UNIVERSITAT POLITÈCNICA DE VALÈNCIA

_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería de Telecomunicación

ESTUDIO DE LA SEGURIDAD EN TARJETAS NFC

Trabajo Fin de Grado

Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación

AUTOR/A: Peris Duque, Alejandro

Tutor/a: López Patiño, José Enrique

CURSO ACADÉMICO: 2021/2022

Agradecimientos

En primer lugar, me gustaría dar las gracias a mis padres, mis abuelos y mi hermana por el apoyo que he recibido por su parte durante estos duros años, sin el cuál no habría podido llegar hasta aquí.

Por supuesto, agradecer a José Enrique, mi tutor, su ayuda brindada en la realización de este proyecto.

Resumen

Este trabajo trata sobre la tecnología de las tarjetas NFC enfocándose principalmente en su fiabilidad y solidez frente a amenazas como la duplicación.

En el proyecto se compromete la seguridad de las tarjetas mediante la realización de duplicados. Estos son realizados copiando tarjetas NFC originales en llaveros reescribibles RFID, empleando dispositivos electrónicos de lectura/escritura que pueden ser obtenidos de manera sencilla y asequible.

En este estudio se pretende analizar la facilidad con la que se puede superar la seguridad de estas tarjetas y observar las prestaciones que ofrecen sus duplicados.

Abstract

This work is round to the technology of NFC targets focusing on the reliability and strength against threats like duplicity.

In this project, cards security is compromised via duping usability. Those are realized by copying original NFC targets to rewritable RFID key chains, employing electronic devices of lecturing/writing that may be obtained in a simple and affordable manner.

This study pretends to analyse how easy its security might be overtaken as well as observing the main benefits this duplicates provides.

Índice de contenidos

Índice de figuras

Índice de tablas

Introducción

En nuestra vida diaria utilizamos regularmente tarjetas con tecnología NFC, ya sea en nuestros hogares, al usar transporte público o al identificarnos en el trabajo. Un claro ejemplo de este uso son los bonometros, bonobuses y tarjetas identificativas para determinados espacios tanto públicos como privados.

El uso de la tecnología NFC se ha propagado ampliamente principalmente por su fácil utilidad, sin embargo, en contraposición a su sencillo uso, existe una amplia variedad de tipos de dispositivos NFC y modos de funcionamiento.

Las tarjetas NFC poseen criptografía que les dota de seguridad para proteger la información que contienen o la información a la que se puede acceder mediante su uso. La intención de obtener, modificar o suprimir dicha información por parte de un tercero, puede realizarse mediante varios tipos de ataques según el propósito de este y la situación.

En el trabajo realizado estudiamos algunos de los posibles ataques que se pueden realizar sobre las tarjetas centrándonos principalmente sobre la clonación de tarjetas en otras tarjetas NFC o llaveros RFID reescribibles. Para poder estudiar este ataque, lo reproducimos sobre diferentes tarjetas y comprobamos el funcionamiento de los duplicados, si podrían suplantar a la tarjeta original en su función.

1. Tecnología NFC

NFC (near-field communication) es una tecnología de comunicación inalámbrica de alta frecuencia que permite la conexión entre dispositivos con el objetivo de autenticarse o de intercambiar información. Tiene su origen en 2002 cuando se unieron las compañías con tecnología Contactless Sony (FeliCa) y Philips (Miafare) para conseguir un protocolo compatible con dichas tecnologías. También se creo en 2004 una asociación para fomentar el uso del NFC y estipular las especificaciones de estos dispositivos y sus protocolos, se conoce como 'Foro NFC'.

Deriva de RFID (Radio-Frequency Identification) y utiliza etiquetas RFID que pueden recibir o transmitir información mediante ondas de radio, las cuales tienen una capacidad de almacenaje que varía entre 96 y 512 bytes. NFC se encuentra, dentro del espectro de radiofrecuencia, en la banda de 13.56 MHz, que no requiere de licencia para su uso.

Si bien esta tecnología dimana de RFIFD, tiene sus diferencias. La tecnología RFID tiene un mayor alcance, llegando a poder establecer la comunicación a varios metros de distancia, por lo que dota de una comunicación menos privada y cercana que NFC, la cuál además es más rápida, fácil y automática.

La potencia de esta tecnología es muy limitada y como consecuencia tiene un alcance reducido, de aproximadamente 20 cm. Tiene una tasa de transferencia de 424 kbit/s, por lo que la velocidad de comunicación es prácticamente instantánea. Otra característica es que un dispositivo puede enviar y recibir información simultáneamente, además de que a diferencia del bluetooth, no hace falta un emparejamiento previo entre los dispositivos que van a realizar la conexión.

1.1 Principales utilidades

NFC ha sido cada vez más utilizada durante esta década y actualmente está muy presente en nuestro día a día. A continuación se muestran algunos usos:

- **Identificación**: En controles de acceso tanto en sector público como privado. Ejemplos: Transporte público, universidades, empresas, conciertos, eventos deportivos, …

- **Autentificación**: Comprueba la autenticidad de personas o productos para evitar fraudes y falsificaciones. Ejemplo: Al pagar con tarjeta de crédito acercándola al datáfono, este la detecta y la autentifica para poder aceptarla.

- **Pago desde el teléfono móvil**: Todos los Smartphones de lanzamiento reciente disponen de la utilidad NFC, con ellos se puede pagar de la misma forma que con una tarjeta, acercando el teléfono al datáfono.

- **Facilitar información**: Mediante el contacto del teléfono con una etiqueta NFC, puedes recibir automáticamente un documento, dosier, imagen, … para una campaña, carta de un restaurante u otras situaciones.

- **Internet de las cosas (IOT)**: Automatizar acciones como encender las luces, cerraduras electrónicas y demás, todo ello mediante el uso de etiquetas NFC.

1.2 Características favorables

Las mayores ventajas de la tecnología NFC son la velocidad con la que dota a sus dispositivos, agilizando procesos de nuestro a día, junto a su versatilidad; es adaptable a gran cantidad de formas: tarjetas, llaveros, pulseras, presente en smartphones.

Además son tecnologías fáciles de usar, simplemente debes acercar un microchip a un lector para que puedan establecer conexión y realizar las gestiones necesarias.

Hay aplicaciones gratuitas descargables en la Play Store del teléfono que permiten escribir o programar tareas en etiquetas NFC y otros chips NFC de manera guiada. Un ejemplo sería NFC Tools, donde puedes realizar una lectura o escritura de una etiqueta NFC.

Figura 1. Icono de la aplicación NFC Tools

2. Funcionamiento de la tecnología NFC

Al igual que la tecnología RFID de la que proviene, NFC intercambia información mediante ondas de radiofrecuencia. Para ello requiere de diferentes elementos que pueden ser clasificados según estándares u organizaciones como es el Foro NFC. Además aparecen varios modos de funcionamiento según la situación, el propósito de la acción o los dispositivos que intervengan.

Encontramos tres modos distintos de funcionamiento, el primero es el de modo lectura/escritura (read/write), el segundo es el modo Peer to Peer y por último el emulador de tarjetas por parte de un smartphone.

Actualmente unos de los dispositivos más importantes son los Smartphones, que desde hace varios años llevan integrada esta tecnología y es usada diariamente ya sea como tarjeta de crédito, como tarjeta identificativa o para dispositivos IoT.

2.1 Elementos en un proceso NFC

- **Etiqueta NFC:** Se componen del chip con la información y la antena para comunicarse.

- **Lector:** Dispositivo con capacidad de establecer conexión con la etiqueta para proceder a la gestión necesaria.

- **Software:** Programa que recibe información del lector y decide la gestión requerida en cada caso.

2.2 Tipos de etiquetas NFC

Según el Foro NFC, encontramos seis tipos de etiquetas NFC. Cada una de ellas tiene diferentes características que las destinan a distintos fines. Las características de estas etiquetas son las siguientes:

- **Tipo 1:**

  · Son económicas y versátiles, se derivan de MIAFARE Ultraligth.

  · Se basan en el estándar **ISO-14443A**.

  · Pueden ser leídas, reescritas (modificables) o designadas como modo de 'solo lectura'.

  · 96 B de memoria que pueden ser ampliados hasta 2KB.

  · Tienen una velocidad de transferencia que alcanza los 106 kbits/s.

- **Tipo 2**

  · Mismas características que el Tipo 1 salvo que en este caso sí que disponen de soporte para la protección de conflictos de datos.

- **Tipo 3**

  · Son más caras que las dos etiquetas anteriores, convenientes para usos más complejos. Vienen de FeliCa (Sony).

  · Pueden ser leídas, reescritas (modificables) o designadas como modo de 'solo lectura'.

  · La memoria puede alcanzar hasta 1 MB.

  · Capacidad de alcanzar dos velocidades de transferencia distintas, 212 kbits/s o 424 kbit/s.

  · Ofrecen protección en conflicto de datos.

- **Tipo 4**

· Semejantes al tipo 1, mismo estándar.

· Puede ser leídas, reescritas (modificables) o designadas como modo de 'solo lectura'.

· La memoria puede alcanzar hasta 32 kB.

· Capacidad de alcanzar tres velocidades de transferencia distintas 106 kbits/s, 212 kbits/s o 424 kbits/s.

· Ofrecen protección en conflicto de datos.

- **Tipo 5**

· Basadas en estándar **ISO-15693**.

· Puede ser leídas y reescritas (modificables).

· Disponen de diferentes capacidades de memoria: 256 bits, 896 bits, 1280 bits o 2528 bits.

· Tienen una velocidad de transferencia que alcanza los 53 kbits/s.

· Ofrecen protección en conflicto de datos.

- **Tipo 6**

· Basadas en estándar **ISO-14443A**, solo compatibles con ciertos teléfonos móviles.

· Pueden ser leídas y reescritas (modificables).

· Disponen de diferentes capacidades de memoria de 1kB o 4 kB.

· Tienen una velocidad de transferencia que alcanza los 106 kbits/s.

· Ofrecen protección en conflicto de datos.

Además de los tipos definidos por el Foro NFC, las etiquetas NFC pueden ser pasivas o activas. Si son pasivas disponen de un microchip y de una antena, pero si son activas, dispondrían además de una alimentación eléctrica propia con la que podrán crear un campo electromagnético.

2.3 Modos de funcionamiento NFC

Como mencionamos anteriormente, existen tres tipos distintos de comunicaciones NFC:

- **Modo lectura/escritura (read/write):**

Consiste en la comunicación entre un dispositivo NFC y una etiqueta NFC, ya sea para modificar los datos existentes en la etiqueta o para leerlos.

Hay definidos protocolos de bajo nivel que regulan la implementación y facilitan que las estructuras NFC se conecten, exponiendo las condiciones de sendos dispositivos; estos serían los estándares **NFCIP-1** Y **NFCIP-2.**

Las especificaciones de bajo nivel cubren el protocolo de transmisión e incluyen codificación de bit, se comprenden 3 partes:

· NFC-A: Hace referencia al estándar **ISO-14443A**.

· NFC-B: Hace referencia al estándar **ISO-14443B**.

· NFC-C: Hace referencia al estándar FeliCa JIS X 6319-4 (incorporado en **ISO-18092**).

Para escribir información en una etiqueta NFC, el dato se encapsula en un mensaje NDEF (NFC Data Exchange Format), el mensaje se envía y se guarda en la memoria de la etiqueta NFC. Al transmitir el mensaje, puede enviarse en 1 solo mensaje NDEF o en varios mensajes divididos, que pueden contener payload.

Un ejemplo de este tipo, en modo lectura, sería la tarjeta de la UPV. En la imagen podemos apreciar la tarjeta, el lector y el software.

Figura 2. Ejemplo de la Tarjeta UPV

- **Modo Peer-To-Peer:**

  Consiste en la comunicación entre dos dispositivos NFC que generan campo electromagnético, es decir, que disponen de etiquetas NFC activas. El intercambio de información se realiza de manera bidireccional pero es half-duplex, es decir, cuando uno emite el otro escucha y viceversa. A continuación, se muestra un esquema de este tipo de comunicación entre dos móviles NFC.

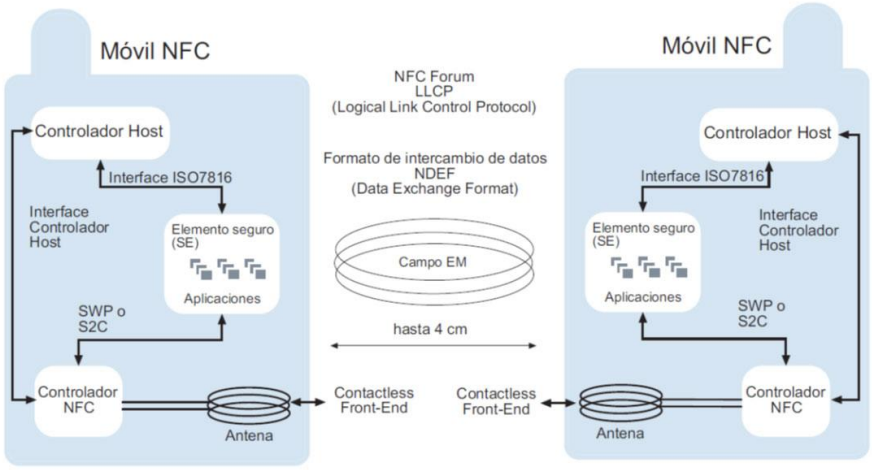

Figura 3. Intercambio de información entre 2 móviles NFC

Al igual que en el modo anterior, utiliza el estándar **NFCIP-1** para el protocolo de transporte. En este caso, ambos dispositivos son definidos antes de la conexión. A nivel superior se intercambia información mediante NDEF, a nivel inferior con **LLCP**.

- **Modo emulación de tarjeta:**

Un teléfono con tecnología NFC actúa como una tarjeta inteligente. El esquema de este proceso sería el siguiente:

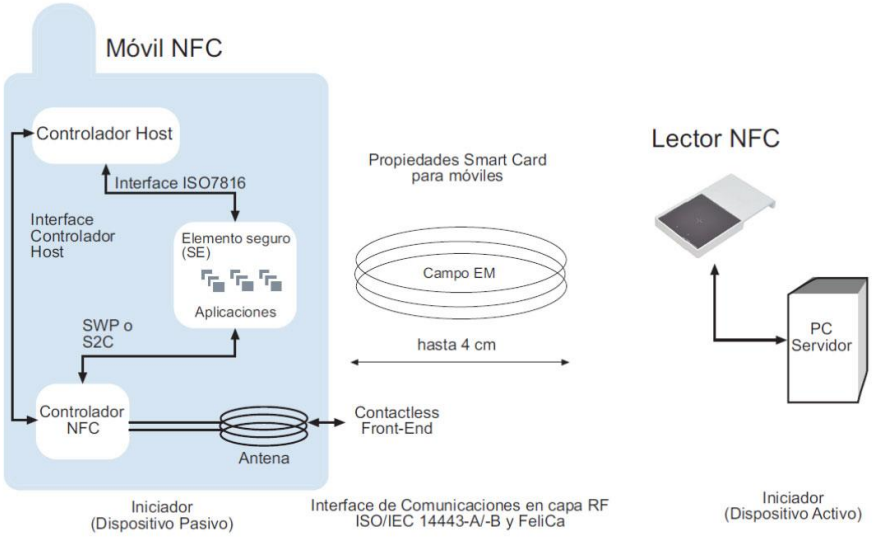

Figura 4. Móvil con NFC emulando Tarjeta Inteligente

El móvil NFC que actúa como tarjeta, utiliza a nivel físico los mismos protocolos que las tarjetas inteligentes. El dispositivo se conecta con las aplicaciones del chip NFC de la tarjeta inteligente que se conocen como elemento seguro (SE), que es el encargado de efectuar la emulación. También se puede realizar mediante una SIM especial que soporte el protocolo **SWP**.

El SE está protegido y necesita permiso del fabricante del sistema operativo del smartphone para tener acceso. Si realizamos la emulación con SIM, el permiso requerido es el del operador.

2.4 Arquitectura NFC en smartphone

La estructura de un móvil NFC, se podría definir con el siguiente esquema:

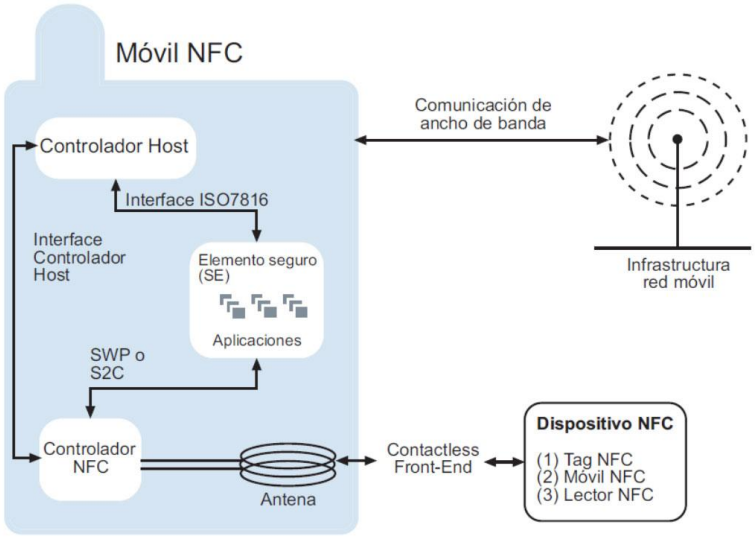

Figura 5. Móvil con NFC

El elemento seguro (SE) se conecta al controlador NFC para asegurar las comunicaciones con el dispositivo NFC, el protocolo de intercambio de datos entre estos es el **SWP**. El SE es controlado por el Controlador Host, que también controla el Controlador NFC mediante el Interface Controlador Host. Además del Controlador NFC, requiere una antena y NFC Contactless Front-End (NFC CLF).

3. Tarjetas NFC

La manera más corriente de encontrar esta tecnología son las tarjetas NFC, ya sea en el transporte público (bonometro, bonobús), tarjetas identificativas (empresas, universidades) o tarjetas de crédito.

3.1 Estructura de una tarjeta NFC

Estas tarjetas utilizan etiquetas de NFC pasivas, es decir, disponen de un chip que contiene la información y una antena. Corresponden al modo lectura/escritura, mayoritariamente al modo de lectura, que se usa para la identificación.

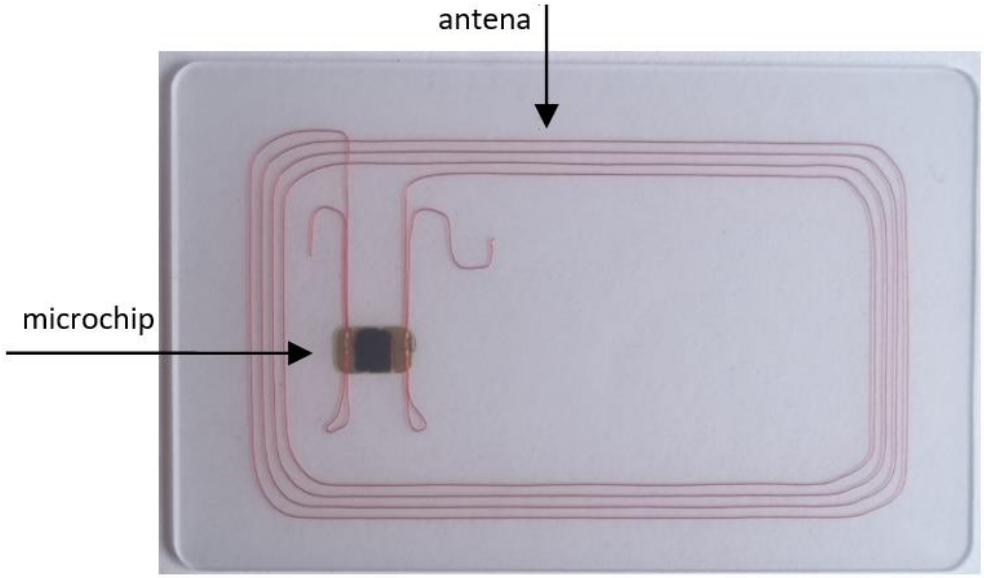

Figura 6. Tarjeta NFC

3.2 Series de tarjetas NFC

Las tarjetas se clasifican en distintas series según las características técnicas de sus etiquetas NFC y a su vez dentro de cada serie se dividen en subtipos.

Una de las principales series es la NTGA cuyos modelos mostramos en las siguientes tablas:

	NTGA203	NTGA210	NTGA212
Memoria total	168 bytes	80 bytes	164 bytes
Memoria disponible	137 bytes	48 bytes	128 bytes
Capacidad retención de datos	5 años	10 años	10 años
Ciclos de Resistencia lectura/escritura	10.000 ciclos	100.000 ciclos	100.000 ciclos
Ventajas	Sustituido por NTGA213	Precio muy bajo, ideal para códigos o URLs cortas	Poco común pero con más memoria que los anteriores.

Tabla 1. NTGA203, NTGA210 y NTGA212

	NTGA213	NTGA215	NTGA216
Memoria total	180 bytes	540 bytes	924 bytes
Memoria disponible	144 bytes	504 bytes	888 bytes
Capacidad retención de datos	10 años	10 años	10 años
Ciclos de resistencia lectura/escritura	100.000 ciclos	100.000 ciclos	100.000 ciclos
Ventajas	Es el chip más versátil	Memoria alta y barato	Más avanzado y con mayor memoria

Tabla 2. NTGA213, NTGA215 y NTGA216

Las etiquetas de la serie NTAG son compatibles con todos los móviles equipados con NFC, dentro de la cuál la clase más difundida es la NTGA213 debido a su versatilidad.

Además de la serie NTAG, también encontramos la serie MIAFARE, una de las series de tarjetas NFC más utilizadas.

	MIAFARE CLASSIC 1K EV1	MIAFARE CLASSIC 4K	MIAFARE ULTRALIGTH EV1
Memoria total	1024 bytes	4048 bytes	64 bytes
Memoria disponible	716 bytes	3440 bytes	46 bytes
Encriptación	Sí	Sí	No
Longitud del texto	709 caracteres	3000 caracteres	39 caracteres
Ventajas	Protocolo Mifare y gran capacidad	Protocolo Mifare y gran capacidad	Recomendada para usos de poca memoria, barata.

Tabla 3. MIAFARE CLASSIC 1K EV, CLASSIC 4K y ULTRALIGTH EV1

Las tarjetas MIAFARE son las más utilizadas en el mundo debido a que su tecnología es económica y rápida, se suelen usar de manera desechable. Tienen una capacidad de cómputo limitada que les impide realizar operaciones criptográficas de autentificación a alto nivel, por lo que se le dan usos más simples como identificación en puntos de controles de acceso. Las podemos encontrar en el transporte público de Valencia en la llamada 'Tarjeta APUNT', también en la tarjeta UPV o tarjeta TUI (Tarjeta Universitaria Inteligente) que utiliza el sistema MIAFARE.

4. Seguridad

La tecnología NFC se utiliza en campos muy sensibles como en el pago con tarjetas de crédito o de móviles emulando tarjetas de crédito, también de identificación para acceder a determinados lugares de empresas de donde pueden obtener información comprometida de esta. Por ello, el tema de la seguridad en este campo es de suma importancia y un relevante objeto de estudio.

4.1 Seguridad en tarjetas Miafare Classic

Principalmente distinguimos entre dos tipos de tarjetas Miafare Classic, por un lado, la 1K que tiene 1024 bytes de almacenamiento que se dividen en 16 sectores, por otro lado, la 4 K que tiene 4096 bytes que se dividen en 40 sectores.

La tarjeta Miafare Classic 1K de 1024 B se divide en 16 sectores y estos a su vez se subdividen en 4 bloques de los cuáles tres llevan información del usuario y el cuarto puede ser modificado por comandos para configurar su lectura, incremento, …; este último bloque de cada sector es conocido como 'Sector Trailer'.

Cada bloque se protege con 2 claves distintas llamadas A y B, en el sector están escritas estas claves en 16 bytes que están reservados tanto para estas claves como los permisos de los que puede disponer: lectura, escritura, incremento o descuento. La clave A (6 B) no puede ser leída pero la clave B (6 B) sí que puede ser configurada para ello. Los 16 bytes reservados se encuentran en el Sector Trailer y se dividen de la siguiente forma:

- Desde el byte 0 al byte 5 se encuentra la clave A
- Desde el byte 6 al byte 9 se encuentran los permisos
- Desde el byte 10 al byte 15 se encuentra la clave B

También encontramos otros bytes en cada sector que son reservados además de los mencionados anteriormente, los 16 primeros. Se utilizan para portar la información del fabricante, el identificador único de la tarjeta (UID) y el Block Check Character (BCC), que se adhiere a la comunicación para facilitar la detección de errores.

La tarjeta Miafare Classic 4K de 4096 B se divide en 40 sectores, los 32 primeros se componen de la misma manera que los bloques de la tarjeta 1K, pero los 8 restantes cuadriplican el tamaño de estos. Se protege con las claves A y B de la misma manera que la tarjeta 1 K.

Cuando la tarjeta es detectada por el lector, comienza a establecer una comunicación cifrada para evitar que un tercero pueda escuchar del canal. Una vez establecido el canal, la tarjeta envía un código de identificación que suele ser el número de serie de la tarjeta aunque puede ser aleatorio. Este código permite la conexión con el lector y que se puedan realizar las gestiones necesarias.

Las tarjetas Miafare Classic tienen como protocolo de seguridad el algoritmo Crypto1, que fue creado para estas etiquetas por la compañía NXP Semiconductors**.** Este algoritmo es un cifrado de flujo, es decir, divide el texto plano en bloques muy pequeños, de 1 B o menos, y utiliza una clave de cifrado distinta para cada uno. La estructura de este cifrador sería la siguiente:

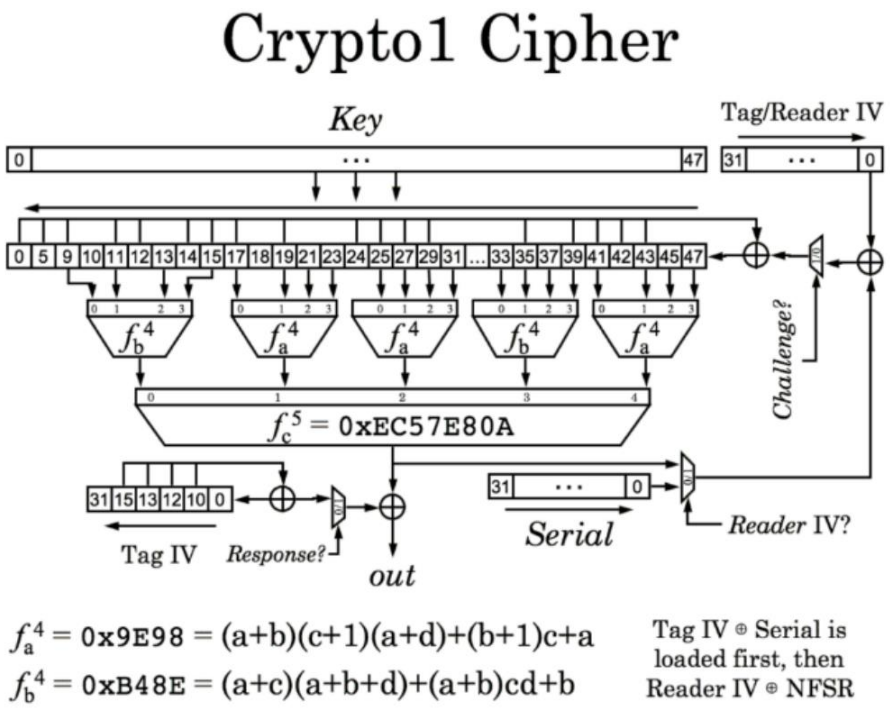

Figura 7. Esquema Crypto-1

El cifrado Crypto-1 está formado por una función no lineal y por un LFSR (Linear Feedback Shift Register) de 48 bits con el polinomio generador (1).

$$x^{48} + x^{43} + x^{39} + x^{38} + x^{36} + x^{34} + x^{33} + x^{31} + x^{29} + x^{24} + x^{23} + x^{21} + x^{19} + x^{13} + x^{9} + x^{7} + x^{6} + x^{5} + 1$$

(1)

Por cada ciclo de reloj pasan 20 bits del LFSR por la función filtro (f_c) generado un bit de la clave. Después el LFSR corre 1 bit a la izquierda y realiza el mismo proceso. La función filtro es la que podemos observar en la ecuación (2).

$$f(x_0 x_1 x_2 \dots x_{47}) = f_c(f_a(x_9, x_{11}, x_{13}, x_{15}),\ f_b(x_{17}, x_{19}, x_{21}, x_{23}),\ f_a(x_{33}, x_{35}, x_{37}, x_{39}), f_b(x_{41}, x_{43}, x_{45}, x_{47}))$$

(2)

Los bits de clave obtenidos se combinan con la información en texto plano para formar el texto cifrado para la comunicación. Este cifrado es el que utilizan las tarjetas Miafare Classic, tanto 1K como 4K, como protocolo de Seguridad.

Uno de los principales pilares en los que se basaba este algoritmo criptográfico es el de 'seguridad por oscuridad', es decir, ocultar la implementación del algoritmo para dotarlo de mayor seguridad. Lo cuál atenta contra uno de los **Principios de Kerckhoffs**, en concreto contra el segundo principio: 'La efectividad del sistema no debe depender de que su diseño permanezca en secreto'.

4.2 Seguridad en tarjetas de crédito con chip NFC

Las tarjetas de crédito son usadas diariamente por gran parte de la población, dichas tarjetas originalmente funcionaban únicamente con la banda magnética, pero esta era fácil de clonar y de llevarse acabo el fraude. Para solucionar este problema se le añadió la tecnología EMV, llamada así por las compañías que la desarrollaron, Europay MasterCard VISA.

Esta tecnología ha sido muy eficaz para solventar el problema del fraude. En Francia comenzaron a implantar el chip EMV en las tarjetas en 2005 provocando una reducción drástica de los delitos de fraudulencia, en 2012 se realizó en Inglaterra con el mismo resultado. Debido a los buenos resultados ofrecidos, fue utilizada en masa a nivel mundial y aceptada por todos los cajeros.

Las tarjetas con EMV son considerablemente más difíciles de clonar que las tarjetas que solo funcionan con banda magnética. Cuando el chip recibe una solicitud de un datáfono genera una clave de uso único, por lo que aunque descubrieran la clave, ya no podrían usarla. Las transacciones se realizan con este cifrado de clave y código PIN, aunque en España, si son menores de 20 €, no es necesario el PIN.

Los datos de una tarjeta NFC pueden ser robados, pero al necesitarse claves emitidas por el banco, se puede averiguar fácilmente el origen de una estafa para investigarle. La criptografía está fundamentada en la idea de clave privada, no podrían realizar una estafa porque no tienen el código correcto.

El estándar EMV define la conexión ente tarjetas y datáfonos a nivel eléctrico, físico, información y aplicación. El aumento de protección que aporta se debe al uso de uno de los siguientes algoritmos:

- **RSA**
- **SHA**
- **DES**
- **Triple DES**

4.2.1 Comandos de la tecnología EMV

Durante la conexión entre la tarjeta y el dispositivo se pueden realizar distintos comandos sobre la transmisión, cuyo protocolo se define en el estándar **ISO-7816**, donde los datos son intercambiados en Unidades de Protocolo de Aplicación. Los comandos que pueden ser utilizados son los siguientes:

- Bloqueo o Desbloqueo de aplicación
- Bloqueo de tarjeta
- Autenticación interna o externa
- Generación de criptograma de aplicación
- Obtención datos u opciones de procesamiento
- Cambio o Desbloqueo de PIN.
- Lectura de registro
- Seleccionar
- Verificar

4.2.2 Esquema de una transacción EMV

Una transacción EMV es un proceso que consta de los pasos que se exponen a continuación:

1. **Selección de Aplicaciones**

Se utilizan Identificadores de Aplicación (AID) para poder identificar una aplicación en la tarjeta que posteriormente es impresa en el recibo EMV. Un AID se basa en un Registro de Proveedores de Aplicaciones (RID) de 5 B y en una extensión conocida como Identificador de Aplicación (PIX). En la siguiente tabla se puede observar como se forman los AID de distintos tipos de tarjetas de crédito y sus subtipos.

Card scheme	RID	Product	PIX	AID
Visa	A000000003	Visa credit or debit	1010	A0000000031010
		Visa Electron	2010	A0000000032010
		V PAY	2020	A0000000032020
		Plus	8010	A0000000038010
MasterCard	A000000004	MasterCard credit or debit	1010	A0000000041010
		MasterCard[2]	9999	A0000000049999
		Maestro (debit card)	3060	A0000000043060
		Cirrus (interbank network) ATM card only	6000	A0000000046000
MasterCard	A000000005	Maestro UK (formerly branded as Switch)	0001	A0000000050001
American Express	A000000025	American Express	01	A00000002501
LINK (UK) ATM network	A000000029	ATM card	1010	A0000000291010
CB (France)	A000000042	CB (Credit or Debit card)	1010	A0000000421010
		CB (Debit card only)	2010	A0000000422010
JCB	A000000065	Japan Credit Bureau	1010	A0000000651010
Dankort (Denmark)	A000000121	Debit card	1010	A0000001211010
CoGeBan (Italy)	A000000141	PagoBANCOMAT	0001	A0000001410001
Diners Club/Discover	A000000152	Diners Club/Discover	3010	A0000001523010
Banrisul (Brazil)	A000000154	Banricompras Debito	4442	A0000001544442
SPAN2 (Saudi Arabia)	A000000228	SPAN	1010	A00000022820101010
Interac (Canada)	A000000277	Debit card	1010	A0000002771010
Discover	A000000324	ZIP	1010	A0000003241010

Figura 8. Tabla de AIDs

2. Inicio de Proceso de Aplicación

El dispositivo envía a la tarjeta el comando 'obtención de datos de procesamiento' y le envía los datos necesarios. La tarjeta como respuesta, le manda el Perfil de Intercambio de la Aplicación (AIP) y el Localizador de Expediente de Solicitud (AFL). El AIP informa de una lista de funciones que deben realizar en la transacción, el AFL facilita registros y archivos.

3. Leer Datos de Aplicación

En la AFL se encuentra la información del chip EMV, que puede ser leída por el terminal con el comando de 'Lectura'.

4. Restricciones de Procesamiento

En este paso se comprueba si la tarjeta es utilizable, para ello el terminal revisa estos elementos:

- Versión de la aplicación
- Uso de la tarjeta
- Fecha de caducidad

En caso de que alguno de los siguientes parámetros sea erróneo, se modifica el bit en los Resultados de la Verificación de Terminal (TVR) para dejar constancia del error y generalmente la tarjeta es rechazada.

5. Autenticación de Datos sin Conexión

El terminal valida la autenticidad de la tarjeta con **criptografía de clave pública**. Para ello existen varios métodos según la situación, son los siguientes:

- **Autenticación de Datos Estática (SDA):** Comprueba que los datos de la tarjeta han sido firmados por la entidad que emitió la tarjeta y que posteriormente no han sido modificados. No evita la clonación de la tarjeta.

- **Autenticación de Datos Dinámica (DDA):** Misma comprobación que la anterior pero además impide la clonación de la tarjeta. Utiliza firma diferente en cada transacción (firma dinámica).

- **Autenticación de Datos Combinada (CDA):** Combina los dos métodos anteriores ofreciendo más seguridad.

6. Verificación Titular

Comprobación de la legitimidad del titular la tarjeta. Para ello el terminal elige entre una lista con varios métodos de autentificar al titular. Entre ellos destaca la firma y el PIN.

7. Gestión de Riesgos del Terminal

Se estudia si la operación es autorizada en línea o fuera de línea y el resultado se plasma en el TVR.

8. Análisis de la Acción Terminal

Según los resultados de las anteriores etapas, se decide si la transacción será aprobada fuera de línea o en línea. Para ello se comprueban el Código de Acción de Terminales (TAC) y el Código de acción del emisor (TAC).

9. Análisis Primera Acción de la Tarjeta

Durante el paso 3 (Lectura) se lee el objeto CDOL1 que contiene unas etiquetas que envía al dispositivo. El terminal devuelve estos datos y pide un criptograma con el comando 'Generación de Criptograma de Aplicación', solicita uno de los siguientes:

- Certificado de Transacción (TC)
- Autorización de Solicitud de Autorización del Criptograma (ARQC)
- Aplicación de Autenticación Criptograma (ACC)

10. Autorización de la Transacción en Línea

El terminal solicita una ARQC y la tarjeta lo envía en su mensaje de autorización tras crearlo mediante una firma digital. El dispositivo responde a este mensaje con la respuesta, una lista de comandos y un criptograma de respuesta.

11. Segunda Acción de Análisis de Tarjeta

El dispositivo envía de manera cifrada CDOL2 (lista de etiquetas) indicando su respuesta para que la tarjeta pueda reajustar sus parámetros.

12. Procesamiento del Emisor

Por último, si el dispositivo quiere realizar modificaciones en la conexión, envía comandos cifrados para cambiar parámetros de la tarjeta o realizar acciones como bloquearla o desbloquearla.

5. Ataques sobre tarjetas NFC

Como hemos visto anteriormente, las tarjetas NFC son muy utilizadas mundialmente y en numerosos campos, por ello son objeto de distintos ataques.

5.1. Tipos de ataques

Existen diversos tipos de ataques a las tarjetas NFC según el objetivo del atacante o la forma de la que se quiera corromper la conexión o información a transmitir:

- **Escuchar la transmisión o Eavesdropping:**

  La tecnología NFC realiza conexiones a una distancia muy cercana, algunos decímetros, aun así es posible escuchar la señal que se transmite para obtener información de ella.

  Ese tipo de ataque puede ser tanto pasivo (de hasta 18 m de distancia), si solo escucha la conversación entre un dispositivo y la tarjeta NFC o uno activo (de hasta 50 cm) si es entre la tarjeta y un dispositivo que pertenezca al atacante.

  Un ejemplo de activo sería el siguiente. en las tarjetas de crédito con tecnología NFC y chip EMV, encontramos este problema ya que EMV no realiza la autenticación al lector. Por lo que al conectarse con un dispositivo que tenga el protocolo de las tarjetas NFC (el cuál es público en internet) y le manda la siguiente información:

  · Nombre del titular
  · Número de tarjeta
  · Fecha de expiración
  · Historial de transacciones realizadas recientemente

  Con los 3 primeros datos de los expuestos anteriormente, es posible realizar compras en varios negocios americanos por internet.

- **Modificación de datos:**

Este ataque puede ocurrir de dos maneras distintas según como se realice, la primera sería usar un dispositivo que permita leer la tarjeta y mostrar la información que se encuentra en sus sectores. Una vez tenemos dicha información, reescribimos el campo que necesitemos. Por ejemplo en caso de tener una tarjeta con viajes del bonobús, podemos modificar el campo que corresponde al número de viajes disponibles.

La segunda forma es modificar los datos que se intercambian entre la tarjeta NFC y un lector. Para ello se inhibe por un momento la comunicación para poder alterar la codificación binaria con el objetivo de corromper la información o cambiar los valores de esta.

En este caso, no se añaden más datos de los que hay, sino que se modifican los ya existentes, es decir, no se le integra ningún campo, solo se cambia el valor de uno de los campos existentes.

- **Denegación de servicio (DoS):**

En este tipo de ataque no es necesario que el atacante acceda a los datos que se transmiten, lo que hace es corromper la comunicación con señales de radio que al mezclarse con las señales originales se convierten en ruido. De esta forma o bien el receptor de los datos no puede descifrar los datos enviados o al descifrarlos carecen de sentido.

La medida que toman los dispositivos NFC para evitar este ataque es verificar la señal de radiofrecuencia durante la transmisión para evitar la filtración de señales.

- **Man in the middle:**

El atacante se sitúa entre el lector y la tarjeta, haciendo creer al lector que es el propietario de la tarjeta NFC que participa en la comunicación. En este caso, el delincuente puede escuchar la comunicación o modificarla de manera más sencilla.

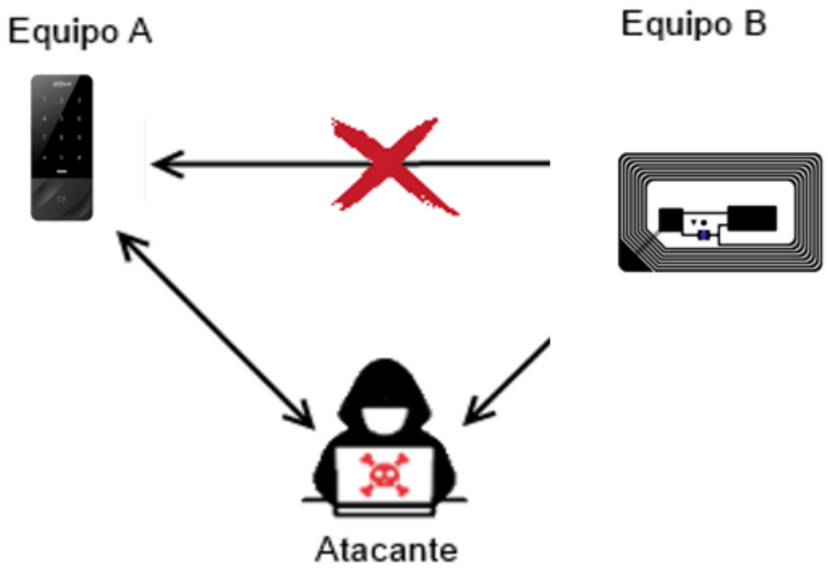

Figura 9. Esquema del ataque Man in the Middle

Como se puede apreciar en el anterior esquema, el atacante se sitúa entre la tarjeta y el lector, Actúa como la tarjeta ante el lector original y como lector ante la tarjeta original, por lo que debe poder funcionar como emulador de tarjeta y como lector.

El problema de este tipo de ataque es que aumenta el tiempo de transmisión entre la tarjeta y lector originales, por lo que el tiempo extra que se demora el paquete de datos en llegar puede provocar que se detecte el ataque y se detenga la transmisión.

Si el atacante es capaz de reducir el tiempo añadido, será más complicado que sea detectado y tendrá más probabilidades de llevarse acabo con éxito.

- **Adición de datos:**

En este caso, el atacante espera a que el transmisor envíe la información que pretende y en el momento en el que el receptor está procesando esa información que ha recibido, le envía más información que se añade a la legítima enviada anteriormente. Solo es posible si se realiza en el momento preciso.

Como contramedida a esta amenaza, se puede realizar una firma de los datos que se van a transmitir o bien cifrar completamente la información. De esta manera se puede verificar que el mensaje sea el original y no se haya añadido información.

A diferencia del ataque de modificación de datos, en este caso sí que se añaden campos a la información transmitida.

5.2 Ataque de diccionario

Como se explica en anteriores apartados, las tarjetas se dividen en sectores y cada uno de ellos dispone de claves de 48 bits (6 bytes), ese tamaño permite que puedan ser obtenidas mediante este ataque.

El ataque de diccionario es parecido a un ataque por fuerza bruta, donde se prueban todas las combinaciones posibles hasta hallar la clave, pero se diferencia en que solo prueba palabras del diccionario del idioma correspondiente,

Para ejecutarlo, se puede utilizar la herramienta MFOC que permite descifrar la encriptación de las claves de la tarjeta con un lector NFC y la tarjeta NFC Miafare Classic. También se puede usar MFCUK, que utiliza el mismo hardware de MFOC y puede realizarse con mayor eficacia, es decir, menos consultas.

6. Clonación de tarjetas NFC

Uno de los mayores ataques que sufren las tarjetas es la clonación, la cuál consiste en copiar todos los datos de una tarjeta en otra creando un duplicado. Para ello, se necesita un duplicador de tarjetas que en caso de que la tarjeta esté encriptada, debe ser capaz de desencriptar los datos para obtener la información.

Cuando se duplica no solo se copian los datos, sino que también se copia el autentificador de la tarjeta para que el lector reconozca la copia como la tarjeta original. Pero no todas las tarjetas pueden modificar su número de serie, algunas mantienen el que les viene de fábrica, lo que puede llevar a que aunque aparentemente el duplicado disponga de los datos y campos que tenía la tarjeta original, no sea capaz de pasar por ella ante un control de acceso.

En este proyecto hemos ejecutado este ataque sobre diferentes tarjetas para probar la facilidad con la que pueden ser clonadas y las prestaciones que ofrecen sus duplicados.

6.1 Duplicadores de tarjetas

En el proyecto se han utilizado dos duplicadores distintos de diferentes características, que han obtenido resultados dispares y los cuáles serán presentados a continuación.

El primero es el Lector NFC/RFID de Tarjetas Inteligentes s9-bu-00-01 USB de la marca Fongwah, una empresa de manufacturación china que se dedica a desarrollar productos de RFID, ya sean tarjetas inteligentes o como en este caso dispositivos de lectura/escritura. El lector incluye tarjetas NFC para usarlas de duplicados y un software descargable en el equipo que permite trabajar con este duplicador.

Para el correcto funcionamiento del dispositivo, se debe conectar al equipo a través de un cable USB y tener el Software correspondiente descargado.

Figura 10. Lector NFC/RFID de Tarjetas Inteligentes s9-bu-00-01 USB

Al acceder al software del producto aparece la siguiente pantalla donde seleccionamos la opción que corresponda a las tarjetas que pretendemos leer.

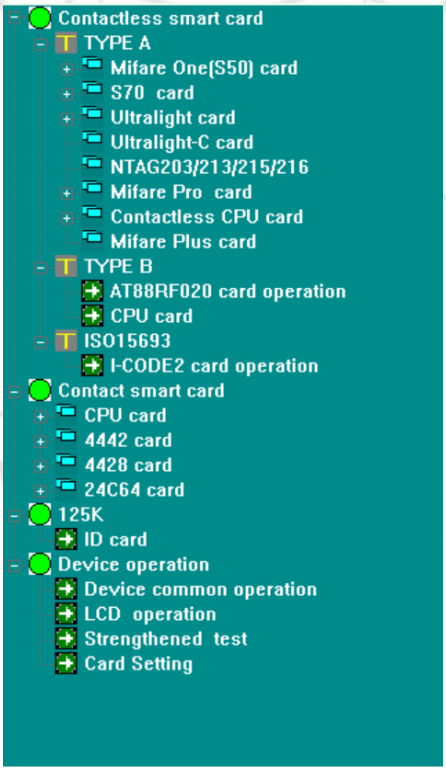

Figura 11. Tarjetas seleccionables en el software del duplicador

En nuestro caso las tarjetas que leeremos son de la clase Miafare Classic por lo que iríamos a la opción de Mifare One(S50) card o S70 card.

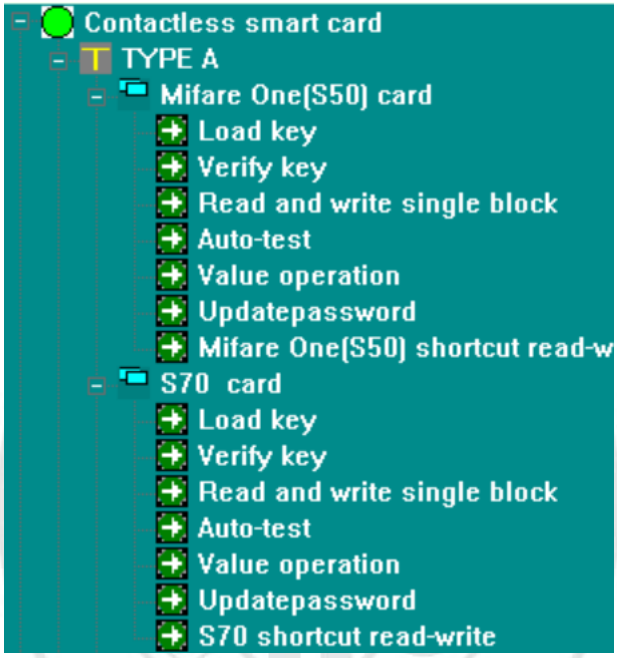

Figura 12. Opciones en Miafare One (S50) card y S70 card

Situamos la tarjeta encima del lector y pinchamos en 'Load key', nos lleva a la siguiente pantalla donde apretando en 'Load Key(L)' cargamos la tarjeta en el lector.

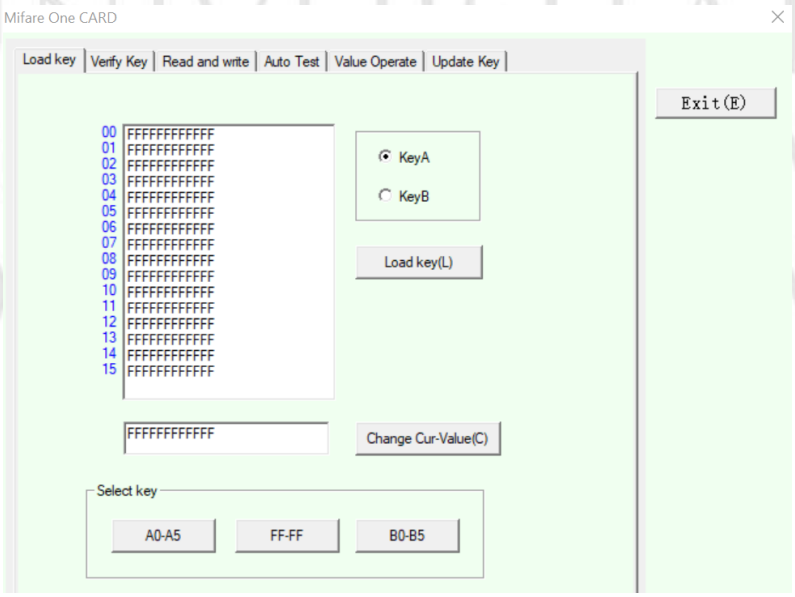

Figura 13. Pantalla 'Load key' en Miafare One (S50) card y S70 card

En caso de que el dispositivo no sea capaz de descifrar el encriptado de la tarjeta, aparece el mensaje que vemos a continuación:

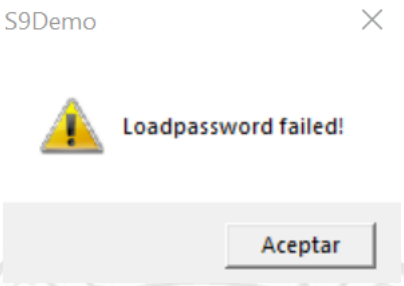

Figura 14. Mensaje de error al no descifrar el encriptado

En la circunstancia de que no se pudiera descifrar, el aparato no leería los campos y no se podría realizar ningún cambio en la estructura de la tarjeta, ni copiar la información para pegarla en una tarjeta nueva.

Si no da ningún error, significará que el lector ha superado el encriptado y que está cargada la tarjeta. Pincharemos en 'Auto-test' para que lea todos los sectores que componen la tarjeta NFC. Se mostrarán distintos sectores por pantalla y el número de serie de la tarjeta.

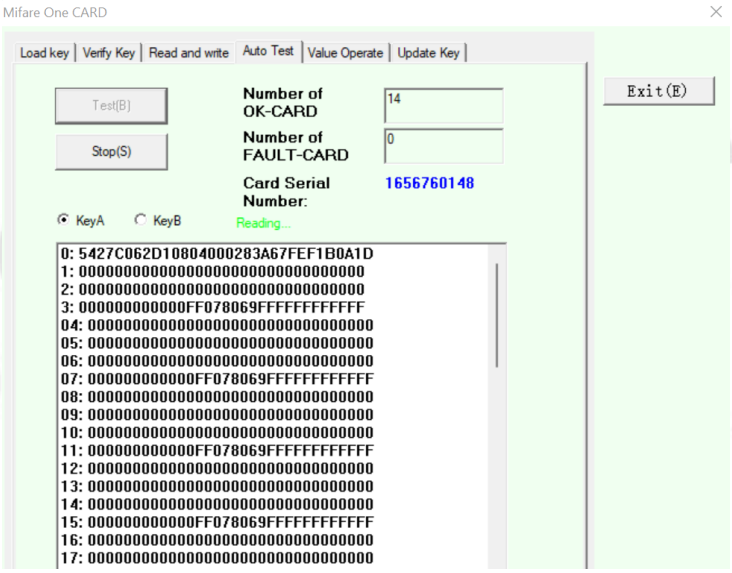

Figura 15. Auto-test de tarjeta de cerradura electrónica

Después yendo a la opción ‘shortcut read-write’ accedemos a los distintos sectores que componen la tarjeta y a la información que contienen.

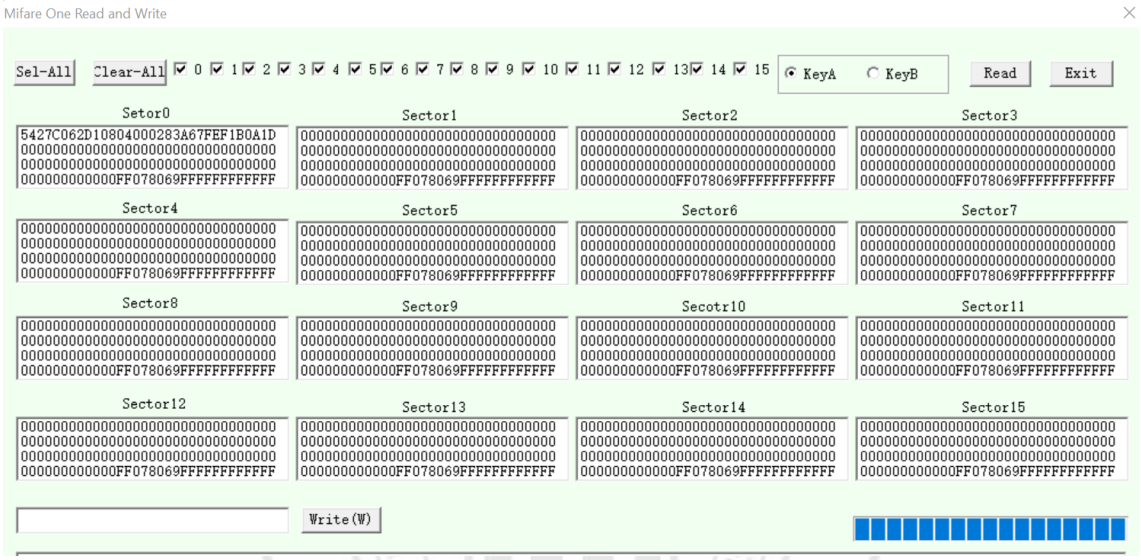

Figura 16. Sectores de la tarjeta de cerradura electrónica

En el sector 0, en el primer bloque se observa información de la tarjeta NFC que está siendo examinada y en el cuarto bloque de cada sector aparece el código de bloque, el cuál es invariable, por lo que no puede ser modificado.

El segundo dispositivo duplicador utilizado en este proyecto, es el escritor de tarjetas de identificación multifrecuencia del fabricante Sonew. Este aparato no requiere una conexión USB con un ordenador ni de un software descargable.

Figura 17. Duplicador de Sonew

A diferencia del anterior, en este aparato no es posible ver los campos con la información de la tarjeta. El dispositivo escanea la tarjeta que colocamos en la parte trasera de este, desencripta la información y la guarda. Seguidamente se coloca la tarjeta o llavero reescribible donde se desea realizar el duplicado y se escribe la información de la tarjeta.

Al escribir la información en una tarjeta, se copia toda excepto el número de serie. En cambio, si la copia se realiza sobre un llavero reescribible, además de toda la información se le asigna el mismo número de serie que la tarjeta.

6.2 Casos estudiados

Las pruebas se han realizado sobre 5 tarjetas NFC distintas, la tarjeta de la UPV, un bonometro de metrovalencia, un bonobús de la EMT de Valencia, un bonobús del servicio de transporte público de Sevilla y una tarjeta que abre una cerradura electrónica.

6.2.1 Tarjeta UPV

El primer caso de estudio es la tarjeta de la Universidad Politécnica de Valencia, en concreto una tarjeta que tiene los permisos de un alumno, es decir, acceder al parking o al aula de estudio.

Figura 18. Ejemplo de la tarjeta UPV

Las características de la tarjeta pueden ser observables mediante una aplicación móvil como NFC Tools, NFC TagInfo o NFC Writer.

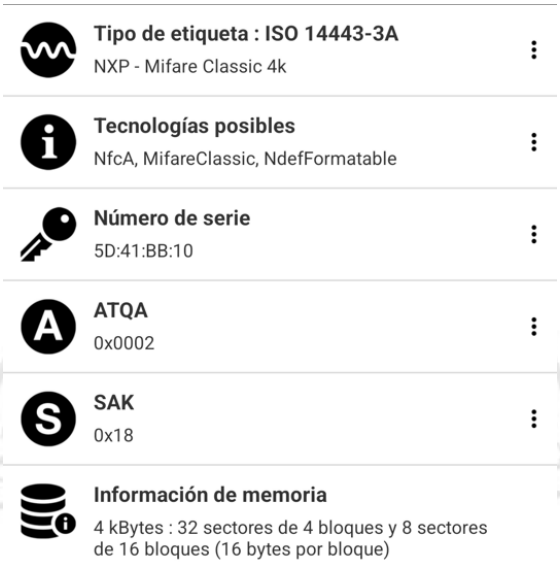

Figura 19. Características de la tarjeta UPV

En la imagen se puede apreciar el tipo de etiqueta, en este caso Miafare Classic 4k, el número de serie de la tarjeta, la tecnología, la información de la memoria, el ATQA (Answer to Request) y SAK (Select Acknowledge). Estos dos últimos sirven para identificar de que tarjeta se trata:

	ATQA	SAK
Miafare Classic 1K	0004	08
Miafare Classic 4K	0002	18
Miafare Ultraligth	0044	00

Tabla 4. ATQA y SAK

Al colocar la tarjeta en el duplicador S9 de Fongwah, el primero descrito, daba el error de la Figura 14, por lo que no es capaz de superar la encriptación de la tarjeta y no puede mostrar la información de los bloques de todos los sectores para poder modificarla o copiarla en un duplicado.

En cambio con el dispositivo de Sonew, el presentado en segundo lugar, sí que es posible realizar la clonación. Para ello colocamos la tarjeta en la parte trasera del aparato y apretamos al botón 'SCAN'. De esa forma lee la tarjeta superando su encriptación y muestra por pantalla el número de la tarjeta.

Una vez ha sido escaneada, retiramos la tarjeta y colocamos detrás el dispositivo NFC donde lo queremos clonar. Le damos a 'WRITE' y escribimos la información de la tarjeta original en el duplicado.

En primer lugar lo escribimos sobre una tarjeta NFC en blanco, nos aparece que la escritura se ha realizado de manera correcta. A continuación, leemos las características del duplicado.

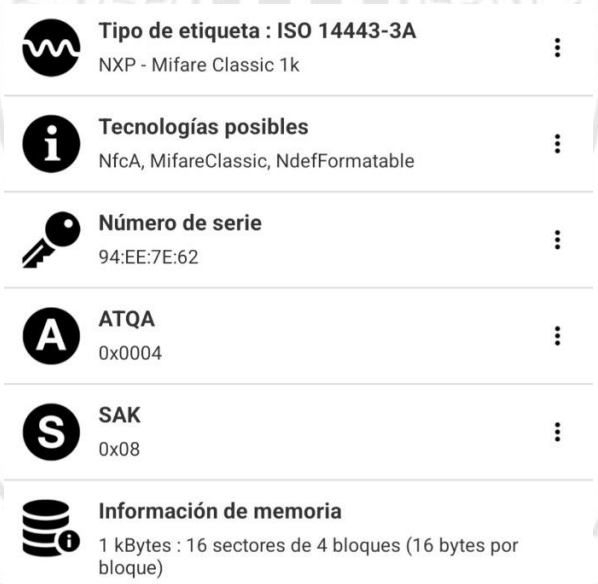

Figura 20. Características duplicado en tarjeta NFC del carnet UPV

La tarjeta del duplicado es Miafare Classic 1K en lugar de Miafare Classic 4K, pero permite copiar la información en ella. El problema de las tarjetas es que aunque estén en blanco tienen un número de serie invariable con el que vienen de fábrica. Al pasar la tarjeta por el lector de la universidad no llega a funcionar debido a que no reconoce el número de serie de la tarjeta.

Se realiza de la misma forma en un llavero reescribible NFC. En este caso el llavero no tiene un número de serie predeterminado y adquiere el de la tarjeta que se copia en él. Quedando de la siguiente manera:

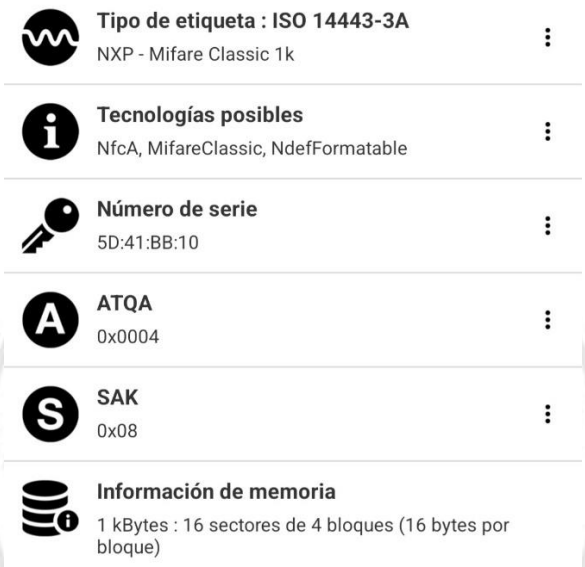

Figura 21. Características duplicado en llavero RFID del carnet UPV

Al igual que con la tarjeta el llavero RFID es Miafare Classic 1K pero en este formato sí que mantiene el Número de serie de la tarjeta original. Se obtiene un duplicado con los mismos datos, mismo número de serie y distinto tipo de tarjeta Miafare pero compatible.

Tras comprobar las prestaciones de este duplicado, se constata que sí funciona y que ofrece las mismas prestaciones que la tarjeta original. Es capaz de abrir la barrera del parking haciéndose pasar como la identificación del carnet.

Por tanto, los resultados obtenidos son que el duplicado en tarjeta NFC no se reconoce al disponer de número de serie distinto y no funciona pero en el caso del llavero RFID sí que funciona el duplicado.

6.2.2 Bonometro

El siguiente caso de estudio se ha realizado sobre un bonometro de metrovalencia. Para ello se ha procedido como en el caso anterior, escanear la tarjeta y después copiarla en una tarjeta en blanco NFC y un llavero reescribible RFID.

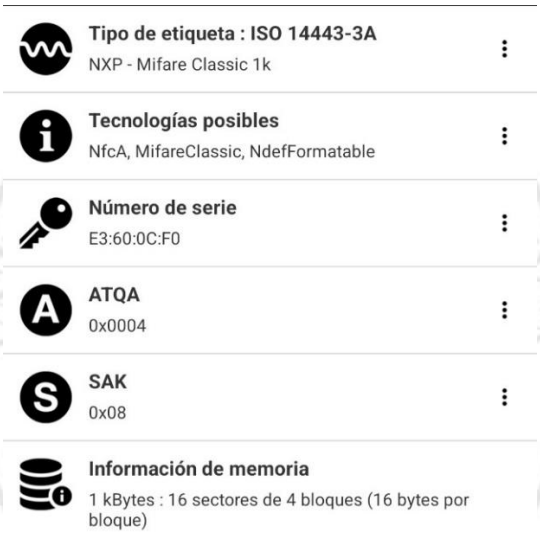

Figura 22. Características de bonometro de metrovalencia

Como se puede observar en la imagen anterior, el bonometro es una Miafare Classic 1K. Al realizar el duplicado de la tarjeta en una tarjeta NFC nos encontramos con que es capaz de copiar toda la información pero no el número de serie de la tarjeta por lo que el lector de la estación de metro da error al no reconocer la tarjeta como una de las emitidas.

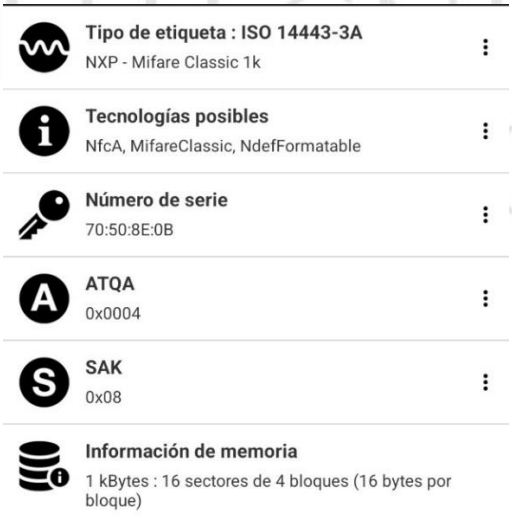

Figura 23. Características duplicado en tarjeta NFC de bonometro de metrovalencia

En cambio si realizamos el duplicado sobre un llavero reescribible RFID, se copia tanto el número de serie como la información.

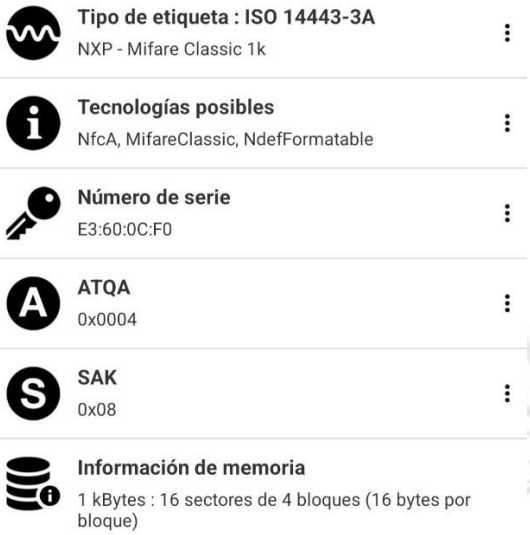

Figura 24. Características duplicado en llavero RFID de bonometro de metrovalencia

Aunque el número de serie coincida y la información que contiene el duplicado sea la misma que la que lleva la original, el duplicado no funciona correctamente. El lector de la estación de metro es capaz de detectar que el llavero RFID no es una tarjeta y da el siguiente error: 'No es una tarjeta Apunt'. Las tarjetas Apunt son las utilizadas en Valencia en transporte público. Por lo que ni en el duplicado en el llavero reescribible ni en el de la tarjeta es posible repetir los resultados de la original.

6.2.3 Bonobuses

En el tercer caso de estudio se realiza la prueba sobre tarjetas bonobús, donde en lugar de tener un sistema donde los lectores estén conectados como en el metro, cada autobús tiene el suyo y no puede conectarse con el resto para contrastar información.

Primero se realiza sobre un bonobús de la EMT de Valencia, como el anterior caso, el primer lector no es capaz de superar la encriptación de la tarjeta. El segundo sí que logra escanear y copiar la información del bonobús en los duplicados.

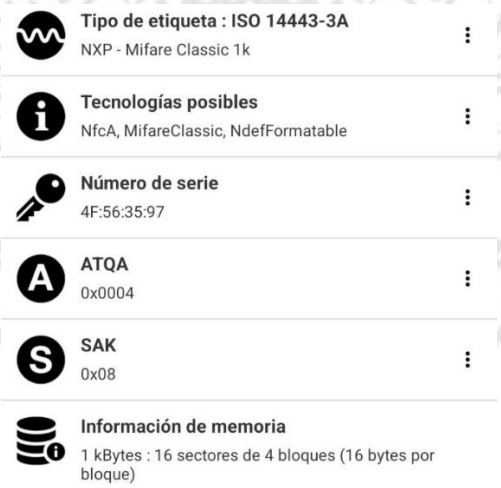

Figura 25. Características bonobús EMT

Al igual que la tarjeta de metro, el bonobús de la EMT también es una tarjeta Miafare Classic 1K. Se realiza la copia sobre una tarjeta NFC en blanco.

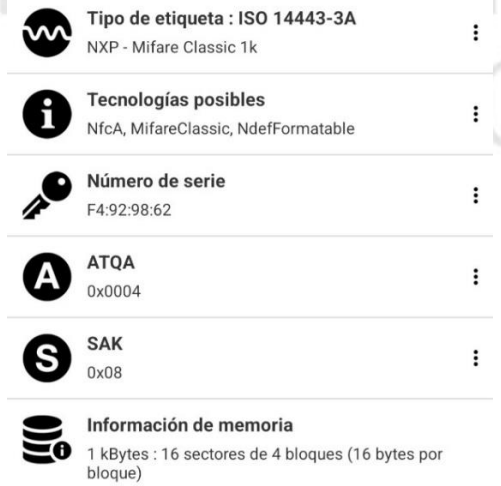

Figura 26. Características duplicado en tarjeta NFC de bonobús EMT

El número de serie del duplicado no coincide con el de la tarjeta original, al probarlo en el lector integrado dentro del autobús, da error al no reconocer la tarjeta como una de las emitidas por la EMT y se puede hacer pasar por la original. De la misma forma, se realiza el duplicado sobre un llavero reescribible RFID, del que se obtienen los datos de la siguiente imagen.

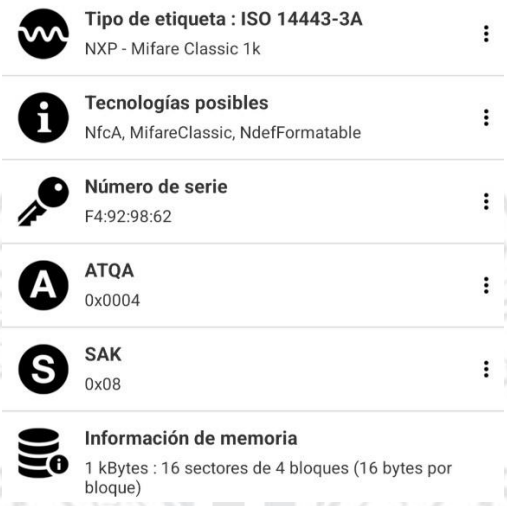

Figura 27. Características duplicado en llavero RFID de bonobús EMT

Como se puede apreciar en la anterior imagen, el número de serie es el mismo que en la tarjeta original. Al probar las prestaciones del duplicado en el lector de un autobús, sucede el mismo problema que en el caso del bonometro. El lector muestra por pantalla el mismo error que el del metro: 'No es una tarjeta Apunt'.

También realizamos la misma propuesta pero con un bonobús de Sevilla que en lugar de funcionar con un número de viajes, lo hace con saldo. Al probarlo, los duplicados no pueden ofrecer las prestaciones de la tarjeta original.

En resumen, se obtienen los mismos resultados en las tarjetas de transporte público tanto aquí en Valencia como en Sevilla. Las copias en tarjetas NFC fallan debido al número de serie y los llaveros RFID aunque poseen la información de la tarjeta y el mismo UID, no son reconocidos como tarjetas oficiales.

6.2.4 Tarjeta de cerradura electrónica

El último caso de estudio se ha realizado sobre la tarjeta NFC que abre una cerradura electrónica del fabricante ALLWIN INC, intentando clonarla sobre otra tarjeta NFC en blanco y sobre un llavero RFID reescribible para comprobar como se comportan sus duplicados.

Figura 28. Cerradura electrónica

A diferencia de las anteriores pruebas, en este caso el primer lector sí que es capaz de superar la encriptación de la tarjeta, de manera que es capaz de leer los distintos campos de la tarjeta.

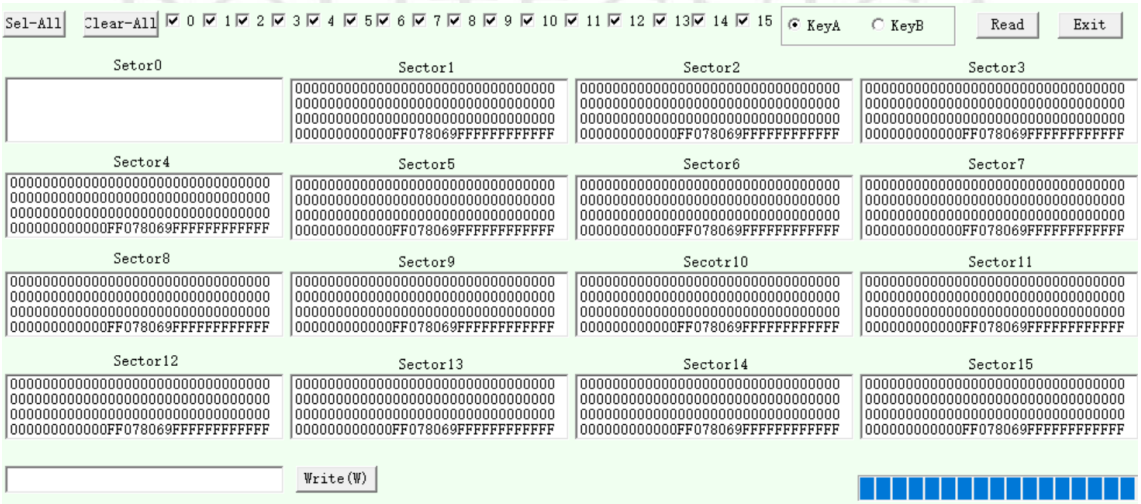

Figura 29. Información tarjeta NFC de cerradura electrónica

Como se puede observar en la anterior imagen, en el primer bloque donde aparece información de la tarjeta, no se llega a superar la encriptación de dicha información. Solo es observable el código bloque del resto de sectores. Además de los campos de la tarjeta NFC, tiene las características que se ven en la siguiente figura.

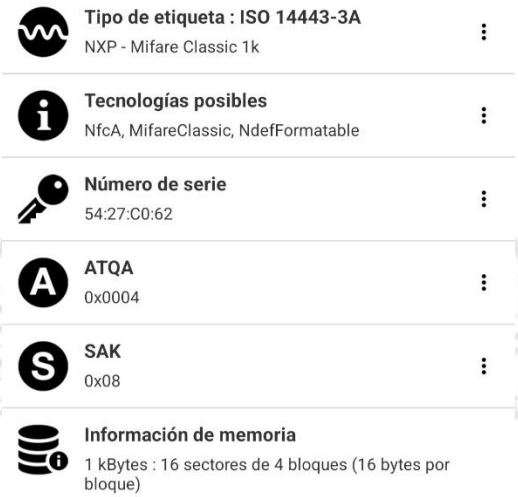

Figura 30. Características tarjeta original de cerradura electrónica

Al realizar un duplicado en el llavero reescribible RFID, se copia el contenido de la tarjeta original, incluido el UID. Al pasar el duplicado por el dispositivo NFC de la cerradura sí que detecta el duplicado como el original y se abre correctamente.

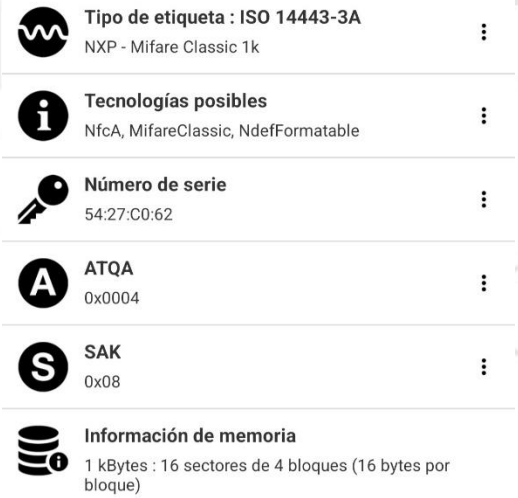

Figura 31. Características duplicado llavero RFID de cerradura electrónica

Al leer los duplicados en le primer lector, tanto el llavero RFID como la tarjeta NFC, el programa muestra de la misma forma los sectores de estos. En cambio, al fijarse en las características de la clonación realizada sobre la tarjeta NFC, no se copia el UID de la tarjeta original. Por lo que el lector de la cerradura no reconoce la tarjeta y no se abre.

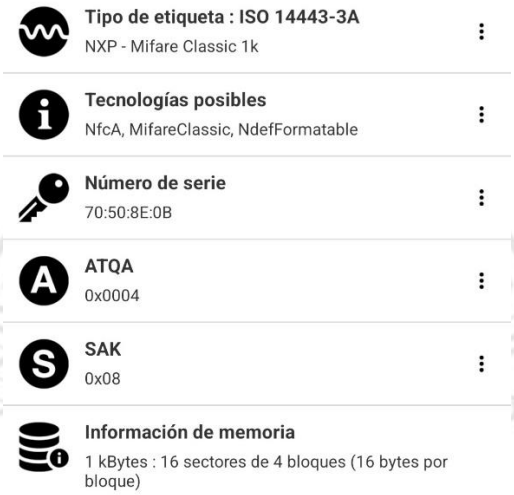

Figura 32. Características duplicado tarjeta NFC de cerradura electrónica

7. Conclusión

El uso de la tecnología NFC está muy extendido en diferentes ámbitos de la vida diaria y en categorías que varían desde el propio hogar hasta identificación para espacios de alta seguridad, pasando por organizaciones de acceso público.

Las tarjetas que se derivan a usos cotidianos como el transporte público o acceso a organizaciones públicas como universidades sin llegar a dar acceso a información sensible, poseen una encriptación que puede ser superada y con el uso de las tarjetas apropiadas, pueden ser duplicadas o realizarse otros ataques como los comentados en el proyecto.

Los identificadores utilizados en lugares que contienen información sensible ya sea de uso empresarial, personal o militar, poseen una encriptación muy superior a la vista donde se requieren conocimientos y equipo muy superiores a los que se pueden obtener en el mercado estándar, por lo que requerirían de unos dispositivos y manejo expertos.

Como consecuencia de lo expuesto en este trabajo, las tarjetas NFC que usamos diariamente pueden ser atacadas y comprometidas, pero dado el equipo necesitado y el bajo efecto que supone para las organizaciones a las que pertenecen, dichas entidades deben ser conscientes de las debilidades de sus tarjetas y plantearse si merece la pena realizar acciones para corregir los defectos o mantener su actual estructura y funcionamiento.

8. Bibliografía

[1] Javier Penalva. (2022) *NFC: qué es y para que sirve en este 2022* [En línea]. Recuperado de:

https://www.xataka.com/moviles/nfc-que-es-y-para-que-sirve

[2] Rocío García (2022) *Qué es NFC, cómo leer o escribir tarjetas y usos para etiquetas* [En línea]. Recuperado de:

https://www.adslzone.net/como-se-hace/internet/leer-escribir-nfc/

[3] THALES *Acerca de EMV* [En línea]. Recuperado de:

https://www.thalesgroup.com/es/countries/americas/latin-america/dis/servicios-financieros/tarjertas/emv/acerca

[4] Orange (2020) *Todo sobre NFC, la conexión sin cables más útil para pagar* [En línea]. Recuperado de:

https://blog.orange.es/consejos-y-trucos/que-es-el-nfc/

[5] Wikipedia *Comunicación de Campo cercano* [En línea]. Recuperado de:

https://es.wikipedia.org/wiki/Comunicaci%C3%B3n_de_campo_cercano

[6] Dipole RFID NFC: *Qué Es Y Como Funciona* [En línea]. Recuperado de:

https://www.dipolerfid.es/blog-rfid/que-es-nfc

[7] El blog del amigo informático (2018) *¿Qué es NFC y cómo funciona?* [En línea]. Recuperado de:

https://elamigoinformaticoblog.wordpress.com/2018/11/30/que-es-nfc-y-como-funciona/

[8] Omnitec (2020) *RFID vs. NFC ¿Cuál es la diferencia? Tecnologías de radiofrecuencia* [En línea]. Recuperado de:

https://www.omnitecsystems.es/omni/blog/rfid-vs-nfc-diferencia-tecnologias-radiofrecuencia#:~:text=Si%20bien%20ambos%20procesos%20sirven,alcance%20mediante%20tarjetas%20de%20proximidad.

[9] FQ Ingeniería Eléctrica (2018) *Tecnología NFC, modalidades operativas y aspectos técnicos* [En línea]. Recuperado de:

https://www.fqingenieria.com/es/conocimiento/tecnologia-nfc-modalidades-operativas-y-aspectos-tecnicos-47

[10] Shenzhen Xinyetong Desarrollo Tecnológico *Guía para principiantes NFC: todo lo que necesita saber sobre NFC* [En línea]. Recuperado de:

https://www.asiarfid.com/es/what-is-nfc.html

[11] Shop NFC *Características técnicas de las Etiquetas NFC* [En línea]. Recuperado de:

https://www.shopnfc.com/es/content/6-caracteristicas-tecnicas-de-etiquetas-nfc

[12] NFC STOCK *Características técnicas de las Etiquetas NFC* [En línea]. Recuperado de:

https://nfcstock.com/es/content/10-caracteristicas-tecnicas-de-etiquetas-nfc-rfid

[13] Wikipedia *Miafare* [En línea]. Recuperado de:

https://es.wikipedia.org/wiki/Mifare

[14] CIO España (2015) *Preocupa la seguridad de las tarjetas contactless* [En línea]. Recuperado de:

https://cso.computerworld.es/tendencias/preocupa-la-seguridad-de-las-tarjetas-contactless

[15] Juan González (2021) *Un fallo en los chips NFC permite romper la seguridad de los cajeros automáticos* [En línea]. Recuperado de:

https://unaaldia.hispasec.com/2021/06/un-fallo-en-los-chips-nfc-permite-romper-las-seguridad-de-cajeros-automaticos.html

[16] Guillermo Cebollero (2018) *Ataques de retransmisión inteligente en protocolos de pago NFC* [En línea]. Recuperado de:

http://webdiis.unizar.es/~ricardo/bsc-msc-projects/pfc/pfcs-finalizados/ataque-retransmision-inteligente-protocolos-pago-nfc/

[17] Josep Rodríguez (2021) *Vulnerabilidades de seguridad en cajeros con NFC* [En línea]. Recuperado de:

https://www.paymentmedia.com/news-5401-vulnerabilidades-de-seguridad-en-cajeros-con-nfc.html

[18] Luís Alberto Nieto (2020) *Teoría y vulnerabilidades NFC* [En línea]. Recuperado de:

https://es.linkedin.com/pulse/teoria-y-vulnerabilidades-nfc-luis-alberto-nieto

[19] Lucas Paus (2015) *Los posibles ataques a la seguridad en tecnologías NFC: ¿nuevos canales?* [En línea]. Recuperado de:

https://www.welivesecurity.com/la-es/2015/09/16/ataques-seguridad-en-tecnologias-nfc/

[20] Wikipedia *EMV* [En línea]. Recuperado de:

https://es.wikipedia.org/wiki/EMV

[21] Radboud University Nijmegen *Wirelessly Pickpocketing a Miafare Classic Card* [En línea]. Recuperado de:

https://www.cs.ru.nl/~flaviog/publications/Pickpocketing.Mifare.pdf

[22] Wikipedia *Crypto-1* [En línea]. Recuperado de:

https://en.wikipedia.org/wiki/Crypto-1

[23] Radboud University Nijmegen *A Practical Attack on the MIFARE Classic* [En línea]. Recuperado de:

https://www.cs.ru.nl/~flaviog/publications/Attack.MIFARE.pdf

[24] Luís Alberto Nieto (2020) *POC – Hacking Tarjetas RFID Mifare Classic* [En línea]. Recuperado de:

https://es.linkedin.com/pulse/poc-hacking-tarjetas-rfid-mifare-classic-luis-alberto-nieto

[25] Roberto Amado (2010) *Hacking RFID, rompiendo la seguridad de Mifare (I)* [En línea]. Recuperado de:

https://www.securityartwork.es/2010/01/29/hacking-rfid-rompiendo-la-seguridad-de-mifare-i/

[26] FQ Ingeniería Eléctrica (2014) Estándares y regularizaciones para RFID [En línea]. Recuperado de:

https://www.fqingenieria.com/es/conocimiento/estandares-y-regularizaciones-para-rfid-36

[27] Wikiwand *ISO/IEC 7816* [En línea]. Recuperado de:

https://www.wikiwand.com/es/ISO/IEC_7816

[28] Archit Dua (2016) *NFC Standars and NFC Forum* [En línea]. Recuperado de:

https://rfid4u.com/nfc-standards-nfc-forum/

[29] Wikipedia *Criptografía asimétrica* [En línea]. Recuperado de:

https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica

[30] Wikipedia *Principios de Kerckhoffs* [En línea]. Recuperado de:

https://es.wikipedia.org/wiki/Principios_de_Kerckhoffs

9. Anexos

9.1 Anexo 1: Estándares

· **ISO-14443:** Estándar para tarjetas NFC basado en la frecuencia de 13.56 MHz que se subdivide en 4 partes distintas:

- ISO 14443-1:2008 Parte 1: Se especifican las características físicas.
- ISO 14443-2:2010 Parte 2: Se especifican el interfaz de la señal y la potencia de Radio-Frecuencia.
- ISO 14443-3:2011 Parte 3: Se especifican las funciones de inicialización y anticolisión.
- ISO 14443-4:2008 Parte 4 Se especifica el protocolo de transmisión.

Existen 2 subtipos dentro de este estándar, A y B, cuyas diferencias residen en la modulación, código y el protocolo de inicialización.

· **ISO-15693:** Estándar para tarjetas NFC basado en la frecuencia de 13.56 MHz, es semejante al ISO-14443 pero se diferencia en dos matices:

- Puede alcanzar una mayor distancia, hasta 1.5 metros.
- Utiliza un campo magnético para su activación de entre 0.15 a 0.5 mA, en cambio, el ISO-14443 requiere de uno entre 1.5 a 7.5 mA.

· **ISO-18092:** Estándar que define el intercambio de información entre sistemas NFC.

· **ISO-7816:** Estándar sobre las tarjetas inteligentes de identificación electrónicas que se divide en 15 partes:

- 7816-1: Características físicas.
- 7816-2: Dimensiones del circuito integrado y búsqueda de contactos.
- 7816-3: Protocolos de transmisión y de interfaz eléctrica.
- 7816-4: Seguridad y comandos de intercambio de información.
- 7816-5: Registro de solicitud de proveedores.
- 7816-6: Interoperabilidad en los elementos de datos para intercambios de información.
- 7816-7: Interoperabilidad de los comandos.
- 7816-8: Comandos de operaciones de seguridad.
- 7816-9: Comandos de gestión.
- 7816-10: Señales electrónicas síncronas.
- 7816-11: Verificación biométrica.
- 7816-12: Tarjetas con contactos y de interfaz eléctrica USB.
- 7816-13: Comandos de administración de aplicaciones.
- 7826-15: Información criptográfica.

· **NFCIP-1:** Estándar que describe el interfaz de la señal de radio-frecuencia, el protocolo de iniciación y de anticolisión, protocolos de transporte y los modos de radio-frecuencia activo, pasivo y peer-to-peer.

· **NFCP-2:** Estándar que describe el modo de selección de la operación.

9.2 Anexo 2: Criptografía

· **Criptografía de clave pública:** El mensaje se cifra con una clave pública y es descifrado por el receptor con una clave privada que solo este posee.

· **RSA:** Algoritmo de cifrado basado en criptografía de clave pública que permite cifrar la información y firmar, por lo que dota la comunicación de confidencialidad y autentificación.

· **SHA:** Algoritmo de cifrado basado en funciones Hash, la cuáles funcionan de manera unidireccional, es decir, fácil cifrarlas pero de gran dificultad para descifrar sin clave.

· **DES:** Algoritmo de cifrado por bloques, se divide por bloques de 64 bits empleando una clave de 56 bits. Es sencillo de descifrar por lo que no se usa de forma habitual, en cambio sí se usa otro algoritmo que deriva de este, el Triple DES.

· **Triple DES:** Algoritmo de cifrado por bloques que realiza un triple cifrado del algoritmo DES, tiene una clave de 156 bits.

9.3 Anexo 3: Protocolos

· **LLCP:** Protocolo de Control de Enlace Lógico que especifica como los datos se transmiten sobre el medio físico.

· **SWP:** Protocolo que define la transmisión de una señal y la conexión física.

9.4 Anexo 4: Principios de Kerckhoffs

Estos principios definen las propiedades deseable de un sistema criptográfico, son los siguientes:

1. Si el sistema no es teóricamente irrompible, por lo menos debe serlo en la práctica.
2. La efectividad del sistema no debe depender de que su diseño permanezca en secreto.
3. La clave debe ser fácilmente memorizable de manera que no haya que recurrir a notas escritas.
4. Los criptogramas deben dar resultados alfanuméricos.
5. El sistema debe ser operable por una única persona.
6. El sistema debe ser fácil de utilizar.