UNIVERSIDAD AUTÓNOMA DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

Grado en Ingeniería Informática

TRABAJO FIN DE GRADO

Metodología de Auditoria de Seguridad en Tecnologías Contactless

Eduardo Arriols Nuñez
Tutor: Alvaro Ortigosa Juaréz

Junio 2016

Metodología de Auditoria de Seguridad en Tecnologías Contactless

AUTOR: Eduardo Arriols Nuñez
TUTOR: Álvaro Ortigosa Juaréz

Escuela Politécnica Superior
Universidad Autónoma de Madrid
Junio de 2016

Resumen

La seguridad informática o más recientemente denominada Ciberseguridad, es un campo relativamente moderno y por este motivo en muchas ocasiones queda relegado a un segundo plano durante el desarrollo y creación de nuevas tecnologías y productos.

Una de las carencias actuales en materia de seguridad es el no contar con metodologías de auditoria de seguridad suficientemente amplias, que permitan a los desarrolladores y auditores de seguridad verificar el nivel de seguridad de los desarrollos realizados.

Dentro de las nuevas tecnologías, desatacan algunas por su rápida implantación, crecimiento, evolución y cada vez mayor uso cotidiano. Un ejemplo claro son las tecnologías Contactless como RFID y NFC, a través de las cuales es posible realizar multitud de acciones como pagos con la tarjeta de crédito.

Por este motivo, se propone realizar una metodología de auditoria de seguridad para tecnologías Contactless que exponga en detalle los pasos necesarios que deben ser realizados para comprobar el nivel de seguridad de esta tecnología en diferentes escenarios e infraestructuras.

Palabras clave

Seguridad Informática, Ciberseguridad, Metodología, Tecnologías Contactless, RFID, NFC, Auditoria de seguridad.

Abstract

The computer security or more recently called Cybersecurity, is a relatively modern field and this is the reason why in many occasions it is set aside during the development and creation of new technologies and products.

One of the current lacks in Cybersecurity field is not having enough wide security audit methodologies, which would allow the developers and security auditors to verify the security level of the development done.

Inside the new technologies, there are some that stand out among the others because of their quickly establishment, development, evolution and more daily use each day. A really clear example are the Contactless technologies as RFID and NFD, through the ones it's possible to do dozens of actions like credit card payments.

This is the reason why it's proposed to create a security audit methodology for Contactless technologies that shows in detail the necessary steps that need to be followed to verify the security level of this technology in different scenes and computer infraestructures.

Keywords

Security, Cybersecurity, Methodology, Contactless Technology, RFID, NFC, Security Audit, Penetration Testing.

Agradecimientos

A Álvaro Ortigosa, por ayudarme y aconsejarme en la realización, ejecución y documentación del presente trabajo.

ÍNDICE DE CONTENIDOS

ÍNDICE DE IMÁGENES

1 Introducción

En este capítulo se explican las causas que motivan la realización de este trabajo. Se describen después los objetivos generales y específicos perseguidos. Finalmente, se expone la estructura completa del documento

1.1 Motivación

La evolución de las tecnologías es cada vez mayor y sigue incrementándose año tras año.

Esto provoca que diariamente sean presentados nuevos dispositivos y nueva tecnología que ayuda de una u otra forma a las personas. A modo de ejemplo podemos encontrar todos los nuevos dispositivos inteligentes o "Smart" ya sean pulseras de actividad, relojes, televisiones y un largo etcétera para la gente común o las ciudades inteligentes, coches y edificios que utilizan las nuevas tecnologías para realizar un consumo eficiente de la energía, permitir la posibilidad de habilitar acciones de forma remota sobre el entorno físico, etcétera.

Todos estos avances son sin duda un gran progreso en el uso y desarrollo de nueva tecnología pero existe un problema emergente y es la cuestión de si todos los dispositivos que se están creando son o no seguros, hablando por ejemplo de seguridad física, seguridad informática o privacidad de los datos que transmiten o contienen.

En la actualidad, muchos de estos avances se implementan sin realizar unas mínimas comprobaciones de seguridad sobre los productos y tecnología desarrollados, lo cual implica posibles vectores de ataque sobre los mismos que puedan afectar a la empresa desarrolladora o sus clientes.

Se identificó la necesidad de tener una metodología que permitiera a desarrolladores de tecnologías contactless y auditores de seguridad, realizar pruebas sobre los dispositivos y escenarios que estuvieran realizando pudiendo comprobar el nivel de seguridad existente.

1.2 Objetivos

Como objetivo principal se fijó desarrollar una metodología que de forma genérica permitiera a cualquier usuario que quisiera realizar pruebas de seguridad sobre tecnologías contactless, seguir una serie de fases que le garantizaran el comprobar el nivel de seguridad del escenario.

Primeramente fue necesario analizar las metodologías de seguridad actuales, su diseño, fases y utilización, para poder aprovechar la experiencia de las mismas en el desarrollo de la nueva metodología.

Posteriormente fue necesario analizar en profundidad las tecnologías contactless, en este caso RFID (*Radio Frecuency IDntification*)[1] y NFC (*Near Field Communication*)[2], permitiendo así una comprensión clara de los protocolos.

[1] https://en.wikipedia.org/wiki/Radio-frequency_identification

Se tuvo como objetivo realizar una metodología que se apoyara en la experiencia de haber auditado diferentes tipos de tecnologías y escenarios. De esta manera, la metodología fue desarrollándose, adaptándose y mejorándose a medida que se realizaban más pruebas.

Esto aporta a cualquier usuario que quiera utilizarla una visión más práctica a la hora de utilizar dispositivos, software o sencillamente plantearse posibles escenarios de ataque según la casuística que este siendo desarrollada.

1.3 Organización de la memoria

Ya que el trabajo desarrollado es un documento en forma de metodología, este se adjunta como documento anexo independiente. La memoria en si consta de los siguientes capítulos:

- **Capítulo 2 – Estado del arte**: Se pone en contexto al lector de la actualidad en las tecnologías y concretamente en el mundo de la seguridad, exponiendo las principales amenazas y la necesidad de realizar comprobaciones realistas, siguiendo metodologías específicas de auditoria.
    - **Revisión de metodologías**: Se realiza un repaso de las metodologías analizadas anteriormente al desarrollo de la metodología expuesta en el presente documento.
- **Capítulo 3 – Tecnologías analizadas**: Se realiza un repaso de las tecnologías analizadas, haciendo hincapié en aquellos detalles necesarios para una mejor comprensión de los temas tratados posteriormente en el documento.
- **Capítulo 4 – Diseño de la metodología**: Se expone la estructura de la metodología desarrollada y el porqué de la elección de dicha estructura.
- **Capítulo 5 – Metodología desarrollada**: Se expone cada una de las fases de la metodología de auditoria de tecnologías contactless desarrollada.
- **Capítulo 6 – Pruebas y resultados**: Se exponen parte de las pruebas y escenarios reales que han sido auditados siguiendo la metodología desarrollada, así como los resultados obtenidos de la misma.
- **Capítulo 7 – Uso de la metodología en simulaciones de intrusión física y ejercicios de Red Team**: Se expone la importancia de comprobar la tecnología contactless en simulaciones de intrusión físicas y ejercicios de Red Team a través de un ejemplo práctico real realizado por el autor en su labor profesional.
- **Capítulo 8 – Conclusiones y trabajo futuro**: Se repasan las conclusiones del trabajo realizado y se desarrolla cual es el trabajo futuro a realizar.

[2] https://en.wikipedia.org/wiki/Near_field_communication

2 Estado del arte

En este capítulo se realiza un repaso del estado del arte en cuanto a la evolución de las tecnologías y la seguridad dentro de estas, así como a las amenazas actuales y la necesidad de métodos de auditoría que permitan prever y controlar estos nuevos riesgos y amenazas.

La seguridad de las tecnologías es un campo realmente amplio, tanto como la propia informática al ser un concepto que va ligado estrechamente a la evolución que están teniendo las tecnologías.

La definición de informática hace ver, y esto es algo conocido por todos a día de hoy, que la información es poder. Solo hay que observar ejemplos como los bancos, donde el activo más crítico al igual que en la mayoría de empresas no son activos materiales, sino la información almacenada en los sistemas informáticos. Es por ello, que cada vez más, la seguridad está cobrando un papel fundamental en el desarrollo de las nuevas tecnologías y comprobación de las ya desarrolladas, pues si un sistema no es seguro los datos están en peligro.

Esta necesidad de seguridad no ha sido siempre así ya que en los inicios de la informática, la prioridad no era la seguridad sino la funcionalidad y efectividad. Este modo de desarrollar la tecnología ha provocado que a día de hoy, donde utilizamos gran cantidad de tecnología heredada de hace varias décadas como puede ser IPv4, convivamos con tecnología vulnerable.

Desde los inicio la seguridad de la información establece tres pilares fundamentales que son la confidencialidad, la integridad y la disponibilidad de la información. Si cualquiera de estos principios no se cumple se puede decir que el activo no es seguro.

2.1 Evolución de las tecnologías

Para comenzar es necesario hablar de la rápida evolución que está teniendo la tecnología en los últimos años y su crecimiento exponencial de cara a futuro.

Y es que este crecimiento está provocando la aparición de todo tipo de dispositivos y tecnología cada vez más inteligente e interconectado como pueden ser los dispositivos inteligentes (Smart-Devices) tales como pulseras de actividad (Smart-Bands), relojes (Smart-Watchs), televisores (Smart-TV) y un largo etcétera.

Todos estos dispositivos de una u otra forma ayuda a la gente o les hacen la vida más fácil, pero una pregunta que debemos hacernos es ¿Son seguros?

Todos estos nuevos dispositivos y tecnología tienen algo en común y es que cada vez se encuentran más interconectados, lo cual a nivel de seguridad supone un grave riesgo pues como es sabido en seguridad la seguridad de un sistema o infraestructura es igual a la seguridad del elemento más vulnerable del sistema. Esto implica que la vulneración de un elemento puede permitir comprometer el sistema o infraestructura completa pudiendo causar un mayor daño.

Si esto lo aplicamos en infraestructuras como las modernas Smart-Cities que están siendo desarrolladas implica que tomar control de una parte de la infraestructura puede permitir llegar a tener control de otros muchos sistemas internos de la ciudad.

A modo de ejemplo, recientemente realice una investigación presentada en diferentes congresos como HLC de ISACA[3], que trataba sobre los denominados edificios inteligentes o Smart-Buildings y que dio como resultado la localización de más de 9000 edificios o complejos de edificio inteligentes totalmente vulnerables. Las implicaciones de esta afirmación es que sobre dichos edificios era posible tomar control del sistema de luces, aguas, generación de energía, control de acceso y videovigilancia, gestión del sistema de alarma, además de poder acceder en muchos casos a la red interna de la organización.

Por otro lado, y es algo que veremos más adelante, todos estos avances carecen de un proceso de seguridad que haya sido seguido durante el ciclo de vida del desarrollo, provocando de esta manera gran cantidad de posibles vulnerabilidades que serán detectadas a posteriori de su implantación en el mercado.

2.2 Definición de seguridad

Algo necesario antes de continuar es discernir entre seguridad de la información y seguridad informática o también llamada ciberseguridad, y es que aunque ambas se utilizan en muchos casos indistintamente, no significan lo mismo.

Según la organización ISACA, una definición correcta de seguridad informática o actualmente llamada ciberseguridad es la siguiente:

"*Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados*"[4]

Por otro lado, cuando esta misma organización habla de seguridad de la información lo define como:

"*La información requiere de medidas de protección adecuadas de acuerdo con su importancia y criticidad, y éste es precisamente el ámbito de la seguridad de la información*"

Como se puede apreciar en las descripciones, la seguridad informática forma parte de la seguridad de la información, pues es la encargada de mantener la seguridad de los sistemas que almacenan la información, asegurando como hemos visto su confidencialidad, disponibilidad e integridad.

[3] http://www.isaca.org/chapters7/madrid/events/eventos/pages/high-level-conference.aspx

[4] Presentación "Ciberseguridad ¿Una moda pasajera o una realidad que influirá en nuestras vidas?", evento de ISACA, UPV, Febrero 2016.

2.3 Perspectivas de la seguridad informática

Según se ha expuesto anteriormente, la seguridad informática debe velar por la seguridad de los sistemas que almacenan la información. Ante esta necesidad se plantean dos perspectivas según su enfoque que son la seguridad defensiva y la seguridad ofensiva.

La hasta la fecha se había planteado en las organizaciones públicas y privadas (exceptuando el ámbito militar) únicamente el punto de vista defensivo, cuya misión consistía en implementar las medidas de seguridad necesarias para proteger y mantener el estado de seguridad de los sistemas existentes en la organización.

Este es un punto de vista completamente entendible y necesario, pero durante los últimos años cada vez más empresas están optando también por realizar auditorías o simulaciones desde un punto de vista de un adversario o competidor.

La cuestión es que ambos puntos de vista son necesarios y a la vez complementarios, ya que una persona encargada únicamente de defender sistemas tiene experiencia en capacidades defensivas y no en capacidades ofensivas. Esto implica que a la hora de securizar los sistemas lo hará siempre de tal forma que se eviten los posibles ataques que un adversario podría realizar y en otras muchas ocasiones, únicamente siguiendo una guía de buenas prácticas ya que él no tiene dicho conocimiento de que podría o no hacer un atacante.

Aquí es donde entra y toma importancia la seguridad ofensiva, que tiene por objetivo tomar el rol de un atacante y encontrar aquellas vulnerabilidades y vectores de ataque que permitan comprometer la seguridad de los sistemas. En este caso, la seguridad encargada de atacar los sistemas tiene amplia experiencia en capacidades ofensivas y no en defensivas, pues una ver comprobada la seguridad, le trasladara las vulnerabilidades al equipo defensivo para que pueda solventarlas.

Sin duda, cuando hablamos de ambos puntos de vista hay que destacar que la seguridad defensiva requiere un mayor trabajo y esfuerzo, pues es necesario securizar todos los sistemas de la organización para evitar que un posible ataque tenga éxito.

Esta tendencia donde las organizaciones utilizan ambos puntos de vista para protegerse frente a potenciales enemigos está teniendo una alta aceptación, pues ambos enfoques en conjunto aportan un gran valor a las empresas identificando de forma más eficaz las vulnerabilidades y protegiendo los sistemas de la organización.

2.4 Ejercicios de Red Team

Como se ha expuesto anteriormente, la seguridad ofensiva está cobrando cada vez más importancia. En la actualidad se está implantando en el ámbito privado un concepto que proviene del ámbito militar, utilizando en los denominados “juegos de guerra”, donde el equipo de defensa (Blue Team) tenía que evitar los ataques del equipo ofensivo (Red Team). En este caso, las empresas realizan simulaciones de ataque donde se pone a prueba la verdadera seguridad de la organización.

Este tipo de ejercicios aporta una visión completamente distinta a las comprbaciones de seguridad realizadas hasta el momento, ya que el objetivo pasa de identifica

vulnerabilidades a identificar realmente cual es el impacto de negocio que provocaría un ataque dirigido, como podría realizarla, a través de que medio, etcétera.

Consiste en la comprobación de seguridad ofensiva más especializada y permite ampliar las capacidades defensivas del equipo de defensa o Blue Team, ya que este se encuentra en constante situación de alerta frente a ataques conocidos o no, realizados por el Red Team

2.5 Riesgos de seguridad y ciberamenazas

Después de exponer el concepto de seguridad informática y de la información, ver las diferentes perspectivas de seguridad y que son los ejercicios de Red Team, es común hacerse ciertas preguntas como, ¿Realmente las organizaciones están en peligro? ¿Es necesario y posible proteger una infraestructura completa de una organización actual, que en muchos casos se encuentra en constante cambio? ¿Hasta qué punto se debe securizar una infraestructura, cual es el punto medio?

Sin duda las organizaciones están cada vez más expuestas y esto es algo que podemos contrastar con datos público como los últimos ataques realizado a grades organización, por poner algunos ejemplos:

- Ataques a la red Swift a través de bancos de Singapur, Vietnam y Ecuador, que han supuesto millones de dólares en fraude para las reservas federales de dichos países.

- Filtraciones de los papeles de panamá a través de los cuales se han identificado gran cantidad de personas que han cometido fraude fiscal.

- Filtración de la base de datos completa de Ashley Madison con más de 32 millones de usuarios.

Estos son solo algunos ejemplos de organizaciones que han sido vulneradas, pero existen otros muchos más casos, empresas privadas, empresas industriales, infraestructuras críticas, organismos públicos, etcétera.

Es verdad que estamos en riesgo, pero por otro lado, es completamente cierto que es imposible securizar la infraestructura de cualquier organización mediana o grande de tal forma que no exista ninguna vulnerabilidad, ya que diariamente se publican vulnerabilidades de todo tipo y requeriría un esfuerzo insostenible.

Por lo tanto, llegamos a la siguiente pregunta ¿Hasta qué punto debemos securizar?. La respuesta a esta pregunta se responde de forma negativa y es que no se debe gastar más en seguridad que lo que costara recuperarse del posible ataque o problema. Hay que ajustar lo máximo posible si se quiere estar lo más protegido posible en base a los recursos e información protegida.

Si ya sabemos cuánto deberíamos invertir en términos de presupuesto y esfuerzo, nos surge otra pregunta que es: ¿Qué debemos asegurar?

Dar una respuesta a esta pregunta depende enteramente de cada organización, la tipología de negocio que siga, la dependencia de clientes, y un largo etcétera. Debido a esta casuística se han desarrollado normativas y estándares como es el caso de la ISO 27001, que exponen como debe realizarse un análisis de la organización para identificar aquellos activos más críticos para la organización en base al riesgo de los mismos, entendiendo el

riesgo como el impacto de que un ataque se produzca por el riesgo de que dicho ataque llegue a producirse.

En dicho análisis se tienen en cuenta todo tipo de problemáticas que pudieran afectar al normal funcionamiento de la organización, desde problemas ambientales como una inundación o incendio hasta ataques digitales sobre la organización.

2.6 Necesidad de metodologías específicas

En base a todo lo expuesto anteriormente, tanto desarrolladores como auditores se encuentran con un problema creciente y es que aun teniendo una perspectiva de seguridad ofensiva, la rápida evolución de las tecnologías provoca que no puedan existir metodologías públicas y aceptadas por la comunidad de seguridad para realizar comprobaciones de seguridad en todas esas tecnologías que se van desarrollando y publicando.

A día de hoy únicamente existen metodologías reconocidas cuyo alcance es global y no suelen centrarse en metodologías concretas. Provocando de esta manera que en muchos casos, los desarrolladores por falta de tiempo y conocimientos no comprueben la seguridad de sus desarrollos y por lo tanto no introduzcan la seguridad como una fase más del ciclo de vida.

Quiero terminar con este último apunte, pues si se tomara conciencia y realmente se introdujera la seguridad desde el inicio en cualquier clase de desarrollo, se reducirían enormemente los costes posteriores y se incrementaría la seguridad desde el inicio.

2.7 Revisión de metodologías

A continuación se van a exponer de manera general las principales metodologías de auditoria de sistemas que han sido analizadas con el objetivo de tomar ejemplo y poder desarrollar una nueva metodología que permita la realización de auditorías de entornos y tecnología contactless (RFID y NFC).

2.7.1 PTES

Las siglas se corresponden con Penetration Testing Execution Standard y es una metodología desarrollada por la organización PTES[5]. Su principal objetivo es la exponer detalladamente el proceso para la realización de un proceso de Test de Intrusión sobre cualquier tipo de entornos, aunque esta principalmente centrada en la realizado de intrusiones en infraestructura de red y sistemas.

Las fases desarrolladas por la metodología son:

- Detalles previos a las pruebas y firma de acuerdo
- Recopilación de información e inteligencia
- Modelado de las amenazas
- Análisis de vulnerabilidades

[5] http://www.pentest-standard.org/index.php/Main_Page

- Explotación de vulnerabilidades
- Post-Explotación de vulnerabilidades
- Realización de la documentación

2.7.2 OSSTMM

Las siglas se corresponden con Open Source Security Testing Methodology Manual y es una metodología de auditoria desarrollada por la organización ISECOM[6]. Su principal objetivo es exponer el concepto de seguridad y todos aquellos puntos que deberían ser evaluados en los diferentes tipos de auditoria, teniendo diferentes puntos de vista según el objetivo de la auditoria:

- Humano
- Físico
- Redes de datos
- Telecomunicaciones
- Wireless

Es una metodología muy completa y aunque no profundiza en detalles técnicos si aporta una visión general de muchos aspectos diferentes. Un punto en contra es que actualmente se encuentra algo desactualizada.

2.7.3 NIST 800-115

En este caso hablamos de una metodología desarrollada por el NIST, siglas del Instituto Nacional de Normas y Tecnologías (National Institute of Standars and Technology) de los Estados Unidos. Su principal objetivo es proveer una metodología para la realización de evaluaciones y auditorias de seguridad donde se exponen además estrategias para solventar los posibles problemas identificados.

Al igual que ocurre con la metodología OSSTMM, NIST 800-115[7] no profundiza en los detalles técnicos sin que aporta una visión general acerca los aspectos fundamentales de la auditoria de seguridad.

Los temas tratados por la metodología son los siguientes:

- Políticas, roles y responsabilidades de seguridad
- Técnicas de monitorización
- Enumeración de objetivos
- Búsqueda de vulnerabilidades
- Planteamiento de una auditoria de seguridad
- Realización de informaciones y recomendaciones

[6] http://www.isecom.org/

[7] http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

2.7.4 OWASP

Las siglas de OWASP[8] se corresponden con Open Web Application Security Project y es una metodología de auditoria de aplicaciones web desarrollada por la organización con el mismo nombre. Su principal objetivo es desarrollar y exponer todas las comprobaciones que deben ser realizadas durante una auditoria a una aplicación web. Al igual que PTES, es una metodología con gran contenido técnico que muestra en detalles las acciones a desarrollar.

La metodología OWASP se divide en:

- Recopilación de información
- Pruebas de autenticación
- Pruebas de filtrado de inputs
- Configuración y pruebas de gestión del despliegue
- Pruebas de autorización
- Gestión de errores
- Lógica de negocio
- Administración de identidades
- Pruebas de gestión de sesiones
- Criptografía

[8] https://www.owasp.org/index.php/Main_Page

3 Tecnologías analizadas

En el presente punto se van a exponer los detalles sobre la tecnología RFID y NFC, así como su funcionamiento a nivel general para facilitar la comprensión de temas posteriores.

3.1 RFID (Radio Frequency IDentification)

3.1.1 Definición

RFID son las siglas de Radio Frecuency IDentificacion (Identificación por radiofrecuencia). Consiste en un sistema de almacenamiento y recuperación de información inalámbrica que usa dispositivos denominados etiquetas, tarjetas, transpondedores o tags RFID.

El objetivo de esta tecnología es transmitir la identidad de un objeto, así como la información contenida en él, que será mayor o menor dependiendo del estándar y tipo de dispositivos utilizados (expuestos posteriormente).

Los dispositivos utilizados tienen por lo general un tamaño reducido y pueden ser incorporados a un producto, animal o persona. Estos dispositivos contienen antenas que les permiten recibir y enviar peticiones por radiofrecuencia a otros dispositivos RFID receptor. El mercado de RFID se estimó en el año 2014 en aproximadamente 20 billones de dólares a nivel mundial.

A nivel histórico, esta tecnología proviene de las investigaciones realizadas por la unión soviética en torno al año 1945, cuando Léon Theremin fabrico una herramienta que permitía transmitir información en formato de audio desde dispositivos pequeños utilizando ondas electromagnéticas. Según otras fuentes, la tecnología usada en RFID habría sido desarrollada en los años 20, creada por el MIT y utilizada ampliamente por los británicos durante la segunda guerra mundial.

3.1.2 Funcionamiento

El modo en el que funcionan los sistemas RFID es muy simple. Básicamente, la etiqueta RFID, que contiene los datos de identificación del objeto y la información que se haya deseado introducir, genera señales de radiofrecuencia con dichos datos.

Esta señal emitida puede ser captada por un lector RFID, que se encargara de leer la información y convertirla a formato digital.

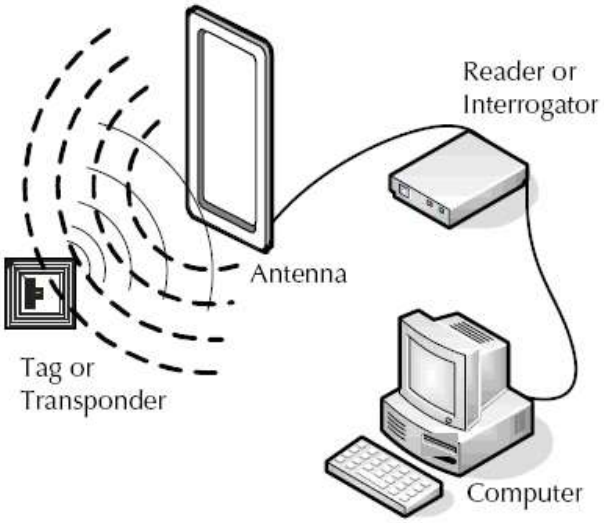

Imagen 1 - Ejemplo de sistema RFID

Para que este escenario sea posible, un sistema RFID ha de constar de tres componentes:

- **Etiqueta RFID**: Consiste en un pequeño dispositivo que contiene la información. Este dispositivo está compuesto por una antena que será la encarga de enviar la información mediante ondas de radio, un chip que contiene una memoria donde se almacena la información en bytes y un transductor que enviara la información del chip a la antena.

  Existen varios tipos de memoria:
  - Solo lectura: La información es única y personalizada durante su fabricación.
  - Lectura y escritura: La información puede ser modificada.
  - Anticolisión: Son etiquetas especiales que permiten la múltiple identificación por parte del lector.

- **Lector RFID**: Consiste en una antena, un transceptor y un decodificador. Su función es enviar periódicamente señales para ver si hay alguna etiqueta próxima. Cuando detecta una señal de una etiqueta RFID, extrae la información que esta envía y se lo transmite al sistema de procesamiento de datos.

- **Sistema de procesamiento de datos**: Normalmente es software utilizado por el lector para procesar los datos y realizar el almacenamiento de los mismos.

3.1.3 Tipos

Las etiquetas RFID pueden ser de diferente tipo en base a si necesitan o no fuente de alimentación interna. A continuación se muestra su clasificación:

- **Etiquetas pasivas**: No requieren de ninguna fuente de alimentación interna. Son dispositivos RFID completamente pasivos, esto significa que únicamente se activan cuando el lector se encuentra en sus proximidades para suministrarles la energía

necesaria para poder enviar la información. Este es el tipo de etiquetas más comunes ya que son a su vez las de menor coste.

A continuación se muestra un esquema del funcionamiento de una tarjeta pasiva de alta frecuencia al recibir el campo magnético del lector:

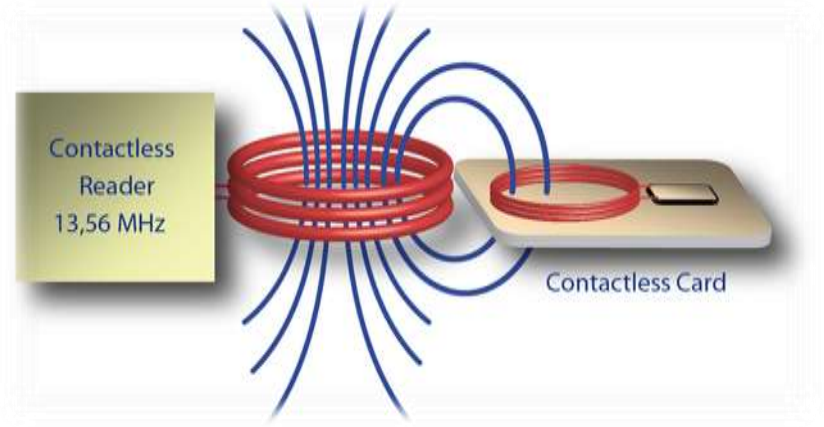

Imagen 2 - Funcionamiento etiquetas pasivas

- **Etiquetas activas**: Requieren de una fuente de alimentación autónoma que les permite dar corriente a los circuitos integrados y con ello propagar la información en forma de señales. Son menos comunes pero son más efectivas en distancias largas.

- **Etiquetas semipasivas**: Son etiquetas similares a las activas ya que tienen una fuente de alimentación propia, aunque en este caso únicamente alimta al microchip y no es suficiente para transmitir información. De cara al lector este tipo de etiquetas son pavisa.

A continuación se muestra una imagen a modo de ejemplo de una etiqueta NFC:

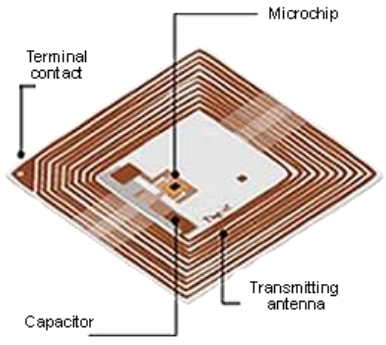

Imagen 3 - Etiqueta NFC

3.1.4 Clasificación

Los sistemas basados en RFID se clasificación en base al rango de frecuencias que utilizan.

Existen cuatro tipos:

- **Baja frecuencia**: Entre 125 y 134.2 Kilohercios.
  Esta clasificación tiene una distancia de comunicación baja y normalmente las etiquetas permiten almacenar poca información.

- **Alta frecuencia**: 13.56 Megahercios.
  Esta clasificación es sin duda la más utilizada actualmente, ya que en muchos casos se hace uso de NFC, una tecnología basada en RFID que será expuesta más adelante. Permite una comunicación a distancia media (entre 10 cm y un metro) y a su vez las etiquetas suelen almacenar una información considerable (hasta 4KB).

- **Frecuencia Ultraelevada**: Entre 868 y 956 Megahercios
  Esta clasificación destaca por una distancia de comunicación bastante grande (Hasta 20 metros), aunque en la actualidad su uso es limitado.

- **Microondas**: 2.45 Gigahercios
  Esta clasificación aunque se encuentra dentro de RFID es muy poco común y genérica con otras tecnologías.

A continuación se muestra un cuadro resumen con los diferentes tipos de clasificaciones:

Band	Regulations	Range	Data speed	Remarks
120–150 kHz (LF)	Unregulated	10 cm	Low	Animal identification, factory data collection
13.56 MHz (HF)	ISM band worldwide	10 cm - 1 m	Low to moderate	Smart cards (MIFARE, ISO/IEC 14443)
433 MHz (UHF)	Short Range Devices	1–100 m	Moderate	Defence applications, with active tags
865-868 MHz (Europe), 902-928 MHz (North America) UHF	ISM band	1–12 m	Moderate to high	EAN, various standards
2450-5800 MHz (microwave)	ISM band	1–20 m	High	802.11 WLAN, Bluetooth standards
3.1–10 GHz (microwave)	Ultra wide band	200 m	High	Requires semi-active or active tags

Imagen 4 - Frecuencias utilizadas

3.1.5 Uso actual

Esta tecnología ha cobrado gran importancia durante la última década, utilizándola en gran cantidad de situaciones. A continuación se muestra algunos de los principales usos de esta tecnología:

- Control de acceso físico
- Seguimiento de comida
- Seguimiento de personas y animales
- Pagos con tarjeta (Contactless payment)
- Pasaporte
- Uso en peajes

- …

Actualmente se están realizado grandes proyectos que utilizan esta tecnología, como los implantes RFID directamente en el cuerpo humano.

3.1.6 Beneficios

Los beneficios de RFID se suelen comparar en muchas ocasiones con el código de barras. Entre los beneficios más destacados se encuentran:

- No requiere una línea de visión
- Es ideal para automatizar acciones ya que no requiere de interacción humana
- Las distancias de lectura más comunes van desde unos pocos centímetros hasta 10 metros
- Es posible realizar la lectura simultanea de múltiples dispositivos (Protocolo anticolisión)
- Es posible realizar hasta 500 lecturas por minuto
- Es posible realizar acciones de lectura y escritura, pudiendo reutilizar los dispositivos RFID

3.1.7 Problemáticas

Aunque es cierto que las tecnologías contactless como RFID permiten dar solución a gran cantidad de problemas cuyas soluciones actuales son más costosas, también tiene una serie de problemáticas asociadas. En este caso, cuando hablamos de seguridad, la más destacada es que este tipo de tarjetas propagan la información mediante ondas y en muchos casos sin ningún tipo de cifrado o control sobre si el receptor es legítimo.

Mas generalmente, atendiendo a la privacidad, podríamos definir otras problemáticas como:

- Esta tecnología es utilizada en gran cantidad de artículos que las personas comunes compran. Estas personas no tienen por qué saber de la presencia de la etiqueta o ser capaz de eliminarla.

- Las etiquetas pueden ser leídas a cierta distancia sin conocimiento por parte del propietario. Esto suele ser uno de los problemas principales con el control de acceso, permitiendo potencialmente la copia de la etiqueta sin interacción con la persona objetivo.

- Algunos gobiernos han o están desarrollando los pasaportes, documentos de identidad, licencias de conducir y demás documentos con tecnología RFID, pudiendo ser utilizados para controlar al individuo.

3.2 NFC (Near Field Communication)

3.2.1 Definición

NFC son las siglas de Near Field Communication (Comunicación por campo cercano). Se trata de una tecnología de comunicación inalámbrica de corto alcance y alta frecuencia que deriva de la tecnología RFID.

Al igual que la tecnología RFID, está pensada para enviar información mediante radiofrecuencia de datos concretos y no grandes cantidades de información.

La principal diferencia es que NFC es una plataforma abierta, pensada desde el inicio para ser utilizada por teléfonos y dispositivos móviles.

3.2.2 Funcionamiento

Los estándares de NFC están basados en la ISO 14443[9] (RFID) y FeliCA[10]. Al igual que en la ISO 14443, NFC se comunica mediante inducción en un campo magnético y trabaja en la banda de frecuencia de 13.56 Megahercios. Esto implica que NFC se encuentra dentro de las tecnologías RFID de alta frecuencia.

El uso de NFC no está limitado como en muchos casos de RFID, por lo tanto no requiere ningún tipo de licencia para su uso.

Respecto al funcionamiento de NFC es idéntico al de RFID, siendo necesario un transmisor, un receptor y un software intermedio.

El protocolo NFCIP-1[11] utilizado en NFC permite el envío de datos a diversas velocidades como 106, 212, 424 o 848 kbits/segundo.

3.2.3 Tipos

Soporta dos modos de funcionamiento y todos los dispositivos del estándar NFCIP-1 deben soportar ambos:

- **Activo**: Se corresponde con las etiquetas activas de RFID, pues se especifica que ambos dispositivos generan su propia energía para el envío de información.

- **Pasivo**: Se corresponde con las etiquetas pasivas de RFID, pues la etiqueta que envía la información necesita el campo magnético que genera el lector para el envío de la información.

[9] http://www.openpcd.org/ISO14443

[10] http://www.sony.net/Products/felica/

[11] http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-340.pdf

3.2.4 Uso actual

Actualmente el uso de NFC es realmente amplio, ya que es una tecnología barata y fácilmente usable. Por poner algunos ejemplos:

- Abonos transporte
- Abonos instalaciones deportivas
- Estacionamiento por ciudad o acceso a parking
- Pagos bancarios
- Control de acceso (No solo empresarial, también de ocio)
- …

3.2.5 Beneficios

Los beneficios más destacados de esta tecnología son los siguientes:

- El tiempo de conexión entre dos dispositivos es extremadamente rápido.
- Tiene más usos que Bluetooth como el pago bancario
- Es posible utilizarlo desde un dispositivo común como un Smartphone.

A estos beneficios habría que sumarles los beneficios de la tecnología RFID de la que deriva.

3.2.6 Problemáticas

La principal problemática al igual que ocurre con todas las nuevas tecnologías que proliferan rápidamente es que en muchas ocasiones no se verifican de forma correcta las medidas de seguridad. Las personas encargadas de implantar este tipo de medidas desconocen muchas veces los problemas de seguridad que implican y la sencillez de realizar ataques contra los clientes de la infraestructura.

4 Metodología desarrollada

En el presente punto se van a exponer los detalles sobre la metodología desarrollada, así como las diferentes fases de las que está compuesta.

Estas fases se describen de forma genérica ya que los trabajos de auditoria pueden ser realizados de múltiples formas, ya sea caja negra (desconocimiento de la infraestructura), caja blanca (conocimiento completo de la infraestructura), etcétera, y dependiendo del enfoque dado, las pruebas se realizaran de una u otra manera. Se han omitido todos los ejemplos prácticos mostrados en la metodología desarrollada.

4.1 Diseño de la metodología

En el presente punto se va a exponer los detalles del diseño acerca de la metodología desarrollada y las fases de las que está compuesta.

Tras estudiar y analizar la estructura seguida por las metodologías expuestas anteriormente se y en base a las pruebas realizadas sobre la tecnología RFID y NFC, se tuvo una imagen clara de las fases necesarias en cualquier auditoria sobre dicha tecnología y con ello se procedió a desarrollar la siguiente estructura:

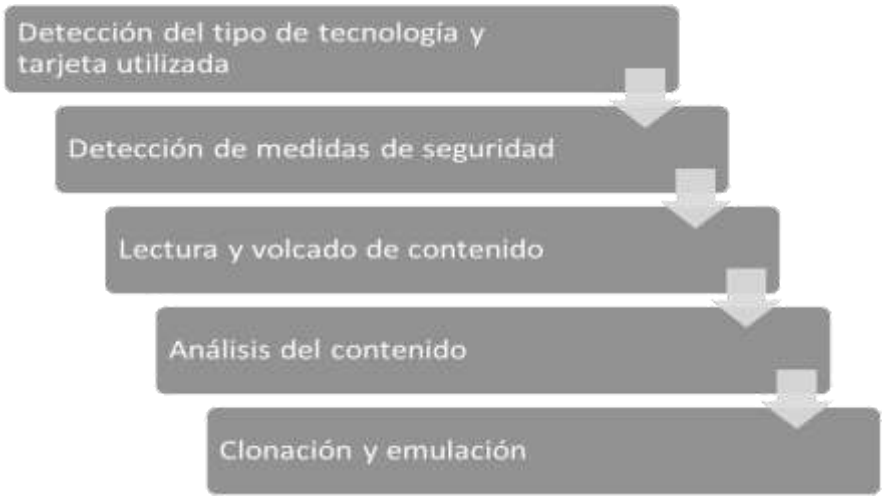

Imagen 5 - Estructura de la metodología desarrollada

La metodología desarrollada no tiene un carácter generalista sino que pretende abordar de forma concreta las acciones necesarias que deben ser realizadas a nivel técnico para comprobar el nivel de seguridad y posibles vulnerabilidades de un escenario o tecnología basada en RFID o NFC. Por ello, la metodología no incluye las fases de estimación del alcance, informe y recomendaciones, etcétera.

Debido al marcado carácter técnico de la metodología, se han incluido las herramientas tanto software como hardware que se necesitan para desarrollar correctamente las pruebas, además de incluir diferentes ejemplos que permitan al lector entender posibles vectores de ataques sobre esta tecnología.

4.2 Fase 1: Detección del tipo de tecnología y tarjeta utilizada

La primera fase a realizar tiene por objetivo detectar el tipo de tecnología y tarjeta que está siendo utilizado en el escenario objetivo.

Es necesario detectar los siguientes detalles en el orden que se indica a continuación:

- Detectar el tipo de frecuencia (Baja, alta o ultraalta)
- Detectar si se está utilizando RFID o NFC
- Detectar el estándar y tarjeta (Mifare[12], Vicinity[13], etcétera)

Para obtener dichos detalles se pueden seguir diferentes aproximaciones que se muestran a continuación:

- **Mediante el análisis del lector**: Si se plantea un escenario donde no se tiene acceso a ninguna tarjeta valida pero si acceso visual al lector de tarjetas, es posible intentar identificar la marca y modelo para posteriormente proceder a buscar información en Internet que permite identificar los detalles necesarios.

- **Mediante el análisis visual de la tarjeta**: Si se plantea un escenario donde no se tiene acceso a ninguna tarjeta valida pero si acceso visual a alguna tarjeta, se puede intentar obtener información existente en la propia tarjeta. Este puede ser un vector un poco más complejo para la obtención de información pero muy efectivo.

- **Mediante el análisis de la tarjeta**: La última posibilidad se da cuando tenemos acceso físico a la tarjeta. Sin duda este es el escenario más sencillo ya que es posible realizar gran cantidad de pruebas sobre la tarjeta.

4.3 Fase 2: Detección de medidas de seguridad

Una vez se ha identificado el tipo de frecuencia utilizada, tecnología y estándar de la tarjeta, es necesario identificar si cuenta con medidas de seguridad y en tal caso, si se encuentran o no implementadas.

Esta fase es realmente importante en caso de que el escenario de auditoria que se plantee no se tenga acceso a la tarjeta, por ejemplo en un escenario de intrusión física.

Para obtener dichos detalles se pueden seguir diferentes aproximaciones que se muestran a continuación:

- **Investigación de las medidas de seguridad**: Con la información anterior es necesario realizar una búsqueda de información a través de buscadores que nos permita conocer si el escenario en cuestión cuenta o no con medidas de seguridad.

[12] https://www.mifare.net/en/

[13] http://www.vicinityrfid.com/

- **Posibilidad de ruptura de la seguridad**: Una vez identificadas las medidas de seguridad con las que cuenta la tarjeta objetivo, es necesario buscar información sobre cómo es posible evitar o vulnerar dichas medidas de seguridad.

4.4 Fase 3: Lectura y volcado de contenido

Conociendo toda la información sobre el escenario (Tipo de frecuencia, tecnología y tarjeta) así como las medidas de seguridad que pueden estar implementadas es hora de proceder a la lectura de los contenidos.

Tal y como se ha expuesto anteriormente, la lectura dependerá de la tecnología, el estándar utilizado por la tarjeta y el dispositivo hardware que haya a ser usado.

4.5 Fase 4: Análisis del contenido

Con el volcado de la tarjeta realizado, es necesario proceder al análisis del mismo de forma más detallada. Aunque no es necesario, si recomendable realizar el volcado de la tarjeta objeto en dos situaciones distintas que permitan obtener las diferencias.

Cada situación y escenario serán diferentes y por lo tanto el auditor deberá identificar el objetivo y después comprobar si le es necesario tener dos tarjetas distintas o una misma tarjeta en situaciones distintas donde el contenido haya variado.

Ya que la mayoría de aplicaciones devuelven el resultado en binario, hay que convertir el volcado binario en hexadecimal, utilizando para ello herramientas como Hexdump[14].

En esta fase es imprescindible realizar una interpretación de los datos obtenidos. Para ello se siguen las siguientes pautas:

- Una vez se tiene el contenido en hexadecimal de una o más tarjetas es momento de analizar el contenido contando con información previa del escenario. Una de las herramientas más simples pero eficaces es Diff[15] que permite comprar dos ficheros, mostrando las diferencias entre ellos.

- Realizar una comparación de dos tarjetas aporta un gran valor ya que suele dar como resultado que pocos bytes han variado.

- Una vez tenemos los datos que varían entre los diferentes volcados es recomendable realizar búsquedas sobre contenido que debería contener dicha tarjeta y que se quiere modificar. Estos datos dependerán completamente del escenario que este siendo comprobado.

[14] https://www.freebsd.org/cgi/man.cgi?query=hexdump&sektion=1

[15] https://www.gnu.org/software/diffutils/

4.6 Fase 5: Clonación y emulación

Con la información crítica del escenario ya identificada, donde se conocen todos los detalles de la tarjeta, donde se encuentran los datos y las claves (en caso de haberlas) para leer y escribir, se pueden dar tres situaciones distintas:

- **Las tarjetas son editables en aquellos datos críticos que quieren ser alterados**: Esta situación provoca que se pueda sobrescribir directamente el contenido de la tarjeta por el que se desee. El modo de edición depende completamente del tipo de tecnología y estándar de las tarjetas, así como del hardware que se esté utilizando.

- **Las tarjetas no son editables pero es posible conseguir tarjetas en blanco (con o sin puertas traseras según se necesite)**: Con los datos obtenidos y la tarjeta en blanco sería posible realizar una copia exacta de la tarjeta objetivo, alterando únicamente aquellos bytes que se quieran. El modo de grabado depende completamente del tipo de tecnología y estándar de las tarjetas, así como del hardware que se esté utilizando.

- **Las tarjetas no son editables y no es posible conseguir tarjetas en blanco**: En este caso la única opción posible es emular la tarjeta objetivo con los bytes alterados. Este es el escenario más complejo ya que requiere que el auditor porte dispositivos como Proxmark[16] junto a un equipo portátil.

  El modo de emulación depende completamente del tipo de tecnología y estándar de las tarjetas, así como del hardware que se esté utilizando. Existen ciertos tipos de tarjetas para los que no existe software desarrollado hasta la fecha que permita la emulación, un ejemplo son las tarjetas bancarias, basadas en la ISO 144443.

  Para realizar acciones de clonación y emulación de tarjetas NFC se recomienda el uso de la suite de herramientas NFC Tools[17] disponible tanto para Linux como para Windows.

  Para realizar acciones de clonado y emulación de tarjetas RFID se recomiendo el uso de la suite de herramientas propia de Proxmark.

4.7 Fase 6: Post-Explotación

Tras finalizar todo el proceso de auditoría sobre el escenario en cuestión, el auditor ya conoce todos los detalles y tiene la posibilidad de leer contenido, escribir contenido (clonar) y emular la tarjeta.

De cara a facilitar ciertas labores es posible realizar algunas acciones secundarias que den mayor facilidad al auditor en caso de querer replicar el escenario.

[16] http://www.proxmark.org/

[17] http://nfc-tools.org/index.php?title=Main_Page

4.8 Dispositivos y software

En el presente apartado se exponen los dispositivos y software necesarios para realizar las pruebas. Estos dispositivos son utilizados dependiendo de las necesidades del escenario que este siendo comprobado.

4.8.1 Dispositivos

4.8.1.1 Lector NFC común (ACR122U)

El dispositivo ACR122U de ACS, consiste en un dispositivo Plug-and-Play que permite interactuar con tecnologías NFC desde un equipo. El dispositivo únicamente acepta tecnología NFC y por lo tanto es capaz de interactuar en la frecuencia de 13.56MHz.

Precio: ~40€

4.8.1.2 Proxmark III

Dentro de los equipos especializados para interactuar con las tecnologías RFID y NFC se encuentra el dispositivo Proxmark III. Este dispositivo fue desarrollado por Jonathan Westhues y permite leer, escribir y clonar la inmensa mayoría de estándares y tipos de tarjetas tanto RFID como NFC.

Precio: ~450€

4.8.1.3 Android

Ya que parte del trabajo se desarrolla sobre la tecnología NFC, también han sido utilizados diferentes dispositivos Android con la funcionalidad de NFC. Esto permite mostrar la sencillez en muchos casos de vulnerar entornos concretos con el uso únicamente de un Smartphone.

4.8.1.4 Tarjetas

Como parte fundamental del trabajo, también han sido utilizadas diferentes tarjetas, tanto aquellas originales del escenario que se fuera a comprobar como en blanco para acciones secundarias como clonado de la tarjeta.

Precio: 2-10€

4.8.1.5 Equipo personal

Además del anterior hardware necesario para realizar el trabajo de investigación y desarrollo de la metodología, también es necesario un equipo personal para poder interactuar con el hardware y software.

4.8.2 Software

4.8.2.1 General

Existe gran cantidad de software desarrollado para interactuar con las tecnologías RFID y NFC, aunque de ellas únicamente han sido utilizados los siguientes programas y suites:

- Software oficial Proxmark
- NFC-tools
- Drivers

4.8.2.2 Apps moviles

Existe gran cantidad de software desarrollado para interactuar con las tecnologías RFID y NFC, aunque de ellas únicamente han sido utilizados las siguientes aplicaciones:

- NFC TagInfo[18]
- RFID NFC Tool[19]
- Mifare Classic Tool[20]
- Smart Card Toolkit[21]
- Jackless[22]
- Lector de tarjetas[23]

[18] https://play.google.com/store/apps/details?id=at.mroland.android.apps.nfctaginfo&hl=es

[19] https://play.google.com/store/apps/details?id=tw.com.method.rfidtool&hl=es

[20] https://play.google.com/store/apps/details?id=de.syss.MifareClassicTool&hl=es

[21] https://play.google.com/store/apps/details?id=sasc.android.smartcard&hl=es

[22] https://play.google.com/store/apps/details?id=com.noSquare&hl=es

[23] https://play.google.com/store/apps/details?id=com.github.devnied.emvnfccard&hl=es

5 Pruebas y resultados

En el presente punto se van a exponer algunas de las pruebas realizadas y los resultados obtenidos sobre entornos e infraestructuras que hacen uso de tecnologías Contactless, donde se ha utilizado la metodología desarrollada.

5.1 Estaciones de sky

Tecnología	**NFC**
Tipo (Estándar)	ISO 15693 (Vicinity)
Nivel de seguridad	Bajo
Escenario vulnerable	Si

5.1.1 Descripción del escenario

Es muy habitual que las estaciones de sky utilicen como forfait (control de acceso a las pistas) tarjetas RFID o NFC con el objetivo de dar mayores facilidades a sus clientes para el acceso a las instalaciones. Utilizado las tarjetas contactless permiten a los esquiadores la posibilidad de acceder a las pistas sin necesidad de sacar nada de los bolsillos y únicamente necesitas aproximarse al lector.

Debido a que habitualmente viajo a estaciones de sky, comprobé el funcionamiento de varias de ellas.

5.1.2 Vector de ataque identificado

El resultado de aplicar la metodología desarrollada sobre estos escenarios permitió averiguar que la mayoría de estaciones hacen uso de la tecnología NFC y el estándar ISO 15693 (Vicinity).

Concretamente durante estas pruebas se comprobó el acceso a las estaciones de GrandValira (Andorra) y Astun.

Las tarjetas Vicinity no tienen ningún tipo de seguridad y pueden ser leídas directamente un dispositivo móvil y la aplicación “RFID NFC Tool” permite además escribir directamente los bloques de información que se quieran.

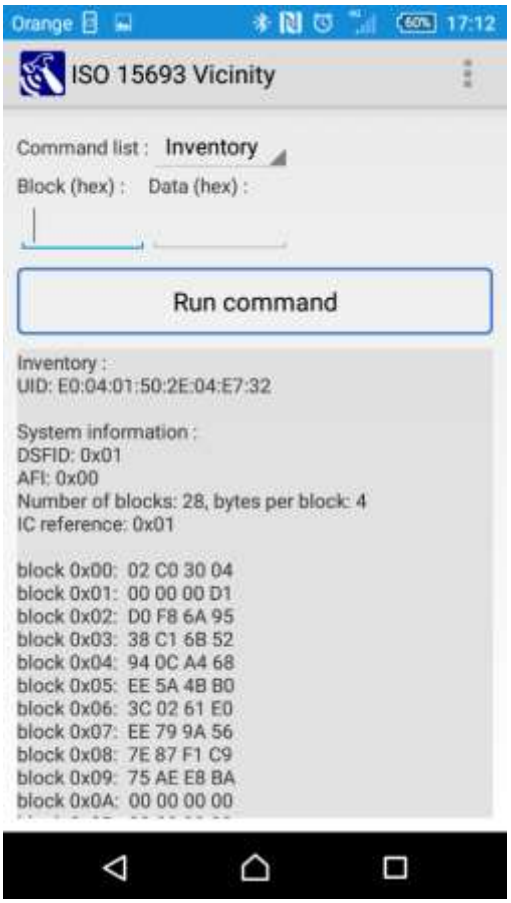

Imagen 6 - Lectura y modificación Vicinity

Siguiendo la metodología, se compararon dos forfait distintos de dos fechas diferentes y se identificaron los bytes de la tarjeta donde se indica el día hasta el que se tiene acceso a la estación.

Debido a que las tarjetas son recargables y es posible escribir en ellas es posible crearse forfaits para una fecha distinta a la original. A modo de ejemplo se creó un forfait de por vida.

5.2 Parquímetros Madrid

Tecnología	**NFC**
Tipo (Estándar)	Mifare Ultralight EV1 (ISO 14443)
Nivel de seguridad	Medio
Escenario vulnerable	Si

5.2.1 Descripción del escenario

En la actualidad las ciudades están implementando cada vez más instrumentos modernos que faciliten la vida a los ciudadanos. Como parte de estos avances y concretamente en la ciudad de Madrid se hace uso de la tecnología RFID / NFC para realizar el pago de estacionamiento de coches en el centro de la ciudad.

Para poder realizar el pago del estacionamiento mediante esta tecnología, es necesario pedir al ayuntamiento de Madrid las tarjetas monedero NFC.

El funcionamiento de las tarjetas permite a los ciudadanos meter dinero una única vez y desde ese momento realizar el pago del estacionamiento a través de la tarjeta NFC monedero hasta que se acabe el dinero de la misma y el usuario deba recargarla.

5.2.2 Vector de ataque identificado

El resultado de aplicar la metodología desarrollada sobre estos escenarios permitió averiguar que las tarjetas monedero hacen uso de la tecnología NFC y el estándar Mifare Ultralight EV1 1K, perteneciente a la ISO 14443.

Durante las pruebas se comprobó que aunque las tarjetas permiten el uso de métodos de seguridad como el uso de dos claves diferentes para la lectura y escritura de cada sector, dichas claves se encontraban siempre por defecto.

Imagen 7 - Uso de claves por defecto

Analizando el contenido de la tarjeta se detectó que está completamente vacío por lo que el método de funcionamiento es el siguiente:

- A cada usuario se le proporciona una tarjeta y se establece una relación entre el cliente y el número único de la tarjeta (UID), grabado por el fabricante.

- Cuando un usuario introduce dinero en una máquina y pasa la tarjeta NFC, el dispositivo del parquímetro comunica con un servidor central y le indica que dicho usuario ha hecho un ingreso de dinero en la tarjeta.

- Cuando el usuario quiere pagar un parquímetro con la tarjeta NFC la maquina establece una comunicación con el servidor central pidiéndole la cantidad de saldo que tiene dicho usuario.

Este escenario implica que el único ataque posible seria realizar la emulación de tarjetas con diferente UID hasta dar con una que tuviera saldo. Este ataque no se considera ni critico ni sencillo por lo que se puede decir que aunque la seguridad es mejorable, no es mala.

5.3 Taquillas electrónicas

Tecnología	**NFC**
Tipo (Estándar)	Mifare Classic 1K
Nivel de seguridad	Bajo
Escenario vulnerable	Si

5.3.1 Descripción del escenario

En multitud de lugares de ocio está proliferando la utilización de la tecnología RFID / NFC para controlar el acceso a taquillas. Un ejemplo común es el acceso a taquillas en los gimnasios.

En el presente escenario se realizaron pruebas con las taquillas existentes en el centro de ocio Xanadu, concretamente en el SnowZone, una zona dedicada a esquiadores donde es posible alquilar taquillas para dejar el material de sus clientes.

5.3.2 Vector de ataque identificado

El resultado de aplicar la metodología desarrollada sobre este escenario permitió detectar que las tarjetas utilizadas hacían uso de la tecnología NFC y el estándar Mifare Classic 1K, perteneciente a la ISO 14443.

Este escenario es potencialmente vulnerable debido a que aunque las tarjetas que utilizan dicho estándar permiten el uso de claves para la lectura y escritura de los diferentes sectores, en muchas ocasiones se encuentras definidas por defecto.

En este caso concreto se identificó que únicamente existía un sector protegido con una clave que no se encontraba por defecto. Tras realizar un proceso de fuerza bruta se obtuvo la clave en cuestión, pudiendo acceder al volcado completo de la información contenida en la tarjeta y la posibilidad de alterar o clonar dicha tarjeta.

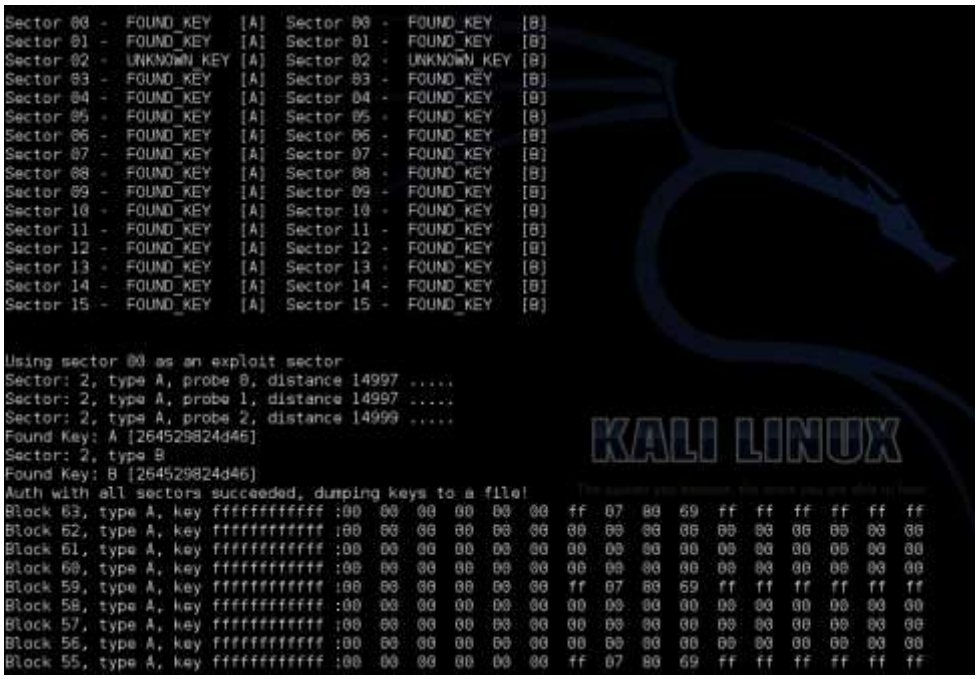

Imagen 8 - Obtención de claves

Tras investigar el contenido de la tarjeta se detectó que el sector que se encontraba cifrado contenía la información necesaria que identificaba la taquilla que podía ser abierta con dicha clave. Alterando dicho valor es posible acceder a cualquier taquilla.

5.4 Control de acceso en empresa privada

Tecnología	**NFC**
Tipo (Estándar)	Mifare Classic 4K
Nivel de seguridad	Bajo
Escenario vulnerable	Si

5.4.1 Descripción del escenario

Uno de los usos más habituales desde que se comenzó a utilizar la tecnología RFID en el ámbito privado es para controlar el acceso a zonas restringidas en las organizaciones. En la actualidad la mayoría de organizaciones cuenta con sistemas RFID / NFC para controlar el acceso de sus empleados.

En este caso, y debido a mi trabajo como consultor de seguridad y dedicado especialmente a la realización de intrusiones tanto a nivel digital como físico, he comprobado la seguridad del control de acceso RFID / NFC de gran cantidad de organización.

En este caso, se van a exponer los resultados de una de las pruebas de intrusión física que tuve que realizar a una entidad bancaria nacional.

5.4.2 Vector de ataque identificado

El resultado de aplicar la metodología desarrollada sobre este escenario permitió detectar que las tarjetas utilizadas hacían uso de la tecnología NFC y el estándar Mifare Classic 4K, perteneciente a la ISO 14443.

En este caso la entidad bancaria había gastado un gran presupuesto en crear el control de acceso por NFC pero no habían modificado las claves de la tarjeta por lo que era posible acceder a todo el contenido. A continuación se muestra una imagen donde se aprecia que todas las claves han sido identificadas por defecto:

Imagen 9 - Claves por defecto

Imagen 10 - Acceso en claro al contenido

Al analizar el contenido se identificó que toda la tarjeta se encontraba en blanco. Esto es algo común cuando se utiliza el UID de la tarjeta como identificado del empleado. De esta manera, cada empleado tiene asignado un identificador único que es el UID de su tarjeta de acceso.

Ya que el UID de la tarjeta es accesible y puede ser leído siempre, se procedió a leer el UID de la tarjeta de un empleado utilizando técnicas de ingeniería social. Tras obtener el UID se escribir en una tarjeta en blanco con puerta trasera y a imprimir de forma similar la tarjeta clonada como la de un empleado verídico.

5.5 Máquinas de vending

Tecnología	**NFC**
Tipo (Estándar)	Mifare Classic 1K
Nivel de seguridad	Bajo
Escenario vulnerable	Si

5.5.1 Descripción del escenario

Otro tipo de aplicación que está actualmente de moda es utilizar la tecnología NFC en las máquinas de vending.

Las empresas proporcionan a los empleados tarjetas monedero NFC con las que realizar la compra de alimentos en dichas maquinas, aplicando un descuento extra por ser empleados.

En este caso concreto, se centró la investigación en las máquinas de vending y etiquetas de la empresa "Your Best break".

5.5.2 Vector de ataque identificado

El resultado de aplicar la metodología desarrollada sobre este escenario permitió detectar que las tarjetas utilizadas hacían uso de la tecnología NFC y el estándar Mifare Classic 1K, perteneciente a la ISO 14443.

Como se ha expuesto anteriormente, estas tarjetas contienen claves para definir el acceso de lectura y escritura a cada sector de memoria aunque en muchas ocasiones dichas claves se encuentran establecidas por defecto.

En este caso, las tarjetas tenían los últimos 4 sectores con clave de lectura y escritura habilitado por lo que se realizó un proceso de fuerza bruta a través del cual fue posible obtener dichas claves en texto claro.

A continuación se muestra el intento de lectura desde la aplicación NFC TagInfo:

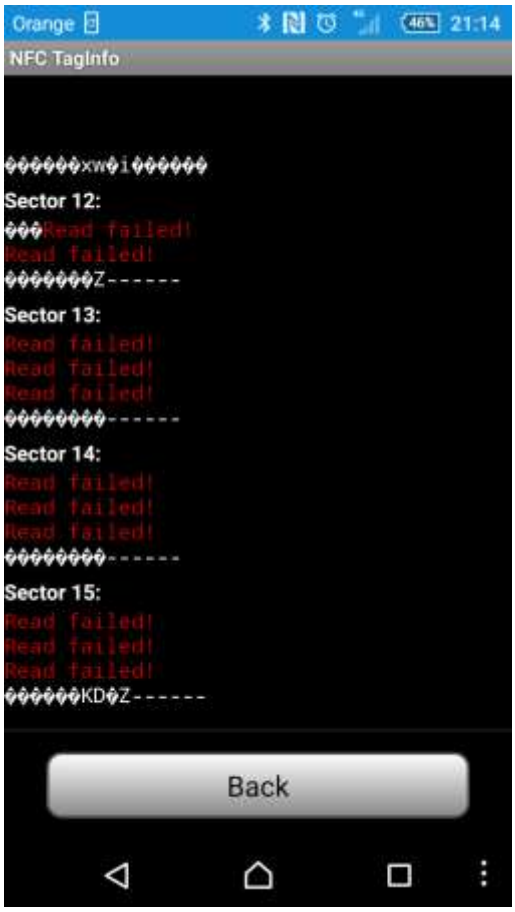

Imagen 11 - Sectores protegidos

Analizando el contenido se identificaron los bytes donde se almacenaba el dinero existente en la tarjeta en texto claro. Para identificar dichos bytes se creó un volcado del contenido con un determinado dinero y otro una vez gastado parte del dinero, posteriormente se compararon los cambios realizados y se identificaron los bytes donde se encontraba la cantidad de dinero en hexadecimal.

En este caso se muestra la edición de un volcado realizado tras obtener las claves de los sectores protegidos.

Imagen 12 - Análisis del contenido

Entre los bytes que se observan en la imagen, aquellos que contenían el dinero eran el "000208" en hexadecimal del sector 12 ya que dicho volcado era de una tarjeta que tenía un total de 5,20€. La relación era la siguiente:

5,20 € → 520 en decimal → 208 en hexadecimal

Conociendo esta información es posible establecer el dinero que se quiera en la tarjeta monedero.

5.6 Tarjetas bancarias (NFC)

Tecnología	**NFC**
Tipo (Estándar)	Mifare Classic 1K
Nivel de seguridad	Medio
Escenario vulnerable	Si

5.6.1 Descripción del escenario

Otro escenario común de ver a día de hoy donde se utiliza la tecnología NFC es en las nuevas tarjetas que proporcionan los bancos a sus clientes. Estas tarjetas permiten realizar los pagos con NFC y en caso de ser los pagos inferiores a 20 € no es tan siquiera necesario introducir el PIN de la tarjeta.

En este escenario se comprobaron las tarjetas de un banco nacional pero posteriormente se realizó la verificación con otros bancos similares y el resultado fue el mismo.

5.6.2 Vector de ataque identificado

El resultado de aplicar la metodología desarrollada sobre este escenario permitió detectar que las tarjetas utilizadas hacían uso de la tecnología NFC y el estándar Mifare Classic 1K, perteneciente a la ISO 14443 pero basado en el estándar de propietario de EMV[24].

El uso del estándar propietario de EMV impide la posibilidad de realizar copias o emulaciones de dichas tarjetas ya que los detalles de la implementación no son públicos.

Aun con dichas dificultades, al realizar la lectura de la tarjeta se obtiene gran cantidad de información sobre la tarjeta y los datos de la misma, así como transacciones realizadas, etc.

Entre la información que es posible obtener, destaca que mediante NFC es posible obtener 5/6 de la información existente en la banda magnética de esa misma tarjeta. Con estos datos es posible crear una tarjeta magnética exactamente igual a la tarjeta leída.

Este escenario permite la copia de la tarjeta ya que aunque no sea a través de NFC, se podrían realizar acciones con la tarjeta copiada utilizando la banda magnética. Para recrear este escenario con existo es necesario tener un dispositivo lector y escritor de tarjetas de banda magnética (En este caso se utilizó el dispositivo MSR206[25]).

A continuación se muestra como sencillamente utilizando la aplicación móvil Jackless es posible obtener prácticamente los 3 tracks existentes en la banda magnética según la ISO 7813[26], directamente desde NFC:

[24] https://es.wikipedia.org/wiki/EMV

[25] http://us.ute.com/products_info.php?pc1=74&pc2=148&rbu=5&pid=386

[26] https://en.wikipedia.org/wiki/ISO/IEC_7813

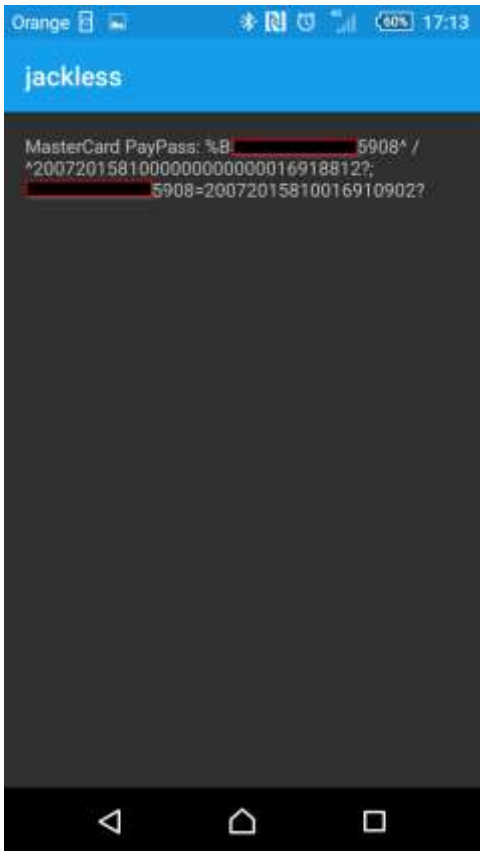

Imagen 13 - Obtención de tracks de la tarjeta bancaria

La problemática principal de este ataque radica en que cualquier persona podría ir andando por la calle con el NFC habilitado y capturando datos de las tarjetas de los viandantes.

6 Uso de la metodología en simulaciones de intrusión física y ejercicios de Red Team

Además de los escenarios y casos reales expuestos a continuación, en los dos últimos años me he dedicado profesionalmente a la seguridad y más concretamente a la simulación de intrusiones tanto a nivel digital como físico.

Dentro del ámbito del presente trabajo, mi experiencia y labor profesional me ha permitido realizar gran cantidad de pruebas de manera autorizada sobre corporaciones a nivel nacional e internacional, donde algunas de ellas han sido expuestas en el presente documento (7.4).

De las simulaciones y ejercicios de hacking ético destacan los denominados ejercicios Red Team, simulaciones de intrusión realistas donde los auditores tienen total desconocimiento de los sistemas e infraestructura de la organización objetivo, siendo su objetivo simular una intrusión realizada por atacantes cuya finalidad es obtener control sobre los activos más críticos de la organización.

Como se ha expuesto anteriormente durante los dos últimos años me he dedicado a esta labor y ello me ha permitido comprobar que el control de acceso es algo que todas las organizaciones poseen pero en muchos de los casos, esto control de acceso se basa en tecnología RFID/NFC y es realmente sencillo de vulnerar.

Sin duda este es un vector de ataque que muchas organizaciones no tienen en cuenta, pero vulnerar el control de acceso permite unos enormes privilegios a un atacante. A modo de ejemplo se van a exponer los pasos e hitos realizados en uno de los trabajos de intrusión con el objetivo de demostrar el verdadero impacto que puede tener.

En este ejemplo, el objetivo es un banco cuya infraestructura de red pública y redes Wi-Fi era realmente segura, es decir los únicos puntos de entrada que podría utilizar un atacante sin contar con el ámbito físico y el uso de la ingeniería social (engaño).

Tras comprobar las medidas de seguridad física se identifica el tipo de lector NFC utilizado para el control de acceso y se identifica que este lector únicamente lee tarjetas Mifare Classic 4K.

Se ejecuta un escenario donde de forma accidental se simula un choque con un empleado copiándole de esta forma la tarjeta NFC (que llevaba en la parte trasera del pantalón). Esto se realiza mediante el dispositivo Proxmark y una Raspberry[27] conectada al dispositivo móvil desde el cual se controla.

Tras obtener un volcado de la tarjeta se imprime una tarjeta idéntica a las originales.

Un par de días después, durante un día lluvioso para evitar la grabación correcta de las cámaras, se procede a entrar a las 7:00 de la mañana al edificio vestido de traje mientras

[27] https://www.raspberrypi.org/

supuestamente se habla por teléfono para evitar levantar sospechas. Se elige esta hora porque la mayoría de empleados accede a las instalaciones a las 8:00 o más tarde.

Durante la investigación a la organización, se identificó que tiene una política donde cualquier empleado puede ocupar sitios distintos cada día. Con este dato, se procedió a subir a las plantas de los empleados.

Una vez allí, se tomó control de un equipo a través del software Kon-Boot[28], el cual permite parchear el inicio de Windows para evitar que este pida credenciales. Al acceder al sistema se instala un malware desarrollado a medida para evitar la detección de los antivirus y que nos permite controlar el sistema de manera remota.

Completada esta acción se sale del edificio a las 7:15 sin ningún problema y teniendo control de un sistema interno.

Con el acceso a la red interna comienza la intrusión digital que da lugar, un mes después, al compromiso completo del entorno Windows y Unix, acceso a las redes de oficinas, sistemas mainframe y un largo etcétera. En resumen, control completo del banco pudiendo sacar dinero de los cajeros de forma remota o realizando transferencias mediante la aplicación verídica del banco.

Esto es un claro ejemplo del objetivo de un Red Team, donde se unen vectores de diferentes ámbitos (digital, físico y social) para simular ataques dirigidos sobre organizaciones.

A la vez pone de manifiesto la necesidad de realizar comprobaciones sobre todos los entornos donde se haga uso de la tecnología y más concretamente, la tecnología NFC.

[28] http://www.piotrbania.com/all/kon-boot/

7 Conclusiones y trabajo futuro

En el presente punto se van a exponer las conclusiones extraídas del trabajo realizado así como las posibles vías de trabajo futuro para continuar con la metodología desarrollada.

7.1 Conclusiones

Con la investigación de las tecnologías RFID y NFC, y el posterior desarrollo de la metodología de auditoria de seguridad para tecnologías Contactless, se facilita la tarea a los auditores y desarrolladores para realizar pruebas de seguridad sobre escenarios e infraestructuras que utilicen este tipo de tecnología.

Con la metodología desarrollada, cualquier persona, sin necesidad de contar con elevados conocimientos en esta tecnología podría realizar comprobaciones de seguridad suficientes para verificar el nivel de seguridad del escenario o infraestructura.

En la actualidad, todas las organizaciones que han desarrollado y siguen desarrollando metodologías de seguridad para realizar auditorías de seguridad han definido con gran éxito cuales son los pasos a seguir y cuál es la mejor forma de llevar a cabo auditorias de seguridad. Por ello, se analizaron diferentes metodologías que permitieron organizar de forma eficaz la metodología desarrollada.

Las metodologías de seguridad son absolutamente necesarias para que la industria y tecnologías actuales puedan seguir evolucionando de forma alineada y no de forma independiente. Para que los consumidores de estos servicios sepan de una forma clara que es lo que contratan y que es lo que pueden esperar, independientemente de la empresa a la que lo contrates.

El gran problema radica en que las tecnologías actuales en pocas ocasiones son auditadas, lo cual provoca que a día de hoy convivamos con tecnología vulnerable a gran cantidad de ataques.

La metodología desarrollada pretende ayudar en esta labor de mejora de la seguridad, aportando las pautas necesarias para comprobar la seguridad de manera específica en tecnologías Contactless como RFID y NFC.

7.2 Trabajo futuro

Dentro de las posibles vías para continuar con el trabajo desarrollado se encuentran las siguientes:

- Hacer pública la metodología, lo cual permitiría a otros auditores de seguridad e investigadores hacer aportaciones al trabajo realizado con su experiencia previa en la auditoria de estas tecnologías. De esta manera la metodología podría ir evolucionando y con ello consiguiendo mayor calidad en el documento.

- Investigar otras tecnologías modernas y de uso generalizado a día de hoy sobre las que no exista ningún tipo de metodología específica de seguridad. Realizar un estudio similar sobre ellas y desarrollar otra metodología de auditoria de seguridad.

Referencias

[1] Miodrag Bolic, David Simplot-Ryl, Ivan Stojmenovic, "RFID Systems: Research Trends and Challenges", Wiley, Septiembre 2010.

[2] B. Song, CJ Mitchell, "RFID Authentication Protocol for Low-cost Tags", Royal Holloway, University of London, 2008.

[3] Flavio D. Garcia, "Wirelessly Pickpocketing a Mifare Classic Card", 30th IEEE Symposium on Security and Privacy, 2009, pp. 3-15.

[4] Andrey Bogdanov. Attacks on the KeeLoq Block Cipher and Authentication Systems. In In RFIDSec, 2007.

[5] M. Roland, J. Langer, Cloning Credit Cards: A Combined Pre-play and Downgrade Attack on EMV Contactless, 7th USENIX conference on Offensive Technologies (WOOT13), Washington D.C., U.S.A., August 13, 2013.

[6] G. P. Hancke, A Practical Relay Attack on ISO 14443 Proximity Cards, Technical report, University of Cambridge Computer Laboratory, February, 2005.

[7] Flavio D. Garcia, Gerhard Koning Gans, Ruben Muijrers, Peter Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs. Dismantling mifare classic. In Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security, ESORICS '08, pages 97–114, Berlin, Heidelberg, 2008. Springer-Verlag.

[8] "ADVANCING PAYMENT SECURITY MASTERCARD CONTACTLESS SECURITY OVERVIEW", MasterCard, 2015, https://www.mastercard.com/contactless/doc/MasterCardContactless_SecurityFactSheet_2015.pdf

[9] Jordi van den Breekel, "Relaying EMV Contactless Transactions using Off-The-Shelf Android Devices", BlackHat Asia, March 2015, https://www.blackhat.com/docs/asia-15/materials/asia-15-VandenBreekel-Relaying-EMV-Contactless-Transactions-Using-Off-The-Shelf-Android-Devices-wp.pdf

[10] Andrew Lee, Timothy Lui, and Bryon Leung, "Security Analysis of the Octopus System", http://euro.ecom.cmu.edu/resources/elibrary/epay/OctopusSecurity.pdf

[11] Roel Verdult, "Security analysis of RFID tags", Radbund University, http://www.cs.ru.nl/~rverdult/Security_Analysis_of_RFID_Tags-2008.pdf

[12] Bitmanufaktur GmbH. OpenPCD Passive RFID Project - OpenPCD. http://www.openpcd.org/, 2012. [Online; Request on April, 2nd of 2012].

[13] Francis Brown, "RFID Hacking", BlackHat USA, Aug 2013, https://media.blackhat.com/us-13/US-13-Brown-RFID-Hacking-Live-Free-or-RFID-Hard-Slides.pdf

[14] Romke van Dijk , Loek Sangers , “Portable RFID Bumping Device”, University of Amsterdam, http://www.delaat.net/rp/2015-2016/p04/report.pdf

[15] Eddie Lee, “NFC Hacking: The Easy Way”, DefCon 20, http://korben.info/wp-content/uploads/defcon/SpeakerPresentations/Lee/DEFCON-20-Lee-NFC-Hacking.pdf

[16] Christian Killer, Christos Tsiaras, Burkhard Stiller , “An Off-the-shelf Relay Attack in a Contactless Payment Solution”, University of Zürich, https://files.ifi.uzh.ch/CSG/staff/tsiaras/Extern/Theses/VA_ChristianKiller.pdf

[17] Márcio Almeida, “Hacking Mifare Classic Cards”, BlackHat Summit Sao Paulo, 2014, https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf

[18] Mathias Morbitzer , “The MIFARE Hack”, Radboud University Nijmegen, http://proxmark.nl/files/Documents/13.56%20MHz%20-%20MIFARE%20Classic/The_MIFARE_Hack.pdf

[19] Wee Hon Tan, “Practical Attacks on the MIFARE Classic”, Imperial College London, http://www.doc.ic.ac.uk/~mgv98/MIFARE_files/report.pdf

Glosario

Tecnología Contactless	Tecnologías inalámbricas de corto alcance (RFID / NFC)
RFID	Radio-frequency identification
NFC	Near field communication
Blue Team	Equipo de defense de una organizacion
Red Team	Equipo ofensivo que toma el rol de un atacante
PTES	*Penetration Testing Execution Standard*
OSSTMM	Open Source Security Testing Methodology Manual
NIST	National Institute of Standards and Technology
OWASP	Open Web Aplication Security Project
ISECOM	Institute for Security and Open Methodologies
Tags	Etiqueta RFID
NFCIP	Near Field Communication Interface and Protocol

Anexos

A Publicaciones personales relacionadas con la temática

A.1 Publicación en la revista Cuadernos de Seguridad

Título: "Red Team: Pensando como el enemigo"

Descripción:
El artículo expone que son los ejercicios de Red Team, como son realizados y su importancia en la identificación de riesgos reales en las organizaciones.

Enlace: https://blog.entelgy.com/cuadernos-seguridad-innotec-red-team/

A.2 Presentación en el congreso "Forum de Empresa 2016 (Andorra Telecom)"

Título: "Red Team: Cuando el ataque es la mejor defensa"

Descripción:
Presentación sobre que son y como son desarrollados los ejercicios de intrusión realizados por los equipos Red Team. Se mostraron en detalle algunos ejemplos reales realizados desde Innotec System.

Enlace: https://www.youtube.com/watch?v=9PdM8hxsH5g

A.3 Presentación en el congreso "itSMF Vision 15"

Título: "Hacking Físico: Vulnerando entornos, evadiendo sensores... ¿Misión Imposible?"

Descripción:
Presentación realizada en el congreso itSMF Vision15 donde se ve la seguridad existente en los dispositivos personales, el Internet de las cosas, y por último la seguridad física dentro del entorno corporativo.

Enlace: http://es.slideshare.net/eduan796/

A.4 Presentación en el congreso "Jornadas Técnicas de ISACA 2015"

Título: "Red Team: Next Generation Penetration Testing"

Descripción:
Exposición de la necesidad de cambiar la mentalidad actual, y aplicar enfoques y ejercicios que permitan prever y protegerse frente a amenazas dirigidas.

Para dar solución a dicho problema se presenta el concepto de Red Team, sus beneficios, equipo, metodología y enfoque aportado desde el proyecto RedTeaming.es.

Para finalizar se exponen una serie de casos de éxito de ejercicios realizados por los integrantes del proyecto RedTeaming.es.

Enlace: http://es.slideshare.net/eduan796/red-team-next-generation-penetration-testing

A.5 Presentación en el congreso "SegurInfo 2015"

Título: "Red Team: Un cambio necesario para la visión holística de la ciberseguridad"

Descripción:
La mentalidad tradicional, es actualmente ineficaz. Las organizaciones realizan comprobaciones aisladas en seguridad que no les permiten conocer el verdadero riesgo al que están expuestas, provocando una falsa sensación de seguridad. Por ello es necesaria una evolución hacia el concepto y mentalidad Red Team.

Enlace: http://archivos.usuaria.org.ar/segurinfo2015/espana/agenda-espana.html

A.6 Presentación en el congreso "RootedCON 2015"

Título: "Physical Penetration Testing"

Descripción:
La realización de un Test de Intrusión Físico tiene como finalidad conseguir acceso físico a una determinada ubicación, y no es una tarea sencilla. Requiere preparación, investigación, análisis, coordinación, mucha simulación y la aplicación de una metodología flexible que pueda adaptarse a las condiciones particulares de cada objetivo.
Analizar el entorno, evadir todo tipo de sistemas de seguridad física y colaborar en equipo (Red Team), son aspectos fundamentales para lograr la intrusión, y con ello posteriormente, el acceso a equipos, red y un sinfín de datos en las instalaciones del objetivo.Si quieres saber qué es un Red Team y profundizar en la realización de intrusiones físicas, esta es tu charla.

URL del video: https://www.youtube.com/watch?v=TTwY2wPTcNg

Enlace: http://es.slideshare.net/Hykeos/physical-penetration-testing-rootedcon-2015

A.7 Más publicaciones del autor

A continuación se adjunta un enlace donde existen más presentaciones realizadas sobre temas de seguridad.

https://www.linkedin.com/in/eduardoarriols