyendo de esta manera al conocimiento existente sobre las vulnerabilidades de los implantes de microchip con tecnología NFC para humanos.

1.4 MARCO TEÓRICO

1.4.1 Ethical hacking

El *Ethical hacking*, es explotar las vulnerabilidades existentes en un sistema de interés, mediante técnicas de instrucción. Existen profesionales expertos en alguna área de informática que ejecutan test de penetración a diferentes sistemas, la diferencia entre estos profesionales es el fin para el cual lo realizan, si el objetivo es probar la seguridad de un sistema de información de quien lo contrate es un hacker ético; en cambio, si sus fines es encontrar vulnerabilidades y utilizarlas para su conveniencia es un *cracker* (Tori, 2018).

1.4.2 Técnicas de *Ethical hacking*

Una técnica es el conjunto de pasos que deben ser realizados, con el objetivo de tener un resultado determinado (Velázquez, 2016). Rojas, Bautista y Medina (2016) determinan que los pasos para el desarrollo de pruebas de penetración son: la recolección de información, el análisis de vulnerabilidades, la definición de objetivos, el ataque y los resultados. En la figura 1, se muestran el flujograma establecido para la ejecución de una técnica de *Ethical hacking*.

A. Recolección de Información

En la primera etapa, se pueden dar dos situaciones. La primera, son pruebas a ciegas, no se tiene ningún tipo de información. La segunda, se tiene información básica, que optimiza el tiempo de pruebas, orientándolas a los objetivos.

B. Análisis de Vulnerabilidades

Descubre problemas de seguridad usando herramientas especializadas, estas herramientas dependen del sistema que se requiera vulnerar. Como resultado de esta etapa, se logra determinar la estrategia a seguir durante las pruebas de seguridad.

C. Definición de Objetivos

Se establecen los objetivos a los cuales se va a llegar, mediante el ataque a las vulnerabilidades detectadas, se determinan cual es el objetivo principal del ataque y los objetivos secundarios para llegar a efectuarlo.

D. Ataque

Se efectúa el ataque a los objetivos seleccionados en la fase anterior. Dentro de esta etapa, se determina el impacto de las vulnerabilidades en la organización, además, pueden surgir nuevas vulnerabilidades no detectadas, que serán incluidas para su verificación.

E. Análisis de Resultados

Se recopilan los resultados obtenidos en cada una de las fases anteriores y se genera un informe, detallando las recomendaciones requeridas para solucionar las vulnerabilidades encontradas. Al lograr alcanzar la meta, se repiten el ciclo, volviendo a la primera etapa.

Figura 1. Pasos para ejecutar una técnica de *Ethical hacking*. Fuente: Autor

1.4.3 Biohacking, definición y términos asociados

El término biohacking, procede de la unión de biología y hacking, apunta a la acción de introducirse en un sistema vivo y modificarlo, tal y como lo hacen los hackers en los sistemas informáticos (Carballude, 2012).

Para Fundación Telefónica (2017), algunos términos asociados en relación al tema de biohacking, son los detallados a continuación:

- Transhumanismo: movimiento cultural e intelectual internacional, cuyo objetivo es transformar la condición humana, mediante el desarrollo de tecnologías que mejoren las capacidades físicas e intelectuales.
- Poshumanismo: es el objetivo final del transhumanismo, cuando el ser humano ya ha superado sus limitaciones físicas e intelectuales, logrando controlar tecnológicamente su propia evolución.
- Hombre aumentado: es el resultado de mejorar las capacidades de los seres humanos, mediante la tecnología, implantes, prótesis, etc.
- *Cyborg*: Asocian dispositivos electrónicos a su cuerpo para monitorizar o ejercer alguna acción sobre el organismo biológico, brindándoles sentidos que les permite una mayor percepción de los que percibe el resto de los seres humanos.

1.4.4 Tipos de dispositivos biohacking

La Fundación Cyborg fue creada en 2010, con la intención de ayudar a los humanos a convertirse en *cyborgs*, defender sus derechos y promover el arte tecnológico. Es una plataforma en línea, en la cual se desarrolla investigación y promoción de proyectos relacionados con la creación de nuevos sentidos y percepciones. Las investigaciones se enfocan en los Sentidos Artificiales (AS); es decir, la tecnología percibe los estímulos pero la inteligencia es creada por el ser humano, esta es la diferencia con la Inteligencia Artificial (IA), donde la inteligencia es creada por la máquina. (Cyborg Fundation, 2019).

La Ley de los Derechos de Cyborgs v1.0, fue desarrollada por la fundación junto con el investigador y activista electrónico de derechos civiles y libertades civiles Rich MacKinnon, en 2016. Los derechos se enmarcan en la defensa de las libertades civiles y la santidad de los cuerpos *cyborg*; engloba los siguientes aspectos: libertad de desmontaje, libertad de morfología, igualdad para mutantes, derecho a la soberanía corporal y derecho a la naturalización orgánica (Cyborg Fundation, 2019).

Existen varias personas que ya han realizado la integración de la tecnología con su cuerpo, incluso la han llevado a otro nivel y forman parte de la fundación como investigadores y ejecutores de proyectos, a continuación, los más conocidos:

1.4.4.1 Implante de prueba de sangre

Oliver (2017), afirma que los Investigadores del Instituto Federal de Tecnología de Suiza en Lausana (EPFL), desarrollaron un implante, que se usará como laboratorio personal de análisis de sangre. El dispositivo aún se encuentra en la fase de prototipo, se recarga a través de la piel del paciente mediante un parche externo, el cual recibe los datos del implante mediante bluethooth y la información obtenida puede ser analizada por un médico. En la figura 2 se puede verificar una fotografía del implante.

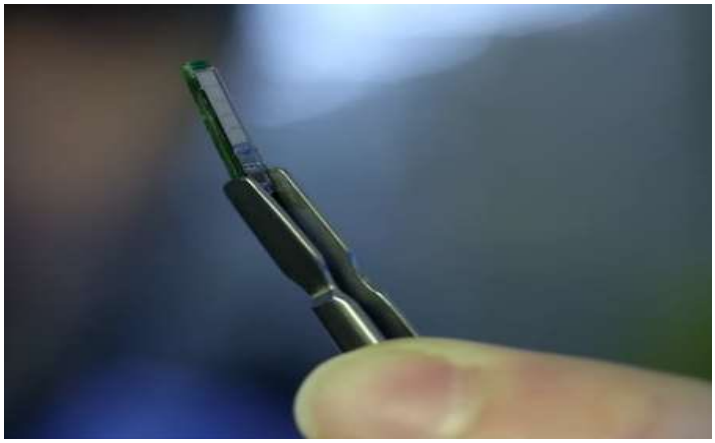


Figura 2. Implante de prueba de sangre. Fuente: Oliver, E. (2017). Recuperado de: https://es.digitaltrends.com/tendencias/ocho-increibles-biohacks/

1.4.4.2 Colores de audición

El artista Neil Harbisson nació completamente ciego a los colores, lo que hizo que se sometiera a un experimento llamado Antena Humana buscando extender su percepción del color. La antena se insertó de manera quirúrgica en su hueso occipital, actualmente los colores que experimenta resuenan a través de los huesos del cráneo, el hueso occipital tiene una ligera vibración que la

emite alrededor de su cabeza (Oliver, 2017). En la figura 3, se puede ver la imagen del artista junto a la antena.

Figura 3. Colores de audición. Fuente: Oliver, E. (2017). Recuperado de: https://es.digitaltrends.com/tendencias/ocho-increibles-biohacks/

1.4.4.3 Eyeborg

Es una creación del cineasta Rob Spence junto con el ocularista Phil Bowel, quienes con la ayuda de un equipo de ingenieros de RF Links, diseñaron una cámara protésica en miniatura con un transmisor de RF. Este proyecto consiste en grabar todo lo que el sujeto ve y transmitirlo en tiempo real a un computador (Oliver, 2017). En la Figura 4, se observa la cámara protésica adaptada a un ojo falso.

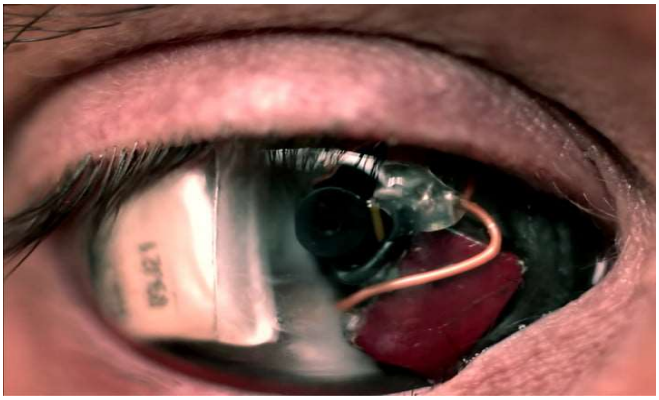


Figura 4. Prototipo de Eyeborg. Fuente: Oliver, E. (2017). Recuperado de: https://es.digitaltrends.com/tendencias/ocho-increibles-biohacks/

1.4.4.4 El sentido del norte

El North Sense from Cyborg Nest, es un modelo "exo-sense", se implanta en la superficie de la piel, como sugerencia en la parte superior del pecho. Su propósito es vibrar de forma ligera cuando el usuario se coloca de manera frontal hacia el norte magnético (Oliver, 2017). En la figura 5, se observa el implante en la ubicación sugerida.

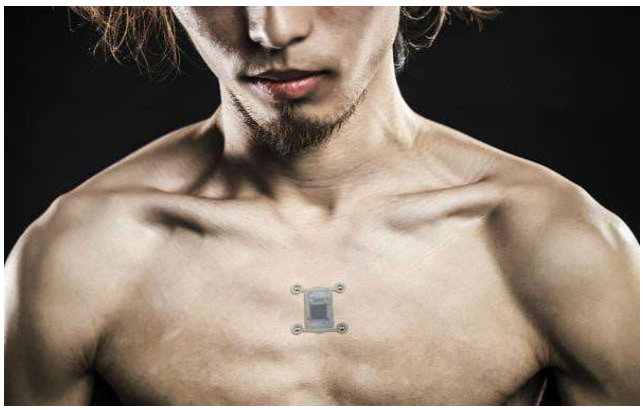


Figura 5. El sentido del norte. Fuente: Oliver, E (2017). Recuperado de: https://es.digitaltrends.com/tendencias/ocho-increibles-biohacks/

1.4.4.5 Biomagnetos

Son imanes que tienen forma de cilindros pequeños, permiten a los usuarios percibir su entorno de manera diferente. Se insertan debajo de la piel en la punta de los dedos o la palma de la mano, mejoran la percepción del sentido del tacto y son considerados como un sistema terapéutico (Oliver, 2017). En la figura 6, se muestra una imagen referencial de los biomagnetos.

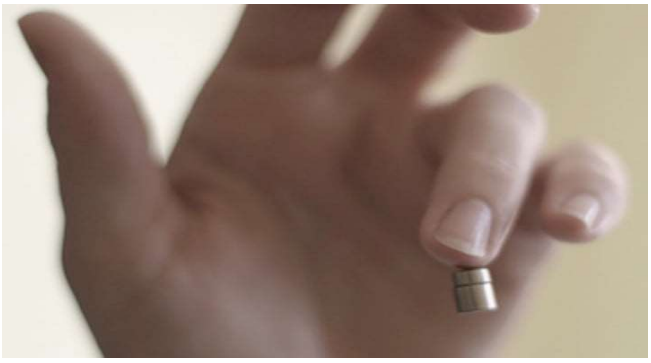


Figura 6. Biomagnetos. Fuente: Oliver, E. (2017). Recuperado de: https://es.digitaltrends.com/tendencias/ocho-increibles-biohacks/

1.4.4.6 Implante de Circadia

Tim Cannon, es considerado un *cyborg* que se implantó Circadia versión 1.0 en su brazo. Es un chip de computadora, que monitorea sus signos vitales y los transmite en tiempo real, a un dispositivo con sistema operativo Android (Oliver, 2017). En la figura 7, se muestra el implante de Circadia versión 1.0.

Figura 7. Implante de Circadia. Fuente: Oliver, E (2017). Recuperado de: https://es.digitaltrends.com/tendencias/ocho-increibles-biohacks/

1.4.4.7 Bioluminiscencia

Es un proyecto creado por Grind House Wetware, es un implante de chip llamado Northstar V1, tiene el tamaño de una moneda y retroiluminación LED. El chip se implanta en las manos, se diseñó para iluminar los tatuajes desde el interior de la piel. Su funcionalidad es limitada (Oliver, 2017). En la figura 8, se puede observar el chip.

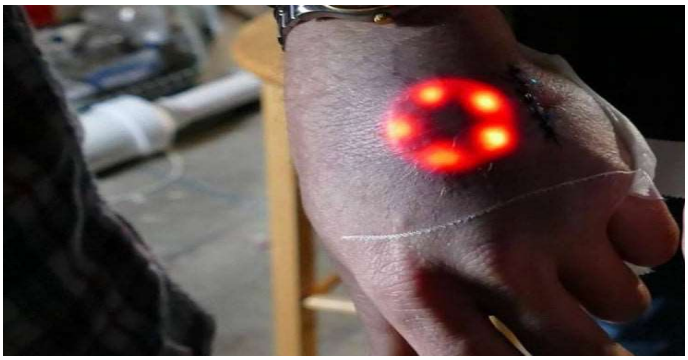


Figura 8. Chip Northstar V1 para Bioluminiscencia. Fuente: Oliver, E. (2017). Recuperado de: https://es.digitaltrends.com/tendencias/ocho-increibles-biohacks/

1.4.4.8 Implantes RFID y NFC

Esta tecnología es una de las modificaciones *cyborg* más funcionales. Son chips que se pueden usar para varios propósitos de identificación, reemplazando claves y contraseñas, permitiendo desbloquear puertas, iniciar vehículos e incluso iniciar sesión en computadoras y dispositivos inteligentes. Además, se pueden usar como almacenamiento de información (Oliver, 2017). En la figura 9, se observa un implante de microchip en uno de los dedos de la mano.

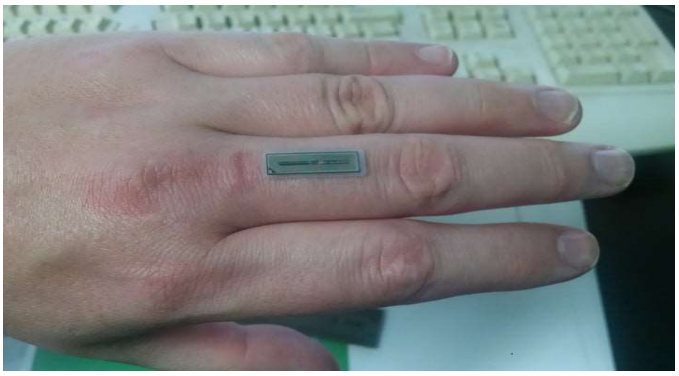


Figura 9. Implantes RFID y NFC. Fuente: Oliver, E. (2017). Recuperado de: https://es.digitaltrends.com/tendencias/ocho-increibles-biohacks/

1.4.5 Tecnología RFID

El significado de su sigla es identificación por radio frecuencia, es un sistema de comunicación inalámbrica, formado por lectores y etiquetas o también llamados transpondedores, donde uno emite señales de radio y el otro responde en función de la señal recibida, logrando su identificación (Ramírez, 2017).

1.4.5.1 Funcionamiento de la tecnología RFID

Tanto los lectores como los transpondedores, están formados por microchips y antenas RF. Cada microchip tiene grabado un número de identificación único (UID), algunos disponen de una pequeña memoria para guardar datos, que los lectores son capaces de leer y escribir. La forma y característica de la antena RF, depende de la banda de frecuencia en la que funcionen (Casero,

2013). La tabla 1, muestra las bandas de frecuencia utilizadas por los diferentes sistemas de RFID, que actualmente están presentes en el mercado.

Tabla 1
Bandas de frecuencia utilizadas en RFID.

Banda de frecuencias	Descripción	Rango
125 kHz	LF (Baja Frecuencia)	Hasta 50 cm.
13,56 MHz	HF (Alta Frecuencia)	De 8 cm.
400 MHz – 1.000 MHz	UHF (Ultra Alta Frecuencia)	De 3 a 10 m.
2,45 GHz – 5,4 GHz	Microondas	Más de 10 m.

Elaborado por el autor. Datos obtenidos de Játiva (2016). Estudio de la tecnología de identificación por radiofrecuencia (RFID), y su convergencia con OiT. Universidad catolica de Santiago de Guayaquil, Guayaquil.

1.4.5.2 Clasificación de la tecnología RFID

Hay tres tipos de etiquetas RFID según el tipo de alimentación: activas, semipasivas y pasivas. Las etiquetas pasivas, se alimentan al estar dentro del campo de cobertura del lector, reciben energía de la antena. Las etiquetas activas, utilizan alimentación propia de una pequeña batería; y las etiquetas semipasivas, tienen una fuente de alimentación propia, usada para alimentar el microchip y no para transmitir una señal (Casero, 2013).

Otros tipos de clasificaciones de los sistemas RFID son: en relación a su capacidad, a su frecuencia y a su protocolo de comunicación. En relación a su capacidad, puede ser de solo lectura, de una escritura y múltiples lecturas, y, de lectura/escritura. En relación a la frecuencia, puede ser de baja frecuencia, alta frecuencia, ultra alta frecuencia y frecuencia de microondas. En relación al protocolo de comunicación, puede ser dúplex, half dúplex, full dúplex y secuencial (Játiva, 2016).

1.4.5.3 Estándares y Normativas de RFID

Los estándares de RFID, describen las características de hardware y software que deben tener un sistema. En cuanto a hardware, se refiere a sus dimensiones, localizaciones de las aéreas de interrogación y señales electrónicas. En cuanto a software, establece procedimientos de reset,

protocolo de transmisión de datos, formato y semántica de los datos, y, certificación de interoperabilidad (FQ Ingeniería Electrónica, 2014).

Coexisten diversas organizaciones que han determinado los estándares para la tecnología RFID, entre ellas están: ISO (International Organization for Standardization), IEC (International Electrotechnical Commission), ASTM (American Society for Testing and Materials) y EPCglobal (Asociación entre EAN International y GS1 Uniform Code Council). Los estándares regulan el desarrollo de la tecnología RFID, permitiendo que los fabricantes realicen equipos compatibles y se puedan conectar entre ellos. (Ver anexo 1).

1.4.6 Tecnología NFC

Sus siglas significan conectividad de campo cercano, se deriva de RFID, trabaja sobre la frecuencia de 13,56MHz. La transferencia de los datos entre el transpondedor y el lector se realiza a través de señales electromagnéticas de manera automática, al estar en el área de cobertura que es de uno a dos centímetros (Montero, 2017).

1.4.6.1 Funcionamiento de NFC

Su funcionamiento es idéntico a RFID, con microchips alimentados de forma activa y pasiva. El dispositivo lector tiene un microchip activo y el transpondedor un microchip pasivo. El lector solicita información al transpondedor, el cual responde a la petición deseada, siempre y cuando exista la confirmación del usuario, que es la acción de acercar el transpondedor a un lector con su consentimiento.

1.4.6.2 Tipos de comunicación de NFC

El modo de comunicación que tienen los dispositivos con tecnología NFC puede ser de tres formas: modo P2P (*peer to peer*), modo de lectura/escritura, y modo emulación de tarjeta o transpondedor. (Montero, 2017)

- El modo *peer to peer*: permite la comunicación entre dos dispositivos NFC de manera directa, su principal aplicación es el intercambio de archivos. Se basa en la norma ISO/ IEC18092.
- Modo de lectura y Escritura: permite a los dispositivos NFC leer y escribir datos en los transpondedores. Se basa en el estándar ISO / IEC 14443.
- Emulación de transpondedor: permite a un dispositivo NFC funcionar como tarjeta sin contacto y posteriormente poder ser leído por un dispositivo lector. Se basa en la norma ISO / IEC 14443 e ISO / IEC 15693.

1.4.6.3 Arquitectura de NFC

La tecnología NFC requiere de cuatro elementos para comunicarse, de un transpondedor, de un lector, de antenas y software. El transpondedor almacena información en la memoria del microchip. El lector, lee esa información. Las antenas transmiten la información; y el software, realizar las acciones requeridas por el usuario.

La comunicación entre los elementos se realiza mediante un proceso de cinco etapas. La primera es el descubrimiento, los dispositivos envían señales para comunicar su presencia. La segunda es la autenticación, verifican si existe algún tipo de cifrado antes del intercambio de información. La tercera es la negociación, se definen los parámetros y la velocidad con que se transmite la información. La cuarta es la transferencia, se intercambia la información; y la última es el reconocimiento, el receptor confirma que recibió los datos (Villavicencio & Mendoza, 2015).

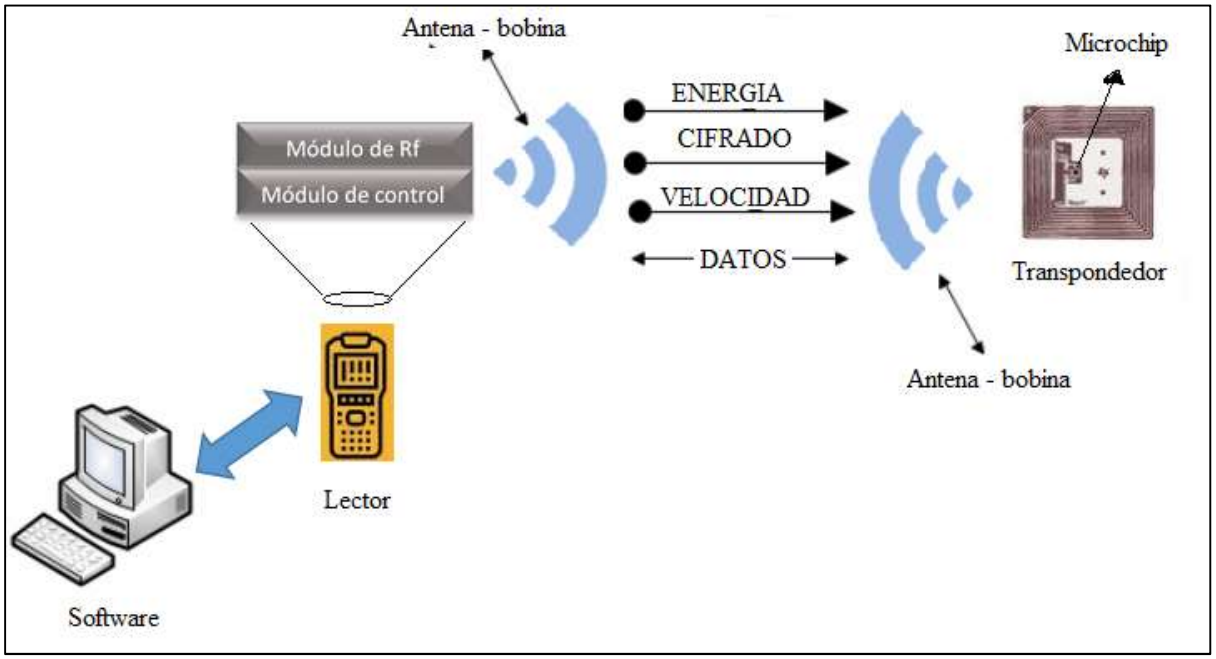


Figura 10. Componente de la arquitectura de NFC. Fuente: autor. Datos obtenidos de: Villavicencio, W; Mendoza, E. (2015), Desarrollo de una aplicación informática utilizando la tecnología NFC para *Smartphone* con sistema Android que permita la selección y facturación de un menú en un restaurante. Universidad Politécnica Salesiana. Guayaquil.

1.4.6.4 Aplicaciones de la tecnología NFC

Según Montero (2017), la tecnología NFC se aplica en varios ámbitos y muchas de ellas se usan diariamente, las principales aplicaciones se describen a continuación:

- Identificación: permite la identificación de un usuario en determinados casos. Se aplica en transporte o para conciertos, tarjetas de acceso restringido o DNI electrónico.
- Recogida/intercambio de datos: permite descargar información de un determinado producto o servicio, de forma similar a la información que podemos obtener a través de un código QR. También es posible compartir información entre usuarios, es el caso de Smartphone con tecnología NFC
- Transacciones comerciales: permite el pago de consumos, puede ser utilizado mediante el pago con móvil o con tarjetas sin contacto (*Contactless*), el cobro está asociado a una cuenta de banco.
- Perfiles en *Smartphone* con NFC: permite configurar desde el dispositivo móvil las funciones o tareas deseadas en un transpondedor, que, al ser acercado al celular, se

ejecutan. Algunos ejemplos son: bajarle el brillo de la pantalla, activar alarma, realizar llamadas, etc.

- Controles de acceso: permitir a las personas el acceso a distintas ubicaciones a las que está autorizado. El administrador del sistema será el encargado de este control.
- Activación de dispositivos electrónicos: permite la activación de ciertos dispositivos como: ordenadores portátiles, vehículos, teléfonos inteligentes, *Tablets*, etc.
- Transporte: algunas empresas permiten que sus usuarios hagan uso de tarjetas NFC para el ingreso a sus flotas. Inclusive compañías aéreas dan la posibilidad de hacer *check-in* mediante teléfonos con NFC.

Algunas de estas aplicaciones no están demasiado extendidas, existen países en los cuales se han desarrollado más que otros, sobre todo en los países europeos, Según Pozo (2018) en ciudades como Madrid o Valencia, la tarjeta de ingreso al metro es con tecnología NFC, inclusive en Málaga se usa el teléfono móvil para pagar el autobús. Con los avances tecnológicos se le augura un futuro muy prometedor a esta tecnología.

1.4.7 Implantes de Microchips con tecnología NFC para personas

El implante también llamado transpondedor, puede ser usado para ingresar a diversos lugares en vez de llaves, o incluso, activar dispositivos electrónicos. Además, posee una memoria limitada por su capacidad, que puede almacenar algunos datos, como números telefónicos, correos electrónicos, enlaces, contraseñas, claves wifi, entre otros. El implante se incrusta bajo la piel, posee un microchip pasivo que se energiza al ser acercado a un lector, la distancia para su activación es pequeña, entre uno a dos centímetros (Bermejo, 2017).

1.4.7.1 Estructura del implante o transpondedor

Según los autores Narayana, Sukruthi y Raj, (2012), el transpondedor consta de cuatro partes: un microchip, una bobina de antena, un condensador y una capsula de vidrio. En la figura 11, se detallan los componentes del implante.

- Microchip: almacena la información en la memoria, entre esta información está un UID de 7 bytes, que es un número de identificación único, otorgado por la empresa fabricante, una vez codificado el número es imposible alterarlo. Esto se realiza antes del ensamblaje.
- Bobina de la antena: Es una bobina simple de cable de cobre alrededor de un núcleo de ferrita o hierro. Esta pequeña antena circular, recibe y envía señales al lector.
- Condensador de sintonía: almacena la pequeña carga eléctrica requerida para activar el transpondedor. El capacitor se sintoniza a la misma frecuencia que el lector.
- Cápsula de vidrio: realizada con material biocompatible, su función es proteger la electrónica de los componentes, de los fluidos corporales. En uno de sus extremos se coloca una funda de material de polipropileno (elemento similar al látex), que permite una colocación permanente del transpondedor en el tejido corporal.

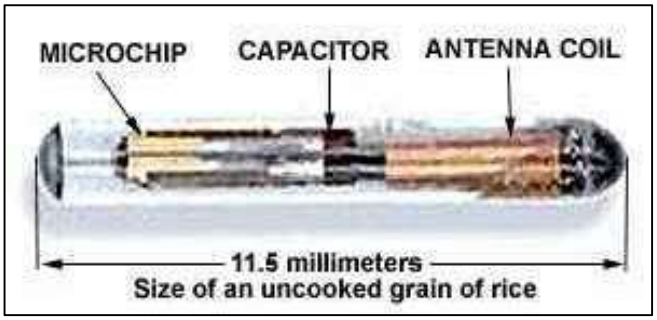


Figura 11. Componentes del implante. Fuente: Narayana et al., (2012) Recuperado de: https://pdfs.semanticscholar.org/7a0f/dd48e50b3bfd53f8673defb144cfe2f8cf66.pdf

1.4.7.2 Implantación bajo la piel

La ubicación del implante en el cuerpo humano, depende del usuario, por lo general se realiza en la mano. De manera subcutánea, debe estar en la dermis, su colocación se realiza mediante una aguja hipodérmica, teniendo en cuenta que la funda de polipropileno, ingrese primero en el organismo, para evitar resistencia. En la figura 12, se observa la manera en la que se debe implantar el transpondedor bajo la piel humana.

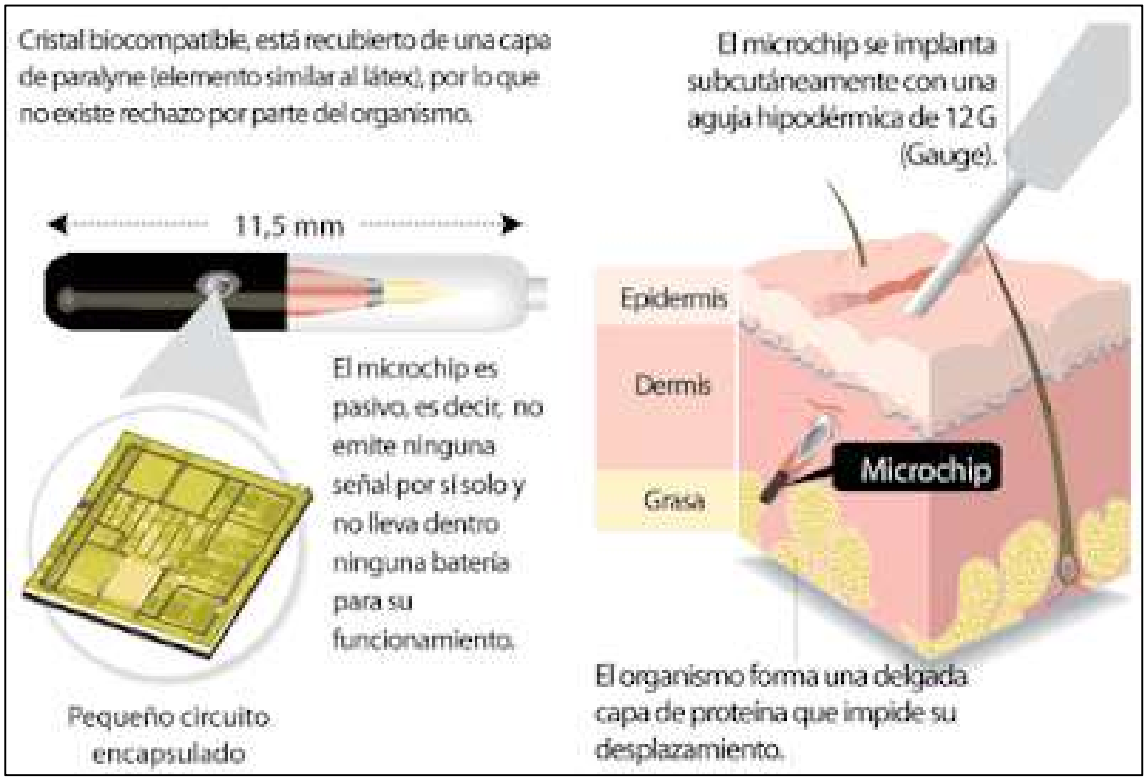


Figura 12. Implantación del transpondedor. Fuente: Ali (2014) Recuperado de: https://www.slideshare.net/mustahidali90/biochips-31961817

CAPITULO 2

ESTADO DEL ARTE

Ethical hacking, es una disciplina que evoluciona constantemente, debido a los avances tecnológicos, cada vez se desarrollan más dispositivos con la finalidad de mejorar la calidad de vida de las personas. Estos avances conllevan a considerar un tema importante, como lo es la seguridad física y lógica de los sistemas informáticos, existen expertos en seguridad que explotan vulnerabilidades existentes en un sistema de interés, mediante técnica de intrusión, una vez identificadas son informadas a las organizaciones, para que tomen las medidas correctivas necesarias.

Haciendo buen uso de la Internet, se encuentran investigaciones de expertos que aplican diversas técnicas de *Ethical hacking*, a tecnologías de transmisión de datos, como: NFC, RFID, WiFi, Bluetooth, etc. Considerando el objeto de estudio de este proyecto, se presentan los trabajos más relevantes en relación a la tecnología NFC.

2.1 Ataques a dispositivos con tecnología NFC

En una conferencia, el investigador Lee (2012), explicó un ataque a tarjetas de crédito, mediante una técnica denominada relay attacks. El ataque busca extraer los datos de una tarjeta inteligente, usando un puente entre la tarjeta y un sistema de pago en tiempo real. El experto demostró este ataque, usando dos teléfonos celulares con sistema operativo Android. El primer teléfono, está cerca de la tarjeta NFC, actuando como lector; y el segundo teléfono, está cerca del terminal, actuando como tarjeta inteligente. En la Figura 13, se muestra una representación gráfica del ataque.

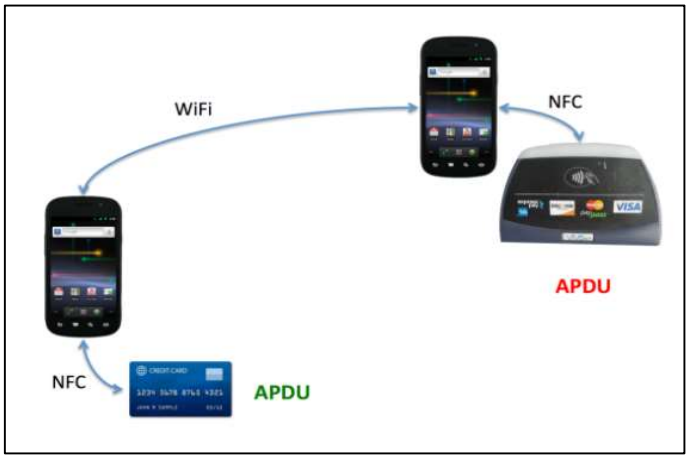


Figura 13. Relay attack a tarjetas de crédito. Fuente: Lee (2012) Recuperado de: https://es.scribd.com/document/210071123/Defcon-20-Lee-Nfc-Hacking

Los autores Shan y Yuan (2017), presentaron un ataque que es una versión mejorada del anterior, llamada "Man in the NFC", usa dos tarjetas especiales con tecnología SDR (Software Defined-Radio) en vez de celulares, establece una conexión dedicada, lo que incrementa la velocidad de comunicación, de igual manera trabaja sobre una red WiFi.

Este ataque busca burlar la distancia que debe existir entre la tarjeta inteligente y el terminal; además, este ataque se puede efectuar no solo en tarjetas bancarias, sino también, en tarjetas de acceso, tarjetas de microbús o cualquier otro tipo de tarjeta que use la tecnología NFC.

Google Pay es la nueva versión de Android Pay, es una aplicación de pago a través de *Smartphone* con tecnología NFC. Según Mendoza (2018), existe una vulnerabilidad que puede ser aprovechada mediante una técnica denominada replay attack. Cuando una persona realiza una transacción NFC con Google Pay, un atacante puede interceptar la transacción, manipularla y almacenarla, para reproducirla después con otro dispositivo, realizando un pago, con el dinero del cliente original de Google Pay. En la figura 14, se muestra el esquema del ataque.

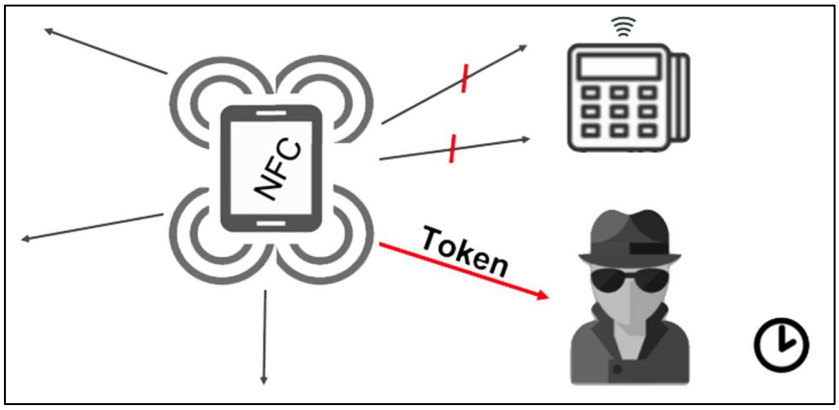


Figura 14. Replay attack a Google Pay. Fuente: Mendoza (2018). Recuperado de: https://tpx.mx/blog/2018/google-pay-replay-attack.html

Desde 2012, se ha popularizado en los vehículos un sistema de llave inteligente. Los autores Kim, Lee, Kim, y Kim, (2013), desarrollaron un ataque sobre una vulnerabilidad es estos sistemas, mediante la técnica relay attack. El ataque requiere un mínimo de dos personas. La primera persona, tendrá un dispositivo que actúa como un escáner / amplificador, se ubicará junto al automóvil; y la segunda persona, con otro dispositivo que actuará como un receptor / transmisor, se debe ubicar cerca de la persona que posee la llave inteligente. En la figura 1, se muestra la idea de cómo ejecutar este ataque.

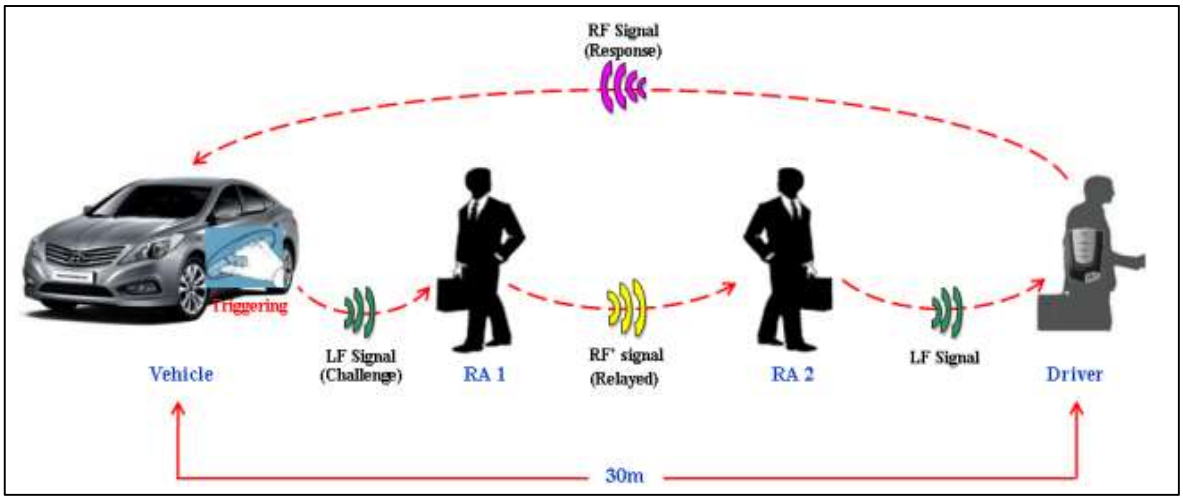


Figura 15. Relay attack a vehículos. Fuente: Kim, G. et al., (2013). Recuperado de: https://www.researchgate.net/publication/272654782_Vehicle_Relay_Attack_Avoidance_Methods_Using_RF_Signal_Strength

Todas las marcas de automóviles equipadas con un sistema de llave inteligente, están expuestas a robos. La señal se copia en lugar de ser descifrada, el objetivo del ataque es burlar la pequeña distancia que debe haber entre el automóvil y la llave, con este ataque se logra que esa distancia aumente considerablemente. El ataque no solo permite abrir la puerta del automóvil sino también arrancar el motor.

El autor Brewsther (2015) afirma que el investigador en seguridad digital Seth Wahle, desarrolló una manera en la cual se puede hackear teléfonos inteligentes con sistema operativo Android vía NFC. Este ataque permite tener el control del dispositivo, a través de la instalación de un malware, transmitido desde el microchip implantado en la mano del atacante al dispositivo, permitiendo su control de manera remota. Según Whale, esta técnica es indetectable, basta que el hacker acerque su mano a un aparato que esté con el NFC habilitado.

2.2 Visión General

Existe un número considerable de investigaciones y trabajos sobre *Ethical hacking* aplicado a la tecnología NFC; sin embargo, no se ha profundizado en investigaciones respecto al tema de vulnerabilidades en implantes de microchips para humanos. Además, en Ecuador el tema de sistemas de biohacking no es muy conocido, menos aún el tema de implantes de microchips.

CAPITULO 3

METODOLOGÍA PARA EL ANÁLISIS DE IMPLANTES DE MICROCHIP PARA HUMANOS CON TECNOLOGÍA NFC.

3.1 Dispositivos requeridos

Los componentes requeridos para la realización de este proyecto, son los establecidos en la arquitectura NFC, se necesita un transpondedor o implante, un lector, software dedicado y por último, aplicaciones y herramientas especializadas que permitan implementar la técnica de clonación.

3.1.1 Implante de microchip de la serie xNT

El transpondedor está formado por cuatro componentes: el microchip, el condensador, la antena y la capsula de vidrio. El microchip es fabricado por la empresa NXP semiconductor y los demás componentes por la empresa Danguerous Thing, quienes ensamblan todo en una capsula de vidrio cilíndrica.

La empresa NXP semiconductor, fabrica varios tipos de microchips denominados NTAG (Ver anexo 2), compatibles con todos los dispositivos con tecnología NFC (teléfonos, *Tablet*, cámaras, relojes y anillos). El transpondedor NFC de la serie xNT, está formado por un microchip NTAG216, regularizado bajo el estándar ISO14443 tipo A y compatible con todos los dispositivos NFC tipo 2 (Company Public, 2015). (Ver anexo 3).

Para la implantación el fabricante otorga un kit de instalación, que cuenta con materiales esterilizados. En la figura 16, se puede ver el kit de instalación y el implante xNT. En la tabla 2, se describe las especificaciones mecánicas y eléctricas del transpondedor.

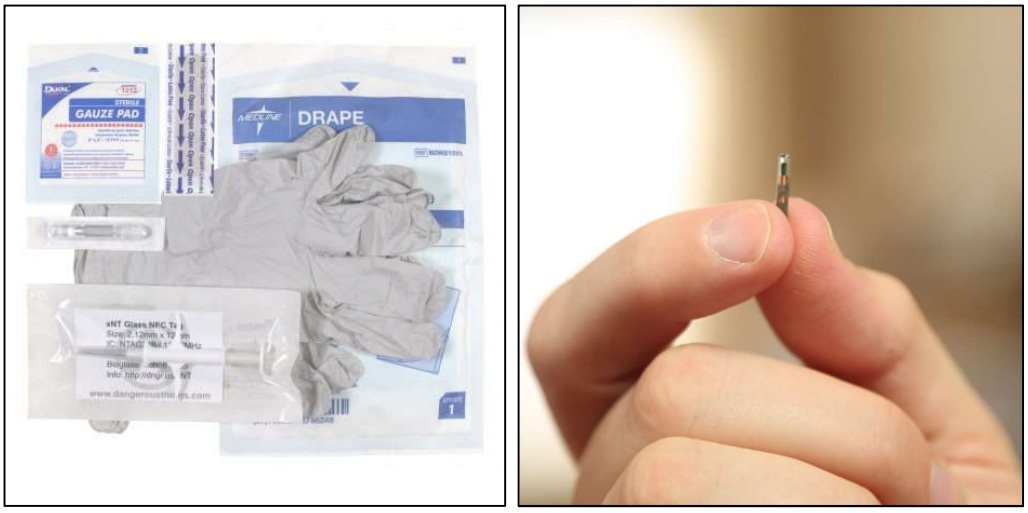


Figura 16. Kit de instalación y Transpondedor xNT. Fuente: Dangerous Things, (2019) Recuperado de: https://dangerousthings.com/product/xnt/

Tabla 2
Características del chip NTAG216.

Característica	Descripción
Energía	Suministro sin contacto y por acercamiento
Transferencia de datos	Velocidad de transmisión de 106 kbit / s
Seguridad	UID programado de 7 bytes a cargo de XNP semiconductor
	Función programable de bloqueo para solo lectura
	Protección de contraseña para operaciones de memoria no autorizadas con límite opcional de intentos fallidos
Frecuencia	13.56 MHz, bajo el estándar ISO/IEC 14443 Tipo A
Distancia	Distancia de funcionamiento entre 1 y 2 centímetros (dependiendo de parámetros como el campo fuerza y geometría de la antena)
Memoria	EEPROM, 888 bytes de escritura y lectura
	Tiempo de retención de datos de 10 años

Elaborado por el autor. Datos obtenidos de Company Public (2015), NTAG213/215/216. NFC Forum Type 2 Tag compliant IC with 144/504/888 bytes. NXP Semiconductors N.V. Rev. 3.2 — 2.

3.1.2 Lector NFC

Para el lector NFC se utilizó dos tarjetas de circuitos integrados. El primero, el módulo de lectura/escritura PN532; y el segundo, el módulo Arduino UNO.

3.1.2.1 Módulo PN532 de Lectura/escritura NFC

Es un módulo fabricado por la empresa Elechouse, la última versión lanzada es la versión 3, opera con la tecnología NFC en la frecuencia de 13.56 MHz, se basa en el estándar ISO/IEC 14443 Tipo A, su diseño incluye la antena en la misma placa (Elechouse, 2015).

Para el desarrollo de este proyecto se ha decidido usar este módulo debido a la compatibilidad con el transpondedor xNT. En la figura 6, se puede ver de manera gráfica el módulo. En la tabla 3, se detallan sus características principales.

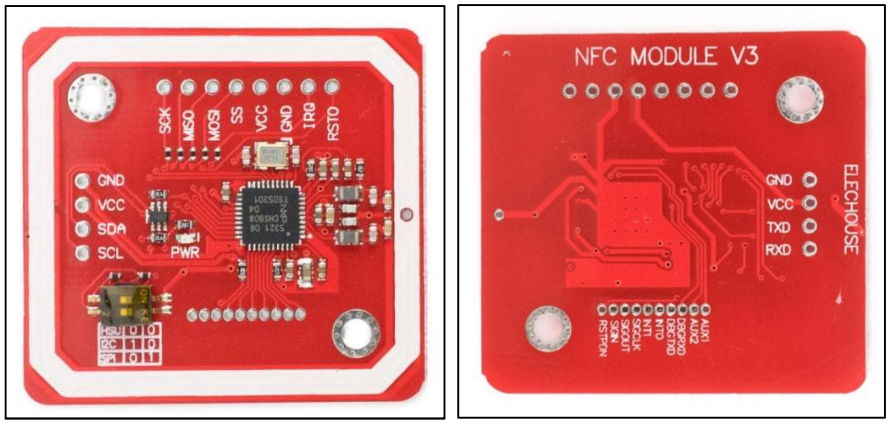


Figura 17. Módulo lectura / escritura PN532. Fuente: autor

Tabla 3
Características del módulo PN532.

Característica	Descripción
Energía	Soporta entre 3,3V y 5V
Comunicación	Puede ser mediante SPI, I2C o HSU (High Speed UART)
Procesador	80C51 con 40 KB ROM y 1 KB RAM
Modo de operación	ISO/IEC 14443A y B /MIFARE Lector/Grabador.
(Marcas y estándares	ISO/IEC 14443A/MIFARE Classic 1K y MIFARE Classic 4K
soportados)	FeliCa Lector/Grabador y FeliCa Card emulación.
Transferencia de datos	Para lectura hasta 212 kbits/s y para escritura hasta 424kbts/s.
Distancia	De 50mm para lectura y escritura, y 100mm para emulación

Elaborado por el autor. Datos obtenidos de Elechouse (2015). PN532 NFC RFID Module User Guide. Initial versión.

La comunicación entre el módulo PN532 y el módulo Arduino UNO, es mediante HSU, SPI o I2C. En la tabla 4, se muestra las características principales de cada uno.

Tabla 4.
Características de los protocolos de comunicación

	HSU	**SPI**	**I2C**
Designación de Pines	• TxD: Transmisión de datos. • RxD: Recepción de datos.	• SCLK: Reloj Serial • MOSI: output maestro, input esclavo. • MISO: input esclavo, output maestro. • SS: Selector de esclavo.	• SDA: Datos • SCL: Reloj Serial
V. Tx Datos	230Kb/s a 460kb/s	10Mb/s a 20Mb/s	3.4Mb/s a 1Mb/s
Comunicación	Asíncrona	Síncrona	Síncrona
Ventajas	Conexión de cableado rápido entre dos dispositivos	Comunicación full duplex Permite mayor velocidad de transmisión.	Solo necesita dos cables para la comunicación. Tiene control de flujo.
Desventajas	Al ser asíncrono, existe mayor riesgo de lecturas erróneas.	Añadir un dispositivo requiere una conexión adicional.	Complejidad al aumentar maestros y esclavos. Comunicación half duplex

Elaborado por el autor. Datos obtenidos de Valencia, N. (2018). Comparación de los tres protocolos más importantes en microcontroladores, UART, SPI y I2C. RF Wireless World.

El protocolo de comunicación usado para este proyecto es el SPI, debido a las ventajas que tienen en relación a los demás protocolos. Es síncrono, su comunicación es full dúplex y su velocidad de comunicación es mayor, lo cual es importante debido a que se requieren lecturas rápidas y precisas del implante xNT.

La comunicación SPI en el módulo PN532, se realiza mediante los pines SCK, MOSI, SS y MISO; y mediante la configuración de los estados lógicos del switch, localizado en la parte inferior del módulo. En la Figura 18, se muestra los estados lógicos que deben ser configurados para SPI.

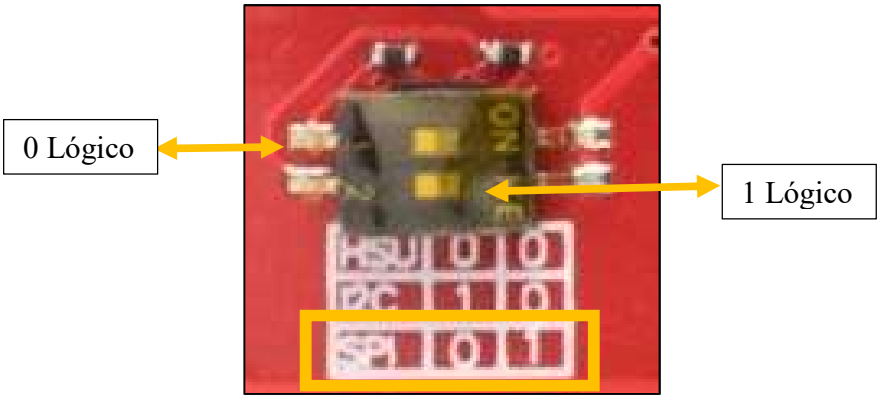


Figura 18. Comunicación SPI en el módulo PN532. Fuente: autor

3.1.2.2 Módulo Arduino UNO

Es un circuito integrado que tiene un microcontrolador basado en ATmega328P, se programa para detectar y controlar objetos en el mundo físico. Es desarrollado por Arduino.cc, la última versión de estas placas es Arduino UNO rev3.

El módulo tiene pines analógicos, un cristal de cuarzo de 16 MHz, una conexión USB, un conector de alimentación, un encabezado ICSP, un botón de reinicio, y por último, pines de entrada / salida digital, que permiten PWM. (Arduino, 2019). En la figura 19, se puede observar la placa Arduino UNO. En la tabla 5, se detalla las especificaciones técnicas.

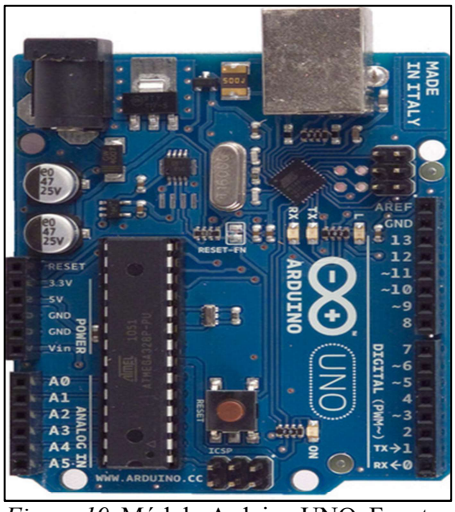


Figura 19. Módulo Arduino UNO. Fuente: autor

Tabla 5.
Especificaciones técnicas del módulo Arduino UNO.

Especificación	Descripción
Microcontrolador	Microchip ATmega328P
Voltaje de funcionamiento	5 voltios
Voltaje de entrada	7 a 20 voltios
Comunicación	Admite HSU, I2C y SPI
Memoria Flash	32KB, 0.5KB utilizados por el gestor de arranque
SRAM y EEPROM	2 KB y 1KB respectivamente
Velocidad del reloj	16 MHz

Elaborado por el autor. Datos obtenidos de Arduino (2019). Arduino UNO Rev3.

La comunicación SPI en el módulo Arduino UNO, se realiza mediante la conexión a los pines 2, 3, 4 y 5 de las entradas /salidas digitales.

3.1.3 Software

Los software utilizados en este proyecto, han sido instalados bajo los sistemas operativos Windows y Android. Cada software cumple una función en específico.

3.1.3.1 Plataforma IDE Arduino para Windows

El módulo Arduino está basado en un microcontrolador que puede grabar instrucciones, escritas mediante un lenguaje de programación llamado JAVA a través del entorno de programación IDE (entorno de desarrollo integrado).

La plataforma IDE, es de software libre y de código abierto, accesible por cualquiera persona para que pueda utilizarlo y modificarlo. La licencia del software es de libre distribución y su código fuente es de acceso público. Se instala en un computador y se conecta con el módulo Arduino UNO median USB, permitiendo cargar los scripts en el módulo (Arduino, 2019). El IDE se descarga de la página oficial, la versión actual es 1.8.9. En la figura 20, se muestra el entorno IDE.

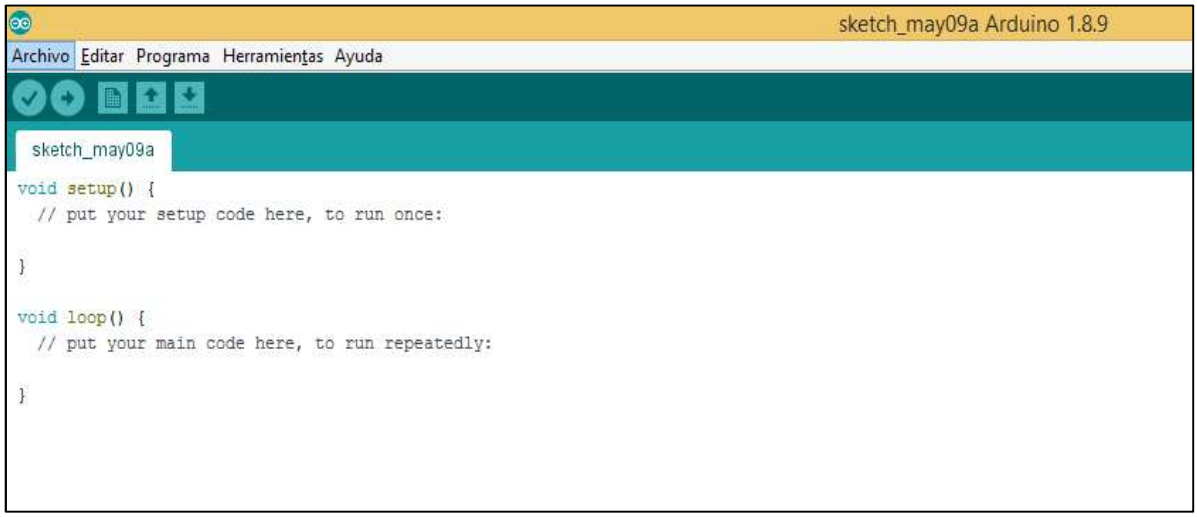


Figura 20. Entorno IDE de Arduino para desarrollar scripts. Fuente: autor

Adicional a la instalación del software, se debe instalar varias librerías que usa el módulo PN532 para leer / escribir tarjetas y comunicarse con Arduino UNO. Estas librerías son: adafruit PN532 y PN532. La instalación de estas librerías permite una interacción correcta entre los módulos, logrando hacer lecturas precisas del transpondedor xNT. (Github, 2018).

3.1.3.2 Aplicación ArduinoDroid para Android

Es una aplicación para sistemas operativos Android, permite trabajar con la plataforma IDE mediante un *Smartphone*, se debe instalar las librerías requeridas por el módulo PN532 para leer / escribir tarjetas y comunicarse con Arduino UNO.

La conexión del *Smartphone* con el módulo Arduino y PN532 requiere de un cable OTG. Esta aplicación se puede usar en teléfonos inteligentes que no tienen la tecnología NFC o para aprovechar las lecturas rápidas y precisas que se puede llegar a obtener con estas placas. En la Figura 21, se observa el entorno de la aplicación.

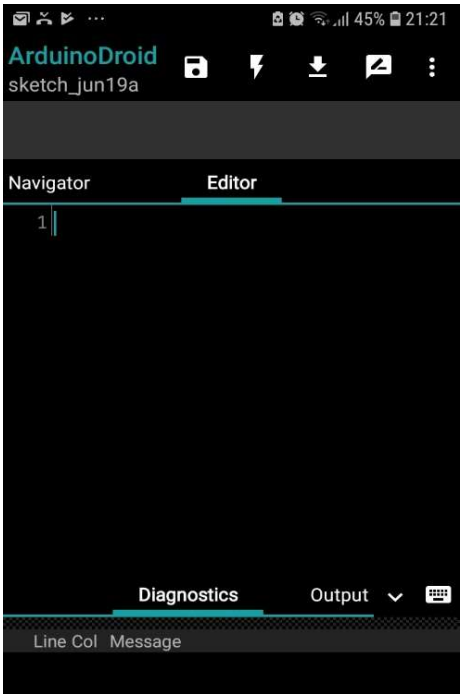


Figura 21. Entorno de la aplicación ArduinoDroid. Fuente: autor

3.1.3.3 Aplicaciones para Smartphone con Tecnología NFC

Existen aplicaciones que pueden instalarse en teléfonos inteligentes con tecnología NFC, que permiten leer y escribir tarjetas basadas en el estándar ISO/IEC 14443A, compatibles con el transpondedor xNT. Las aplicaciones utilizadas en este proyector son: NFC Tools y NFC Tasks. Se pueden instalar mediante Play Store en celulares con sistema Android. El rango de lectura y escritura de cada aplicación depende del fabricante del *Smartphone*.

A. NFC Tools

Es una aplicación que permite leer, escribir información, ejecutar protecciones de seguridad sobre el transpondedor y por último, programar tareas, con el fin de automatizar acciones repetitivas en los teléfonos inteligentes. En la figura 22, se puede observar las ventanas de la aplicación.

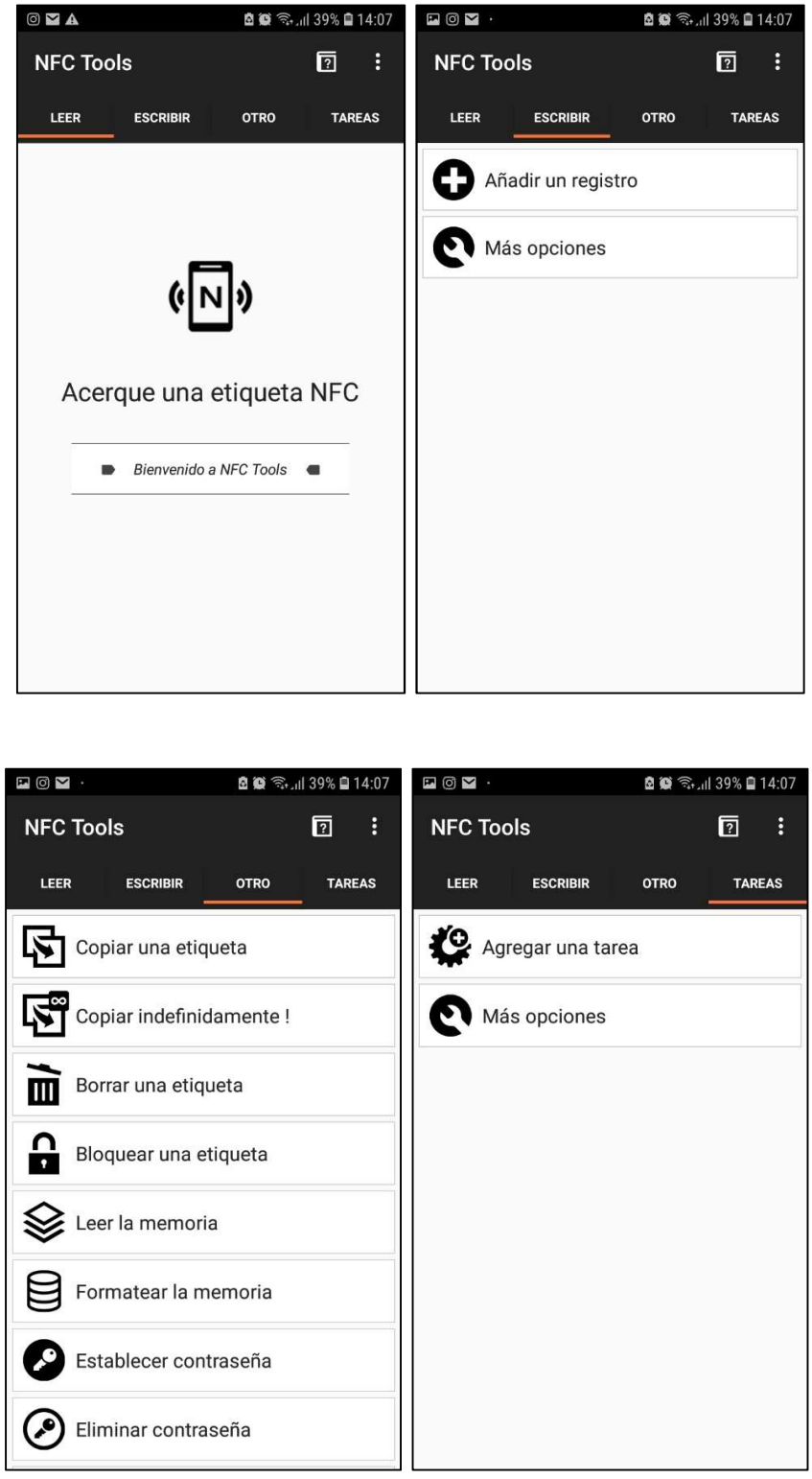


Figura 22. Ventanas de la aplicación NFC Tools. Fuente: autor

B. NFC Tasks

Es una aplicación complementaria a NFC Tools, lee el transpondedor xNT y ejecuta las tareas almacenadas en la memoria de forma automática. En la figura 23, se puede observar las ventanas de la aplicación.

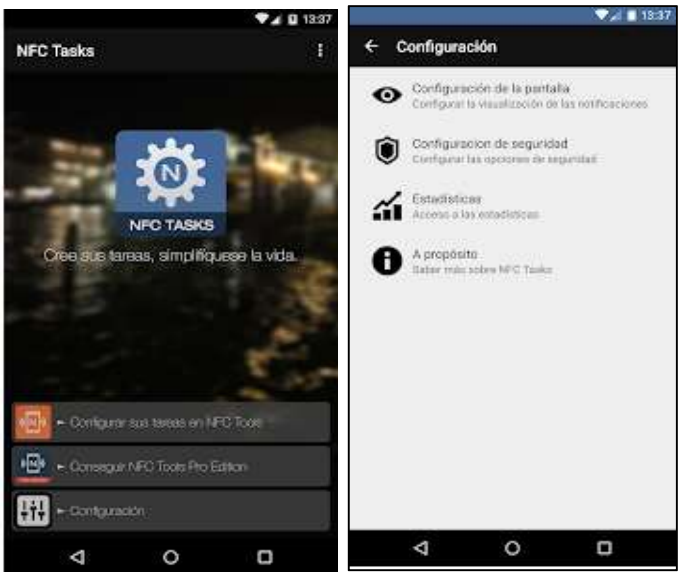


Figura 23. Ventanas de la aplicación NFC Tasks. Fuente: autor

3.1.4 Módulo Chameleon Mini (Tarjeta de clonación)

Es un circuito integrado que puede emular y clonar tarjetas sin contacto, detectar contraseñas de las tarjetas Mifare classic 1k, cargar y comparar archivos DUMP para programación de transpondedores y realiza ataques de UID sniffing, Es desarrollado por la empresa Kasper & Oswald, es portátil, de código abierto y se usa para el análisis de seguridad NFC. (Hacker Warehouse, 2019)

Existes varias versiones de estos dispositivos, la utilizada en este proyecto es la versión RevE Rebooted, permite grabar hasta 8 tarjetas virtuales en comparación a sus otras versiones que graban solo una, teniendo una mayor versatilidad. Contiene un batería que puede hacerlo funcionar de manera independiente. En la figura 24, se muestra una imagen del dispositivo. En la tabla 6, se describen las características de la tarjeta.

Figura 24. Tarjeta Chameleon Mini. Fuente: autor

Tabla 6.
Características de la tarjeta Chameleon Mini

Especificación	Descripción
Modelo	RDV2.0
Frecuencia	13.56 MHz
Compatibilidad ISO	ISO 14443 e ISO 15693
Microcontrolador	ATXmega32a4u
Voltaje de funcionamiento	2,2 – 3,5 V.
Modo de emulación	MIFARE Classic® 1K (UID de 4 bits y 7 bits)
	MIFARE Classic®4K (UID de 4 bits y 7 bits)
	MIFARE Ultralight® (UID de 7 bytes)
	Capacidad de emular (con firmware personalizado)
	MIFARE NTAG®, ICODE, MIFARE DESFire®
UID sniff	Detecta los UID (generación de claves o una emulación simple)
UID Fuzzing	Capacidad para aleatorizar UIDs, para aumentar/disminuir UIDs

Elaborado por el autor. Datos obtenidos de Lab401 (2019). Chameleon Mini: RevE Rebooted

El firmware de Chameleon Mini, se configura y se carga a través de USB, mediante líneas de comando o a su vez mediante un software GUI. También existe una aplicación para *Smartphone* con sistema operativo Android, llamada Chameleon-mini app. En la figura 25 y 26, se muestra la interfaz gráfica que permite establecer los parámetros de configuración.

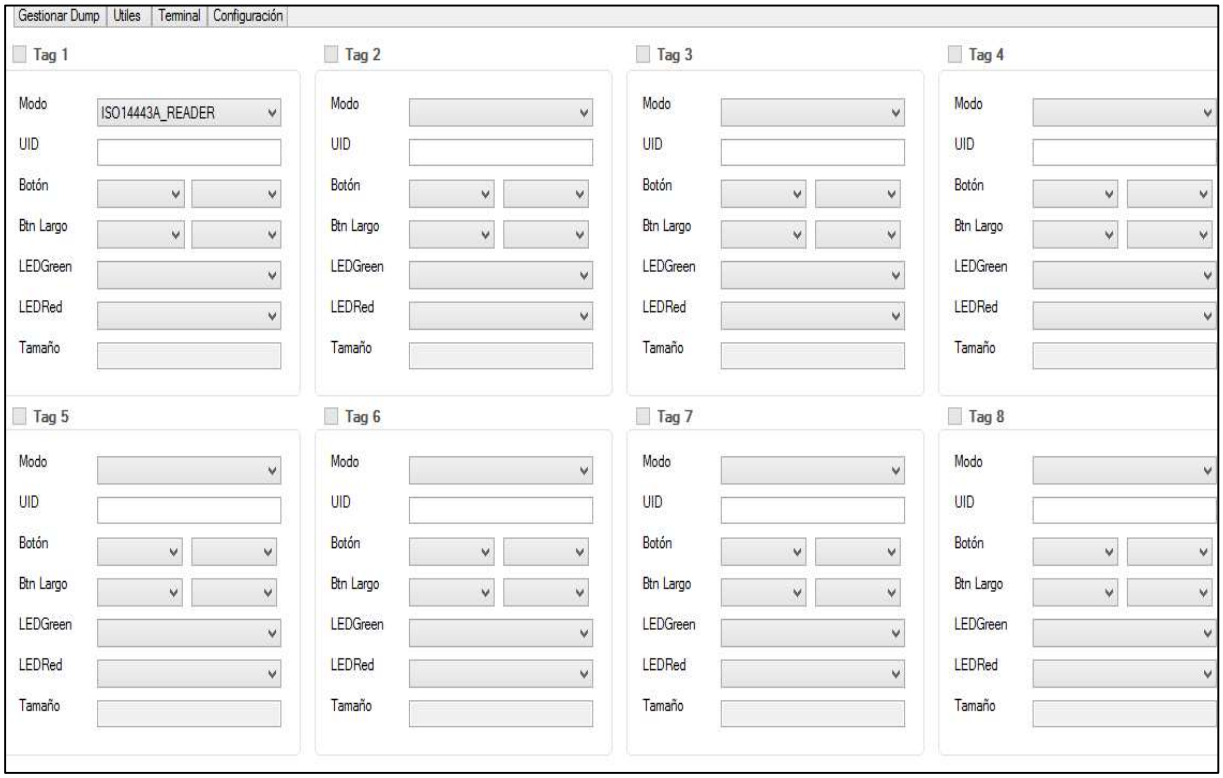


Figura 25. Interfaz GUI del dispositivo Chameleon Mini. Fuente: autor

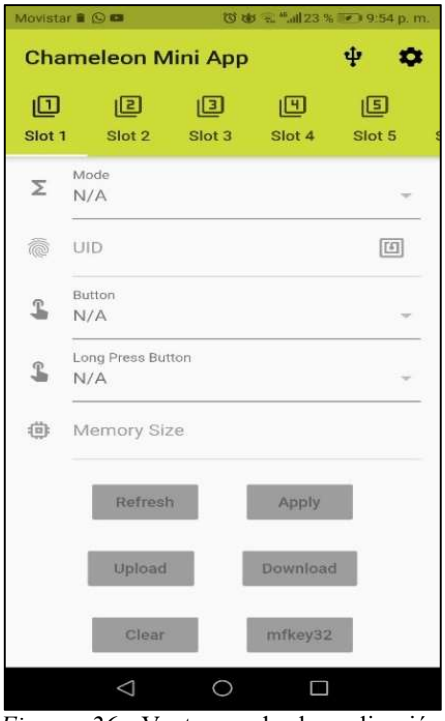


Figura 26. Ventanas de la aplicación Chameleon-Mini App. Fuente: autor

3.2 Aplicaciones del transpondedor xNT

La tecnología NFC se aplica en varios ámbitos, de los cuales el implante de microchip xNT, se aplica en los siguientes:

- Identificación: se almacena los datos personales del usuario en la memoria del chip.
- Intercambio de datos: puede almacenar textos, fotografías, archivos que sean de menor tamaño a la capacidad de la memoria y ser leídos por un lector o un *Smartphone*.
- Tareas en *Smartphone*: el implante puede almacenar tareas en su memoria, que al ser leídas por un teléfono inteligente son ejecutas, se debe instalar las aplicaciones requeridas.
- Controles de acceso: el administrador de los sistemas de ingreso a distintas ubicaciones, deben registrar el UID a sus sistemas de control, así el usuario del implante tendrá acceso.
- Activación de dispositivos: mediante un lector que funcione como un teclado USB HID (Dispositivo de Interfaz Humana), el UID se escribirá como si se usara el teclado activando el dispositivo.

Dentro de los ámbitos en los cuales se aplica el implante, se puede mencionar algunos proyectos que utilizan los transpondedores xNT (Dangerous Things, 2019).

- Desbloqueo e inicio de sesión de sistemas operativos (computadores y *Smartphone*);
- Acceso a domicilios, a gimnasio y transporte;
- Desbloqueo de puertas y encendido de vehículos;
- Pagos con bitcoin (moneda digital);
- Autenticación de doble factor para envió de emails.

3.3 Escenario de prueba del transpondedor xNT

De acuerdo con las aplicaciones que tiene el implante xNT, el escenario de prueba de funcionamiento en este proyecto se centró en dos ámbitos: control de acceso y tareas en un teléfono inteligente...

3.3.1 Control de acceso

Para realizar el control de acceso se debe considerar dos componentes: hardware y software. El hardware se complementó de los módulos PN532 y Arduino UNO; y el software, se ejecutó mediante la plataforma IDE de Arduino.

3.3.1.1 Hardware del control de acceso

La conexión de los pines entre los módulos PN532 y Arduino UNO, se debe realizar bajo el protocolo de comunicación ISP. En el caso del módulo PN532 se debe tener en cuenta la configuración de los estados lógicos del switch. En la figura 27, se observa la conexión de pines entre los módulos Arduino UNO y PN532. En la tabla 7, se establecen los pines que deben conectarse.

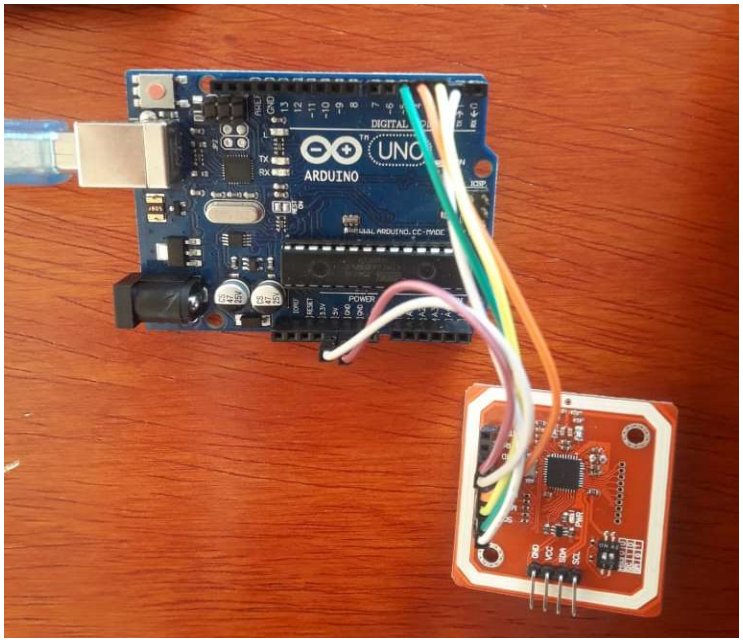


Figura 27. Comunicación SPI entre los módulos Arduino UNO y PN532. Fuente: autor

Tabla 7.
Conexión de pines entre los módulos Arduino UNO y PN532

Arduino UNO	PN532
5V	VCC
GND	GND
Pin 2	SCK
Pin 3	MOSI
Pin 4	SS
Pin 5	MISO

Elaborado por el autor

La conexión de los módulos forma un solo circuito, que se energiza y se comunica con un módulo de control (computador o *Smartphone*) mediante cable USB.

3.3.1.2 Software del control de acceso

La plataforma IDE de Arduino permite crear y ejecutar las líneas de código, que leen el implante y simulan el control de acceso a través del UID del implante. (Ver anexo 4). Las primeras líneas de código usadas en el script, permiten llamar a las librerías NFC instaladas con el software, estas librerías permiten leer el implante xNT y establecer el protocolo de comunicación ISP.

```
#include <Wire.h>
#include <SPI.h>
#include <Adafruit_PN532.h>
```

Luego se define los pines del módulo Arduino UNO, que se usaran para establecer la comunicación ISP con el módulo PN532.

```
#define PN532_SCK (2)
#define PN532_MOSI (3)
#define PN532_SS (4)
#define PN532_MISO (5)
```

A continuación, se verifica si se encuentra conectado correctamente el módulo PN532. Si se encuentra conectado correctamente, se activa el modulo para la lectura del implante.

```
Adafruit_PN532 nfc(PN532_SCK, PN532_MISO, PN532_MOSI, PN532_SS);
 nfc.begin();
 uint32_t versiondata = nfc.getFirmwareVersion();
          if (! versiondata) {
          Serial.print("No está conectado el módulo PN532");
           while (1); // detener
          }
 nfc.setPassiveActivationRetries(0xFF);
 nfc.SAMConfig();
```

La activación del módulo ocasiona que el lector esté en modo de espera, cuando se acerca el implante al lector se obtiene su UID, el cual se almacena en una constante en formato hexadecimal.

```
 boolean success;
  uint8_t uid[] = { 0, 0, 0, 0, 0, 0, 0 };
  uint8_t uidLength;
 success=nfc.readPassiveTargetID(PN532_MIFARE_ISO14443A, &uid[0], &uidLength);
  if (success) {
  String hex_value = "";
```

Obtenido el UID del implante, se realiza una comparación con los UID almacenados en el script, si el UID es correcto autoriza el acceso; si no lo es, se deniega el acceso. La verificación de resultados se puede observar en la figura 28, que es la ventana de monitoreo de la plataforma IDE, establecida a 115200 baudios.

```
if (hex_value == "98132130115") {
    Serial.println("ACCESO AUTORIZADO");
}
else
    Serial.println("ACCESO DENEGADO");
```

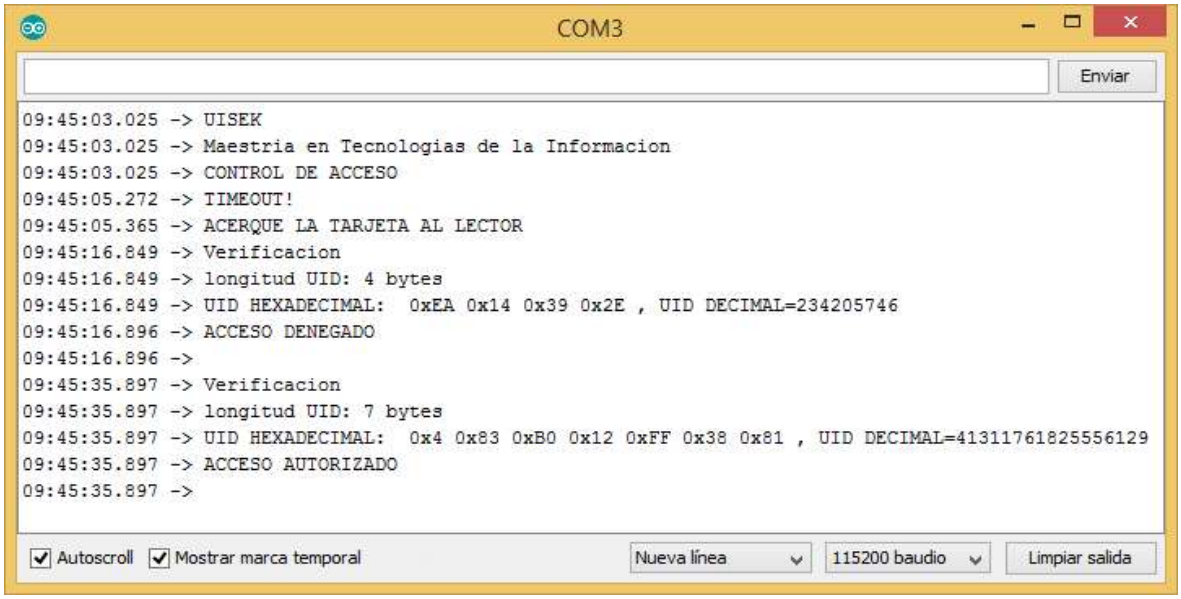


Figura 28. Ventana de monitoreo de la plataforma IDE. Fuente: autor

3.3.2 Tareas en un *Smartphone*

Para el segundo escenario de prueba, se configuro el transpondedor xNT con una tarea, la cual es ejecutada al ser leída por un *Smartphone*, para realizarlo se consideraron dos aplicaciones: NFC Tool para escribir en el implante y NFC Tasks para ejecutar la tarea. Ambas aplicaciones son compatibles con sistemas Android y es para versiones superiores a 4.0

3.3.2.1 NFC Tools

Permite escribir en el teléfono inteligente diversas tareas, algunas de ellas son: enviar correo electrónico, SMS, llamadas, disminuir el brillo del celular, etc. La tarea elegida para demostrar el funcionamiento del implante, es la de realizar una llamada a un número telefónico. En la figura 29, se muestra la ventana de configuración del número telefónico.

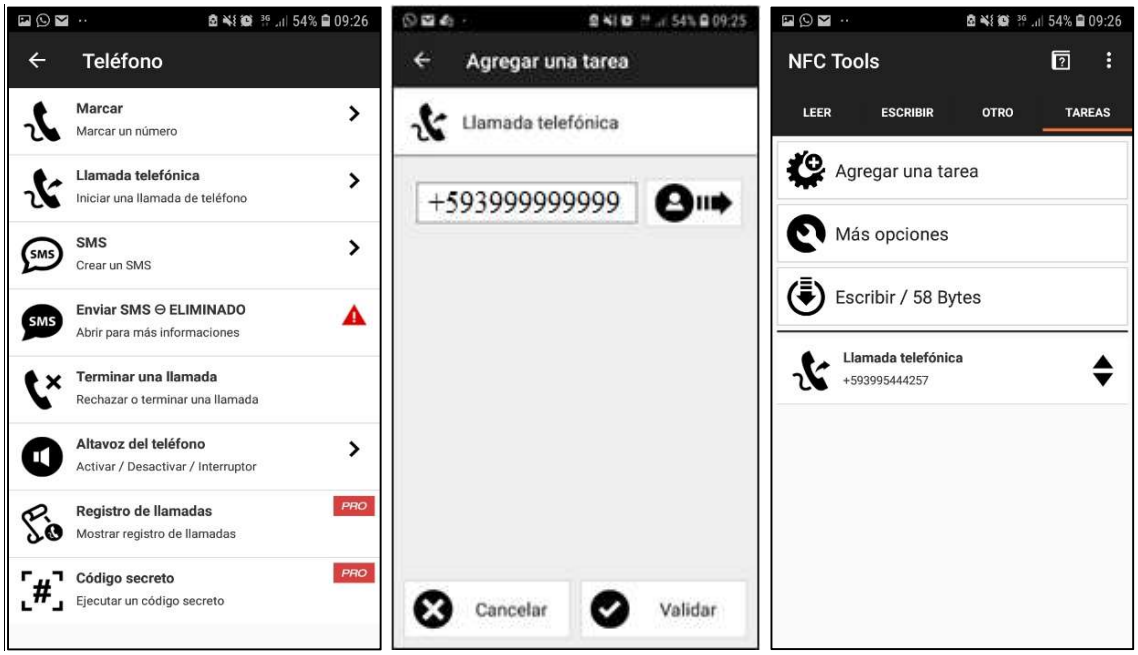


Figura 29. Configuración del número telefónico. Fuente: autor

En la memoria del implante las tareas se escriben como datos NDEF, que es un formato estandarizado para intercambiar datos NFC y usado por los *Smartphone* para leer datos y ejecutar acciones. Los datos NDEF están formados por mensajes NDEF y por registros NDEF. Los mensajes NDEF, contiene uno o más registros NDEF y se encargan del transporte. Los registros NDEF contienen una carga útil que específica la acción a ejecutar (Villavicencio & Mendoza, 2015).

3.3.2.2 NFC Tasks

Al acercar el implante xNT al lector del *Smartphone*, se lee el dato NDEF y se ejecuta la tarea grabada en la memoria del implante, segundos después se efectúa la llamada al número telefónico configurado. En la figura 30, se muestra la ventana de la llamada en ejecución.

Figura 30. Ventana de la llamada en ejecución. Fuente: autor

El establecer un escenario en el cual se verifique el funcionamiento del implante xNT en uno de los ámbitos en los cuales se aplica, permite a más de probar su funcionamiento, verificar si su uso es seguro o si tiene alguna vulnerabilidad.

3.4 Seguridad en los transpondedores xNT

Los parámetros de seguridad que tienen el implante xNT, buscan garantizar la confidencialidad, integridad y disponibilidad de los datos, el implante tiene tres parámetros: distancia de lectura, discreción de su utilización; y por último configuraciones de seguridad para lectura y escritura.

3.4.1 Distancia de lectura

Uno de los parámetros de seguridad del implante es sin duda alguna, el rango de distancia que debe existir entre el lector y el implante para ser leído, el cual es pequeño. Si un atacante quiere obtener información del UID o de los datos NDEF almacenados en el implante, deba estar en primera instancia cerca de él; y en segunda, buscar el momento preciso y exacto, para que el portador no se dé cuenta.

3.4.2 Discreción en la utilización del implante

No se debe divulgar su ubicación, ni la información que contiene, mucho menos su uso. No todos deben saber que posee una llave de acceso o información transcendental entre sus manos; es más, no tienen por qué saber que se tiene un implante.

3.4.3 Configuraciones de seguridad para lectura y escritura del implante

Las configuraciones de seguridad para lectura y escritura se establecen en el los bytes de la memoria del implante. La memoria tiene 231 páginas de 4 byte, cada byte cumple una función específica y se establece en formato hexadecimal. Las paginas E5 y E6 no pueden ser leídas por ningún lector, debido al diseño efectuado por su fabricante. Siempre aparecerán como bytes establecidos en 00. En la figura 31, se observar la organización de la memoria del implante.

Page Adr		Byte number within a page				
Dec	Hex	0	1	2	3	Description
0	0h	serial number				Manufacturer data and static lock bytes
1	1h	serial number				
2	2h	serial number	internal	lock bytes	lock bytes	
3	3h	Capability Container (CC)				Capability Container
4	4h	user memory				User memory pages
5	5h					
...	...					
224	E0h					
225	E1h					
226	E2h	dynamic lock bytes			RFUI	Dynamic lock bytes
227	E3h	CFG 0				Configuration pages
228	E4h	CFG 1				
229	E5h	PWD				
230	E6h	PACK		RFUI		

Figura 31. Organización de la memoria del microchip NTAG216. Fuente: Company Public (2015). Recuperado de: https://www.nxp.com/docs/en/data-sheet/NTAG213_215_216.pdf

3.4.3.1 UID programado de 7 bytes único

El UID se establece en los primeros 9 bytes. En la página 0h, el byte 0 es el ID de fabricante (semiconductores NXP). Los bytes 3 y 0 de las paginas 0h y 2h respectivamente, son los bytes de verificación. El byte 1 de la página 02h está reservado para datos internos del fabricante. Los bytes son programados por el fabricante y protegidos contra escritura. En la Figura 32, se puede observar la distribución de bytes para el UID.

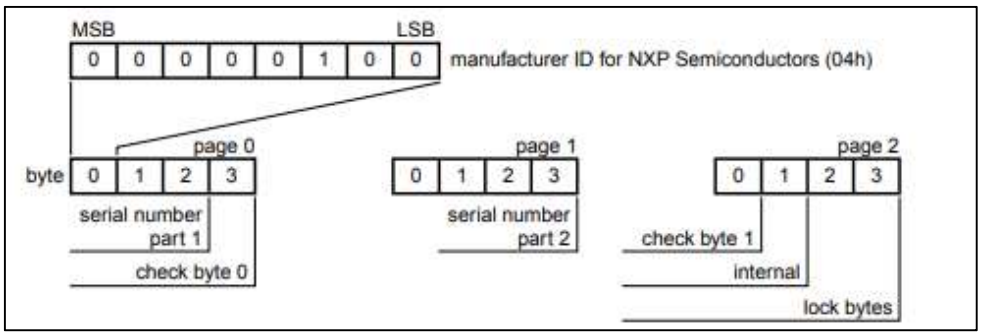


Figura 32. Organización de Bytes para el UID. Fuente: Company Public (2015). Recuperado de: https://www.nxp.com/docs/en/data-sheet/NTAG213_215_216.pdf

3.4.3.2 Configuración de bloqueo para solo lectura

La configuración de bloqueo se realiza en dos grupos de páginas, unas de manera estática y otras de manera dinámica. El bloqueo estático se aplica a páginas individuales, mientras que el bloqueo dinámico, se aplica a un conjunto de páginas.

A. Bytes de bloqueo estático

Los bytes de bloqueo estático, son los bytes 2 y 3 de la página 2h, bloquean las páginas 03h hasta 0Fh. El valor por defecto de los bytes de bloqueo estático es 0 lógico. Lx bloquea una a una las páginas, mientras que BLx bloquea todo un conjunto de páginas. Por ejemplo, si BL15-10 se establece en la lógica 1, los bits L15 a L10 también se establecen en 1 lógico. En la figura 33, se observa la organización de los bits.

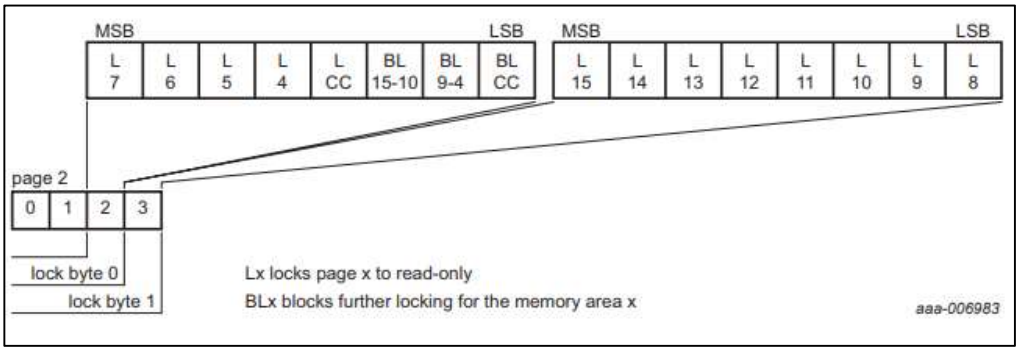


Figura 33. Organización de Bytes para el bloqueo estático. Fuente: Company Public (2015). Recuperado de: https://www.nxp.com/docs/en/data-sheet/NTAG213_215_216.pdf

B. Bytes de bloqueo dinámico

Los bytes de bloqueo dinámico se encuentran en la página E2h y son los bytes 0, 1 y 2, bloquean las páginas 10h hasta E1h, estos bytes, trabajan de manera similar a los de bloqueo estático. Su valor predeterminado es 0 lógico. En la figura 34, se observa la organización de los bits.

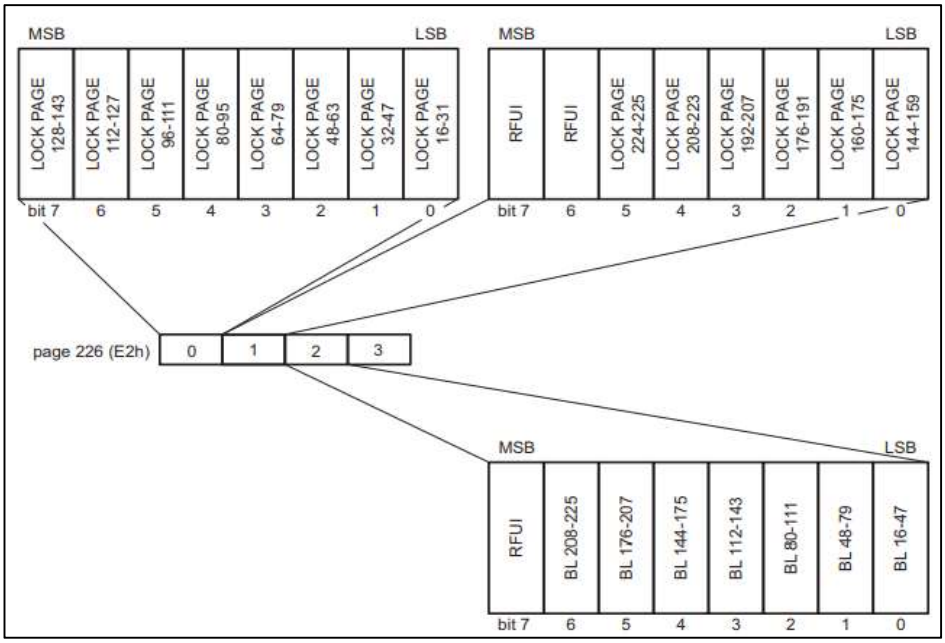


Figura 34. Organización de Bytes para el bloqueo dinámico. Fuente: Company Public (2015). Recuperado de: https://www.nxp.com/docs/en/data-sheet/NTAG213_215_216.pdf

Si un bit se establece en la lógica 1, no se puede volver a cambiar a la lógica 0. Una vez que los bytes de bloqueo se activan para proteger los bloques de memoria, nunca se pueden desbloquear y siempre serán de solo lectura, lo que no es ideal y no se aconseja configurar si se quiere reutilizar el transpondedor.

3.4.3.3 Configuración de verificación de contraseña

Esta protección pretende evitar operaciones de escritura y escritura/lectura de memoria no autorizadas, las páginas E3h a E6h, se utilizan para configurar la restricción de acceso a la memoria, en la gráfica 35, se detallan los bytes que conformar estas páginas.

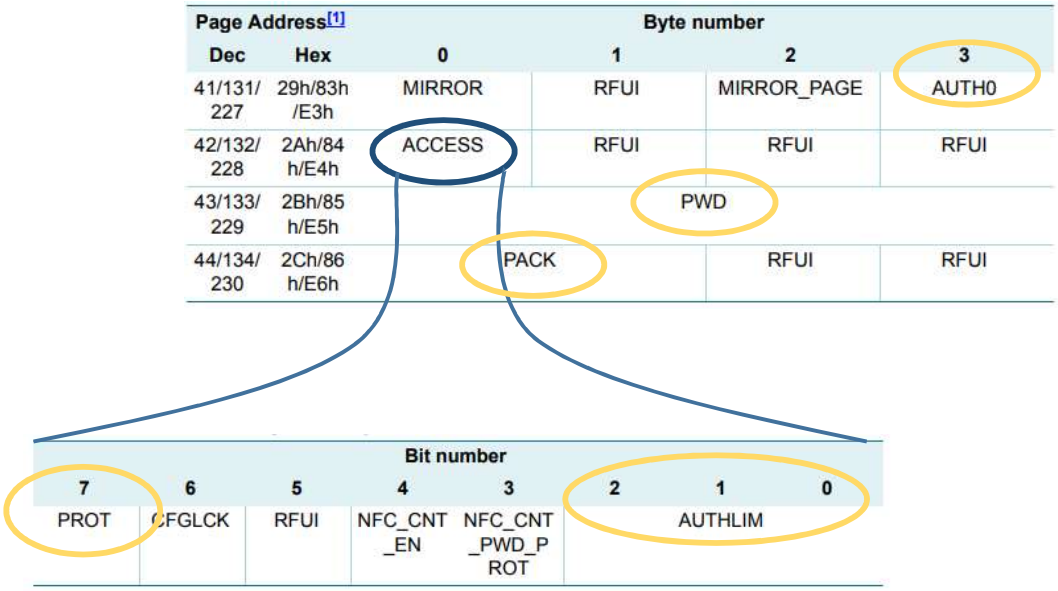


Figura 35. Bytes de configuración de contraseña. Fuente: Company Public (2015). Recuperado de: https://www.nxp.com/docs/en/data-sheet/NTAG213_215_216.pdf

Los bits considerados para establecer una contraseña son los siguientes:

- AUTH0: es el byte que define las páginas en las que se establecerá la verificación de contraseña. Los valores que puede tomar son de 00 a FF. El valor por defecto es FF que significa deshabilitado. Si AUTH0 se establece en una dirección de página mayor a la última página de la configurada por el usuario, la verificación de contraseña esta desactivada.
- PROT: es un bit que define el tipo de protección que tendrá la memoria. Con 0 lógico, se protege del acceso a escritura; y con 1 lógico, se protege del acceso a escritura y lectura.
- AUTHLIM: son bits que limitan el número de ingresos de contraseñas incorrectas. Por defecto se encuentra en 000 que es deshabilitado, el número de intentos es de 1 a 7. Esta configuración se usa para evitar ataques de fuerza bruta, cuando se alcanza el número de

intentos especificado, se bloquea de manera permanente la parte protegida de la memoria, imposibilitando su lectura.

- PWD: es la contraseña elegida por el usuario con un tamaño de 32 bits, permite 4 dígitos (8 bits cada uno) entre letras, números o símbolos. Se ubica en los 4 bytes de la página E5h. Por defecto el valor de la contraseña se establece en FFFFFFFF.
- PACK: son los bytes 0 y 1 de la página E6h, es una respuesta de reconocimiento de contraseña

3.5 Vulnerabilidades del transpondedor xNT

Existen diversos ataques de seguridad a la tecnología NFC, cada uno se aplica de diferente manera y aprovecha alguna vulnerabilidad. De acuerdo con los autores Kulkarni, Sutar, Mohite y Shelke (2014), en su estudio "RFID security issues and challenges", realiza un resumen de los principales ataques aplicados a esta tecnología. En la figura 36, se muestran los ataques en función a las referencias que existen sobre cada uno. En la tabla 8, se realiza una descripción de cada uno.

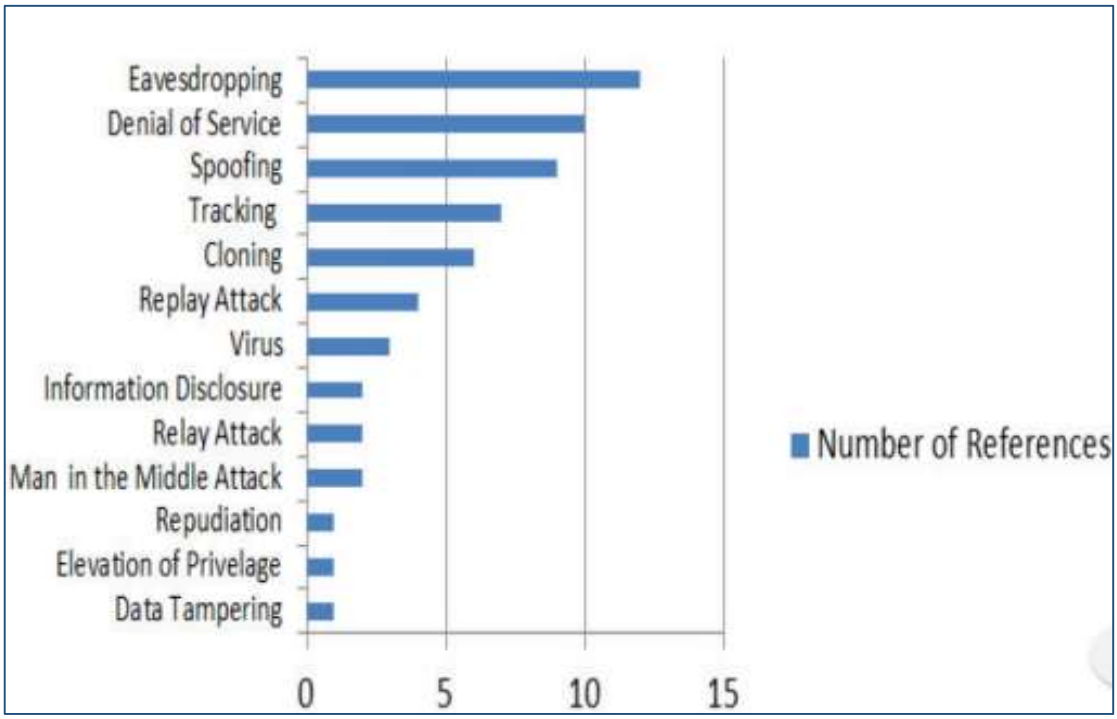


Figura 36. Ataques a la tecnología RFID vs referencias del ataque. Fuente: Kulkarni et al., (2014). Recuperado de: https://www.researchgate.net/publication/260548942_RFID_security_issues_challenges

Tabla 8
Característica de los ataques NFC

Nombre	Descripción
Eavesdropping	El atacante busca la manera de escuchar la comunicación entre el transpondedor y el lector NFC de forma secreta.
Denial of service	Deniega la comunicación entre en transpondedor y el lector NFC, puede ser de forma temporal o de manera permanente.
Spoofing	El atacante suplanta la identidad de un transpondedor, mediante la falsificación de información. Se produce al comunicarse con un lector
Tracking	Es un ataque que pretende obtener información de los archivos de registro de un lector, acciones ejecutadas en él.
Cloning	Este ataque permite duplicar el UID de un transpondedor y en otros casos duplicar la información que tiene el microchip en su memoria.
Replay Attack	El atacante captura una comunicación entre un transpondedor y un lector, guarda la información y luego la usa para su beneficio.
Virus	El ataque consiste en inmiscuir un malware a un lector a través de un transpondedor.
Information Disclosure	Se divulga la información contenida en un transpondedor de manera que deja de ser privada, el atacante se encarga de propagar esta información.
Relay Attack	Este ataque burla la distancia corta de lectura, mediante el uso de dos dispositivos que simulan ser un lector y un transpondedor.
Man in the middle attack	Hombre en la mitad, el atacante intercepta una comunicación, puede modificar la información, cambiarla completamente o simplemente leerla
Repudiation	Cuando el sistema NFC no registra correctamente las acciones ejecutadas por el transpondedor, el atacante puede aprovechar esta vulnerabilidad registrando datos incorrectos en los archivos de registro
Elevation of privelage	El ataque busca que un transpondedor tenga privilegios adicionales a los establecidos en primera instancia.
Data Tampering	El ataque intercepta los datos y los manipula de manera deliberada, mediante canales no autorizados, se asemeja al ataque de hombre en el medio.

Elaborado por el autor. Datos obtenidos de Kulkarni et al., (2014). RFID security issues & challenges. En International Conference on Electronics and Communication Systems (ICECS). IEEE.

Cada ataque se efectúa sobre algún componente del sistema de NFC o a la comunicación de todo el sistema. En base a este precedente, los ataques se pueden clasificar dependiendo del componente al que se va a realizar. En la tabla 9, se indican los ataques a la tecnología NFC y a que componente del sistema afecta.

Tabla 9
Ataques de acuerdo al componente del sistema NFC.

Componentes	**Ataque**
Comunicación del sistema (Todos)	Eavesdropping
	Denial of service
	Replay Attack
	Relay Attack
Software y Lector NFC	Spoofing
	Tracking
	Virus
	Repudiation
	Elevation of privilege
Transpondedor	Cloning
	Information Disclosure
	Denial of service

Elaborado por el autor.

Establecidas las seguridades y conocidos los ataques que se pueden efectuar sobre el transpondedor, se pueden definir las vulnerabilidades que tiene el implante xNT.

- El UID no es seguro porque se puede duplicar. Existen tarjetas en blanco que permiten la configuración de un UID; por lo tanto, un atacante puede descubrir el UID del implante, configurarlo en una tarjeta en blanco y burlar un control de acceso.
- La configuración de bloqueo para solo lectura, se aplica a los bloques de memoria que almacenan datos distintos a los del UID, permite que no exista una sobre escritura o que la

información sea borrada, pero no asegura que estos datos no se puedan duplicar en otra tarjeta o que no puedan ser leídos por un atacante.

- La configuración de verificación de contraseña evita sobre escrituras o lecturas sin autorización, su inconveniente radica en que no es cifrada, se transmite al microchip desde el lector en texto plano.
- Los datos de memoria tampoco están encriptados bajo ningún algoritmo criptográfico, se almacenan en texto plano, el atacante puede leer el bloque de memoria del microchip y saber que está almacenado.
- Dejar las configuraciones por defecto, permite a un atacante leer, sobre escribir o borrar la información que este almacenada en la memoria, inclusive hasta configurar el bloqueo de solo lectura o una contraseña, así el usuario no puede seguir usando su implante xNT.
- La configuración de AUTHLIM evita un ataque de fuerza bruta, pero si se llega a efectuar bloquearía el implante de tal manera que será imposible volver a utilizarlo (no legible), deja una puerta abierta para un ataque de denegación de servicio.
- La frecuencia en la que opera el implante xNT, es una banda libre que puede ser interferida, el atacante puede usar un inhibidor de señal (jammers) que bloquea la comunicación, impidiendo el uso del implante.
- Un usuario puede ser víctima de un ataque en el cual se active un generador de pulsos (DIY) cerca del transpondedor, esto puede llegar a dañar el microchip del implante, imposibilitando su uso.
- Un usuario que no sea cuidadoso y que de alguna manera haga conocer que tiene un implante con información importante, puede ser víctima de un ataque drástico, como extraerlo de forma física.

3.6 Clonación del Transpondedor xNT

Para efectuar un ataque de clonación, el atacante debe conocer en que lo utiliza la víctima y estar al tanto de las actividades cotidianas que realiza. El implante siempre estará dentro del usuario y lo llevará consigo a todas partes; por lo tanto, el perpetrador debe planificar un ataque dirigido hacia alguien en específico, determinar un lugar y el momento exacto en el cual se pueda obtener la información requerida del implante.

3.6.1 Clonación de UID para burlar un control de acceso

Para duplicar el UID del implante, se utilizó la tarjeta Chameleon mini, la cual permite una operación de UID sniffing, que lee el implante y captura el UID, configurándolo en uno de los ocho espacios de tarjetas virtuales que posee el módulo.

El clonar el UID de un implante permite burlar todos los controles de acceso en los cuales este registrado el usuario legítimo sin ser detectado. En la figura 37, se pueden observar los parámetros usados para la clonación del implante.

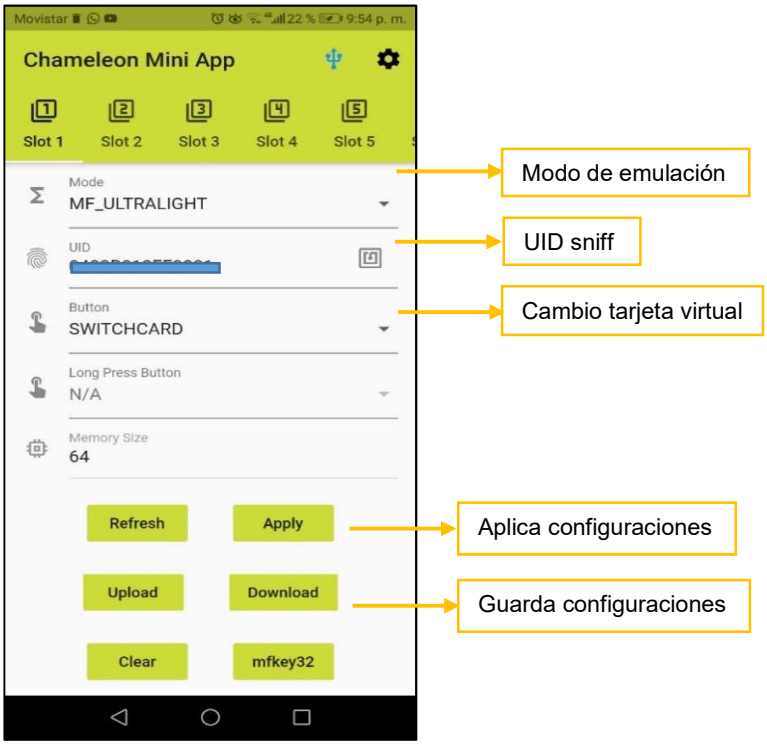


Figura 37. Parámetros para clonar el UID del implante. Fuente: autor

El UID se puede leer por cualquier lector, inclusive si el implante está configurado con PROT=1 y AUTH0=00, debido a su diseño de fábrica como parte de la norma ISO14443. Por lo tanto, no tiene sentido configurar este tipo de protección de contraseña, debido a que no existe protección y más bien afecta la vida útil del implante, en un sistema NFC la principal función del transpondedor es responder a una solicitud de presencia.

3.6.2 Clonación de los datos NDEF para ejecutar tarea.

Las configuraciones recomendadas por el fabricante para la protección del implante xNT, contra bloqueos accidentales permanentes o ataques maliciosos de negación de servicio, se pueden efectuar mediante la aplicación DNFC (Dangerous NFC), propia del fabricante. La aplicación modifica las páginas 02 y E2 (bloqueo estático y dinámico de solo lectura), AUTH0 = E2, PROT = 0 y AUTHLIM = 000. En la tabla 10, se describe las funciones configuradas. En la figura 38, se observa la ventana de la aplicación.

Tabla 10
Configuraciones mediante la aplicación DNFC

Configuración	Característica
PROT = 0	Verificación de contraseña para escritura.
AUTH0 =E2	Protege los bytes de configuración y no los del uso de memoria, los cambios que se deban realizar, se efectuarán luego de que exista un proceso de autenticación.
AUTHLIM=000	Deshabilita el conteo de ingreso de contraseñas incorrectas, evita que el implante quede inutilizable de manera permanente al existir ingresos incorrectos de autenticación.
PWD	El usuario del implante ingresa 4 dígitos alfanuméricos en formato hexadecimal, no se recomienda ingresar símbolos, debido a las inconsistencias entre lectores y aplicaciones.
PACK	Dos bytes en hexadecimal que verifican una autenticación correcta, la aplicación los establece en 4454 (DT)
Page 02: 54 48 **0F** 00 Page E2: 00 00 **7F** BD	Esta configuración bloquea los bytes de bloqueo estático y dinámico, este cambio es irreversible, usa su poder contra sí mismo.

Elaborado por el autor. Datos obtenidos de Dangerous Things, (2019). Chip NFC xNT.

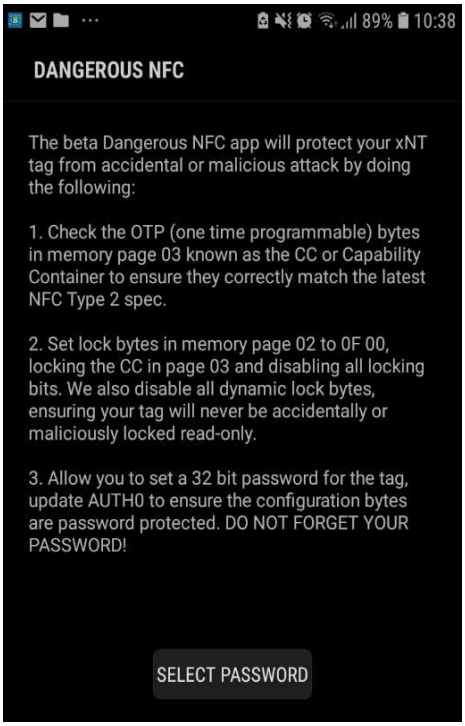


Figura 38. Ventana de la aplicación DNFC
Fuente: autor

Con la configuración recomendada por el fabricante, se efectúa una protección de sobre escritura y no de lectura. Un atacante puede leer el contenido de la memoria del implante, lo único que necesita es el tiempo y espacio suficiente para efectuarlo, inclusive puede cambiar la información almacenada en el implante para generar un ataque hacia el dispositivo lector.

El UID y los datos almacenados en memoria se manejan de manera indistinta, equivalente a una cedula de identidad. Las tareas en el implante se almacenan en formato hexadecimal, ordenados en cuatro bytes a partir de la página 04, cada byte representa un carácter ASCII. Esta codificación permite la comunicación entre el implante y el *Smartphone*, el cual determina la tarea a ejecutar.

Para la clonación de la tarea se utilizó la aplicación NFC Tools que, a más de leer el implante, permite duplicar los valores hexadecimales en otra tarjeta o en otro implante, emulando el contenido en el dispositivo lector de destino. En la figura 39, se muestra las ventanas para la duplicación de mensajes NDEF.

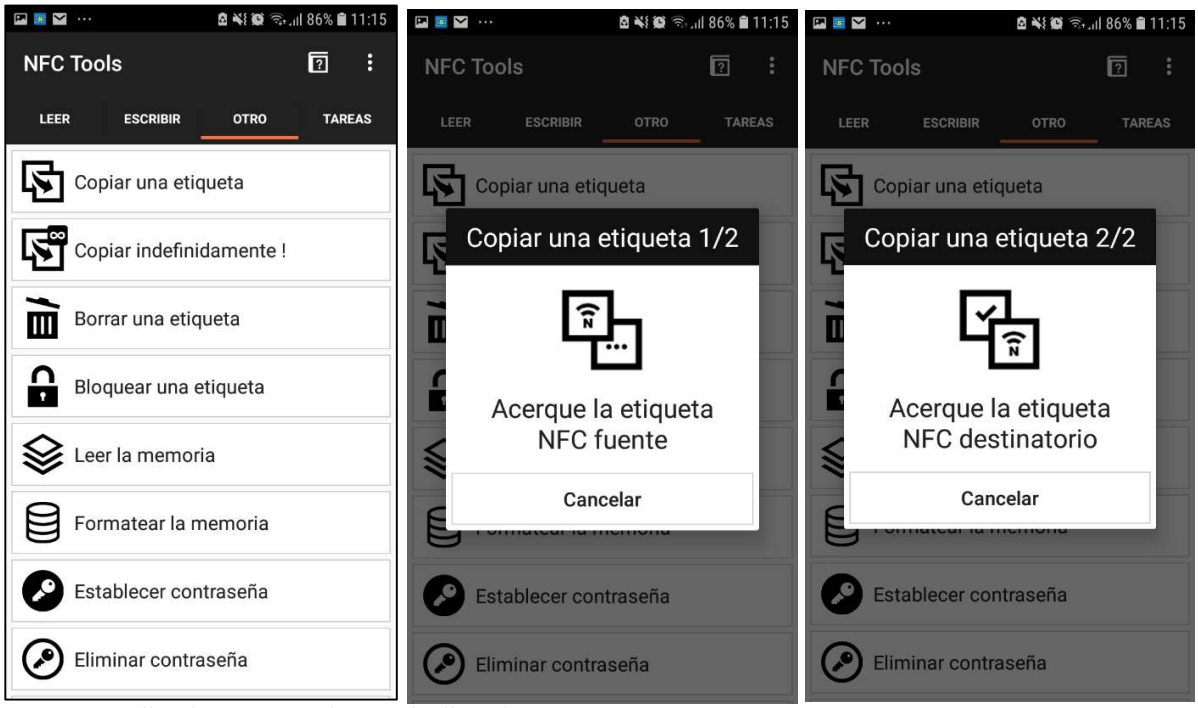


Figura 39. Aplicación NFC Tools para duplicar datos NDEF. Fuente: autor

Si se modifica el parámetro AUTH0=04 en la configuración recomendada por el fabricante, se establece la protección de escritura desde la página 04, esto le da un mayor nivel de seguridad al implante, un atacante podrá leer la información, pero no podrá escribir sin antes autenticarse.

Si se aumenta aún más el nivel de seguridad del implante, modificando AUTH0 = 04, PROT = 1 y AUTHLIM = 111, un atacante no podrá leer ni escribir el implante sin antes autenticarse. Pero aumentar el nivel de seguridad implica disminuir su capacidad de utilización; es decir, no todos los lectores pueden leer la información almacenada o ejecutar la tarea requerida, debido a la compatibilidad con el uso de contraseñas de algunas aplicaciones, su software no está desarrollado correctamente, mostrando al implante como no compatible con la aplicación.

Para modificar los parámetros de configuración se puede utilizar la aplicación NFC Shell, que permite enviar al implante comandos avanzados de manera simultánea, siempre el primer comando a enviar debe ser la contraseña configurada en el implante. En la figura 40, se muestra la ventana de la aplicación y la manera en la cual se deben enviar los comandos para poder escribir en un implante protegido con contraseña.

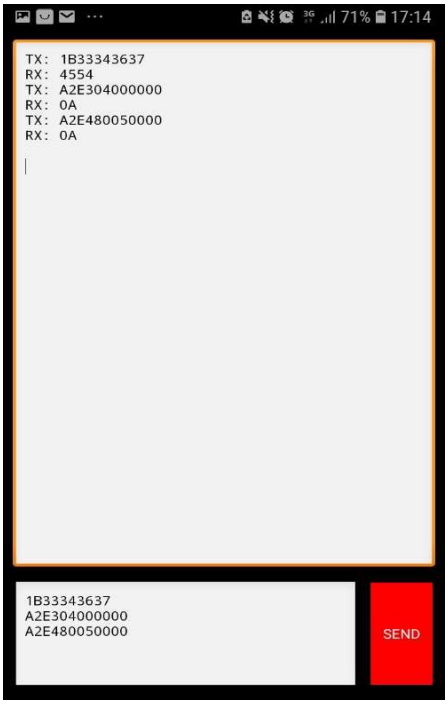


Figura 40. Aplicación NFC Shell para comandos de configuración. Fuente: autor

3.7 Futuras condiciones de seguridad a implantes de microchips de la serie xNT

El parámetro de AUTHLIM facilita a un hacker a realizar un ataque de denegación de servicio, por lo cual este parámetro debe ser corregido, al superarse el número de contraseñas erróneas permitidas no se debe dañar el implante, sino que se debe bloquear la lectura y/o escritura de manera temporal, hasta que se vuelva a establecer los parámetros de configuración, alertando a la víctima.

El software de los dispositivos lectores debe estandarizarse, de manera que toda comunicación entre lector y transpondedor se realice mediante autenticación, aumentando el nivel de seguridad. Si el implante se utiliza para control de acceso, tendría un doble factor de autenticación que sería el UID y la contraseña.

El implante debe tener un parámetro configurable que establezca el número de ingreso de contraseñas correctas, superado este número, el lector deberá solicitar el cambio de contraseña. Esta condición mejorará la seguridad. En el caso de un control de acceso un perpetrador tendría

un tiempo limitado para usar su ataque; en cambio, la víctima de un ataque exitoso no tendrá acceso debido a una clave incorrecta, esto lo alertaría y daría aviso al administrador del sistema, quien puede revisar los videos de vigilancia del intento actual y el del último acceso.

Sin duda alguna, una de las mayores vulnerabilidades del implante xNT, es el almacenamiento de la información en texto plano, esta vulnerabilidad se debe corregir aplicando un algoritmo de cifrado que dificulte el trabajo a los hackers.

CAPITULO 4

CONCLUSIONES, RECOMENDACIONES Y TRABAJOS FUTUROS

4.1 Conclusiones

Una vez identificados los componentes que tiene un implante de microchip de la serie xNT con tecnología NFC, a través del estudio de cada uno de sus elementos, se logró determinar la estructura general que tienen estos transpondedores, los cuales en la actualidad pueden ser de dos formas: cilíndricos o laminas flexibles; de esta manera se comprobó que la forma del implante puede cambiar, pero no cambiará su funcionamiento, será el mismo en cualquier diseño.

Investigadas las técnicas de *Ethical hacking* existentes para el análisis de vulnerabilidades de la tecnología NFC, se seleccionó la técnica de clonación, debido a que esta se aplica al transpondedor que es el objetivo principal de este trabajo, como resultado se identificaron las vulnerabilidades que tiene el implante.

La técnica de clonación se empleó con la ayuda de dos mecanismos: Chameleon mini, herramienta especializada para la clonación del UID; y mediante NFS Tools, aplicación que permite la duplicación de la información almacenada en el transpondedor. La ejecución de estos procesos demostró el peligro al cual se encuentran expuestos los usuarios.

Con la ejecución de la técnica de clonación se evidenció que la seguridad del implante debe mejorar, para ello se debe modificar algunos parámetros de configuración y considerar estrategias que perfeccionen su funcionamiento, esto logrará aumentar la seguridad de la información y reducir el riesgo de uso de esta tecnología.

Conocidas las vulnerabilidades existentes en un implante de microchip de la serie xNT y los riesgos a los cuales se encuentran expuestos sus usuarios, es necesario para su uso definir la aplicación que tendrá el implante, y en base a ello establecer un factor de seguridad adicional.

Cabe mencionar que la seguridad absoluta es imposible, siempre existirá la posibilidad de ser atacados.

Se determinó que la configuración recomendada por el proveedor no brinda la seguridad necesaria, por cuanto solo bloquea configuraciones incorrectas que causarían daños permanentes al implante. El bloqueo de solo lectura o la activación de AUTHLIM, en lugar de garantizar protección es una puerta abierta para un ataque de negación de servicio.

Se comprobó que la distancia corta de lectura es sin duda alguna, la mayor seguridad que tiene el implante xNT, puesto que para realizar un ataque es necesaria la aproximación del atacante a la víctima. Para clonar el UID, se debe estar cerca del implante entre uno a dos segundos aproximadamente; mientras que, para leer los bloques de memoria del implante, es necesario tener más tiempo y estabilidad para su lectura.

Se evidenció que la configuración de contraseña protege el contenido del microchip y depende directamente de los parámetros configurados. El UID puede ser leído por cualquier lector, mientras que los datos almacenados en memoria no, existe una incompatibilidad entre algunas aplicaciones, su software no está desarrollado correctamente para considerar la configuración de contraseña en implantes.

4.2 Recomendaciones

En un sistema NFC con contraseña, el dispositivo lector es quien envía la contraseña al implante, el cual responde con una confirmación de contraseña. Se produce un proceso comparativo entre la contraseña escrita en el dispositivo lector y la contraseña almacenada en el implante. La aplicación NFC Tools no está configurada de esta manera, no se recomienda su uso si el implante está configurado con contraseña desde la página 04. La aplicación no efectúa ninguna operación, muestra un mensaje indicando que el implante no es compatible.

El uso del implante xNT en un control de acceso, debe estar apoyado de otros factores de seguridad, que disminuyan el riesgo de ser atacados. Aparte de utilizar el implante, se puede utilizar una

alarma que sea desactivada al cruzar el control, inclusive se puede usar cámaras de seguridad, la combinación de estos factores debe buscar aumentar el nivel de seguridad.

La protección de contraseña configurada en los implantes xNT, debe ser pensada como una manera de evitar accesos no autorizados a los parámetros de configuración y no a los datos almacenados. El implante xNT almacena y transmite los datos en texto plano, por lo tanto, si se requiere un nivel más alto de protección, se puede implementar métodos criptográficos a los datos antes de escribirlos en el implante, aumentando la seguridad.

4.3 Trabajos Futuros

A medida que la tecnología avanza, las versiones de implantes de microchips para humanos aumentan, junto con su seguridad. Algunas versiones son: xDF2, flexDF2 y VivoKey Spark; estas versiones pueden requerir una investigación a cerca de las vulnerabilidades que puedan tener.

En relación al implante xNT, las investigaciones futuras se pueden enmarcar en dos aspectos. El primero, desarrollar un sistema de control de acceso con doble factor de autenticación, que sería el UID y la contraseña. El segundo, obtener la contraseña del implante mediante herramientas especializadas, con el fin de sobre escribir un virus que permita la ejecución de tareas en segundo plano, tomando control del dispositivo lector.

REFERENCIAS

Ali, M. (2014). Biochips. Retrieved from SlideShare website: https://www.slideshare.net/mustahidali90/biochips-31961817

Arduino. (2019). Arduino Uno Rev3. Retrieved from https://store.arduino.cc/usa/arduino-uno-rev3

Bermejo, D. (2017). Así funcionan los microchips implantados para controlar a los trabajadores. Retrieved from El Mundo website: https://www.elmundo.es/f5/comparte/2017/03/09/58c03226e5fdea01398b4595.html

Brewster, T. (2015). Hacker Implants NFC Chip In His Hand To Bypass Security Scans And Exploit Android Phones. Retrieved from Forbes website: https://www.forbes.com/sites/thomasbrewster/2015/04/27/implant-android-attack/#18dc3c681d23

Carballude, A. (2012). *Biohacking*. Universidad Católica "Nuestra Señora de la Asunción," Asunción.

Casero, E. (2013). *Tecnología de identificación por Radio Frecuencia. Lectura de pedidos rfid en un almacén*. Universidad de la Rioja, Logroño.

Coenen, C. (2017). Biohacking: New Do-It-Yourself Practices as Technoscientific Work between Freedom and Necessity. *Proceedings*, *1*(3), 256. https://doi.org/10.3390/IS4SI-2017-04119

Company Public. (2015). *NTAG213/215/216 NFC Forum Type 2 Tag compliant IC with 144/504/888 bytes user memory*.

Cyborg Foundation. (2019). Desing yourself, cyborg art, cyborg rinhts and history. Retrieved from https://www.cyborgfoundation.com/

Danguerous Things. (2019). xNT NFC Chip. Retrieved from https://dangerousthings.com/product/xnt/

Diéguez, A. (2013). Biología sintética, transhumanismo y ciencia bien ordenada. In *Viento Sur* (131st ed., pp. 71–80).

Elechouse. (2015). *PN532 NFC RFID Module User Guide*.

FQ Ingeniería Electrónica. (2014). Estándares y regularizaciones para RFID. Retrieved from https://www.fqingenieria.com/es/conocimiento/estandares-y-regularizaciones-para-rfid-36

Fundación Telefónica. (2017). Biohacking. Conviértete en la mejor versión de ti mismo. *Lo + Visto*, *8*, 20.

Github. (2018). Arduino NFC library using PN532 to read/write card and communicate with android. Retrieved from https://github.com/Seeed-Studio/PN532

Giusto, D. (2018). Seguridad en dispositivos móviles: resumen de lo que fue el 2018. Retrieved from WeLiveSecurity website: https://www.welivesecurity.com/la-es/2018/12/21/seguridad-dispositivos-moviles-resumen-2018/

Hacker Warehouse. (2019). Chameleon Mini RevE reiniciado. Retrieved from https://hackerwarehouse.com/product/chameleon-mini-reve-rebooted/

Játiva, C. (2016). *Estudio de la tecnología de identificación por radiofrecuencia (RFID), sus aplicaciones y la convergencia con el internet de las cosas (IoT)*. Universidad Catòlica de Santiago de Guayaquil, Guayaquil.

Kim, G.-H., Lee, K.-H., Kim, S.-S., & Kim, J.-M. (2013). Vehicle Relay Attack Avoidance Methods Using RF Signal Strength. *Communications and Network*, *05*(03), 573–577.

https://doi.org/10.4236/cn.2013.53B2103
Kulkarni, G., Shelke, R., Sutar, R., & Mohite, S. (2014). RFID security issues and challenges. *2014 International Conference on Electronics and Communication Systems (ICECS)*, 1–4. https://doi.org/10.1109/ECS.2014.6892730
Lab401. (2019). Chameleon Mini: RevE Rebooted. Retrieved from https://lab401.com/products/chameleon-mini-reve-rebooted
Lee, E. (2012). NFC Hacking: The Easy Way. *Blackwing Intelligence*, 1–24. La Vegas: DEFCON 20.
Mendoza, S. (2018). Google Pay-Replay attack. Retrieved from Tpx mix website: https://tpx.mx/blog/2018/google-pay-replay-attack.html
Montero, R. (2017). *Estudio de tecnología de comunicación de campo cercano, NFC*. Universidad Politécnica de Madrid, Madrid.
Narayana Rao, Tv., SukruthiG, S., & Raj, G. (2012). Biochip Technology-A Gigantic Innovation. *International Journal of Emerging Technology and Advanced Engineering*, *2*(3), 129–135.
Oliver, E. (2017). Ocho biohacks que rompen los límites entre el ser humano y la máquina. Retrieved from Digital Trends Español website: https://es.digitaltrends.com/tendencias/ocho-increibles-biohacks/
Pozo, D. (2018). Qué es NFC y cómo saber si mi móvil lo tiene. Retrieved from 20 minutos website: https://www.20minutos.es/noticia/3241971/0/que-es-nfc-movil/
Ramírez, A. (2017). *Diseño e implementación de un prototipo de venta (POS) utilizando tecnología RFID*. Escuela Politécnica Nacional, Quito.
Rojas, A., Bautista, R., & Medina, C. (2016). Pentesting empleando técnicas de ethical hacking en redes IPv6. *Revista Ingenio UFPSO*, *11*, 79–96.
Rojas, E., & Ferney, E. (2015). *Hacking Ético: Una herramienta para la seguridad informática*. Universidad Piloto de Colombia, Bogotà.
Sanchez, G. (2014). *We are Biohackers: Exploring the Collective Identity of the DIYbio Movement*. https://doi.org/10.13140/RG.2.1.4279.9448
Shan, H., & Yuan, J. (2017). Man in the NFC. *Code Blue*, 1–30. Tokio: DEFCON 25.
Tori, C. (2008). *Hacking Ético* (1st ed.). Rosario.
Valencia, N. (2018). UART vs SPI vs I2C | Difference between UART,SPI and I2C. Retrieved from RF Wireless World website: https://www.rfwireless-world.com/Terminology/UART-vs-SPI-vs-I2C.html
Velazquez, L. (2016). Metodología de la investigación. *Investigación, Formación y Desarrollo (PROMETEO)*, 58.
Villavicencio, W., & Mendoza, E. (2015). *Desarrollo de una aplicación informática utilizando la tecnología NFC para Smarphone con sistema Android que permita la selección y facturación de un menù en un restaurante.* Universidad Politecnica Salesiana, Guayaquil.

ANEXOS

ANEXO 1

Estándares y regularizaciones para RFID.

Estándar	Descripción
ISO 14443	Basado en la frecuencia de 13,56 MHz, conocido como el estándar de tarjetas con circuito integrado sin contacto. Tiene dos tipos de etiquetas, el tipo A y el tipo B, diferenciados por el método de modulación, Se divide en cuatro partes: Parte 1: especifica las características físicas Parte 2: especifica la potencia RF y el interface de señal Parte 3: especifica las funciones de inicialización y anticolisión entre chips Parte 4: especifica el protocolo de transmisión
ISO 14223	Sistemas usados en animales. Esta norma es una extensión de los estándares ISO 11784 e ISO 11785.
ISO 15692	Estándar para el intercambio de información entre los sistemas RFID, procesamiento de datos y la presentación en los transpondedores.
ISO 15693	Estándar conocido como el estándar para los transpondedores de vecindad (vicinity cards). La diferencia principal es la distancia de lectura/escritura que este estándar regula llegando a alcanzar 1,5 metros de distancia.
ISO 180000	Estándar que describe las diferentes tecnologías y/o frecuencias para la gestión a nivel de ítem. Las diferentes partes de este estándar, describen la interfaz de comunicación vía aire de estas distintas frecuencias, para establecer los distintos comportamientos físicos. Parte 1: referencia a la arquitectura y definición de los parámetros a estandarizar Parte 2: parámetros para la comunicación en la frecuencia de 135 KHz Parte 3: parámetros para la comunicación en la frecuencia de 13,56 MHz Parte 4: parámetros para la comunicación e la frecuencia de 2,45 GHz Parte 5: parámetros para la comunicación entre la frecuencia de 860 y 960 MHz
ISO 18092	Estándar que describe el intercambio de información sin contacto entre sistemas, conocido como NFC-tipo-1

ISO 18185	Estándar que define el protocolo de comunicación de los sellos electrónicos para los contenedores de transporte de mercancías
ISO 21481	Sistemas de intercambio de información y telecomunicaciones entre sistemas, NFC-tipo-2
EPC UHF	Estandariza los chips RFID pasivos, establece su EPC (Electronic Product Code) en la identificación de los ítems en la cadena de suministro a nivel mundial.
EMV	Especificaciones para los sistemas de pago, que define la arquitectura y requisitos generales, puntos de partida, especificaciones del kernel y el protocolo de comunicaciones. Se basa en la ISO 7816 y la ISO 14443

Fuente: autor. Datos obtenidos de FQ Ingeniería Electrónica, 2014

ANEXO 2

Características de los microchips de la serie NTAG2xx.

	Ntag203	**Ntag210**	**Ntag212**	**Ntag213**	**Ntag215**	**Ntag216**
Memoria	137 bytes	48 bytes	128 bytes	144 bytes	504 bytes	888 bytes
Compatibilidad	Si	Si	Si	Si	Si	Si
Forum NFC T2	Si	Si	Si	Si	Si	Si
Cryptography	No	No	No	No	No	No
Contraseña	No	Si	Si	Si	Si	Si
UID	7 bytes	7 bytes	7 bytes	7 bytes	7 bytes	7 bytes

Fuente: autor. Datos obtenidos de Company Public (2015).

ANEXO 3

Tipos de transpondedores NFC.

Tipo	Descripción
Tipo 1	Se configura como solo lectura y se las puede reescribir, su tamaño va desde los 96 bytes hasta los 2 KB de memoria, con una velocidad de 106 kbits/s, esta no tiene protección contra colisión.
Tipo 2	Similares a las de tipo 1, la diferencia es que si incluyen soporte anticolisión.
Tipo 3	Su memoria varía hasta 1 MB, la velocidad con que se comunica va desde 214 hasta los 424kbits/s
Tipo 4	Similares a las de tipo 1 y 2, vienen configuradas para que sean de lectura, de re-escritura y lectura-escritura, su memoria varía hasta los 32 KB por cada servicio, está diseñado para soportar anticolisiones y posee una velocidad de 106,212 o 424KBits/s
Tipo 5	Estas permiten leer y escribir mensajes en formato NDEF (Data Exchange Format)

Fuente: Autor. Datos obtenidos de Company Public (2015).

ANEXO 4

Script del control de acceso en la plataforma IDE de Arduino UNO

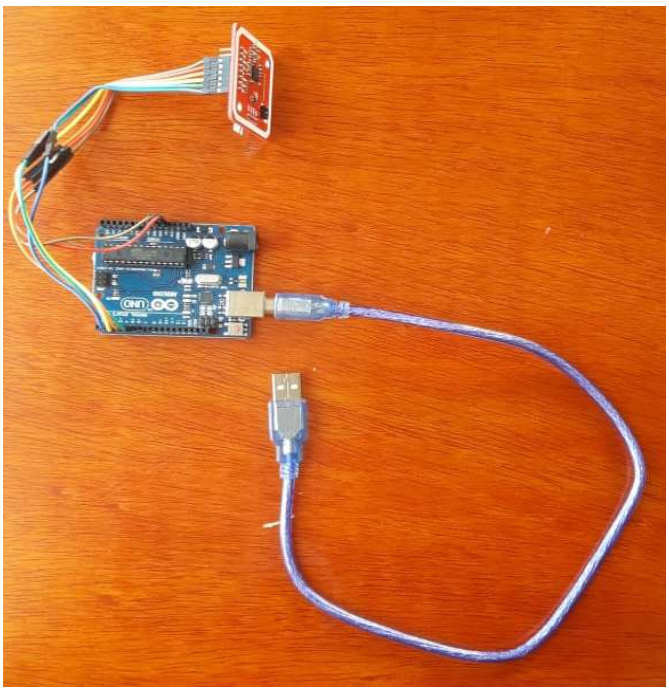
```
// Se tomó como base el ejemplo del software y script del autor Luis LLamas:

//Librerias NFC para leer el implante xNT y establecer el protocolo de comunicación ISP.
#include <Wire.h>
#include <SPI.h>
#include <Adafruit_PN532.h>

// Pines del módulo Arduino, que se usaran para establecer la comunicación ISP con el módulo PN532
#define PN532_SCK (2)
#define PN532_MOSI (3)
#define PN532_SS (4)
#define PN532_MISO (5)

// conexión SPI a nivel de software:
Adafruit_PN532 nfc(PN532_SCK, PN532_MISO, PN532_MOSI, PN532_SS);

void setup(void) {
 //pinMode(7, OUTPUT); //habilita al pin 7 como salida
 //pinMode(8, OUTPUT); //habilita al pin 7 como salida

 Serial.begin(115200);
 Serial.println("UISEK");
 Serial.println("Maestría en Tecnologías de la Información");
 Serial.println("CONTROL DE ACCESO");
 nfc.begin();

 // Detecta si el módulo PN532 está conectado al módulo Arduino
 uint32_t versiondata = nfc.getFirmwareVersion();
 if (! versiondata) {
 Serial.print("No esta conectado el modulo PN532");
 while (1); // detener
 }

//Establecer el número máximo de intentos para leer un UID
//Esto nos impide esperar por siempre una tarjeta, que es el comportamiento por defecto del PN532.
 nfc.setPassiveActivationRetries(0xFF);

// Activa la lectura de tarjetas
```

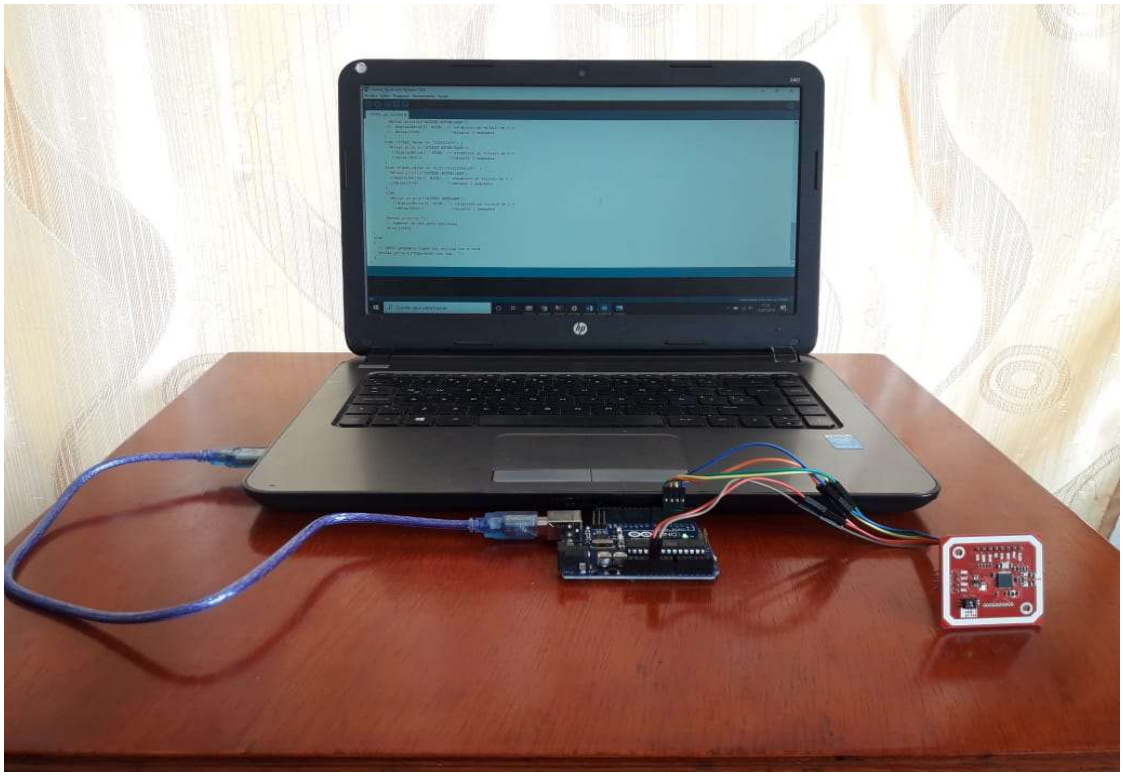
```
 nfc.SAMConfig();
 Serial.println("ACERQUE LA TARJETA AL LECTOR");
}
void loop(void) {
 boolean success;
 uint8_t uid[] = { 0, 0, 0, 0, 0, 0, 0 }; // permite almacenar el UID
 uint8_t uidLength; // Longitud del UID (4 o 7 bytes según el tipo de tarjeta ISO14443A)

// Establece lectura para tarjetas de tipo ISO14443A
// En 'uid' almacena el UID y en "uidLength" indicará si el uid es 4 bytes (Mifare Classic) o 7 bytes
(Mifare Ultralight)

 success = nfc.readPassiveTargetID(PN532_MIFARE_ISO14443A, &uid[0], &uidLength);

 //Lectura de UID de tags
 if (success) {
 Serial.println("Verificacion");
 Serial.print("longitud UID: ");Serial.print(uidLength, DEC);Serial.println(" bytes");
 Serial.print("UID HEXADECIMAL: ");
 String hex_value = "";

 for (uint8_t i=0; i < uidLength; i++)
 {
 Serial.print(" 0x");Serial.print(uid[i], HEX);
 hex_value += (String)uid[i];
 }

 Serial.println(" , UID DECIMAL="+hex_value);

 //Comparación de UID para permitir o denegar acceso
 if(hex_value == "98132130115") {
 Serial.println("ACCESO AUTORIZADO");
 // digitalWrite(7, HIGH); // establece un voltaje de 5 v
 // delay(3000); //durante 3 segundos
 }
 else if(hex_value == "230522426") {
 Serial.println("ACCESO AUTORIZADO");
 //digitalWrite(7, HIGH); // establece un voltaje de 5 v
 //delay(3000); //durante 3 segundos
 }
 else if(hex_value == "41311761825556129") {
 Serial.println("ACCESO AUTORIZADO");
 //digitalWrite(7, HIGH); // establece un voltaje de 5 v
 //delay(3000); //durante 3 segundos
 }
 else
```

```
 Serial.println("ACCESO DENEGADO");
 //digitalWrite(8, HIGH); // establece un voltaje de 5 v
 //delay(3000); //durante 3 segundos
 Serial.println("");
 // Esperar un seg para continuar
 delay(1000);
 }
 else
 {
 // PN532 probably timed out waiting for a card
 Serial.println("Esperando una tag...");
 }
}
```

ANEXO 5

Fotografías del proyecto






Fabian Aguinsaca
SAMSUNG
DANGEROUS
13.56MHz RFID Field Detector
Use this field detector with any 13.56MHz reader to find the best performing location and orientation for your x-series transponder.


SAMSUNG
DANGEROUS
13.56MHz RFID Field Detector
Use this field detector with any 13.56MHz reader to find the best performing location and orientation for your x-series transponder.


SAMSUNG
DANGEROUS
THINGS
13.56MHz RFID Field Detector
Use this field detector with any 13.56MHz reader to find the best performing location and orientation for your x-series transponder.