Escuela Superior
de Ingeniería y Tecnología
Universidad de La Laguna

Trabajo de Fin de Grado

Estudio de seguridad en aplicaciones de transporte

Security issues in transport applications

Zuzanna Elzbieta Szalaty Szalaty

La Laguna, 14 de mayo de 2020

Dña. **Pino Caballero Gil**, con N.I.F. 45.534.310-Z Catedrática de Universidad adscrita al Departamento de Ingeniería Informática y Sistemas de la Universidad de La Laguna, como tutora

Dña. **Jezabel Molina Gil**, con N.I.F. 78.507.682-B profesora Ayudante Doctora de Universidad adscrita al Departamento de Ingeniería Informática y Sistemas de la Universidad de La Laguna, como cotutora

C E R T I F I C A (N)

Que la presente memoria titulada:

”*Estudio de seguridad en aplicaciones de transporte*”

ha sido realizada bajo su dirección por Dña. **Zuzanna Elzbieta Szalaty Szalaty**, con N.I.F. 70.651.890-F.

Y para que así conste, en cumplimiento de la legislación vigente y a los efectos oportunos firman la presente en La Laguna a 14 de mayo de 2020

Agradecimientos

Pino Caballero Gil, tutora.

Jezabel Molina Gil, cotutora.

Licencia

Resumen

El objetivo de este proyecto ha sido el análisis de las tecnologías más comunes utilizadas en la validación de billetes del transporte público, para poder determinar de esta forma si son suficientemente seguras y destacar las debilidades para que las aplicaciones puedan ser fortalecidas.

Para ello se ha analizado la tecnología del código QR, sus debilidades y las formas en las que podrían ser utilizadas sus vulnerabilidades. Se ha demostrado además la forma en la que una vulnerabilidad específica del QR podría llevar a un atacante a una exitosa distribución de un billete válido y a su posterior uso por pasajeros que no han pagado por el trayecto recorrido.

Además de la tecnología QR, se ha descrito el funcionamiento de la tecnología NFC ya que dicha tecnología se utiliza cada vez más en diferentes sectores de la sociedad, facilitando tareas como es la validación de billetes. Por otra parte se han demostrado en este proyecto dos ataques. En uno de ellos, se demuestra que la tarjeta inteligente utilizada en la validación del billete podría ser manipulada y utilizada de forma conveniente por un atacante. Además se ha descrito otro ataque que podría darse en caso de que el atacante tuviera acceso al lector de billetes NFC del transporte público, pues de esta forma podría utilizar la autorización obtenida del servidor tanto en situaciones legítimas como en situaciones no legítimas.

Palabras clave: NFC, QR, validación de billetes, vulnerabilidades.

Abstract

The objective of this project has been the analysis of the most common technologies used in the validation of public transport tickets, in order to determine in this way if they are sufficiently secure and to highlight the weaknesses so that the applications can be strengthened.

For this, the technology of the QR code, its weaknesses and the ways in which its vulnerabilities could be used have been analyzed. It has also been demonstrated how a specific vulnerability of the QR could lead an attacker to a successful distribution of a valid ticket and its subsequent use by passengers who have not paid for the route traveled.

In addition to QR technology, the operation of NFC technology has been described since this technology is increasingly used in different sectors of society, facilitating tasks such as ticket validation. On the other hand, two attacks have been demonstrated in this project. In one of them, it is shown that the smart card used in ticket validation could be conveniently manipulated and used by an attacker. In addition, another attack has been described that could occur in case the attacker had access to the NFC ticket reader of public transport, since in this way he could use the authorization obtained from the server in both legitimate and non-legitimate situations.

Keywords: NFC, QR, ticket validation, vulnerabilities.

Índice general

Índice de Figuras

Índice de Tablas

Capítulo 1

Introducción

1.1. Motivación y objetivos

El transporte público es una herramienta fundamental hoy en día, es para muchas personas la única forma de desplazarse a diario. Al usar este servicio podemos darnos cuenta de que las tecnologías utilizadas para validar un billete y el propio billete han ido cambiando. Antes se solía utilizar tan solo un billete de papel mientras que hoy en día podemos utilizar una aplicación del móvil, que almacena nuestros datos, para pagar el trayecto.

Sin embargo, es común leer una noticia sobre algún ataque nuevo o que los datos personales registrados en alguna aplicación o dispositivo de alguna persona han sido expuestos. Muchas veces las tecnologías afectadas son las que solemos utilizar diariamente. Esto nos hace pensar sobre si las aplicaciones de transporte, en las que queda registrada una gran cantidad de información personal, son del todo seguras o si todavía hay algunas amenazas existentes que podrían llegar a afectarnos.

Los objetivos de este trabajo son los siguientes:

- Analizar las diferentes tecnologías que se utilizan hoy en día, además de investigar sobre las posibles formas en las que se puede encontrar un billete.
- Elegir las tecnologías más utilizadas y analizarlas, descubrir cómo funcionan y sus posibles vulnerabilidades.
- Con la información recogida sobre las debilidades de las tecnologías estudiadas, elegir algún ataque y replicarlo para demostrar así su funcionamiento. Explicar además los posibles ataques de forma teórica.

1.2. Impacto de COVID-19 en este proyecto

Una ventaja de desarrollar este tipo de proyecto ha sido la facilidad de acceso a los recursos necesarios para la realización del mismo a pesar del COVID-19. Por ello el

impacto que ha tenido la cuarentena y la enfermedad no ha sido tan notorio como podría haber sido.

La información utilizada en este proyecto ha sido encontrada en Internet y por ello no ha sido necesario el acceso a información física algo que habría resultado imposible durante el confinamiento. Para la realización de las demostraciones de las vulnerabilidades y para la implementación de los ataques el material necesario no ha tenido que ser adquirido. Esto se debe a que todos los materiales utilizados son de uso común, y en cuanto a los tags NFC éstos afortunadamente fueron obtenidos antes del comienzo de esta situación extraordinaria.

1.3. Estado del arte

El uso intensivo de vehículo propio hoy en día es no sostenible. Por tanto, cada día incrementa la demanda de transporte público, eficiente y de buena calidad. El transporte público es, en la actualidad, algo fundamental para cualquier ciudadano [1]. El transporte es un servicio por el cual el usuario debe abonar una cantidad, establecida por la compañía que lo ofrece, para hacer uso del mismo. Para controlar el pago, se introduce el concepto de billete que permite identificar al usuario y verificar que posee los recursos suficientes para realizar el pago [2, 3].

Junto a la evolución de las tecnologías también ha habido un cambio en la forma en la que se presenta el billete. Como consecuencia, se puede clasificar los billetes en cuatro generaciones dependiendo de la forma física y la tecnología utilizada para su verificación, algunas de ellas no se usan hoy en día, mientras que otras pueden incluso coexistir en la misma ciudad.

La primera y más antigua generación es la de los billetes de papel o tokens que, a pesar de ser una forma antigua de billete, se sigue utilizando en la actualidad. La desventaja de los billetes de papel es que el usuario debe adquirirlos en algún punto de venta oficial, y al ser de papel el billete se deteriora con facilidad, además de que normalmente son de un solo uso. El uso de este tipo de billetes se suele evitar, por el gran gasto que supone debido a su corta vida [4, 5].

Posteriormente, se introducen en los años 70 los billetes con banda magnética. Este tipo de billete, al igual que su equivalente de papel, implica la compra del mismo en establecimientos oficiales de venta; sin embargo, al verificarse a través de esa banda magnética y un dispositivo de verificación, permiten que un billete sea utilizado más de una vez, además del cobro por la distancia recorrida en vez del papo de una cuota fija como pasaba con su predecesor. Tras estas dos generaciones, surgen generaciones de billetes cada vez más automatizados [6].

En los años 90 surgen los billetes basados en tarjetas inteligentes. Se trata de tarjetas de plástico que incluyen un chip que almacena una gran cantidad de información que permite conocer las zonas donde puede ser utilizado, así como el saldo restante y el cobro

por la distancia recorrida. Estas tarjetas o smartcards suelen ser contactless, es decir billetes que no necesitan contacto directo con la máquina para poder ser verificados. Proporcionan muchas ventajas con respecto a las generaciones anteriores por lo que sustituyen rápidamente a las mismas. Este tipo de billetes usa tecnología RFID, o identificación por radiofrecuencia y también pueden usar tecnología NFC o comunicación de campo cercano, para comunicar la tarjeta con el dispositivo de validación. Ambas tecnologías quedarán explicadas en el apartado correspondiente al NFC que se puede encontrar más adelante. Un ejemplo de smartcard sería la Oyster card utilizada en el transporte público de Londres, que se verifica utilizando dicho sistema [7].

La última generación de billetes es la de los billetes móviles. Este tipo de pasaje puede presentarse de dos formas diferentes. Por un lado, existe el billete que se puede comprar utilizando una aplicación móvil y llega en forma de un código QR o de barras, o simplemente el billete llega al móvil del usuario a través del SMS, como el caso de la empresa Paybox en Austria, Proximus en Bélgica o Mobipay en España. En el caso del código de barras o el código bidimensional (QR), el usuario debe presentarlo al conductor que leerá y comprobará la validez del mismo. Los usuarios también pueden optar por comprar los billetes por una aplicación móvil, en el caso de que la empresa de transporte la proporcione, y obtener el mismo en la propia aplicación y que este sea utilizado de la misma forma que una tarjeta inteligente, utilizando RFID o NFC para su verificación como es el caso del Touch & Travel en Alemania. Un ejemplo de billete que hace uso del código QR es el transporte público de Portugal, concretamente en la ciudad de Oporto, en la que se utiliza dicho código bidimensional como billete validándolo en la entrada al transporte y también al salir del mismo (el usuario paga únicamente por el tramo recorrido) [8].

Además de los tipos de billetes y tecnologías mencionadas anteriormente, también existen otras formas cuya implementación fue probada, pero que hoy en día o bien no se usan o bien no están tan extendidas como las anteriores. Se trata de los billetes basados en Bluetooth que se intentaron implementar en Alemania, cuyo objetivo era que el usuario al entrar en un determinado tipo de transporte público se conectara a un dispositivo con tecnología Bluetooth, y se desconectara del mismo al salir del vehículo. En ese caso el cobro del trayecto se calcularía comprobando cuándo se conectó el usuario por Bluetooth y cuándo se desconectó. No obstante, esta forma de verificación no resultó práctica, debido a que por el metal del vehículo y la gran cantidad de dispositivos conectados, las señales eran débiles además de poco precisas y la prueba de esta forma de verificación daba resultados poco eficientes. Se ha propuesto también un sistema basado en la biométrica, que consta de la verificación basada en la lectura del iris del usuario para la verificación se sus credenciales; sin embargo este sistema no se ha implementado y de momento se trata de una simple propuesta, ya que implica una gran cantidad de información personal por lo que podría atentar contra la privacidad del usuario [9].

En el transporte público surge el concepto de *e-ticketing* o billetes electrónicos que corresponden con las dos generaciones de billetes más recientes. Cabe destacar que dicho término no solo incluye la forma de validación del billete sino también el pago del mismo. Dentro del grupo de billetes electrónicos se distingue el término *m-ticketing* que corresponde a los billetes móviles que se basan en el uso de NFC y QR para la verificación de credenciales y el pago del trayecto. Se especifican tan solo esas dos tecnologías a pesar de la existencia de otras, ya que actualmente esas dos son las formas más comunes

en el campo del transporte público.

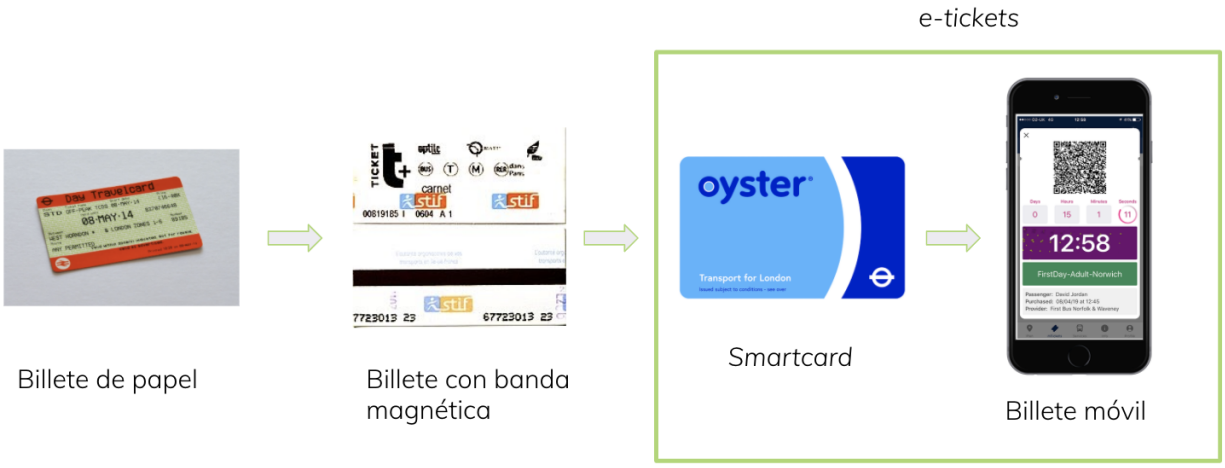

Figura 1.1: Esquema de las cuatro generaciones del billete.

1.4. Estructura de la memoria

El capítulo dos y tres se centran en las dos tecnologías más comunes utilizadas hoy en día para la validación de billetes tal y como fue explicado en este capítulo. El segundo capítulo trata de la tecnología NFC y el tercero sobre los códigos QR, en ambos capítulos se trata la arquitectura, el funcionamiento, los ejemplos de uso y las vulnerabilidades de la tecnología correspondiente. El objetivo de esos capítulos es la explicación en detalle del NFC y los códigos QR para tener de esta forma un conocimiento base sobre las mismas. En los capítulos siguientes, el cuarto y quinto, se describen diferentes ataques tanto teóricos como prácticos para poder de esta forma comprender el funcionamiento de los mismos.

Capítulo 2

Tecnología NFC

En este capítulo se explicará una de las tecnologías más utilizadas para la verificación de billetes. Además de analizar su funcionamiento y sus diferentes usos, se describe también las diferentes vulnerabilidades que existen y las diferentes formas que pueden ser utilizadas por un atacante para corromper el sistema.

2.1. Introducción

La tecnología NFC, *Near Field Technology*, basa su funcionamiento en el Touch and Connect, es decir, tocar y conectar ya que permite la conexión inalámbrica y el intercambio de información a través de dispositivos NFC o de tarjetas inteligentes [9, 10]. Se trata de una tecnología basada en la inducción electromagnética y en la proximidad que permite la interacción de los dispositivos a una distancia máxima de unos 10 cm. Por lo tanto, dicha interacción no tiene por qué implicar un contacto directo de ambos dispositivos, sino un intercambio producido dentro del rango de distancia establecido.

La comunicación inalámbrica de corto alcance y alta frecuencia es una extensión de RFID, *Radio Frequency Identification*, por ello opera en el espectro de alta frecuencia a unos 13.56 MHz con una velocidad máxima de 424 kbps, pero además de dicha velocidad también puede transmitir a 216 kbps o 106. De igual manera, se comunica mediante inducción en un campo magnético, en donde dos antenas son colocadas dentro de sus respectivos campos. Al trabajar en la banda de los 13,56 MHz mencionada no se le aplica ningún tipo de restricción, ni requiere ninguna licencia específica para su uso [11, 12]. En cuanto a las diferencias con RFID son que NFC es bidireccional, opera a una distancia máxima de 10 cm, mientras que RFID es unidireccional y puede funcionar hasta una distancia de un metro [13]. El hecho de que NFC sea bidireccional, le otorga la ventaja de poder recibir y enviar información a la vez, es decir, que por el mismo canal de comunicación originado puede transmitir a la vez que recibe información.

Los estándares en los que está basada la tecnología *Near Field Technology* son varios. El primero, usado principalmente en EEUU y Europa, es el ISO14443 y el otro es el JIS X

63194 conocido además como SonyFeLiCa cuyo uso destaca sobre todo en Asia.

La interfaz puede operar de diferentes formas. El dispositivo NFC por lo tanto puede ser activo o pasivo, dependiendo de si crea su propio campo electromagnético que usará para transmitir sus datos (activo), o como en el caso de las tarjetas inteligentes, solo un dispositivo genera dicho campo, el activo, y el otro dispositivo hace uso del mismo para transmitir los datos (pasivo). Si se trata del dispositivo activo éste debe de tener una fuente de alimentación para ser capaz de generar el campo mencionado, como por ejemplo la batería del móvil, mientras que el pasivo no tiene que tener ningún tipo de alimentación como es el caso de una tarjeta inteligente, debido a que se alimenta de la fuente de energía del dispositivo activo con el que se comunica. Cabe destacar que aunque los dispositivos puedan ser activos o pasivos, para que se puedan comunicar, al menos uno de ellos ha de ser activo como por ejemplo el móvil, la terminal de pago o el dispositivo verificador dentro del autobús (en el caso del transporte público) [14, 15]. Además, NFC tiene tres formas en las que puede operar: *peer-to-peer* (dos dispositivos NFC), lector/escritor y emulación de tarjeta.

Una de las ventajas de NFC es la simplicidad, el intercambio de información que se activa automáticamente cuando se establece el contacto entre los dispositivos NFC, un lector o un transpondedor. Por ello, es importante y supone una ventaja en el campo del transporte público ya que un billete puede ser verificado por el usuario o un controlador de billetes, usando una tarjeta inteligente o el propio dispositivo móvil del usuario de forma rápida y sencilla. Un ejemplo de uso de NFC a través de una smartcard es el caso de Alemania que utiliza el Touch & Travel o la Suica Card en Tokio. La ventaja del uso de NFC en el transporte, puede plantear e incrementar posibles problemas de privacidad y seguridad. Esto se debe a que al tratarse de una comunicación inalámbrica, el robo de datos sensibles del usuario puede producirse en cualquier lugar.

Otra ventaja es que facilita al usuario el uso de NFC en caso de que éste no posea un dispositivo con tales características. Esto se debe a la existencia de unos chips NFC pasivos también llamados pegatinas o Tags que actúan del mismo modo que un dispositivo pasivo. Por lo que si el usuario cuenta con un móvil sin dicha capacidad podría obtenerla con la adición de dicha pegatina a su móvil [16].

2.2. Aspectos tecnológicos

En este tipo de comunicación la idea principal es la transmisión de información sin ningún tipo de contacto físico. Este tipo de comunicación está basado en ondas electromagnéticas que viajan desde el transmisor al receptor. La información se modula en una onda portadora en el transmisor y se demodula en el receptor para ser usada. Esa onda portadora es propagada por el medio de transmisión hasta el receptor que demodula la onda.

El funcionamiento y las especificaciones tecnológicas del proceso de intercambio de datos dependerá del modo en el que se ejecute dicha acción. Lo primero que se debe

conocer son los modos en los que se pueden comunicar los dispositivos, se trata de tres modos diferentes que son: *peer-to-peer*, lectura/escritura y emulador de tarjeta NFC [11].

2.2.1. Arquitectura

Durante la comunicación NFC los dispositivos que intercambian información pueden tener diferentes arquitecturas, ya que no tendrá los mismos elementos un dispositivo móvil y un tag (o pegatina NFC). Cabe destacar que para poder comunicarse utilizando este tipo de tecnología, sea el tipo de dispositivo que sea, debe constar de una antena. Las antenas son las encargadas de transmitir la información entre los dispositivos involucrados en la comunicación.

Asimismo, si se trata de una tarjeta o *smartcard*, además de la antena tiene un chip que constituye el elemento seguro. El *Security Element* (SE) constituye un elemento clave, ya que almacena información cifrada, y tiene su propio sistema operativo permitiendo de esta forma la comunicación con un lector, y la ejecución de tareas como el pago por NFC (si se trata de una tarjeta de crédito) o una validación de billete en caso de que se trate de una tarjeta de transporte. Dicho elemento seguro también se encuentra en los dispositivos móviles siendo el chip de la tarjeta SIM del mismo.

Específicamente, la arquitectura de un dispositivo móvil con NFC activado está formado por circuitos integrados, Elemento Seguro (*Secure Element*, SE) y la interfaz del propio NFC, que a su vez consta de un frontend (es decir de la interfaz del usuario) y un controlador o antena que controla la comunicación. El Elemento Seguro es lo que le proporciona seguridad parcial a la comunicación producida, esto es, proporciona un entorno para que los dispositivos puedan interactuar [12].

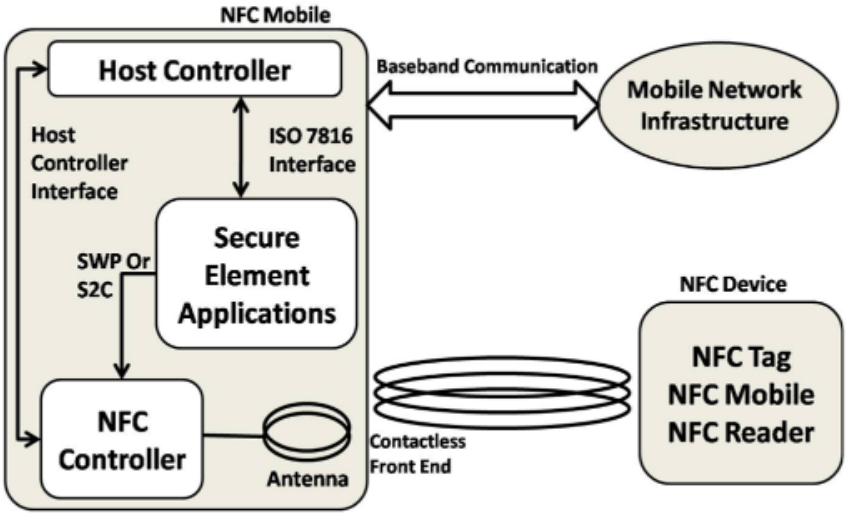

Figura 2.1: Arquitectura básica de un dispositivo NFC.

2.2.2. Comunicación entre dispositivos

Las ondas electromagnéticas son generadas por la antena del dispositivo. En caso de un teléfono móvil se puede encontrar dicha antena en el interior de la batería o en la carcasa trasera del mismo. En caso de un tag o pegatina NFC, se puede descubrir un patrón que actúa como antena. A través de estas antenas, los dispositivos son capaces de interactuar entre ellos. Los diferentes lugares en los que se encuentra la antena se pueden observar en la figura 2.2. En la imagen posicionada a la izquierda, la antena se sitúa en la carcasa trasera mientras que en la imagen intermedia se encuentra en la propia batería. En la imagen más a la derecha se puede observar el tag con la antena correspondiente.

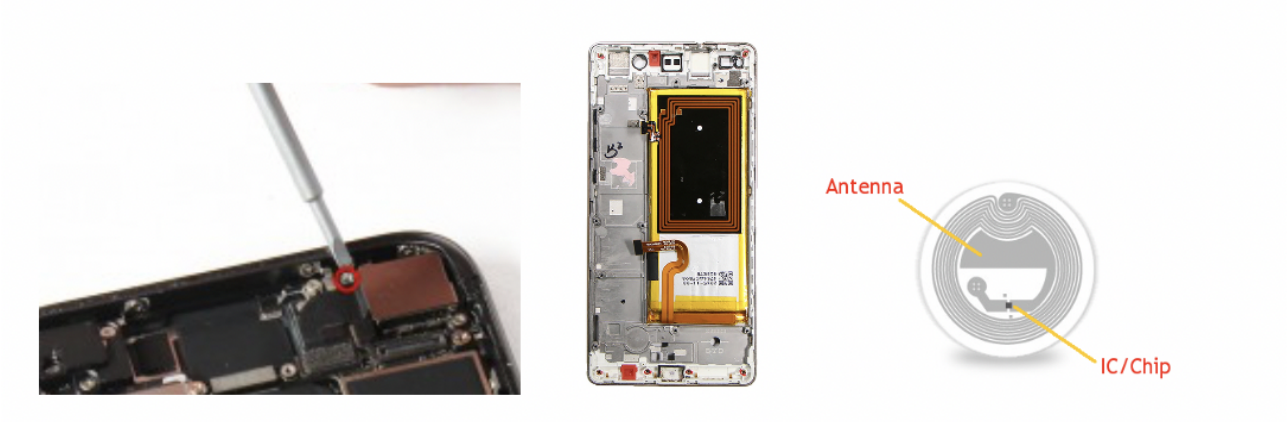

Figura 2.2: Diferentes lugares donde se sitúa la antena NFC del dispositivo.

2.2.3. Modos de funcionamiento

El primer modo, *peer-to-peer*, consiste en un intercambio bidireccional entre dos dispositivos activos, que tienen habilitado NFC utilizando un mismo canal en modo *half-duplex*, es decir, que se permite la transmisión de información en ambas direcciones pero no a la vez. Dichos dispositivos se comunican a una frecuencia de 13.56 MHz generando las ondas electromagnéticas alternativamente, cuando un dispositivo comunica algo por el canal, el otro dispositivo escucha. Para empezar el intercambio de datos, uno de los dispositivos debe buscar al otro para iniciar la comunicación, por lo que se puede distinguir entre el dispositivo iniciador y el dispositivo objetivo. Este tipo de conexión podría utilizarse para el intercambio de credenciales [12].

En el caso del modo de emulación de tarjeta, un dispositivo puede emular el comportamiento de una tarjeta inteligente. Se produce una comunicación entre un dispositivo activo y otro también activo, pero uno de dichos dispositivos actúa como pasivo. El dispositivo que emula el funcionamiento de una tarjeta inteligente no genera sus propias ondas electromagnéticas sino responde a las peticiones del dispositivo activo. En este modo el lector externo, esto es, el dispositivo activo, no podrá distinguir de qué dispositivo se trata, de si es un móvil en modo de emulación de tarjeta o si es una tarjeta inteligente. Este modo es útil en los casos de pago o aplicaciones de validación de tickets. Los dispositivos que trabajan en este modo cuentan con el software de emulación de tarjeta que

proporciona una ventaja que es la interoperabilidad de dispositivos NFC con sistemas de validación de tarjetas inteligentes. En el transporte público tiene la ventaja de posibilitar al usuario la validación haciendo uso del móvil en ese modo y usar los dispositivos de validación de tarjetas inteligentes preexistentes sin ser necesario la modificación de los mismos para el funcionamiento correcto con dispositivos móviles [14].

El modo NFC lectura/escritura permite que un dispositivo activo altere información que contiene un dispositivo pasivo. Por ello se trata de una comunicación de un dispositivo activo con uno pasivo. El usuario, por lo tanto, puede acceder a información de tarjetas inteligentes *contactless*, transpondedores RFID y las NFC tags, o básicamente puede interactuar con cualquier chip que puede comunicarse a través de NFC y tenga memoria para almacenar información. Son tags, o pegatinas, que un usuario puede leer con su móvil al establecer el contacto entre dicho dispositivo activo y el tag (dispositivo pasivo) y leer e incluso modificar la información almacenada. Esta forma de operar es bastante parecida al RFID, por lo que usando este modo se puede interactuar con tags RFID. El dispositivo puede leer o escribir datos utilizando el principio de inducción electromagnética. El dispositivo activo genera las ondas; el dispositivo pasivo (por ejemplo una tarjeta inteligente) las recibe con su antena y las utiliza para proporcionar voltaje al circuito, es decir para obtener la energía necesaria para poder activar su chip interior. A través de la modulación de la carga se le envían los dispositivos al dispositivo activo [11].

2.3. Ejemplos de uso

Los ejemplos de uso proporcionados son del ámbito de transporte, aunque su uso se encuentra extendido también en otros escenarios como aparcamiento, ocio, pagos por móvil o publicidad personalizada [17].

Un ejemplo de uso es la tarjeta *Oyster*, que ha sido implementada en Londres, que consiste en una tarjeta inteligente contactless, que utiliza NFC para poder cobrar los viajes de un pasajero. Esta tarjeta a su vez, cuenta con una alternativa y es el uso directo de una tarjeta de crédito contactless que emula el funcionamiento de la Oyster card sin necesidad de poseer dicha tarjeta. Ambas opciones utilizan NFC a la entrada y a la salida del servicio público correspondiente, tal y como queda explicado en el esquema de la figura 2.3 [18].

El servicio *Touch & Travel* alemán también cuenta con el uso de tecnología NFC. No obstante, en este caso en vez de utilizar una tarjeta inteligente se utiliza el móvil del propio usuario. En este caso el usuario debe validar el billete en los *Touchpoints* habilitados para ello tanto en la entrada como en la salida del transporte público. Se trata de un sistema sencillo y fácil; sin embargo también conlleva una desventaja, y es que a pesar de la evolución de las tecnologías, existen móviles sin NFC.

Otro ejemplo sería el de *MiMuovo*, una tarjeta inteligente utilizada en Italia en 2014, cuyo uso consistía en la validación en la entrada y salida de la misma. Durante la investigación de su uso, se comprobó que a pesar de que la información intercambiada en la

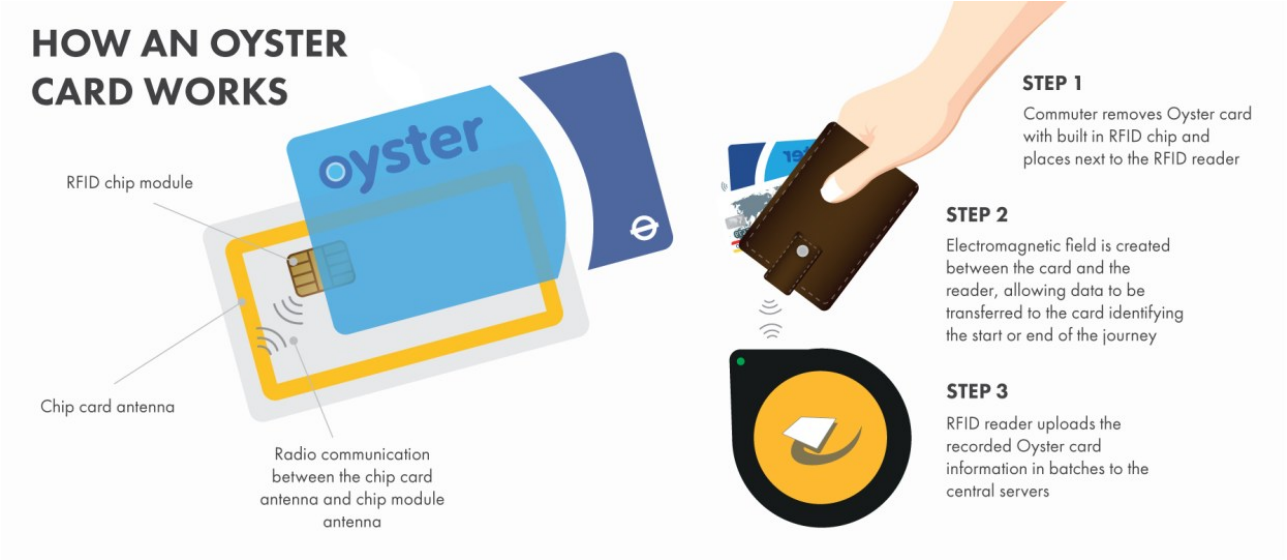

Figura 2.3: Esquema de funcionamiento de la Oyster card.

validación del billete se guardara de forma anónima para el usuario, era posible obtener datos que facilitaban la identificación del usuario. Esto se debía a que la información almacenada, además del identificador del usuario, era el precio, la fecha, hora y la parada en la que se bajó el usuario. El precio permitía identificar si el usuario era estudiante, las paradas en las que se bajaba permitían conocer el grado que estudiaba, y si además utilizaba el transporte público para ir a la residencia, se podría unir todos los datos descubiertos y comprobar la identificación del usuario haciendo uso de las listas de los habitantes de las residencias que permanecen públicas [19].

2.4. Vulnerabilidades

NFC es una ventaja y una tecnología sencilla de utilizar e implementar, sin embargo, como en cualquier tecnología conlleva algunas vulnerabilidades e inseguridades para el usuario que opta por utilizarla. Es considerado “seguro” debido al corto alcance de transmisión, lo que dificulta la captura de la señal por otro dispositivo. Sin embargo, dicha captura de la señal no es imposible.

Actualmente no está definido ningún estándar que garantice la integridad y la seguridad durante las transacciones, comunicaciones o pagos móviles que utilizan NFC. Por ello a continuación se listan los posibles ataques que podrían llevarse a cabo. Para dificultar que éstos se produzcan se debería establecer un canal seguro de comunicación y el uso de protocolos basados en claves [20].

2.4.1. Denegación de servicio

Los dispositivos NFC no se encienden, es al entrar en contacto cuando se activan automáticamente. Esto conlleva un riesgo, y es que una persona cualquiera puede intentar por ejemplo validar un billete no válido, y de esta forma aunque el validador muestre simplemente un mensaje de error, ya se encuentra ocupado por lo que imposibilita el servicio a otro usuario.

Otra forma de implementar este ataque sería enviar frecuencias válidas desde otro dispositivo, para que de esa forma el validador no pueda recibir la señal legítima del dispositivo del usuario. Una medida que se podría tomar para evitar esta situación es la detección de campos de ondas del atacante [20].

2.4.2. Espionaje

El espionaje o escucha secreta (en inglés *eavesdropping*) consiste en la posibilidad de que un tercero escuche la información transmitida entre dos dispositivos sin que estos lo sepan o lo consientan. Este tipo de ataque es común para todas las tecnologías que usan ondas de radio para transmitir información. En la comunicación NFC, ambos dispositivos ya sea en modo activo o pasivo se comunican a través de un canal. Dicho canal podría ser escuchado por un atacante a través del uso de una antena de gran potencia, ya que la interacción entre los dispositivos NFC tiene lugar en un entorno inalámbrico, fácilmente interceptable. La información transmitida por el canal no se encuentra cifrada a nivel de enlace por lo que si no existe un cifrado en alguna capa superior, la información interceptada sería todo el contenido enviado. El uso de una antena potenciadora hace que la distancia máxima de funcionalidad del NFC de 10 cm, aumente hasta 25 centímetros.

Otra preocupación de los usuarios es la privacidad. Esto se debe a que la información transmitida es privada y personal, y en la comunicación de los dispositivos NFC se envía el identificador único del dispositivo, como por ejemplo de una tarjeta inteligente. Si alguien obtiene dicho identificador, podría ser capaz de conocer todos los movimientos del usuario, algo que atenta contra la privacidad del mismo.

Un ejemplo de ataque que podría darse es en el momento en el que un datáfono se comunica con un teléfono móvil que opera en modo de emulación de tarjeta o una tarjeta de crédito *contactless*. En dicho ejemplo la información bancaria que se transmite de la tarjeta al dispositivo no se cifra de ninguna forma y tampoco requiere ninguna verificación adicional del usuario (PIN) en caso de que no se supere la cantidad de 20€. Sin embargo, si alguien intercepta dicha información podría usarla para realizar pagos fraudulentos, y a pesar de que las transacciones sin PIN son limitadas, el usuario podría sufrir pérdidas económicas. Una forma de luchar contra este ataque es potenciar el uso de fundas que inhiben las ondas de radio, permitiendo que solamente se produzca la comunicación cuando la tarjeta se encuentra fuera de la funda. Otra medida de seguridad es implementar el cifrado de los datos transmitidos, haciendo uso de algoritmos criptográficos como el RSA o el 3DES [13].

2.4.3. Corrupción de datos

La corrupción de datos es una gran vulnerabilidad, ya que si una persona intercepta la información podría modificarla, utilizarla o borrarla. Esto podría tener efectos negativos, que podrían ser temporales, es decir, que se modifican en una comunicación. Por otro lado, también podrían ser definitivos, por ejemplo en el caso de una pegatina o *tag*, si alguien modifica la información almacenada podría ser modificada y quedar inutilizable.

Para intentar imposibilitar este tipo de ataque, se puede implementar como medida de seguridad un sistema de claves que solamente permita la modificación de la información de la pegatina a quien tenga esa clave. O también establecer que dicha tag solo se use para que un dispositivo lea la información contenida en la misma y que no sea capaz de modificarla. Sin embargo, estas dos medidas no tendrían efecto en la práctica porque aunque la información contenida en la etiqueta no sea modificable, o solo lo sea para dispositivos autorizados, el atacante podría colocar una etiqueta nueva con el contenido dañino deseado. Por ello, la medida más eficiente es el establecimiento de unas firmas digitales que aseguren la legitimidad del contenido.

2.4.4. Man-in-the-Middle

Man-in-the-middle o ataque de intermediario no se suele producir debido a la corta distancia a la que tiene lugar la interacción entre los dispositivos, sin embargo sigue siendo una posible vulnerabilidad del NFC.

Este ataque consiste en que durante la comunicación entre dos usuarios, una tercera persona influye en ella fingiendo ser uno de los participantes. A diferencia del espionaje explicado en la sección 2.4.2 en este ataque el atacante puede intervenir en la comunicación entre los dispositivos. Los participantes no saben que la tercera persona, el hombre en medio, está interceptando información e incluso mandando información modificada como si fuera uno de los participantes de la misma. Lo que podría hacer esa persona ajena a la conversación, es escuchar la información intercambiada por el canal, interceptar y utilizar la información, o interceptar y modificar los datos a su antojo [21].

2.4.5. Retransmisión

El *relay attack* es un tipo del *man-in-the-middle* debido a que el atacante interviene en la comunicación haciéndose pasar por uno de los participantes de la comunicación. Este ataque puede ser explicado mediante el ejemplo de una partida de ajedrez. El atacante representado en la figura 2.4 como el maestro del sombrero reta a dos maestros del ajedrez (caballo blanco y negro) a una partida, realizada a través del correo postal, contra él. Ambos jugadores creen que están jugando contra el maestro del sombrero mientras que en realidad están jugando entre ellos. El atacante, que podría incluso desconocer las reglas del juego, lo que hace es tan solo recibir la respuesta de uno de los jugadores y

enviársela al otro jugador [22].

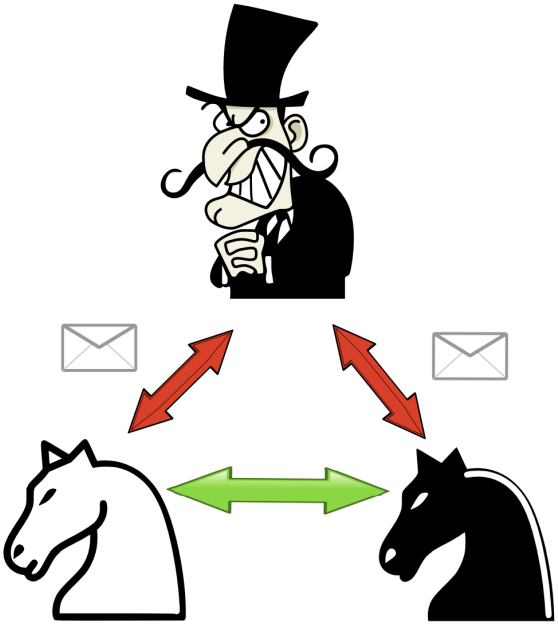

Figura 2.4: Esquema del ejemplo del ataque de retransmisión

Este ataque puede ser utilizado para aumentar el rango de comunicación haciendo uso del propio canal de comunicación entre dos dispositivos. Esto hace posible la comunicación a una distancia mayor a la que supuestamente esto es posible. Para ilustrar la forma en la que se produce este ataque a continuación se propone un ejemplo, como sería pagar usando una tarjeta de crédito. En este caso se pretende comunicar un dispositivo en modo de emulación de tarjeta con un dispositivo en modo lector/escritor. El atacante aprovechará esta oportunidad y haciendo uso de su propio dispositivo, fingirá que dicho dispositivo es el lector legítimo, y después podrá utilizar la información obtenida en otro dispositivo en modo de emulación de tarjeta, para usarlo con un lector verídico fingiendo ser la tarjeta legítima de la víctima. Dicho dispositivo en emulación no tiene por qué encontrarse cerca de la víctima ni del lector del atacante; podría encontrarse en cualquier lugar mientras que los dispositivos del atacante se comuniquen entre ellos.

Para intentar proteger al usuario de este tipo de ataques se pueden implementar restricciones temporales en la comunicación, que no permitirán que la información sea retransmitida de forma ilegítima. Sin embargo, esta medida puede entrar en conflicto en algunos escenarios en los que se dispone de comandos que permiten extender el tiempo de la comunicación en caso de que sea necesario, por lo que se trata de una medida efectiva pero a la vez conflictiva. Otra medida que se puede tomar es filtrar las comunicaciones y solamente permitir los identificadores NFC, que se generan aleatoriamente cuando un dispositivo se encuentra en modo de emulación de tarjetas, permitidos en determinadas situaciones. Esa medida tiene el inconveniente de que no es posible conocer dicho identificador de antemano.

Capítulo 3

Códigos QR

3.1. Introducción

Es un tipo de tecnología que cuenta con la certificación ISO 27001. Se trata de un código de respuesta rápida o *Quick Response code*, de ahí las siglas de su nombre. Se utiliza en muchas partes del mundo ya que se trata de una forma sencilla de almacenar y compartir información. Su estructura consiste en un cuadrado grande que es la matriz exterior y por dentro se encuentra compuesto por conjuntos de cuadrados blancos y negros. Usando este tipo de código se pueden codificar unos 7.366 caracteres y unos 4.464 símbolos alfanuméricos [23].

Un código QR es un tipo de código de barras, de tipo bidimensional que posee la ventaja de que puede ser leído por un dispositivo móvil, y no requiere de un dispositivo especial de lectura como en el caso de la validación de un código de barras. Cuando el móvil entra en contacto con el código bidimensional puede conectarse instantáneamente a Internet y acceder a la información almacenada en el propio QR o alguna otra acción especificada en los ajustes del código. Dicha información se encuentra almacenada en una matriz de forma gráfica, llegando al máximo de almacenamiento de 7 kilobytes de datos, una cantidad grande de información considerando el tamaño del propio código [23]. Se habla de que el código es bidimensional ya que la información puede ser transmitida tanto vertical como horizontalmente [24].

3.2. Aspectos tecnológicos

El código bidimensional para poder ser leído debe contar con algún tipo de tecnología capaz de interpretarlo, sin embargo, el código en sí puede ser impreso en cualquier tipo de superficie ya sea papel o plástico. Esto supone una ventaja ya que lo hace más accesible y reduce el precio de su distribución.

3.2.1. Arquitectura

Cualquier código QR sin importar la información que incluye en su interior, consta de una estructura común. En dicha estructura se pueden diferenciar zonas que tienen un determinado objetivo.

La primera zona consta de tres cuadrados que se encuentran en las esquinas del código, dos en la parte superior y uno en la parte inferior izquierda, que forman los patrones de reconocimiento o de posición. A través de estos patrones un dispositivo puede reconocer que se trata de un código QR. A través de estos patrones el dispositivo es capaz de conocer la orientación correcta del código y también la forma en la que debe interpretar los bits de información. Los patrones de reconocimiento se encuentran rodeados por unos marcos blancos, que son los separadores, que sirven para facilitar la distinción de los patrones de reconocimiento del resto de la información que contiene el código bidimensional.

Los tres cuadrados localizados en las esquinas se encuentran unidos a través de unos cuadrados negros, cuya función es la de mostrarle al dispositivo lector de código QR, cuál es tamaño de los módulos del código, es decir, cómo son los pequeños cuadrados que contienen la información. Dichos cuadrados corresponden a los patrones de sincronización. El patrón de alineamiento corresponde a un pequeño cuadrado que se encuentra dentro de la estructura del código, en la parte inferior derecha y al igual que los patrones de reconocimiento, sirve para reforzar el conocimiento del dispositivo sobre la orientación del propio código.

Además de los patrones, en el código QR se encuentran diferentes zonas que corresponden a distintos tipos de información. En primer lugar se encuentra la información del formato, que consta de 15 bits separados utilizando separadores que almacenan la información sobre la forma en la que se ha creado el código QR, es decir, el patrón elegido para su creación y el nivel de corrección de errores correspondiente al mismo. El nivel de corrección de errores consiste en que dependiendo del mismo, se podrán restaurar más o menos datos en caso de que el QR quede dañado. Cabe destacar que a medida que aumenta el nivel (se pueden recuperar más datos) disminuye la capacidad de almacenamiento de información. Los niveles pueden ser L (se puede recuperar un 7 %), M (un 15 %), Q (25 %) y por último el nivel H (30 % de información restaurable [25].

También se encuentra la zona que da la información sobre la corrección de errores y la información sobre la versión, es decir qué densidad de código se está utilizando. La parte central del código restante, corresponde a los datos almacenados en el mismo. Los patrones y zonas descritas se pueden identificar en la Figura 3.1.

3.2.2. Características

El código QR presenta una ventaja con respecto al código de barras tradicional ya que permite almacenar desde varias docenas a cientos de veces más información de lo que puede almacenar el código de barras que corresponde a 20 dígitos. Además el tamaño

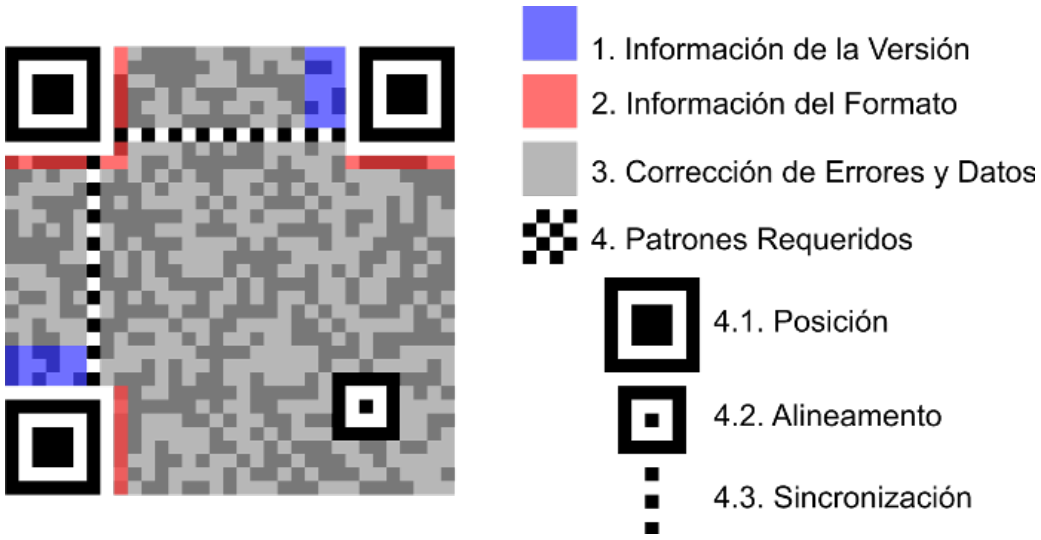

Figura 3.1: Estructura de un código QR.

del QR corresponde a una décima parte del código tradicional, siendo esta otra ventaja considerando la cantidad de información que es capaz de almacenar el código QR.

La información almacenada dentro de este código 2D puede estar almacenada en cualquier formato (numérico, símbolos, kanji, binario. . .), llegando a un máximo de 7.089 caracteres por QR. En caso de que el código quede parcialmente sucio o dañado es posible restaura hasta un 30 % de la información almacenada en él.

El QR cuenta con la posibilidad de ser leído de forma flexible en 360 grados. Como su propio nombre incluye la palabra rápido, *quick*, este código bidimensional puede ser leído de una forma rápida llegando a leerse en 30 milisegundos hasta 100 dígitos numéricos. Esto se debe a su diseño, ya que cuenta con tres patrones de detección, los mencionados patrones de reconocimiento [24].

Sin importar cómo se presente el código al dispositivo de lectura, será leído por el mismo ya que una de sus ventajas es la posibilidad de su lectura en cualquier dirección y además dicha lectura, gracias a los patrones de detección, será estable y se producirá a gran velocidad. Aunque el código QR suela presentarse en forma de cuadrado en blanco y negro, también podría estar diseñado usando diferentes colores y formas, e incluso contener imágenes en su interior [23].

3.2.3. Uso del código QR

Para generar un QR primero se debe agrupar e identificar la información que se pretende almacenar. El siguiente paso es utilizar un codificador, en este caso se podría utilizar alguno encontrado en internet, que permiten insertar la información que se pretenda codificar ya sea una url, texto, imagen, etc. Después de utilizar la herramienta se obtendrá un código QR. Para utilizar el mismo el código debe quedar guardado de alguna forma, ya sea de manera digital, impreso en un papel, en un póster, etc. [26].

Para que un usuario pueda acceder a la información almacenada en el código debe utilizar un decodificador, aunque esto quizás no suene como una tarea fácil, es bastante sencilla ya que hoy en día una gran cantidad de móviles cuentan con un decodificador de códigos QR en la cámara, por lo que bastaría con enfocar la cámara a donde se encuentre el mismo, como si se pretendiera sacar una foto, y se redirigirá al usuario a la información almacenada. En caso de que el móvil no tenga dicha información integrada, se puede usar alguna aplicación disponible para cumplir con esa funcionalidad.

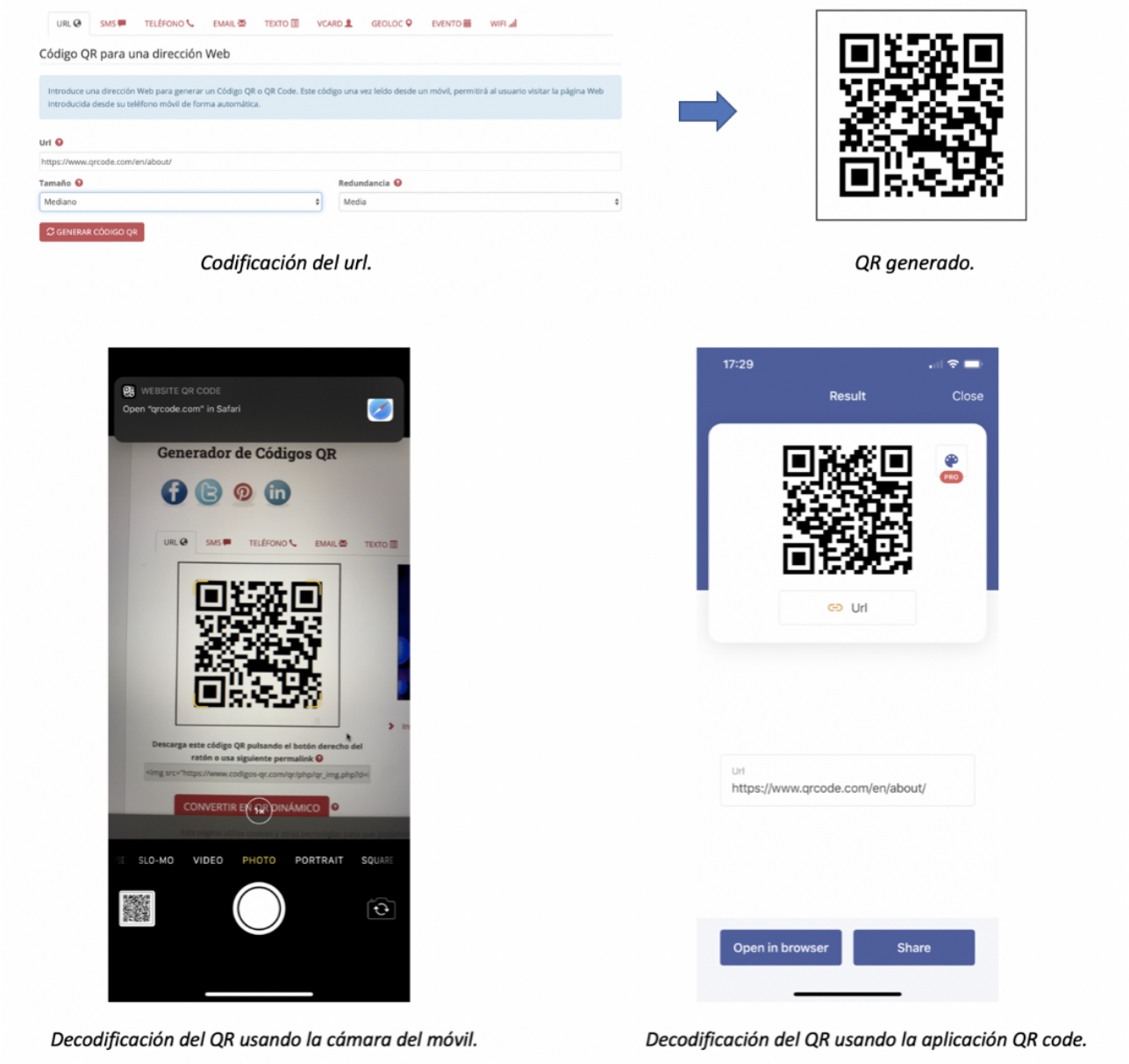

Figura 3.2: Ejemplo de codificación y decodificación del QR.

En la Figura 3.2 se muestra un ejemplo de codificación y decodificación de información a través de un código, siendo la información almacenada en el mismo la página de descripción de códigos QR [24].

3.3. Ejemplos de uso

Dada la sencillez tanto en la generación como en el uso del código QR, el uso de este se puede encontrar en muchos sectores y actividades de la población. Se utiliza como un enlace con medios online, es decir, en el código se incluye el link de la página de alguna empresa o de algún tipo de información asociado al mismo, como se ha mostrado en el ejemplo en la figura 3.2. En Australia se utiliza para identificar a los animales, para la distribución y etiquetado de botellas de gas y además se usan en el proceso de las pruebas de sangre [27].

En este trabajo el uso del código QR será específicamente orientado al sector del transporte, basando la venta de billetes para el transporte público y su validación a través de QR. Este es el caso de Justride que se basa en una nube implementada en transportes públicos como el MTA de Nueva York y El Metrolink de Los Ángeles en los que el usuario puede acceder a los servicios públicos utilizando la aplicación para comprar el billete que consta de un código QR y validarlo utilizando los lectores, lo que permite la identificación de los pasajeros [8].

Otro ejemplo es *ten+*, la aplicación móvil del transporte público de Tenerife. A través de la utilización del servicio, un usuario puede comprar un billete o abono utilizando la aplicación móvil. Una vez obtenido dicho billete, cuando el pasajero entre al transporte público deseado, deberá leer el código QR que encontrará dentro del mismo para validar y pagar por el viaje. En este caso hay que establecer la distinción entre el viaje en autobús y en tranvía. Si se trata del tranvía el usuario solo debe validar/leer el código QR cuando entra en el vehículo, sin embargo, en caso de que esté viajando en autobús debe validar el billete tanto a la entrada como a la salida. La doble validación se debe a que el usuario pagará únicamente por el tramo recorrido, en contraste al tranvía en el que el pasajero paga una cuota única que no depende del número de paradas ni la distancia recorrida [28].

3.4. Vulnerabilidades

La principal vulnerabilidad o ataque directo a la integridad del código QR consiste en una manipulación del mismo. En este caso se podrían distinguir dos escenarios diferentes. El primer caso sería que un atacante puede simplemente adoptar el estilo del QR existente y generar, es decir imprimir, uno nuevo con la información que quiera y sustituir el original por el QR del atacante. En dicho caso un usuario podría leer el código pensando que obtendría información verídica, sin embargo caería en la trampa del atacante.

Podría tener lugar también otra manipulación del código, esta no requiere tanta preparación ya que un atacante podría simplemente modificar algún módulo del QR pintando de blanco o negro, y de esta forma modificando el contenido del mismo. Este ataque tendría el mismo resultado para el usuario que desee decodificarlo usando un dispositivo móvil, sin embargo sería más sencillo de hacer [25].

Además de los ataques y las vulnerabilidades del código bidimensional cabe destacar que también podría ser afectado el dispositivo móvil que posee el software que permite al usuario la lectura del mismo. En este caso, el *phishing* o la suplantación de identidad consiste en la modificación del código QR en caso de que contenga un link para de esta forma redirigir al usuario a una página web fraudulentas. El objetivo de este ataque es que el usuario proporcione sus credenciales o sus datos bancarios pensando en que está accediendo a una determinada página web, mientras que el atacante obtiene dichas credenciales que puede utilizar de cualquier forma que quiera suplantando su identidad. Para que un usuario evite este tipo de ataques una recomendación es el uso de aplicaciones de lectura del código que permitan la muestra de una previsualización de la página o el contenido que se mostrará al acceder para que el usuario así compruebe si se trata de un sitio o unos datos legítimos y no de una estafa.

El fraude es otra amenaza para el código QR. En una situación en la que el usuario vea alguna oferta o quiera obtener información sobre algún producto en concreto, si el código QR está manipulado, podría ser redirigido a una página idéntica pero dicha web no sería propiedad de la empresa que el usuario cree. Por lo que podría llegar a comprar algún producto de forma fraudulenta sin saberlo.

Además del QR, el software del dispositivo dedicado a la lectura del QR podría ser atacado a través de inyección de comandos o desbordamientos del búfer en caso de que la información codificada no sea comprobada. Si eso ocurriera, el atacante podría llegar a tener un control total del dispositivo que usó el usuario en la decodificación del código bidimensional. Si el usuario accede a un sitio no legítimo podría ser víctima de una propagación de malware, es decir, el usuario al entrar en la supuesta página instalaría en su dispositivo un programa maligno que podría empezar a controlar el mismo o incluso obtener las contraseñas y huellas del usuario que se encuentran almacenadas [21].

Por último cabe destacar que los ataques basados en ingeniería social son bastante populares y peligrosos. En este tipo de ataques se incluye el *spear phishing*, un ataque consistente en el envío de correos con información fraudulenta, en este caso códigos QR personalizados según las preferencias del usuario para que este caiga en la trampa. Otro ejemplo sería la colocación de estos códigos, que podrían llevar al usuario a páginas web fraudulentos o a información manipulada cuya lectura podría otorgarle el control del dispositivo al atacante, en lugares públicos por ejemplo en un restaurante fingiendo que proporciona un descuento en un servicio, o en alguna empresa utilizando la misma técnica.

Todos los ataques mencionados podrían ser utilizados en el entorno de uso de los códigos QR en el transporte público donde podrían suponer una amenaza para los usuarios, su identidad e incluso los detalles de pago de los billetes.

Capítulo 4

Ataques utilizando tecnología NFC

La tecnología NFC utilizada en el campo de transporte público se puede usar de dos formas diferentes. Por una parte el pasajero puede verificar su billete utilizando su dispositivo móvil con la aplicación de la empresa de transporte correspondiente instalada. Sin embargo, esa opción no es válida para todos los usuarios debido que a pesar del avance de la tecnología, hoy en día, no todos los dispositivos móviles cuentan con la tecnología NFC integrada.

La otra opción de validación se puede realizar a través de una *smartcard* o tarjeta inteligente. Una tarjeta inteligente podría ser de tres tipos. El primer tipo es el de tarjeta con chip integrado de lectura. Este tipo de tarjetas tiene una banda magnética electrónica que almacena los datos que posteriormente serán leídos; en la misma no se realiza ninguna operación lógica, se trata exclusivamente de una lectura de datos almacenados. El segundo tipo es el de las tarjetas con chips basadas en circuitos integrados. Este tipo de tarjetas se basa en que el contenido que queda almacenado en las mismas se encuentra encriptado y el acceso a los datos almacenados debe ser autenticado. En este tipo de tarjetas se incluyen las smart cards tales como la MIFARE.

El último tipo de tarjetas es el de las tarjetas con chip basadas en circuitos y con un microcontrolador seguro. Gracias a este microcontrolador, es decir, a un sistema operativo integrado, son capaces de realizar cálculos lógicos de forma interna con los datos almacenados. Este tipo de tarjetas son como miniaturas de PC. Los últimos dos tipos de tarjetas son los que se llaman tarjetas inteligentes [2].

Cuando un usuario desea validar un billete utilizando NFC, ya sea a través de una smartcard o el dispositivo móvil, el funcionamiento es el mismo. Al entrar en el transporte debe acercar su dispositivo NFC al lector, y dicho lector se comunicará con el servidor correspondiente con el objetivo de proporcionar los datos necesarios para poder validar la autenticidad del billete y proceder al pago del mismo.

4.1. Clonación de tarjetas Mifare

Las tarjetas MIFARE son tarjetas que tienen un chip basado en circuitos integrados. Toda la información del interior está cifrada, y no debería ser accesible a cualquiera sino las personas autorizadas al acceso de los datos en su interior. Sin embargo, el hecho de que estas tarjetas cuentan con un cifrado y un control de acceso no siempre significa que la información en su interior esté segura.

4.1.1. Tarjetas Mifare Classic 1K

Las tarjetas MIFARE Classic son unas de las tarjetas más utilizadas mundialmente. Se trata de unas tarjetas baratas y cuyo uso está extendido mundialmente por diferentes sistemas de entradas autorizadas a edificios, en el transporte público, etc.

Aunque este tipo de tarjetas no cuenta con una gran variedad de funcionalidades, destacan sobre todo por el almacenamiento de datos cifrados. En cuanto a su estructura, constan de una memoria dividida en bloques de datos de unos 16 bytes de almacenamiento.

La tarjeta MIFARE de tipo classic 1K consta de 16 sectores formados por 4 bloques de 16 bytes. Los otros tipos de tarjetas se distinguen según la cantidad de sectores que contienen. El bloque 0 del sector 0 contiene datos que se consideran especiales, ya que los primeros bytes de dichos datos contienen el UID, esto es, el identificador único de la tarjeta correspondiente. El siguiente byte corresponde al BCC (*bit count check*), que se obtiene del cálculo de las XORs de los primeros 4 bytes, es decir, del UID. Por último, los 11 bytes sobrantes corresponden a los datos del fabricante.

Para que se pueda producir la lectura de los datos almacenados en la tarjeta inteligente se debe de autenticar el acceso al contenido del sector de datos correspondiente. Dicha autenticación está basada en un sistema de dos claves, ambas de 6 bytes denominadas “Clave A” y “Clave B”. Además de esas claves se hace uso de los permisos de acceso que se encuentran en la parte de Access Condition, una parte de 3 bytes, quedando sobrante un byte llamado “byte U” que no tiene ninguna funcionalidad determinada. A través de este sistema el acceso a los bloques se realiza de forma independiente, es decir, que el lector sólo accede al sector que le interesa para leer los datos almacenados en el mismo [29].

4.1.2. Ejemplo práctico de la clonación de una tarjeta

En este caso práctico se va a demostrar que existe la posibilidad de clonar una tarjeta MIFARE Classic 1K. Este tipo de tarjeta es utilizado en el transporte público de Suecia. El contenido de este tipo de tarjeta no debería ser obtenido a no ser que se tengan las claves para la misma, es decir, la clave A y B mencionadas anteriormente.

El problema de algunas tarjetas es que dejan como claves de los sectores de datos las claves predeterminadas que vienen por defecto. Esto desencadena una vulnerabilidad en la misma. En este ejemplo práctico se utilizará la aplicación para Android llamada “MIFARE Classic Tool”. Esta aplicación tiene como objetivo la lectura y escritura de tarjetas MIFARE Classic 1K.

El proceso de lectura de la tarjeta haciendo uso de la aplicación mencionada se realiza utilizando un archivo con claves que tiene la aplicación. El archivo consta de una gran cantidad de claves por defecto de las tarjetas de este tipo, además de claves utilizadas comúnmente. Por ello, esta técnica tan solo funcionará con tarjetas cuyas claves de fábrica no fueran cambiadas. En este caso se procede a la lectura de una tarjeta de transporte público sueco.

En el menú principal de la aplicación se hallaron diferentes opciones: la opción de leer una etiqueta (tarjeta), escribir etiqueta y varias más que no son relevantes para este trabajo y que aparecen mostrados en la figura 5 (en la parte izquierda de la misma). Para leer los datos de la tarjeta se elige la opción de leer la etiqueta. Al elegir dicha opción se observa que aparecen varias características que se puede tener en cuenta durante la lectura, se puede especificar el sector que se desea leer y el archivo de clave. Se va a proceder a la lectura completa de la tarjeta por lo que la opción de sectores se deja intacta, mientras en la opción de archivo de claves se eligen las claves “extended-std.keys” y std.keys” que son los archivos con las claves por defecto que vienen con la aplicación, tal y como se muestra en la parte derecha de la figura 4.1.

Después de elegir todas las características del mapeado se procede a la lectura de la tarjeta. Para ello se debe acercar la tarjeta al dispositivo móvil y elegir la opción de “Comenzar mapeo y leer etiqueta”. Después de pulsar el botón, la aplicación procederá a la lectura de la smartcard.

Tal y como se observa en la figura 4.2, después de unos minutos de lectura se obtienen todos los sectores de la tarjeta con sus claves A y B, y con los códigos de acceso. El sector 0 es de los más importantes ya que en él se encuentra el identificador único de la tarjeta. Con estos datos (la aplicación permite la opción de guardar el archivo generado) se puede realizar una copia de la tarjeta. Se puede copiar tan solo el sector 0 de la tarjeta para obtener una tarjeta con un identificador idéntico o se puede clonar cada uno de los sectores. En caso de obtener tan solo el primer sector, al ser el identificador idéntico, la tarjeta con el sector clonado sería reconocida como la legítima. Mientras que si se clona la tarjeta entera, la tarjeta ilegítima contaría con todos los datos de la tarjeta clonada, esto podría proporcionar una ventaja al usuario que la utilice , ya que si clona un billete o bono en el que tiene una cantidad de dinero determinada, si la clona al principio con la cantidad de dinero intacta, después de gastar el dinero podría generar una tarjeta con la información de su tarjeta original teniendo la totalidad del dinero. Sin embargo, para proceder de esta forma se debe de tener, no solo una tarjeta MIFARE Classic 1K en blanco, sino una tarjeta que permita que se sobreescriba el UID de la misma, algo que no permiten todas las tarjetas que se puede encontrar en el mercado.

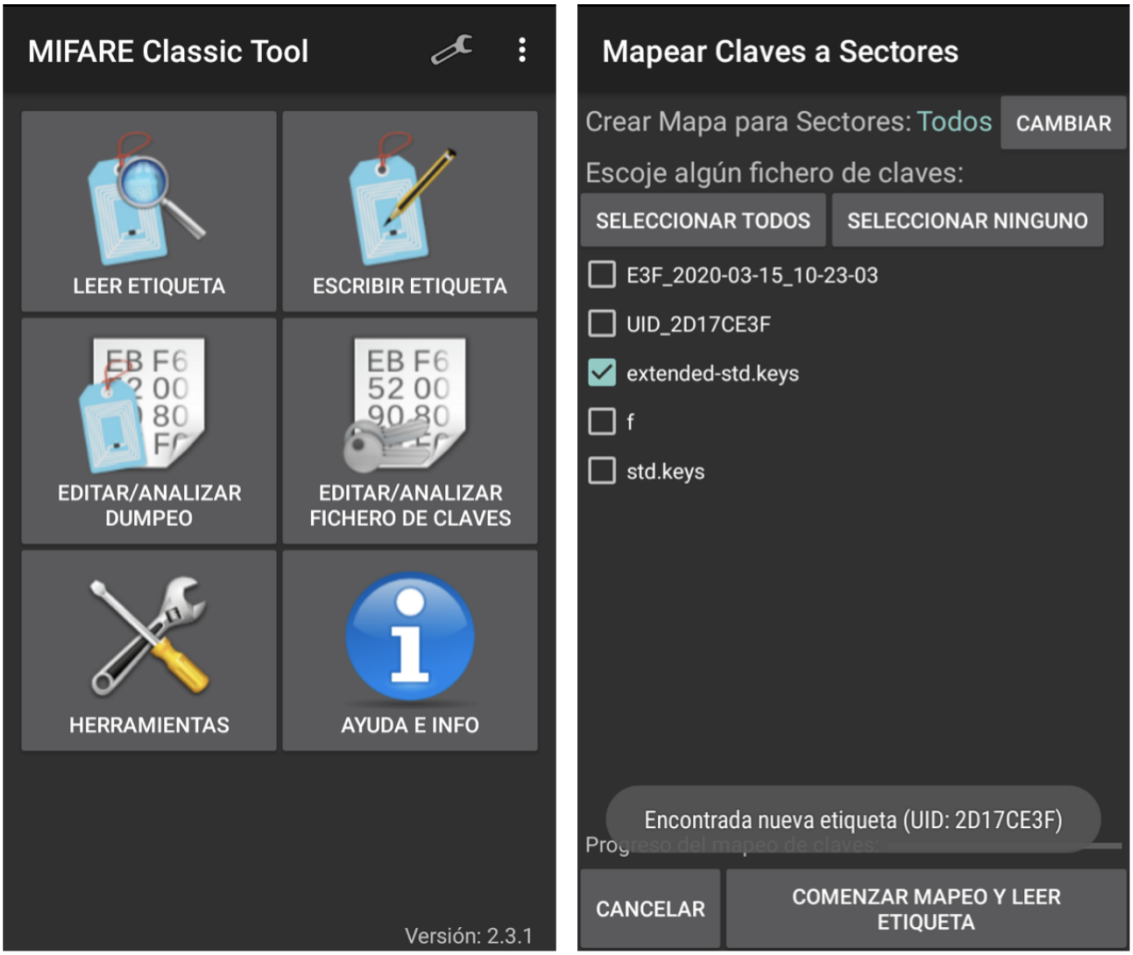

Figura 4.1: Muestra del menú principal y opciones de lectura de la tarjeta.

4.2. Relay Attack

La comunicación entre la *smartcard* y el lector NFC se basa en la autenticación mutua. Es decir, ambos participantes deben demostrar que poseen las acreditaciones necesarias para que la comunicación tenga lugar. Después de autenticarse mutuamente tiene lugar la comunicación encriptada, por lo que cualquier intento de intercepción de la información intercambiada sería difícil y requeriría de mayor conocimiento de manipulación de hardware y conocimiento sobre el criptoanálisis para intentar romper el algoritmo.

Es por ello que los ataques de retransmisión o *relay attack* no consisten en la intercepción de los datos intercambiados, sino en el engaño de los dispositivos de que el atacante es una tarjeta o un lector legítimo [30].

4.2.1. Funcionamiento de la comunicación

En este caso para probar que este tipo de ataque podría llevarse a cabo, se tiene en cuenta que la estructura del sistema mediante el cual se comunica una *smartcard*

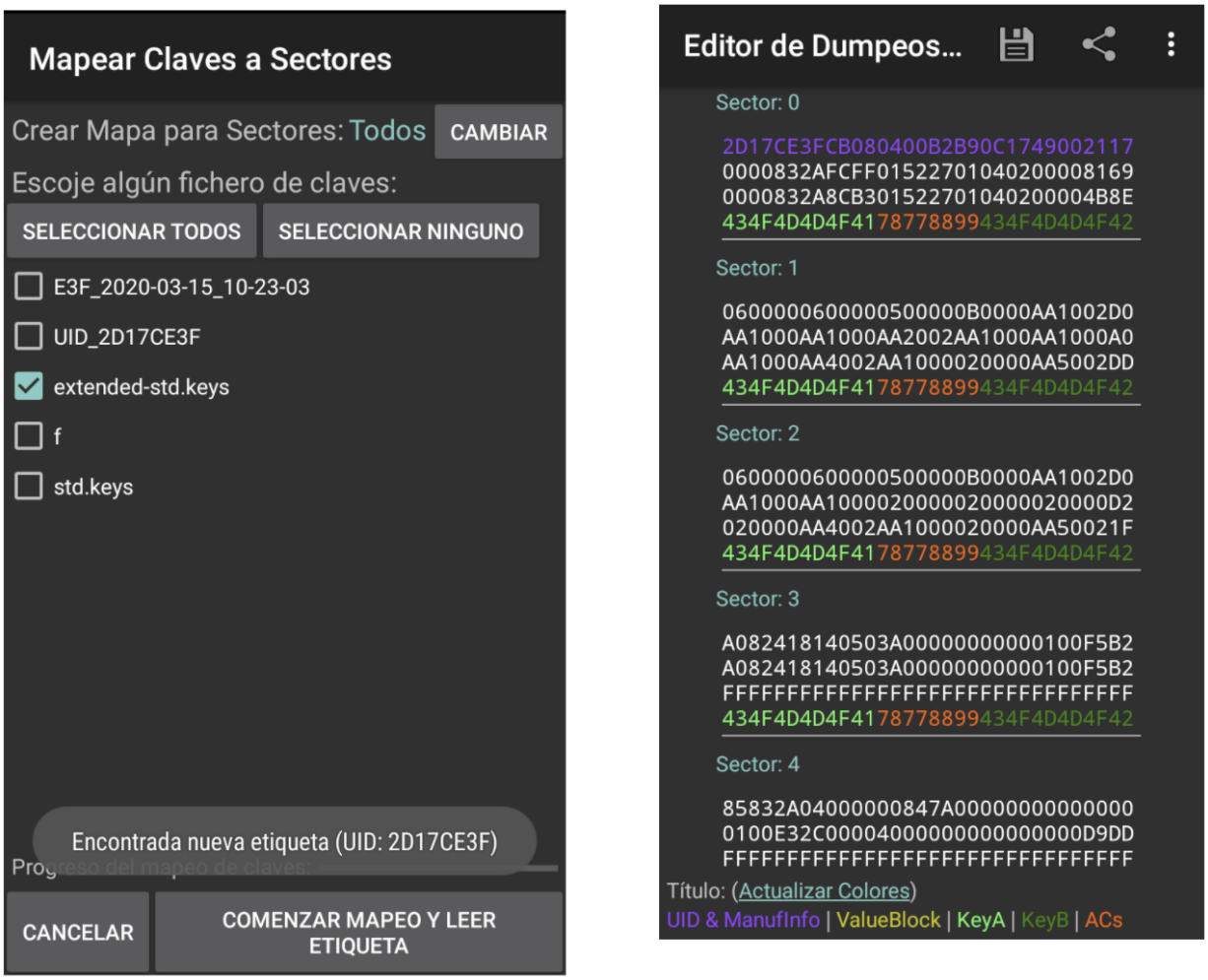

Figura 4.2: Archivo que proporciona la información de los bloques de la tarjeta.

y un lector NFC es la presentada a continuación en la figura 4.3. Se puede observar que consiste en la validación de la tarjeta del usuario a través de un lector dentro del transporte elegido o en la parada del mismo. Al validar la *smartcard* que corresponde a la tarjeta de transporte correspondiente, el lector se comunica con el servidor de la compañía de transporte para verificar los datos del usuario, verificando la autenticidad y comprobando los recursos del usuario, es decir, si su tarjeta contiene el saldo suficiente para realizar el viaje.

En caso de que el servidor compruebe que el usuario tiene todo lo necesario para poder subirse al vehículo, devuelve una respuesta de confirmación, o en caso de que durante la comprobación resulte que el usuario no tiene los medios necesarios para viajar, una respuesta de denegación. Al abrir esa respuesta en el lector NFC se muestra el mensaje para que de esta forma el usuario sepa si la validación ha tenido lugar o no. Además del usuario, en caso de que la validación del billete se produzca dentro del vehículo de transporte, el mensaje de comprobación también le sirve al conductor para que sepa que todo se ha realizado correctamente.

Después del procedimiento mostrado en la figura 4.3, el último paso del mismo consiste en la comunicación del lector NFC con la tarjeta. Durante esta comunicación, el lector escribe en la tarjeta datos que demuestran que en este momento contiene un billete

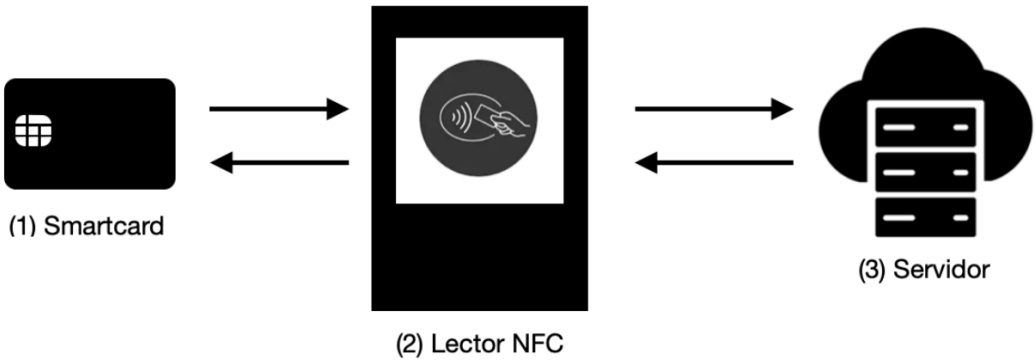

Figura 4.3: Funcionamiento de la comunicación de la tarjeta de transporte con el lector.

válido.

4.2.2. Implementación del ataque

El objetivo del ataque de retransmisión es conseguir ese mensaje del servidor que autentica la validez del billete. Esto se debe a que no en todos los medios de transporte la validación del billete se realiza delante del conductor. En algunos casos es obligación y responsabilidad del usuario validar el billete haciendo uso de los lectores NFC disponibles. Para comprobar que los usuarios han pagado por el uso del transporte, se suelen emplear medidas como la comprobación aleatoria de billetes por medio de los trabajadores de la empresa de transporte. Durante esa comprobación, los trabajadores utilizan un lector NFC para verificar la tarjeta de transporte del usuario y asegurarse de que en su contenido se encuentra una confirmación del billete.

A través del uso de este ataque se va a copiar la confirmación del billete original en otra tarjeta, que no ha sido validada, para que en el caso de que alguien quiera comprobar su autenticidad, aparezca la misma confirmación que en la tarjeta original proporcionando así una validación en la segunda tarjeta por la que el atacante no ha pagado. De esta forma este ataque se basa en el funcionamiento de los ataques de retransmisión, ya que se le hace pensar al lector de la persona que comprueba el billete que este es verídico.

4.2.3. Material usado en el ataque

Para simular el ataque descrito en el apartado 4.2.2 se hace uso de los siguientes materiales:

- *Dos NFC tags*: un tag que hará de tarjeta de transporte válida. Y el otro tag que tendrá la función de recibir la confirmación del otro tag para simular que es un billete válido.

- *Un móvil con Android*: en el que se encuentra instalada una aplicación que se encarga de comunicarse con el servidor, almacenar la respuesta obtenida y grabar esa respuesta en las tags.
- *Un servidor*: que será implementado en un portátil en este trabajo.

4.2.4. Funcionamiento del ataque

En la figura 4.4 se muestra el funcionamiento de la comunicación que tiene lugar entre las tags, el dispositivo móvil y el servidor. Tal y como se observa en la figura 4.4, el tag que hace de tarjeta legítima se comunica con el teléfono que manda el identificador del tag al portátil. Cuando el servidor recibe la información perteneciente a el tag, comprueba que es válida, devuelve una respuesta al lector NFC. Cuando recibe la respuesta, el lector en vez de escribir esa confirmación en el tag legítimo, la almacena en su memoria para poder escribir dicha respuesta no solo en el tag legítimo sino también en el ilegítimo.

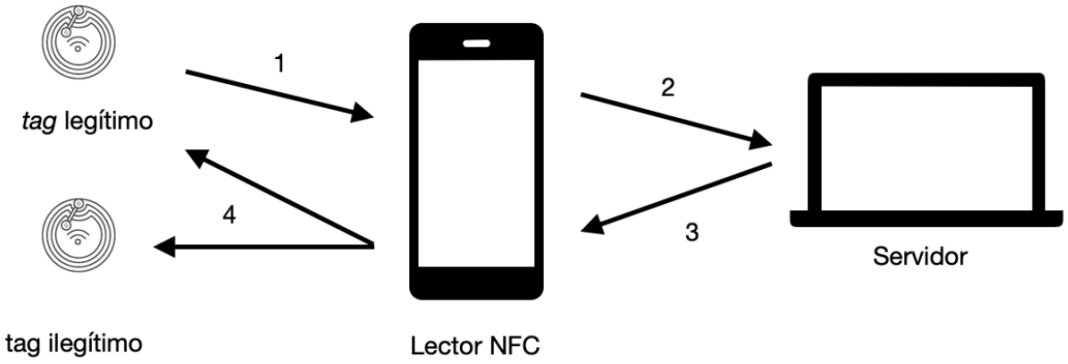

Figura 4.4: Comunicación de los tags con el lector y el servidor.

Comunicación del tag legítimo con el lector NFC

La comunicación del tag cuya función es la de una tarjeta de transporte legítima que se produce con el NFC del móvil, corresponde a la comunicación número 1, de la figura 4.4. El móvil detecta de forma automática el tag y se muestra un aviso con el identificador del tag en el lector. En caso de que el tag no se encuentre lo suficientemente cerca del dispositivo del móvil se mostrará un error. En caso de que el NFC no esté disponible en dicho dispositivo, la aplicación se cerrará automáticamente.

Para mostrar el identificador del tag, se utiliza una función, dentro de la aplicación, que convierte la información leída del tag que viene en formato de bytes, en una cadena hexadecimal. Tal y como se muestra en la Figura 4.5, lo primero que se hace es comprobar que el tag esté disponible y el dispositivo móvil pueda comenzar la comunicación. Se lee de esta forma la pegatina, guardando el identificador en un array de bytes, el *tagID*, que posteriormente se recorre en un bucle para transformarlo en una cadena hexadecimal y

mostrarlo en la pantalla. La variable *id* contiene el identificador formateado y se muestra en la parte de la pantalla que corresponde a *Contenido*. La última parte del código mostrado corresponde a una condición que será explicada más adelante ya que no forma parte de este primer paso.

```
private void readFromIntent(Intent intent) {
    String action = intent.getAction();
    if (NfcAdapter.ACTION_TAG_DISCOVERED.equals(action)
            || NfcAdapter.ACTION_TECH_DISCOVERED.equals(action)
            || NfcAdapter.ACTION_NDEF_DISCOVERED.equals(action)) {

        byte[] tagId = getIntent().getByteArrayExtra(NfcAdapter.EXTRA_ID);
        id = "";
        assert tagId != null;
        for (byte b : tagId) {
            String x = Integer.toHexString(((int) b & 0xff));
            if (x.length() == 1) {
                x = '0' + x;
            }
            id += x + ' ';
        }
        Contenido.setText(id);
        if(!read){
            send_data();
            read = true;
        }
    }
}
```

Figura 4.5: Lectura del tag y el envío del identificador.

En la figura 4.6 se muestra la aplicación de Android desarrollada. En la imagen a la izquierda se muestra la aplicación que se muestra en el inicio. En la parte de arriba se muestra el campo en el que se mostrará el identificador del tag leído en esta primera comunicación. Después se muestra un botón cuya función será la de mostrar la respuesta del servidor, un espacio en el que se mostrará dicha respuesta y por último el botón correspondiente a la función de escribir la información en el tag. Las últimas funciones mencionadas serán explicadas en sus apartados correspondientes. En la imagen de la derecha de la figura 4.6, se puede ver cómo el identificador leído se muestra dentro de la aplicación.

Comunicación entre el lector NFC y el servidor

Después de que el lector reconozca el tag correspondiente, el servidor recibe el identificador del dispositivo móvil a través de la función *send_data* que se muestra en la Figura 4.5. Cabe destacar que dicha función se encuentra dentro de un una condición *if* ya que el objetivo es que solo se reciba la respuesta del servidor una vez. Es decir, en cuanto el tag se acerca al lector, éste automáticamente se comunica con el servidor y recibe una respuesta. Sin embargo, para escribir la respuesta en el tag, también se

Figura 4.6: Muestra de la aplicación y la detección del tag por el lector NFC.

debe acercar el tag al lector, por ello para evitar que al escribir en el tag se vuelva a solicitar una respuesta del servidor, se utiliza una variable booleana que en caso de que se haya producido la primera comunicación cambia su valor a *false* y no permita pedir más respuestas al servidor.

En el servidor tal y como se muestra en la figura 4.5, se mostrará el mensaje de "Petición recibida del id del tag" y el servidor comprobará el identificador para comprobar sus credenciales. Si todo ha salido correctamente tal y como se muestra en la parte izquierda de la figura 4.7, el servidor envía el mensaje y muestra que la respuesta ha sido enviada.

En el lector se muestra la notificación con el mensaje recibido del servidor. Tal y como se ve reflejado en la figura 4.7, el mensaje de confirmación consta del id del tag, de un mensaje que refleja si ha sido aceptada (Aceptado) o no (Denegado) y por último la hora y la fecha de la comprobación. Cabe destacar que esa notificación desaparecerá en unos segundos, por lo que queda habilitado el botón de "Mostrar respuesta" en caso de que el usuario quiera volver a leer su contenido.

Figura 4.7: Muestra del identificador del tag en el servidor y la respuesta del mismo.

Escritura de la respuesta/autenticación en los tags

En este momento, la respuesta del servidor que contiene los datos de autenticación se encuentra almacenada en la aplicación. Por ello, basta con apretar el botón *Escribir respuesta en el tag* en la aplicación, acercar el tag al que se quiere transmitir el mensaje, y tal como se ve reflejado en la figura 4.10, quedará almacenado en el interior del mismo.

Para poder escribir en el tag la aplicación hace uso de la función mostrada en la figura 4.8. La primera línea de la función utiliza a su vez otra función *createRecord* que formatea el mensaje recibido a un formato permitido para poder ser escrito dentro del contenido del tag y después se convierte en un mensaje NFC. La siguientes líneas del código corresponden a la definición del tag en el que se va a escribir, su posterior conexión, escritura del mensaje y por último la desconexión de la comunicación.

```
private static void write(Tag tag) throws IOException, FormatException {
    NdefRecord[] records = { createRecord(MESSAGE)};
    NdefMessage message = new NdefMessage(records);
    Ndef ndef = Ndef.get(tag);
    ndef.connect();
    ndef.writeNdefMessage(message);
    ndef.close();
}
```

Figura 4.8: Función para escribir la respuesta en el tag elegido.

En caso de que dicha función se ejecute con éxito se mostrará al usuario un mensaje en el móvil correspondiente a la captura de pantalla mostrada en la parte izquierda de la figura 4.9, en caso de error se mostrará el mensaje de error correspondiente a la parte derecha de la figura 4.9.

Figura 4.9: Notificaciones sobre el estado de la escritura de la información.

Este paso hay que realizarlo tanto con el tag legítimo como con el ilegítimo. Después de este último paso se procede a la lectura de ambos tags, con cualquier aplicación que conste de la opción de lectura de dispositivos NFC, y se podrá descubrir que ambos tags cuentan con una verificación auténtica proporcionada por el servidor. En la figura 4.10 se muestra el contenido leído de ambas pegatinas NFC haciendo uso de la aplicación Android llamada “Lector NFC”.

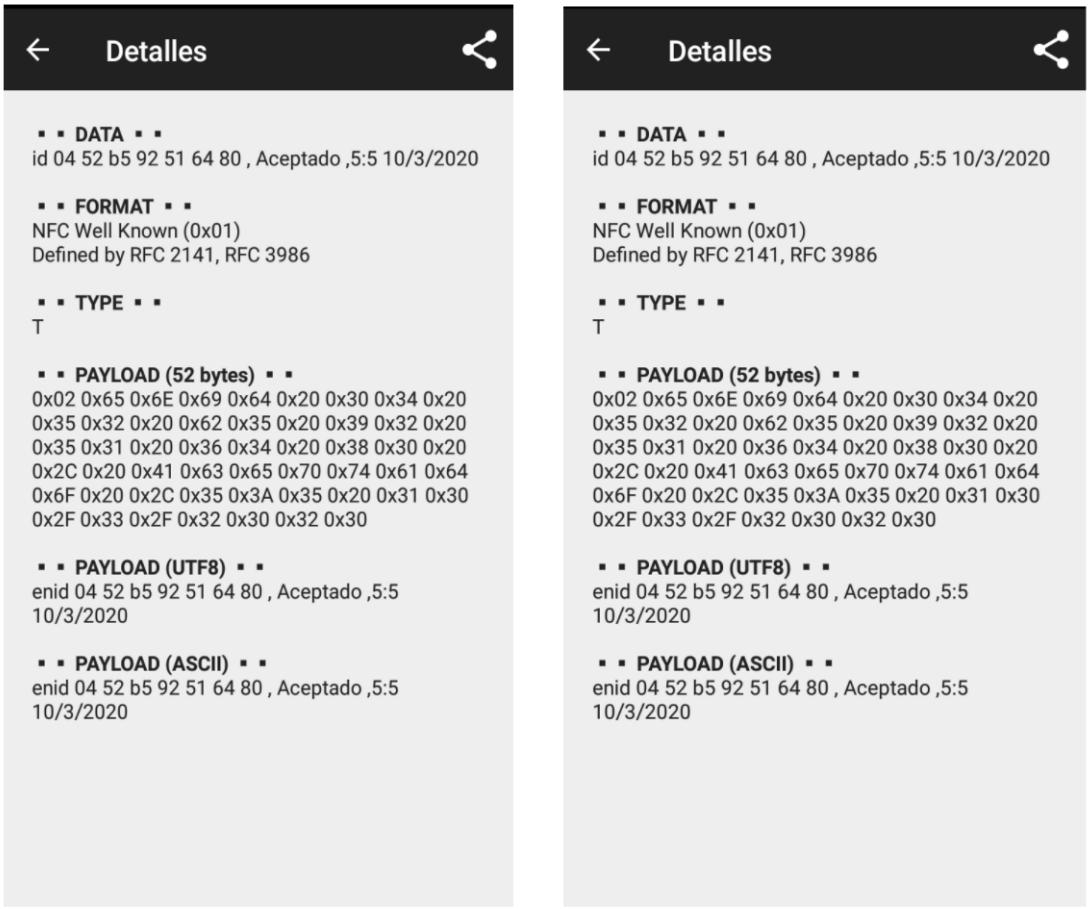

Figura 4.10: Contenido de ambos tags.

Capítulo 5

Ataques utilizando códigos QR

En este capítulo se propone un ataque teórico que podría utilizarse para producir un funcionamiento errático de un dispositivo utilizado en la validación de billetes en el transporte público. Como se ha descrito anteriormente este tipo de validación consiste en la lectura de un código QR dentro del vehículo de transporte al menos una vez, ya que en algunos casos esto debe realizarse tanto a la entrada como a la salida del transporte y otras veces (al tratarse de un pago único, en contraste al pago por el recorrido realizado) se debe validar tan solo una vez. En esos casos, el dispositivo utilizado para la lectura del código bidimensional es el teléfono móvil, ya que hoy en día cualquier móvil que posea una cámara cuenta con la función de lectura de dichos códigos incorporada o la puede adquirir descargando una aplicación con ese propósito. El caso de ataque descrito a continuación tiene como objetivo corromper el dispositivo del usuario.

5.1. Funcionamiento de validación utilizando QR

La utilización de un sistema de validación basado en la lectura de un código QR supone una ventaja para el usuario. Esto se debe a que hoy en día la mayoría de los dispositivos móviles cuentan con la posibilidad de leer dichos códigos. Además cuando se aplica el uso en estas circunstancias es propio de la empresa proporcionar un software, compatible con todos los diferentes tipos de dispositivos utilizados en la validación de billete, que cuente con la funcionalidad de lectura del código QR.

El sistema consiste en que el usuario al entrar en el transporte público debe buscar el código bidimensional. Ese código puede encontrarse en diferentes sitios. Por ejemplo en el caso del transporte público de Alemania, el *Touch & Travel*los QR se encuentran en las estaciones de trenes o guaguas en los denominados *touchpoints* que no son más que unas pegatinas que contienen el código que debe ser leído. Cuando una persona entra en el transporte público de Alemania, si quiere utilizar la validación por medio del QR debe validarlo utilizando la aplicación, antes de subirse es decir, en la parada de subida y al bajarse en la parada final. Al realizar esto, se le descontará el precio del camino recorrido.

En contraste al sistema utilizado en Alemania, en Tenerife, la empresa de transporte Titsa, utiliza un sistema de funcionamiento exactamente igual el del *Touch & Travel*, pero con una pequeña diferencia que es que dicho código no se encuentra en las estaciones correspondientes si no que se encuentran dentro del propio vehículo.

5.2. Manipulación del código QR

Cuando se realiza la lectura del código, la aplicación se comunica con el servidor central de la empresa de transporte, validando los datos del pasajero y enviando la confirmación a la aplicación del usuario. Esa comunicación podría ser interceptada, pero el éxito de esa intercepción, es decir, de ese ataque denominado *Man in the Middle* dependería de la seguridad proporcionada por la empresa de transporte. Por ello en caso de que utilicen técnicas de cifrado, a pesar de que la información intercambiada entre el usuario y el servidor sea interceptada podría ser inservible si se desconoce la clave del cifrado.

La manipulación del propio código QR es un ataque más simple y directo. Un atacante podría imprimir su propio código y sustituir el original proporcionado por la empresa de transporte. La manipulación de dicho código podría realizarse de diferentes formas. Por una parte podría consistir en la manipulación directa del mismo, es decir, el atacante no proporcionará un QR nuevo, sino cambiaría el ya existente. Basta tan solo con cambiar uno de los módulos del mismo para que este quede totalmente inutilizable. Además de quedar inutilizable, algo que impediría al usuario leerlo correctamente, se podría modificar el código para que ataque el lector de QR utilizado, que en este caso es el dispositivo móvil.

En cuanto al ataque al dispositivo del usuario cabe destacar que para que se pueda realizar la validación del billete del pasajero, la aplicación utilizada por este debe tener acceso a internet. Por ello si un atacante añade información maliciosa en el código, podría generar la instalación de algún programa malicioso cuyo objetivo sería el de interceptar la información personal almacenada en el dispositivo del usuario.

Por otra parte el atacante podría proceder a la sustitución completa del código bidimensional de validación del billete. Podría por ejemplo, proporcionar un QR de la empresa de transporte pero con información adicional. Esos datos adicionales serían código malicioso que podría utilizarse para emplearla técnica de *SQL Injection*. Dicho ataque consiste en la obtención de los datos directamente de la base de datos. Esto se debe a que en el QR se inyectan sentencias SQL que, dependiendo de la seguridad de la propia Base de datos ante este tipo de vulnerabilidades, podría proporcionar datos personales de la misma al atacante.

Además de la inyección de sentencias SQL se podrían incluir instrucciones dirigidas al Sistema Operativo del servidor encargado de la verificación de billetes, que al ser ejecutadas podrían causa la denegación de servicio e incluso la instalación de programas maliciosas en el mismo. Cabe destacar que el éxito de dicho código malicioso depende en su totalidad de las medidas de seguridad tomadas para evitar este tipo de vulnerabilidades [31].

5.3. Implementación de un ataque

Han sido expuesto ejemplos de ataques que podrían amenazar el proceso de validación de billetes, el dispositivo del usuario y el servidor. Sin embargo, hace falta destacar que después de verificar el billete este podría ser usado más de una vez, algo que no debería ser permitido a pesar de ser posible.

5.3.1. Reutilización de billetes

Para describir el funcionamiento de esta vulnerabilidad se describe el funcionamiento de una aplicación de transporte público de Tenerife. El funcionamiento del pago por el billete consiste en la instalación de una aplicación en el dispositivo del usuario. Para poder hacer uso de ella, se debe registrar escribiendo todos sus datos personales necesarios.

Un usuario registrado, debe iniciar sesión para poder proceder a la compra del billete. Dentro de la aplicación se puede encontrar diferentes secciones, la de información que consta de información general de la propia aplicación y del horario de las guaguas, la sección de billetes en el que se encuentran los billetes con los que actualmente cuenta el usuario, los recibos en los que se haya el historial de movilidad del usuario y por último la sección de compra en la que el usuario puede adquirir diferentes tipos de billetes.

Cuando un usuario quiera hacer uso del transporte público debe tener un billete válido en la sección de billetes de su aplicación. Cuando entre en el transporte, por ejemplo en la guagua, debe elegir el billete que quiere validar y se le abrirá la cámara para que pueda validar el código QR que encontrará en el interior del vehículo. Cuando le llegue a la aplicación la confirmación del servidor, el usuario obtendrá su billete que tendrá que mostrar al conductor.

El billete consta de diferentes elementos, los datos del usuario, el número del billete, un código QR estático y una imagen en movimiento. La figura en movimiento es lo que será verificado por el conductor para asegurarse que el pasajero haya pagado por el viaje. La mencionada imagen giratoria contiene números con colores alrededor, se encuentra en movimiento y varía dependiendo de la hora en la que se crea el billete y del tipo de transporte e incluso el número de la guagua. Cabe destacar además que dicha imagen rotatoria solo aparece en un rango de tiempo determinado que desaparece con el tiempo, al igual que el código QR.

El sistema descrito es sencillo para el usuario, y también para el conductor del vehículo ya que con verificar que la imagen esté presente en el billete se puede verificar que se trata de un billete verídico. Esto a su vez tiene una debilidad. Y es que al ser la figura la única forma de comprobación del billete (podrían serlo los datos personales del pasajero comprobando su documentación de identificación personal, algo que no suele ocurrir) ésta fácilmente podría ser duplicada.

En la figura 5.1 se muestra a la izquierda un billete válido y a la derecha un billete

ya utilizado. A pesar de que la imagen giratoria cambie en diferentes trayectos se debe considerar la situación en la que un pasajero se sube en la primera parada del trayecto. Valida el billete, saca una captura de pantalla del mismo y utiliza un sistema de grabación de pantalla que le proporciona un vídeo del propio billete del que puede recortar únicamente la imagen que fácilmente puede convertir en un gif (es decir, una imagen en movimiento). Si envía este gif a otro usuario que pretende utilizar el mismo vehículo pero en la siguiente parada, este fácilmente puede utilizar el gif enviado para simular figura giratoria y pega el código QR del billete del usuario principal además de modificar los datos del billete como el número y la fecha.

Al realizar el procedimiento anterior, se puede observar que de esta forma el segundo pasajero tendría un billete falsamente válido, que el conductor del vehículo dejaría pasar sin ningún problema. Cabe destacar que la acción de duplicado del billete podría llevarse a cabo más de una vez, proporcionando un viaje gratuito a los usuario que quieran hacer uso de ese vehículo.

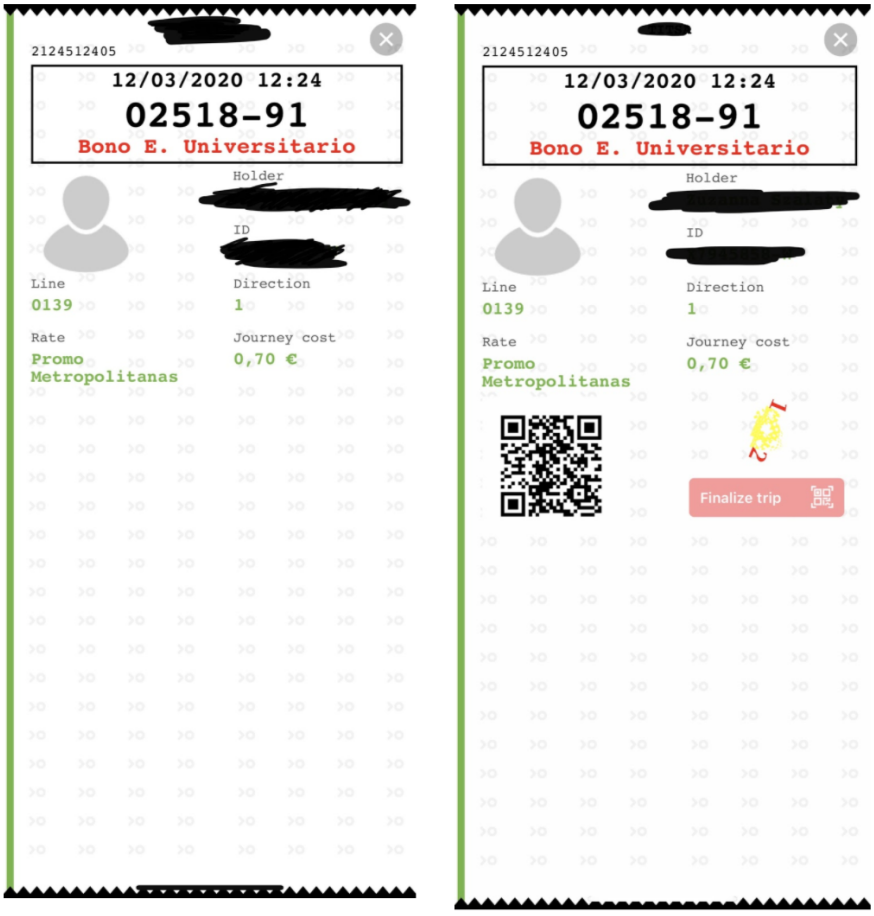

Figura 5.1: Muestra de un billete no válido (a la izquierda) y otro válido (derecha).

La forma de evitar que un billete sea utilizado más de un vez en este transporte en específico, sería que en vez de que el conductor compruebe visualmente el billete proceda a leer el código QR que se encuentra en el mismo, ya que los datos del código QR no podrían ser modificados tan fácilmente como en el caso anterior.

Capítulo 6

Presupuesto

En este capítulo se encuentran los costes estimados de los diferentes elementos de software y hardware que fueron utilizados durante la realización de los ejemplos prácticos.

6.1. Coste hardware

Nombre	Uds.	Precio/ud.
Ordenador personal	1	∼1500€
Tags	2	1€
Móvil con Android	1	∼300€
Smartcard	1	5€

Tabla 6.1: Tabla de costes del hardware

6.2. Coste software

Nombre	Uds.	Precio/ud.
Android Studio	1	0€
NetBeans	1	0€
MiFare Classic	1	0€

Tabla 6.2: Tabla de costes del software.

6.3. Coste humano

Tarea	Jornadas (8 horas)
Análisis de NFC y códigos QR.	25
Análisis de las vulnerabilidades.	30
Explotación de vulnerabilidades.	35
Realización del informe.	12

Tabla 6.3: Tabla de costes de los recursos humanos.

Estimando un sueldo de 14€/hora.

6.4. Coste total

Tipo	Total
Coste del software	0€
Coste del hardware	∼1800€
Coste de RRHH	∼11.424€
Total	∼13.224€

Tabla 6.4: Tabla del coste total.

Capítulo 7

Conclusiones y líneas futuras

Después del estudio en detalle de las tecnologías NFC y QR escogidas para este estudio queda claro que aunque se utilicen cada vez más, siguen teniendo vulnerabilidades que podrían ser explotadas. Esto es debido a que a medida que avanza el despliegue de cualquier tecnología, lo hacen también los intentos de atacarla o manipularla. Por ello, es importante que todas las vulnerabilidades detectadas se corrijan poco a poco con el transcurso del tiempo.

Cabe destacar que aunque se mencionan vulnerabilidades de QR o NFC, eso no significa que cualquier dispositivo con dichas tecnologías implementadas pueda verse afectado. Esto se debe a que los dispositivos constan de diferentes medidas de seguridad, de ahí que unos dispositivos no se vean afectados por un ataque mientras que otros podrían quedar totalmente manipulados por el atacante.

Las debilidades así como los ataques demostrados en este estudio se describen con el único propósito de mejorar y promover la implantación de soluciones dado que todavía existen usuarios con dispositivos que podrían verse afectados.

Es preciso señalar que algunos ataques mencionados se basan en el mal uso del sistema de verificación. Por ello, no se trata de una vulnerabilidad que podría ser descubierta mediante un análisis del correcto funcionamiento del sistema de verificación sino mediante el análisis del uso del mismo. Ya que a pesar de que la autenticación del billete usando este sistema sea segura y precisa, un usuario podría descubrir cómo manipularla basándose en el conocimiento práctico que posee de este procedimiento.

En el futuro, se pretende continuar con este trabajo analizando amenazas que no han sido tratadas aquí. En particular, creemos que las tecnologías NFC y QR deben seguir siendo estudiadas para intentar descubrir nuevas vulnerabilidades, con objeto de fortalecer las aplicaciones basadas en dichas tecnologías antes de que sean explotadas por algún atacante.

Capítulo 8

Conclusions and future work

After a detailed study of the NFC and QR technologies chosen for this study, it is clear that although they are increasingly used, they still have vulnerabilities that could be exploited. This is because as the deployment of any technology progresses, so do attempts to attack or manipulate that technology. Therefore, it is important that all detected vulnerabilities are corrected little by little over time.

It should be noted that although QR or NFC vulnerabilities are mentioned, that does not mean that any device with such technologies implemented can be affected. This is because the devices have different security measures, hence some devices are not affected by an attack, while others could be totally manipulated by the attacker.

The weaknesses as well as the attacks demonstrated in this study are described with the sole purpose of improving and promoting the implementation of solutions since there are still users with devices that could be affected.

It should be noted that some of the aforementioned attacks are based on the misuse of the verification system. Therefore, it is not a vulnerability that could be discovered through an analysis of the correct functioning of the verification system, but through an analysis of its use. Since despite the fact that the authentication of the ticket using this system is secure and precise, a user could discover how to manipulate it based on their practical knowledge of this procedure.

In the future, it is intended to continue this work by analyzing threats that have not been addressed here. In particular, we believe that NFC and QR technologies should continue to be studied to try to discover new vulnerabilities, in order to strengthen applications based on these technologies before they are exploited by an attacker.

Bibliografía

[1] O. D. Cardozo, J. Gutiérrez Puebla, and J. C. García Palomares, “Influencia de la morfología urbana en la demanda de transporte público: análisis mediante SIG y modelos de regresión múltiple”, *GeoFocus (Artículos)*, vol. 10, pp. 82-102, 2010.

[2] M. Mezghani, “Study on electronic ticketing in public transport”, *European Metropolitan Transport Authorities (EMTA)*, vol. 56, p. 38, 2008.

[3] H. J. Herrera Losada, “Estado del arte para el sistema de pago electrónico para el sistema integrado de transporte”, *Master’s thesis*, Universitat Politècnica de Catalunya, 2014.

[4] J. Kos-Łabędowicz and A. Urbanek,“Korzystanie z płatności bezgotówkowych w miejskim transporcie zbiorowym przez młodych konsumentów w świetle badań ankietowych”, *Studia Ekonomiczne*, vol. 316, pp. 123-135, 2017.

[5] J. L. Oyón, “Transporte público y estructura urbana:(de mediados s. XIX a mediados s. XX): Gran Bretaña, Francia y países germánico”, *Ecología Política*, vol. 17, pp. 17-35, 1999.

[6] E. Bañobre Nebot and A. Romero Requejo,“Los BRT en corredores segregados como sistema óptimo de transporte urbano. En Administrando en entornos incierto”, *XXIII Congreso Anual AEDEM*, pp. 1-20, 2009.

[7] C. Seaborn, J. Attanucci, and N. H. M. Wilson,“Using smart card fare payment data to analyze multi-modal public transport journeys in London” *Transportation Research Record: Journal of the Transportation Research Board*, vol. 2121, pp.55-62 ,2009.

[8] M. Campos Ferreira, T. Galvão Dias, and J. Falcão e Cunha, “Codesign of a Mobile Ticketing Service Solution Based on BLE”, *Journal of Traffic and Logistics Engineering*, vol. 7, no 1, 2019.

[9] R. Steffen, J. Preißinger, T. Schöllermann, A. Müller, and I. Schnabel ,“Near field communication (NFC) in an automotive environmen”, *Second International Workshop on Near Field Communication. IEEE*, pp. 15-20, 2010.

[10] J. P. Santos Reis Leal,“Ticket Validation in Public Transportation Using the Smartphone”, *Dissertation*, Faculdade de Engenharia Universidade do Porto, 2015.

[11] G. Madlmayr, J. Langer, C. Kantner and J. Scharinger,“NFC devices: Security and privacy”, *Third International Conference on Availability, Reliability and Security*, pp. 642-647, 2008.

[12] N. A. Chattha, “NFC—Vulnerabilities and defense”, *Conference on Information Assurance and Cyber Security (CIACS)*, pp. 35-38, 2014.

[13] “Comunicación de campo cercano (Near Field Communication - NFC). Vulnerabilidades”, *Informe de Amenazas CCN-CERT IA-05/16*, 2016. [Online]. Available: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1378-ccn-cert-ia-05-16-comunicacion-de-campo-cercano-near-field-\communication-nfc-vulnerabilidades/file.html. [Accessed: 10-March-2020].

[14] M. Roland,“Software Card Emulation in NFC-enabled Mobile Phones: Great Advantage or Security Nightmare?”, *Fourth international workshop on security and privacy in spontaneous interaction and mobile phone use*, pp.1-6, 2012.

[15] E. Haselsteiner and K. Breitfuß,“Security in near field communication (NFC)”, *Workshop on RFID security*, pp. 12-14, 2006.

[16] E. Brumercikova, B. Bukova, and L. Krzywonos,“NFC Technology in Public Transport”, *Communications*, vol. 18, no. 2, pp. 20-25, 2016.

[17] D. Chavarría, “Tecnología de comunicación de campo cercano (NFC) y sus aplicaciones”, *Universidad de Costa Rica. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica*, pp. 8-9, 2011.

[18] R. Giustolisi, “Free Rides in Denmark: Lessons from Improperly Generated Mobile Transport Tickets”, *Secure IT Systems. NordSec 2017. Lecture Notes in Computer Science*, vol. 10674, pp. 159-174, 2017.

[19] G. Avoinea, L. Calderoni, J. Delvauxa, D. Maio and P. Palmieric, “Passengers information in public transport and privacy: can anonymous tickets prevent tracking?”, *International Journal of Information Management*, vol. 34, pp. 682-688, 2014.

[20] “Touch & Travel.” [Online]. Available: https://www.transportticket.com/touchandtravel. [Accessed: 20-March-2020].

[21] R. Focardi, F. L. Luccio and H. A Wahsheh, “Usable security for QR code”, *Journal of Information Security and Applications*, vol. 48, p. 102369, 2019.

[22] J. V. Bausili, “Ataques de relay en NFC con dispositivos Android”, *Ataques de relay en NFC con dispositivos Android*, Universidad Zaragoza, 2014.

[23] A. García, J. Carlos and S. Okazaki, “El uso de los códigos QR en España”, *Distribución y consumo*, pp. 46-62, 2012.

[24] “QR Code.” [Online]. Available: https://www.qrcode.com/en/about/. [Accessed: 20-March-2020].

[25] P. Kieseberg, M. Leithner, M. Mulazzani , L. Munroe, S. Schrittwieser, M. Sinha and E. Weippl, “QR code security”, *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia*, pp. 430-435, 2010.

[26] “Generador de códigos QR.” [Online]. Available: https://www.codigos-qr.com/generador-de-codigos-qr/. [Accessed: 20-March-2020].

[27] T. J. Soon, “QR code”, *Synthesis Journal*, vol. 2008, pp. 59-78, 2008.

[28] “Metro Tenerife.” [Online]. Available: https://metrotenerife.com/billetes_y_tarifas/. [Accessed: 22-March-2020].

[29] G. de Koning Gans, J. H Hoepman and F. D. Garcia, “A practical attack on the MIFARE Classic”, *International Conference on Smart Card Research and Advanced Applications*, pp. 267-282, 2018.

[30] G. P. Hancke, “A practical relay attack on ISO 14443 proximity cards”, *Technical report, University of Cambridge Computer Laboratory*, vol. 59, pp. 382-385, 2005.

[31] N. Castro-Acuña, M. Leguizamón-Páez and A. L. M. Lancheros, “Análisis de métodos y técnicas existentes para minimizar agujeros de seguridad al usar códigos QR”, *Revista UIS Ingenierías*, vol. 18, pp. 157-172, 2019.