Universidad de Buenos Aires
Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Aspectos de Seguridad en Sistemas de Boleto Electrónico

Autor: MAREY, Amadís Diego <lic.marey at gmail.com>
Tutor: BAADER, Rodolfo

2011

Resumen

El presente Trabajo Final de Especialización busca analizar, tanto los ataques que pueden producirse, como los posibles controles y mitigaciones que pueden implementarse para minimizar su impacto en un sistema de boleto electrónico que implemente tecnología de tarjetas inteligentes sin contacto, en especial de tipo Mifare Classic.

La metodología empleada ha sido la investigación de los posibles ataques a dichas tarjetas sin contacto y los controles preventivos y correctivos que pueden compensar dichos ataques.

Sin embargo, en el desarrollo de los capítulos, no se profundiza en el criptoanálisis sobre el método de cifrado CRYPTO-1 de MIFARE, en el entendimiento que hay numerosos trabajos, muchos de ellos citados como referencia bibliográfica con el objeto de obtener de cada uno de ellos su punto de vista en la metodología de los ataques y las consecuencias sobre un sistema de transporte, que abordan la temática de análisis criptográfico reversible de una manera mucho más completa, profunda y detallada de lo que se pretende en este Trabajo Final.

El trabajo comienza un capítulo de Antecedentes, el cual es introductorio a la temática tratada, luego se realiza una descripción de los posibles Fraudes y Riegos asociados a la tecnología, y en base a ellos, se proponen algunas Mitigaciones que describen los controles y las posibles medidas de técnicas y operativas que se entienden como convenientes de implementar para que un sistema de boleto electrónico sea razonablemente seguro.

Palabras clave:

Transporte, Mifare Classic, Fraude, Controles, Clonado, Ticketing, Backoffice, Cuadratura de Saldos, CRYPTO-1, RFID, Tarjeta Inteligente sin contacto.

Este trabajo está dedicado a mis dos grande amores: Amaia y Alexia, por el apoyo constante y la paciencia infinita.

El presente documento es mi primer experiencia con LaTeX.

Índice general

1. Antecedentes **3**

1.1. Un poco de Historia 4

1.2. Tipos de Fraude 5

1.2.1. Falsificación del dispositivo 6

1.2.2. Modificación del valor contenido en la tarjeta 6

1.2.3. Emulación del dispositivo 6

1.2.4. Factores de Autenticación 6

1.3. Tarjetas inteligentes sin contacto 7

1.3.1. Mapping 8

2. Potenciales Fraudes en TISC **12**

2.1. Tipos de Fraudes en TISC 13

2.1.1. Falsificación de TISC 13

2.1.2. Modificación de la carga en TISC 13

2.1.3. Emulación de una TISC 14

2.1.4. Metodología de los ataques 15

2.1.5. En resumen 16

2.2. Riesgos 16

3. Mitigaciones **18**

3.1. Algunas medidas 19

3.1.1. Referidas a la Tarjeta 19

3.1.2. Referidas al sistema en general: 24

3.2. Evolución de las TISC 26

4. Conclusiones **28**

Capítulo 1

Antecedentes

1.1. Un poco de Historia

El sistema de transporte público tuvo que lidiar históricamente con distintas implementaciones que permitan el tarifado del servicio. Como cualquier otro tipo de prestación arancelada, en paralelo con el sistema de tarifas se debe tener la previsión de la implementación de controles de evasión y de fraude.

> En sistemas de transporte, los ticket estaban disponibles mucho antes de la introducción de la electrónica y la informática, a pesar de que son relativamente nuevos en comparación a la historia de la criminalidad. Por lo tanto, no sorprende que la gente ha tratado de cometer fraude en materia de transporte y los objetivos fundamentales no han cambiado mucho en los viajes es decir, viajar sin ticket o con un ticket falso. Para apreciar la magnitud de este fraude, Transport for London (Compañia de transportes de Londres) calcula que los abusos de su antiguo sistema de ticket de papel (eliminado hace casi una década) tenía pérdidas valuadas en £ 10 millones por año en sus sistemas de metro y autobús. [1]

En Argentina, particularmente en Buenos Aires, al igual que en cualquier gran ciudad del mundo, el boleto en papel, los cospeles y los molinetes fueron históricamente los medios mas utilizados para efectuar dicho control.

Figura 1.1: Boletos y cospeles

Todos ellos conllevaban también la posibilidad de fraude por falsificación de los elementos y necesariamente revelaron la necesidad de implementar controles adicionales como ser guardas o inspectores o seguimiento de estadísticas de uso de cada medio de transporte.

> Se cuenta que el primero (de los colectivos) no expedía boletos inicialmente y para recibir el importe de los viajes colocó alcancías en sus coches. . . . convengamos que las *avivadas* ya existían: aparte de monedas, se depositaban chapitas, botones y diversos objetos que completaban una recaudación heterogénea. [2]

En dicho contexto, fueron varios los sistemas electrónicos que se buscaron imponer para facilitar el cobro y la administración de pasajes, algunos con mayor o menor éxito.

> La primera máquina de lectura en el transporte apareció en la década de 1980 y se basaban en papel o cartón impreso, con una banda magnética en la parte posterior. La capacidad

[1] [MMH09]
[2] [Tra07]

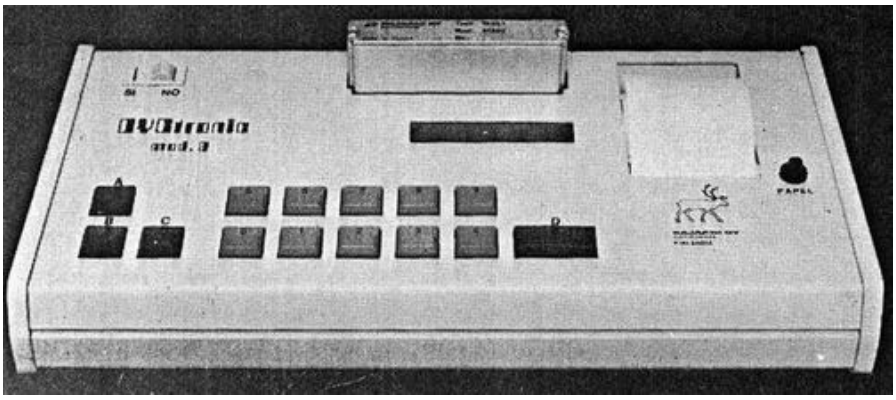

Figura 1.2: Boletera computada DYC Tronic

> de almacenamiento de datos de la banda era muy limitada y el contenido puede hoy ser fácilmente copiado, sin embargo, el punto importante era que se trataba de lectura mecánica (por ejemplo, a través de un lector en una estación de puerta o barrera) y no que era más seguro que el billete de papel.[3]

En la figura 1.2 se muestra una foto de 1981 cuando se ensayó en la Argentina el uso de una boletera computada finlandesa de la línea 51.[4]

> Se trataba de una consola con visor, alimentada por un módulo removible, donde se insertaba un código, fecha y ruta. En viaje, solo había que informarle del pase de sección y del valor del boleto solicitado, mediante distintas teclas, para que la maquinita expidiera el boleto: papelito rectangular, como de máquina registradora, donde figuraba número de línea e interno, fecha, hora, sección y valor del viaje. Otra tecla informaba, al finalizar el turno, el monto de la recaudación. Luego se descargaba el módulo en una terminal concentradora, para la estadística. Si bien aliviaba la parte administrativa, el colectivero seguía manejando dinero a bordo. Poco después el sistema fue probado en las líneas 162 y 194, sin éxito. [5]

1.2. Tipos de Fraude

Existen tres tipos de fraudes genéricos, cuya ocurrencia está fuertemente asociada a la naturaleza tecnológica del dispositivo [6]:

1. Falsificación del dispositivo
2. Modificación del valor almacenado en el dispositivo
3. Emulación del dispositivo

[3] [MMH09]
[4] [Tra07]
[5] [Tra07]
[6] [Pér02]

1.2.1. Falsificación del dispositivo

Este tipo de fraude ocurre principalmente en los dispositivos de bajo costo, como por ejemplo las tarjetas con banda magnética, cuya duplicación es trivial y necesita de un equipo de muy bajo costo. El costo de una tarjeta magnética en blanco es muy bajo, mientras que el equipamiento necesario es relativamente simple de conseguir y su costo es accesible. En general, ningún sistema que implique el grabado de los datos en una cinta, está libre de este problema.

1.2.2. Modificación del valor contenido en la tarjeta

Este tipo de fraude está presente en la gran mayoría de los sistemas de prepago, principalmente en aquellos que utilizan marcas físicas para almacenar el número de viajes realizados. Una cuestión a tener en cuenta con este fraude es que, aún con el contenido cifrado de una tarjeta válidamente adquirida, si es posible transferir ese contenido a otra tarjeta, el cifrado de la información no es suficiente, ya que si bien no es posible alterar el contenido almacenado si este contenido es almacenado y de alguna forma *congela* el estado actual de esa tarjeta, puede transferirse dicho contenido a nuevas tarjetas.

1.2.3. Emulación del dispositivo

En las tarjetas con contacto, que implementan el cifrado de los datos, se ha detectado, desde finales de los años noventa, la proliferación de emuladores de tarjetas. Un emulador es un dispositivo que posee un funcionamiento similar a uno legítimo, pudiendo agregar, modificar o inhibir algunas de sus funciones. En el caso específico de las tarjetas de prepago, estos dispositivos inhabilitan el cobro de la tarifa o simulan mediante software o electrónicamente (por variaciones de voltaje) la existencia de carga en la tarjeta. Estos fraudes se dieron principalmente en las tarjetas de prepago telefónicas con contacto en los años 90. El equipamiento necesario es relativamente simple y fácil de adquirir.

Todos estos fraudes, relacionados específicamente con el medio de pago, no impiden la existencia de otro tipo de fraudes que tienen que ver con, por ejemplo, saltear las barreras físicas (ver 1.3), evadir controles o pagar una tarifa menor a la estipulada para ese viaje, todas situaciones que difícilmente puedan controlarse con soluciones tecnológicas.

1.2.4. Factores de Autenticación

Mucho se habla de la debilidad de los sistemas de banda magnética, y como, a pesar de ello, sigue siendo utilizando en tarjetas de crédito. La explicación se puede reducir a que mientras en los sistemas de transporte se utilizaba como *un único factor de autenticación*, en las tarjetas de crédito suele utilizarse combinado con algún otro factor de autenticación.

Figura 1.3: Usuarios evadiendo molinetes en el Metro de Barcelona

> A pesar de sus debilidades, las tarjetas de banda magnética se mantienen en uso en las tarjetas de crédito durante mucho tiempo. No así en transporte, donde la seguridad de su uso como billete de viaje era fundamentalmente más débil ya que era un sistema de autenticación de un factor (algo que sólo usted tiene, por ejemplo el billete). En comparación, la tarjeta de crédito o en las transacciones en cajeros automáticos, siempre se usan dos factores, siendo además que la tarjeta tiene una firma o un Número de Identificación Personal (PIN). De hecho, la tecnología ha avanzado pero esta debilidad se ha mantenido en virtud de la naturaleza de rápido flujo de emisión de billetes electrónicos. En transporte no se puede tener, por razones de comodidad y seguridad, autenticaciones *lentas* de dos factores en las puertas de acceso.[7]

Otra diferencia con respecto a las tarjetas de crédito / cajero automático es que las transacciones del sistema de transporte se suelen utilizar fuera de línea a fin de garantizar velocidad y viabilidad de la gestión. El hecho de tener una seguridad *menor* con respecto a una tarjeta de crédito o débito se justifica por la suposición de que las transacciones son usualmente de bajo valor. La mayor seguridad y control del fraude en transacciones bancarias suelen ser proporcionados por tratarse de sistemas cerrados y el soporte de un back-end.

1.3. Tarjetas inteligentes sin contacto

Las tarjetas sin contacto (o de proximidad) permiten el intercambio de información estando ubicadas cerca de un lector a una distancia no superior a 10 centímetros. Dicho intercambio se realiza mediante ondas de radiofrecuencia. Para ello tanto la tarjeta como el lector cuentan con una antena interna. El mecanismo se denomina genéricamente *Identificación por Radiofrecuencia* o RFID.

Los sistemas de cobro basados en TISC suelen denominarse AFC por sus siglas en inglés: *Automatic Fare Collection*.

Mifare © es la tecnología de tarjetas inteligentes sin contacto (TISC) más ampliamente instalada en el mundo con aproximadamente un billón de TISC y 1.5 millones de módulos lec-

[7] [MMH09]

tores vendidos. Esta tecnología cumple con las 3 primeras partes de la norma ISO 14443 Tipo A de 13.65 MHz. La distancia típica de lectura es de 10 cm (unas 4 pulgadas). La distancia de lectura depende de la potencia del módulo lector, existiendo lectores de mayor y menor alcance. La tecnología Mifare es propiedad de Philips Austria Gmbh. La tecnología es económica y rápida, razón por la cual es la más usada a nivel mundial.

Las tarjetas inteligentes sin contacto suponen numerosas ventajas por sobre otros sistemas de cobro[8], como ser:

- ◇ Durabilidad
- ◇ Posibilidad de Recarga
- ◇ Múltiples aplicaciones en una sola tarjeta
- ◇ Bajo costo de mantenimiento
- ◇ Número de serie único
- ◇ Posibilidad de uso en ambientes y climas adversos
- ◇ Cifrado del contenido

Las aplicaciones de las TISC no se limitan al transporte público, sino que también son usados en diferentes campos desde el control vehícular o el acceso a eventos (ver figuras: 1.4; 1.5 y 1.6).

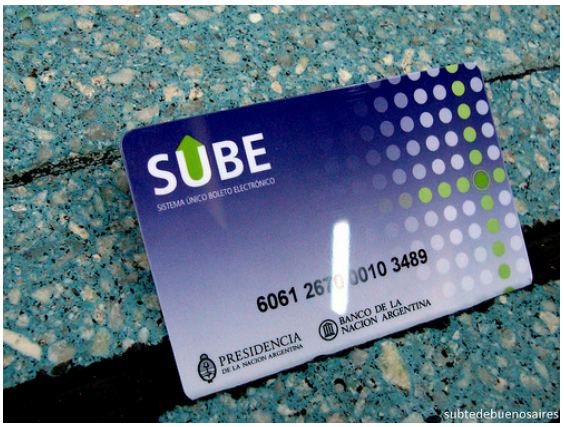

Figura 1.4: Transporte público

1.3.1. Mapping

Las TISC en general poseen una estructura de memoria (la mayoría entre 1Kb y 4Kb) que se encuentran segmentados para su acceso de lectura o escritura de manera similar a como se segmenta y direcciona una memoria RAM.

[8] [Net11]

Figura 1.5: Entrada a un concierto

Figura 1.6: Entrada a un Evento Deportivo

En particular, la tarjeta Mifare Classic es básicamente un chip de memoria segura con capacidad de comunicación inalámbrica (ver Fig. 1.7). La memoria de la tarjeta está dividida en sectores, cada uno de ellos se divide en bloques de 16 bytes cada uno. El último bloque de cada sector es el trailer del sector y contiene dos claves secretas y las condiciones de acceso para ese sector.

Para llevar a cabo una operación en un bloque específico, el lector debe autenticarse para el sector que contiene ese bloque. Las condiciones de acceso determinan cuál de las dos claves debe de ser utilizada. En la Figura 1.8 se puede apreciar un diagrama de la memoria de una Mifare Classic.[9]

Una de las propiedades del protocolo de autenticación de tres vías es que esta diseñado para resistir ataques de fuerza bruta[10] dado que no brinda indicios acerca de si la clave es correcta hasta tanto no haga una operación:

> Podemos observar que este protocolo dificulta los ataques a las tarjetas, si bien no los hace totalmente imposibles. Esto incluye los ataques de fuerza bruta ¿Cómo es esto posible? Vemos que la tarjeta nunca contesta todo lo que tiene que ver con la clave secreta antes que realmente el terminal pruebe el conocimiento de esta clave secreta con un criptograma de 8 bytes elegido libremente por el lector. La probabilidad de que un lector falso puede

[9] [GvRVS09a]
[10] [Cou09]

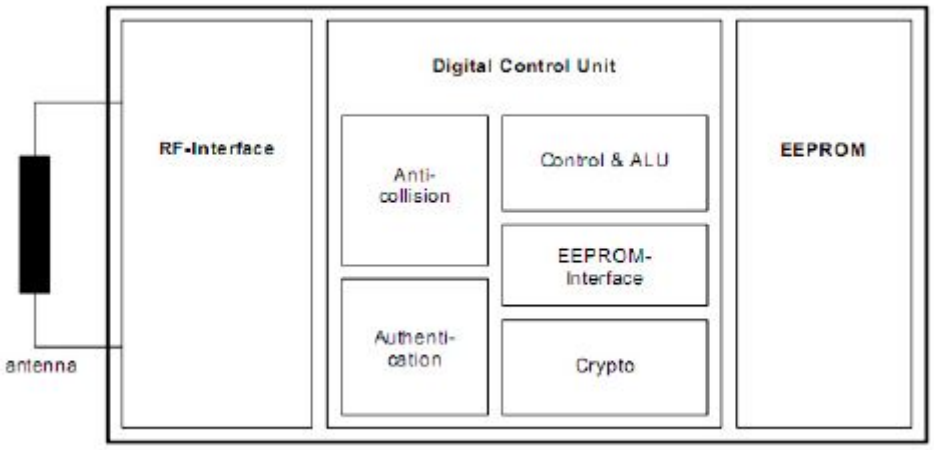

Figura 1.7: Diagrama de Bloques Mifare[CDT09]

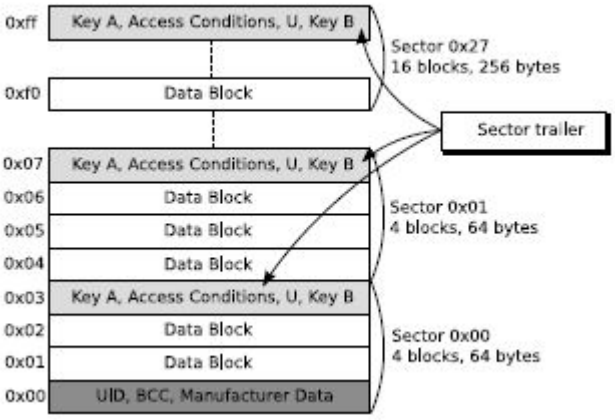

Figura 1.8: Memoria Mifare Classic 4K

producir una respuesta válida es de 2^{32}. Esto brinda una protección contra ataques de fuerza bruta: incluso si el atacante adivina la clave, para confirmar esta clave (o rechazar una clave equivocada) necesita consultar la tarjeta al menos una vez. Cada consulta permite rechazar 2^{48-32} claves para las que este criptograma de 8 bytes sea válido. Para llevar a cabo un ataque de fuerza bruta se necesitan entonces unos unos 2^{47} cálculos y alrededor de 2^{32} consultas a la tarjeta. Teniendo en cuenta que cada transacción con la tarjeta dura unos 0,5 s. el ataque de fuerza bruta requeriría unos 93 años. *Por ello el ataque de fuerza bruta no es factible*.

La estructura interna de la memoria (denominada mapping) suele definir una porción de memoria que contendrá información relacionada con el saldo de carga remanente para viajes. Este saldo se suele almacenar en lo que se denomina monedero electrónico o e-purse.

Las diversas implementaciones incluyen también datos de titularidad, contadores de movimientos (o transacciones), de viajes realizados y aplicaciones más complejas como combinaciones de medios de transporte o el control de entradas y salidas de un bus o un tren

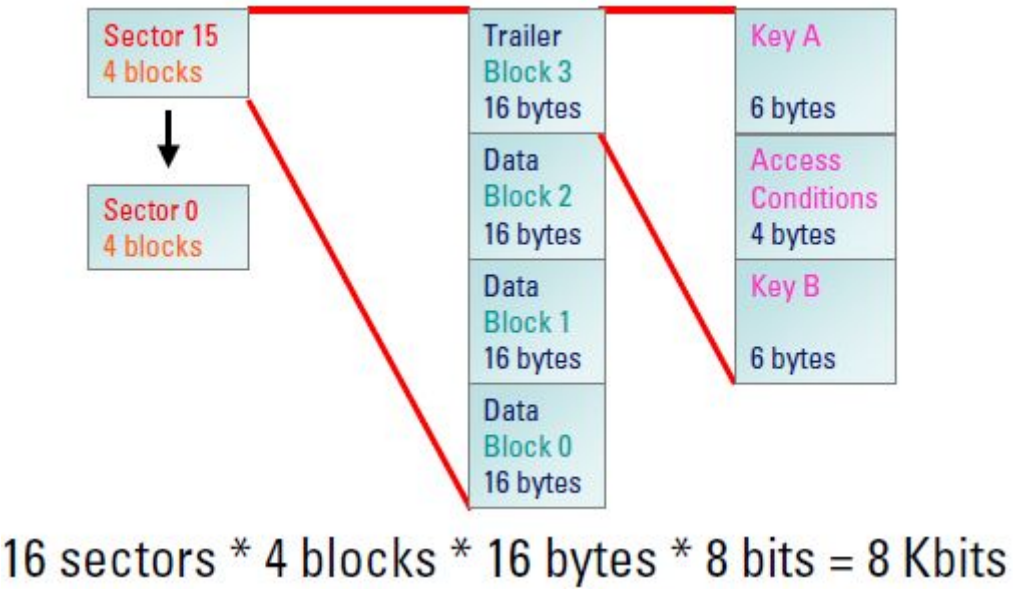

Figura 1.9: Estructura de datos en Mifare 1K (Gemalto Datasheet)

(check-in / check-out).

El mapping suele ser un elemento confidencial de las implementaciones, pues su conocimiento ofrecería, a un posible atacante, información valiosa para focalizar y aprovechar las debilidades expuestas en la sección 2 de página 12 del presente trabajo.

El concepto de monedero electrónico o e-purse es la capacidad de contar, dentro de un mapping, con un registro de tipo numérico que proporcione información del saldo cargado en dicha tarjeta.

Capítulo 2

Potenciales Fraudes en TISC

2.1. Tipos de Fraudes en TISC

De los tres tipos de fraudes genéricos mencionados en el capítulo anterior, se desarrollan a continuación su posible aplicación en el contexto de las Tarjetas Inteligentes sin Contacto, en especial de las tarjetas Mifare Classic, pero que potencialmente podrían trasladarse a diferentes tecnologías de TISC:

2.1.1. Falsificación de TISC

Como se mencionaba anteriormente, este fraude consiste básicamente en la duplicación de un dispositivo. En una TISC, esto implicaría la posibilidad de duplicar una tarjeta válida en otra tarjeta que no lo sea, respetando todas las funcionalidades de la misma para poder ser utilizadas en un sistema de cobro y que esto sea aceptado por dicho dispositivo. Si bien las TISC almacenan la información de manera cifrada[1], numerosos trabajos de investigación han desarrollado la factible falsificación de tarjetas mediante el acceso a las claves de cifrado.

Entre las investigaciones más detacadas en la materia podemos encontrar los trabajos *Practical Attacks on the MIFARE Classic* (de Wee Hon Tan [Tan09]), y *Wirelessly Pickpocketing a Mifare Classic Card* (de Garcia, F. D.; van Rossum, P.; Verdult, R. Schreur, R. W. [GvRVS09a]) donde desarrollan, por diversos métodos, la factibilidad de ataques sobre el cifrado aplicado en las tarjetas MIFARE Classic.

2.1.2. Modificación de la carga en TISC

En su trabajo de Septiembre de 2009[2] Wee Hon Tan formuló el desarrollo de un ataque práctico sobre la Oyster Card, esto es, el billete electrónico utilizado en el servicio de transporte público en Londres. Se trata de una tarjeta del tamaño de las de crédito, sin contacto, con el valor de carga almacenado en la tarjeta. Tiene dos modalidades de uso, cuando los pasajeros entran o salen del sistema de transporte, deben pasar sus tarjetas por los lectores para deducir los fondos (viaje por tramos) o se puede también validar el viaje de una sola vez. El valor de la tarjeta se puede aumentar o recargar en persona, por operación bancaria o por compra en línea. El importe máximo del crédito que se puede almacenar es de £ 90.

En dicho trabajo, lograron los siguientes resultados[3]:

> La estructura de datos de los diferentes tipos de tarjetas Oyster son exactamente los mismos. Con excepción de la agrupación de los bloques a nivel sectorial, hay más subgrupos lógicos que corresponden a sus funciones. Los bloques importantes son los bloques de *crédito*, los bloques de datos *Travelcard*, y los bloques del historial de transacción. Si se modificasen correctamente estos dos primeros, se puede viajar de forma gratuita, mientras que el último permite divulgar datos privados como información histórica del dueño de la tarjeta.

[1] [Net11][CDT09]
[2] [Tan09]
[3] [Tan09]

Es decir, en su investigación, lograron interpretar (a medida que fueron haciendo cambios en la misma) el *mapping* de la tarjeta (ver Figura 2.1). Como se dijo anteriormente (1.3.1 pág. 8), esta información es valiosa y debe ser protegida por el operador del sistema, ya que muestra aquellos puntos de interés para un atacante, como puede ser el e-purse, por sobre otros que sean menos significativos.

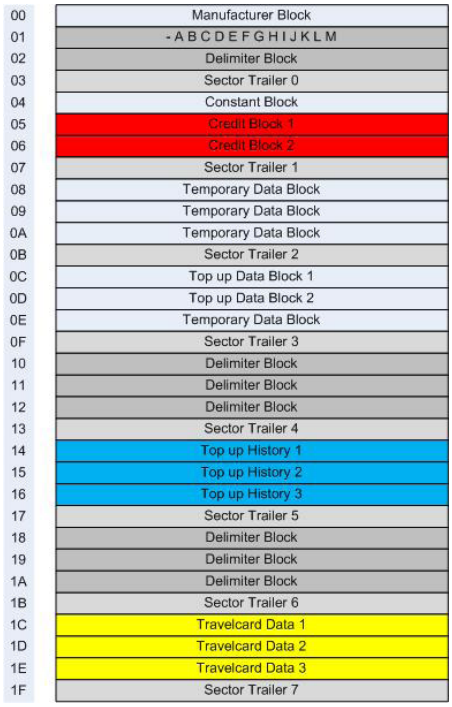

Figura 2.1: Mapping Oyster interpretado en la investigación de Wee Hon Tan

A su vez, en dicho trabajo se intentó vulnerar una tarjeta combinada denominada Barclaycard OnePulse [4] la cual sirve simultáneamente como tarjeta para viajes compatible con Oyster Card, tarjeta para micropagos y tarjeta de crédito. En este caso, el resultado no fue exitoso ya que la misma no era vulnerable a los ataques practicados. En el avance del trabajo, se podrán entender algunos de los motivos por el cual esta tarjeta no pudo ser vulnerada.

2.1.3. Emulación de una TISC

El trabajo de Wee Hon Tan[5] desarrolla un ataque práctico sobre un sistema de acceso Universitario donde indican:

> Hemos probado con éxito nuestro ataque en varios lectores de todo el campus de South Kensington, y se puede entrar en cualquier puerta utilizando nuestra tarjeta emulada como si tuviéramos la tarjeta auténtica.

Si bien para el caso de transporte este tipo de validación no es la misma implementada en los sistemas de transporte (recordemos la necesidad de contar con un mapping especifico

[4] http://ask.barclays.co.uk/help/loans_credit/onepulse
[5] [Tan09]

y un e-purse para el control del valor de la tarjeta), sirve como evidencia de la facilidad con la que se puede simular una TISC, lo que exige algunos controles adicionales a la hora de establecerlos como elemento integrante de un sistema de control de acceso o barrera de entrada. También en los trabajos de García y otros[dKHG08] se desarrollan ataques similares.

2.1.4. Metodología de los ataques

Para los casos descriptos anteriormente, los investigadores utilizaron mayormente una técnica de *sniffing*, es decir, interceptando la comunicación entre un lector válido y una tarjeta genuina. La recuperación de las claves se realizó de manera *offline* una vez capturado dicho tráfico. Para realizar esto, existen numerosos dispositivos y librerías de dominio público como el lector *Proxmark 3* [6] que es mostrado en la Figura 2.2 (pág. 15) el cual no sólo permite la lectura de tarjetas, sino también emular las mismas.

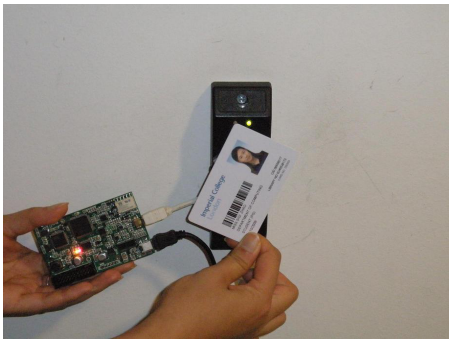

Figura 2.2: Proxmark 3 haciendo sniffing en la investigación de Wee Hon Tan

También De Gans Koning [dKGHG08] propuso un ataque a una Mifare Classic que explota la maleabilidad del cifrado CRYPTO-1 para leer información parcial de una etiqueta, sin conocer siquiera el algoritmo de cifrado. Por otra parte, a través de cortes microscópicos del Chip Mifare, Nohl [NEP08] y Courtois [CNO08] indicaron que el cifrado CRYPTO-1 es susceptible a los ataques algebraicos y Nohl demostró también en ellos una debilidad estadística del cifrado.

Una descripción completa del cifrado fue dado por el trabajo de [GvRVS09a] a través de ingeniería inversa al protocolo de autenticación. También describen un ataque con la que un atacante puede recuperar una clave del sector por comunicarse con un lector genuino o por escuchas ilegales de una autenticación exitosa.

Todos los ataques descriptos en estos documentos tienen en común que necesitan acceso a un conjunto lector / tarjeta legítimo y trabajan en base a la intercepción de la comunicación.

[6] http://cq.cx/proxmark3.pl

2.1.5. En resumen

A partir de todos estos trabajos, NXP Semiconductors (Fabricante de las TISC Mifare Classic) resumió [7] los ataques realizados por los distintos investigadores de la siguiente forma:

- ◇ Espionaje de la comunicación entre una tarjeta legítima y un lector legítimo.
- ◇ Espionaje e interferencia en la comunicación entre una tarjeta legítima y un lector legítimo con la interferencia en campo de la radiocomunicación a fin de que la misma no se complete.
- ◇ Lectura o modificación del contenido de una tarjeta legítima con un ataque de dispositivo.
- ◇ Reproducción de la información espiada entre una tarjeta legítima y un lector legítimo. Una transacción válida es repetida maliciosamente entre una tarjeta y un emulador de lector válido o entre una tarjeta válida y un lector fraudulento.
- ◇ Presentación de un UID clonado de una tarjeta legítima o de una falsa UID hacia un lector legítimo.
- ◇ Clonación de una tarjeta: Se copia el contenido de una tarjeta legítimo a una tarjeta en blanco. Para obtener una tarjeta en blanco, puede que no sea posible establecer un UID dedicado.
- ◇ Emulador de Tarjeta: El contenido de una tarjeta legítima se pueden copiar en un emulador de tarjetas. Un emulador de tarjetas es capaz de emular una tarjeta legítima, incluido el UID y simula el comportamiento de una tarjeta legítima. El atacante tiene control total sobre el software que se ejecuta en el emulador y, en particular, es capaz de restaurar un contenido anterior (memoria de la imagen) en cualquier momento.

2.2. Riesgos

Los ataques mencionados deberían ser parte de un análisis de riesgo lógico para cualquier sistema de transporte basado en TISC. A continuación se expone un acercamiento de dicho tipo de análisis. El mismo no se supone abarcativo de todos los riesgos asociados al sistema, sino simplemente un ensayo teórico de aquellas vulnerabilidades que deben tenerse en cuenta para su implementación como validación en un sistema de tarifado de transporte público.

Se entiende por *riesgo*[8] la relación de la probabilidad de sucesos futuros inciertos. En los sistemas de información, los riesgos de seguridad se definen como “la posibilidad de que una amenaza concreta se aproveche de las vulnerabilidades de un activo o grupo de activos y por lo tanto cause daño a la organización”

[7] [NXP08]

[8] http://en.wikipedia.org/wiki/Risk

De lo analizado hasta el momento, se pueden diferenciar dos tipos de amenazas: a la tarjeta y al sistema.

El fabricante también catalogó los tipos de amenazas que existen hoy en el uso de las tarjetas Mifare Classic[9]:

Suplantación de identidad: Esto ocurre cuando un atacante se hace pasar por un usuario autorizado del sistema y es capaz de obtener acceso a algunos servicios, por ejemplo, acceso no autorizado a un edificio, un viaje gratis a expensas del transporte público empresa o por cuenta de un usuario inocente. En este modelo, la amenaza de suplantación de los derechos cubre varias amenazas que tienen diferentes niveles de gravedad dependiendo de la aplicación. Obtener acceso no autorizado a una instalación nuclear es mucho más grave que obtener un único viaje gratis en transporte público.

Alteración de contenido de la tarjeta: Un atacante modifica, añade, elimina o reordena datos en una tarjeta para, por ejemplo, cambiar el producto de viajes en una tarjeta (de un solo viaje a una suscripción con validez anual), o revertir los datos a un valor que era anterior (ataque de retroceso o *roll back*).

La divulgación de información: el contenido de la tarjeta es leída por una persona no autorizada. Para ello, o bien el atacante obtiene acceso al contenido de la tarjeta mediante un lector fraudulento o bien el contenido de la tarjeta es espiado durante la comunicación entre un lector y la tarjeta sin el conocimiento del dueño de la tarjeta. Esto puede infringir la privacidad de la información del propietario de la tarjeta, por ejemplo, si el nombre y / o la dirección está almacenada en una tarjeta y esta puede ser leída por una persona no autorizada.

Denegación de servicio: La denegación de servicio se produce cuando una tarjeta válida no puede funcionar adecuadamente para prestar el servicio previsto, por ejemplo, listas negras con una tarjeta legítima, bloqueo de una tarjeta etcétera. Al dueño de la tarjeta (en principio válida) no sólo se le estaría negando acceso al servicio, sino que potencialmente podría perder el dinero de la carga efectuada, así como la confianza en el sistema.

[9] AN155010[NXP08]

Capítulo 3

Mitigaciones

3.1. Algunas medidas

Como se pudo apreciar en la sección 2, son diversas las maneras de atacar un sistema basado en tarjetas sin contacto. Sin embargo, a lo largo de la presente sección, se podrán apreciar también que son varias las medidas que puede tomar el órgano administrador del sistema para contrarrestarlas.

Entre ellas podemos destacar las que se exponen a continuación [1]:

3.1.1. Referidas a la Tarjeta

De las medidas que pueden tomarse referidas a la tarjeta, en particular se pueden resaltar, por su eficacia respecto a los ataques descriptos, la diversificación de claves y el cifrado de datos adicional:

Diversificación de Claves

Esta medida, significa basicamente que cada tarjeta posee claves de acceso específicas para dicha tarjeta. El origen de esta contramedida se origina, según las distintas investigaciones, en los diversos sistemas donde se implementó una única clave de acceso a los sectores del mapping en la totalidad de las tarjetas del sistema. Esta clave simétrica (compartida entre las tarjetas y los lectores) de ser potencialmente descubierta por un atacante, permitiría el acceso a todas las tarjetas del sistema.

Uso de la misma clave en todas las tarjetas Planteemos la posibilidad de la existencia de un Sistema de Boleto Electrónico donde todas las claves en todas las tarjetas son idénticas, aún cuando no sea una única clave para todos los sectores, sino que se hayan definido varias claves para las tarjetas (un *keyset*), pero ese mismo conjunto de claves está en *todas* las tarjetas. Para dicho supuesto, NXP[2] plantea la siguiente situación:

> Imaginemos ahora una organización delictiva que invirtió una cantidad considerable de tiempo y dinero para alterar el diseño del chip con el fin de conseguir *una* clave de un chip en una tarjeta válida para el sistema e imagine, aún siendo poco probable, que tenga éxito. Con dicha clave pueden leer el contenido del chip en la tarjeta. Y con la clave y el contenido de la tarjeta, puede poner esta información en las tarjetas en blanco y venderlas en las calles. Para el sistema, las tarjetas en blanco se verán de la misma que la tarjeta original y la gente podría viajar con ellas. La única diferencia es el UID, pero a menos que el sistema este diseñado para trabajar con listas blancas, lo cual no es práctico para los sistemas con muchas tarjetas, el sistema no tiene manera de saber que es el UID de una tarjeta que no es parte de el sistema. Como alternativa, los hackers podrían publicar en Internet el software y la clave

[1] Algunas de estas son destacados por Wee Hon Tan y García y otros en sus trabajos[Tan09] [GvRVS09a] así como también NXP en AN155010[NXP08] recoge algunos de ellos.

[2] [NS10]

para que todo aquel que tenga un lector (que puede obtenerse por menos de 25 dolares) pueda actualizar el saldo de sus tarjetas propias.

Por ello, con la diversificación de claves se logra una mayor seguridad para el *keyset* de claves, dado que, aún si mediante algún ataque las claves de una tarjeta se descubran, dicho hallazgo no implicará que se hayan descifrado las claves del resto de las tarjetas del sistema.

La implementación de la diversificación de claves también evita el clonado de una tarjeta legítima a otra tarjeta legítima que tengan una UID diferente, ya que para el clonado de una tarjeta con claves diversificadas, el UID y sus correspondientes claves deben ser duplicadas.

El principio de diversificación clave es, básicamente, que *no hay dos tarjetas que posean la misma clave o conjunto de claves*. Cada tarjeta tiene un UID y esto se puede utilizar para determinar la clave o el conjunto de claves a utilizar. En la figura 3.1 podemos observar el esquema de como se compone la clave diversificada a partir de una clave maestra o Master Key (que en dicho esquema se encuentra almacenada en un módulo SAM) y otros elementos como pueden ser el UID de la tarjeta, la posición de la clave y algún otro dato (por ejemplo la versión de la clave utilizada).

Cabe destacar que la diversificación de claves no evita una potencial clonación de una tarjeta válida con un *emulador de tarjetas* ver 2.1.3 pág. 14 ya que en ese caso el UID se podría simular y por ende duplicar.

La implementación de una diversificación de claves generalmente está asociada a la implementación de Módulos de Seguridad o módulos SAM por sus siglas en inglés *Security Acces Module*, los cuales pueden contener ciertas claves maestras y *derivar* las mismas a la TISC en base al UID o algún otro elemento del mapping. En su cartera de productos, Mifare cuenta con tarjetas de mayor nivel de seguridad que se basa en este tipo de SAM.

> El terminal tiene una clave maestra (puede estar alojada en un SAM). Junto con el UID y otros datos concatenados se realiza un cifrado y el resultado es la clave diversificada. Hay varias formas de criptografía para hacer la operación de diversificación de clave.(...) Incluso si su sistema no tiene implementados SAM por el momento, puede ser beneficioso utilizar el mismo algoritmo que utiliza el SAM, ya que este algoritmo se ha verificado criptográficamente y permite la introducción de SAM más tarde sin tener que cambiar las claves de la tarjeta. Si cada tarjeta tiene un conjunto de claves (que consiste en varias claves para múltiples propósitos), el proceso en la figura 3.1 se realiza para cada una de las claves en el conjunto de claves (excepto por ejemplo, una clave para recuperar el UID). La clave resultante o el conjunto de claves se graba inicialmente en las tarjetas durante la etapa de personalización, después de haber leído el UID de la tarjeta. Es decir, el terminal lee el UID y luego calcula la clave diversificada o el conjunto de claves que necesita para la operación y a continuación, esta clave o conjunto de claves se utilizan para establecer la comunicación segura a la tarjeta [3].

[3] [NS10]

Figura 3.1: Principios de la diversificación de claves

Cifrado de datos adicional

Dadas las vulnerabilidades y debilidades descriptas en el cifrado CRYPTO-1 (ver punto 2.1 en pág. 13), un *workaround* que permita incrementar la confidencialidad de los datos almacenados en la TISC, consisten en utilizar un esquema de cifrado adicional en los lectores, que sea suficientemente robusto y permita así independizar el cifrado propio de Mifare con el cifrado del mapping. Esta acumulación de cifrados, que pueden ser algoritmos estándar como 3DES o AES, pueden incluso ser cifrados por el lector con llaves diversificadas de manera independiente de las claves propias de la tarjeta. En este caso, diversificando las claves por tarjeta y por solicitud se mejora sustancialmente la confidencialidad de los datos intercambiados entre el lector y la tarjeta.

Si bien esta medida parece ser altamente efectiva, un elemento no menor a tener en cuenta en su implementación es el incremento del tiempo de cálculo asociado al procesamiento de cada solicitud, en especial en los equipos de campo que suelen ser instalados en los medios de transporte, los cuales suelen ser deficitarios en los que respecta a su capacidad de procesamiento.

Por ello, este tipo de medidas debe ser debidamente mesurada ya que una inadecuada implementación de algoritmos que superen en pocos mili segundos una transacción de viaje o carga, atentaría a la dinámica necesaria para su implementación como medio de pago, tal cual se indicó en el punto 1.2.4 de la página 6.

Firmar los datos a partir del UID

Para implementar esta mitigación, lo que debe hacer el lector es calcular una o más firmas criptográficas fuertes en una combinación de los datos almacenados en la tarjeta (por ejemplo el e-purse o el contador de transacciones) y el UID. Estas firmas se pueden almacenar en otros sectores de la tarjeta. Por lo tanto, los datos clave de la tarjeta estarán asociadas a la tarjeta a través de la UID. Las firmas pueden ser, por ejemplo, un valor hash con una clave simétrica.

El lector verificará las firmas para constatar la integridad de la información y su unión con el UID. Este procedimiento de control evitará la aparición de tarjetas clonadas en tanto tengan un UID diferente puesto que dicha firma será incorrecta y por lo tanto rechazada por el lector. Esta medida es efectiva no sólo para repeler intentos que impliquen la modificación del e-purse, sino también para contrarrestar alguna modificación maliciosa del contenido de la tarjeta para descontar viajes realizados o la modalidad de viajes con que esté cargada la misma. Sin embargo, esta medida no impediría la utilización de un emulador que simule un UID correcto al haber clonado una tarjeta así como tampoco impedirá la restauración de un contenido anterior en la misma tarjeta con la firma válida al momento del backup.

Arquitectura del Mapping

A continuación se resumen algunas medidas adicionales que pueden tomarse relacionadas al armado del mapping de la tarjeta:

Utilizar diferentes bloques para realizar la autenticación de una tarjeta válida. Ello obligaría al potencial atacante atacante a obtener acceso a los 16 sectores de la tarjeta.

No utilizar valores por defecto. El uso de valores por defecto provee una puerta de entrada al atacante para comunicarse con la tarjeta. Es una buena practica cambiar dichas claves y no dejar valores por defecto en ninguno de ellos, aún cuando no sean utilizados en el mapping.

No dejar bloques en blanco, De la misma manera que el punto anterior, no deben dejarse claves sin especificar, aún cuando no todos los sectores sean parte del mapping.

Revocación de Tarjetas Un número de tarjeta puede ser revocada por un lector cuando se la identifica como fraudulenta. El lector puede escribir datos en la tarjeta que indica que ha sido revocada. La revocación de la tarjeta no requiere la propagación de una lista negra a los lectores fuera de línea. Por ejemplo, una tarjeta MIFARE Classic puede ser revocada mediante el establecimiento de la aplicación de ciertos bits para condicionar el acceso a todos los sectores, deshabilitando la lectura o escritura de datos a ese sector de aplicaciones.[4]

Implementar contadores dobles La implementación de un doble contador de transacciones que disminuyan progresivamente, pueden ser implementados realizan a través de formas diferentes: dos números de transacción dedicados a la auditabilidad de las transacciones:

Contador 1 como un campo de valor: Activado después de la inicialización y que sólo funcione a través de operaciones de decremento[5]. Este contador está protegido con la

[4] Esta medida es eficaz para una tarjeta clonada, pero no para una tarjeta emulada. La información que indique la revocación podría ser removida de la tarjeta de emulador.

[5] El contador es decremental en lugar de incremental, porque las condiciones de acceso pueden configurarse de manera que sólo se permite disminuir un campo de valor.

misma clave que los datos (por ejemplo, el de tarifas). El contador se decrementa antes de que el saldo de nueva tarifa sea escrito, pero después de la autenticación, de modo que si un atacante trata de eliminar el decremento del contador, la escritura del nuevo saldo no se mantendrá integra.

Contador 2 como un campo de datos: Esta medida dificulta los ataques de repetición. Por ejemplo, el lector puede rechazar la tarjeta si los contadores no están iguales.

Evitar cifrar textos conocidos Para efectuar un ataque de las claves criptográficas, un atacante necesita una combinación de *texto cifrado* / *texto plano*. Para evitar esto, el lector debe cifrar sólo los datos que se desconocen o no puedan ser adivinados. Esta medida restringe la extracción de texto cifrado a partir de texto plano y dificulta el descubrimiento de claves.

Comprobar el UID de la tarjeta El lector puede verificar que el UID utilizado durante la secuencia de anti-colisión sea idéntico al UID almacenado en la tarjeta. Se puede suponer que si hay una discrepancia la tarjeta fue manipulada y en este caso, el lector puede decidir bloquear la tarjeta agregandola a la lista negra o gris, o bien proceder a la revocación de la tarjeta.

Mantenimiento del estado de entradas y salidas en la tarjeta Para las tarjetas utilizadas en sistemas que utilizan estados de entrada y salida (por ejemplo trenes con check-in / check-out), se puede implementar que el usuario de la tarjeta no pueda entrar en una infraestructura antes de salir de ella. Esta medida hace más difícil el ataque, pues obliga a rastrear vestigios de múltiples transacciones y no de sólo una.

Rotación de claves Las claves de una tarjeta pueden actualizarse después de un cierto número de transacciones. El cambio de las claves puede hacerse periódicamente como política de seguridad o después de cada transacción, por ejemplo, para evitar ataques de repetición. La actualización de la clave al final de una transacción protege contra un ataque de repetición ya que intentaría usar la clave de sesión caducada.[6] Sin embargo, este mecanismo sólo pueden aplicarse en un ambiente controlado donde la tarjeta no pueda ser sacada del campo de radiofrecuencia del lector antes de la finalización de la actualización de claves. El *apagado* de la tarjeta durante la escritura de las claves puede resultar en el almacenamiento de un valor indeterminado, lo que hará que la memoria quede con una clave inaccesible. Un buen ejemplo de un ambiente controlado para actualizar las claves es un lector que retenga físicamente la tarjeta, mientras la escribe y la libere recién cuando la actualización se llevó a cabo. Estos dispositivos no suelen ser utilizados en transporte debido a la rapidez que se necesita para transaccionar.[7]

Poner los datos de autenticación en la primera sección. Algunos datos de identificación de la tarjeta se pueden añadir al primer sector o archivo al que se accede por el lector. Por

[6] Esta técnica no impide la clonación de una tarjeta con la consistencia de los datos y claves.

[7] Ver caracterísitcas Mifare Plus del siguiente punto.

ejemplo, esto podría ser una versión cifrada de la UID. Un lector puede detectar una tarjeta clonada por la discrepancia entre el UID y esta información de autenticación adicional. La discrepancia se produce cuando los datos de autenticación se copian en una tarjeta clonada con un UID diferente de la tarjeta original. Tan pronto como un lector detecte una tarjeta maliciosa, debe dejar de leer el resto de los datos para evitar la exposición de texto cifrado y su combinación de texto plano conocido o adivinable.

3.1.2. Referidas al sistema en general:

De las medidas que pueden tomarse referidas al sistema de administración, la cuadratura del sistema es aquella que, combinada con el manejo de listas negras (tarjetas bloqueadas) resulta de mayor efectividad. Cabe destacar que en general, todos estos controles son detectivos y correctivos pero difícilmente preventivos, es decir, pueden protegernos para detener un fraude en progreso pero difícilmente evitarlo.

Cuadratura del Sistema

La inclusión de un número de transacción en cada operación realizada nos permite efectuar lo que se denomina Cuadratura del sistema. Esta solución implica el agregado a la tarjeta de un número que pueda ser trazado y seguido por el sistema backend. En general, el número de transacciones autenticadas se implementa en la tarjeta y se disminuye antes de realizar cualquier operación con su contenido. Este número, junto con el UID de la tarjeta y una marca de tiempo y dispositivo se debe comunicar al servidor. Paralelamente, para cada UID, el back-end registrará las transacciones y las marcas de tiempo haciendo así más difícil el uso de tarjetas clonadas y ataques de reversión ya que el sistema de back-end pueden detectar una tarjeta fraudulenta en los dos casos siguientes:

Discrepancia en las transacciones: Cuando para un UID el número de transacción recibido es igual o mayor que el número de transacción que ha sido registrado por el sistema de back-end, ya que esto implicaría (al ser decremental) que se aplicó una tarjeta con una preimagen.

Discrepancia en el tiempo Cuando se realiza una transacción en un momento en que no es secuencial en el tiempo (fuera de de la ventana de tolerancia del reloj) y genera una discrepancia entre el número de transacción esperado y el recibido.

Discrepancia en el Saldo Si dentro de la transacción el sistema backend recibe también información relativa al saldo, se puede implementar un control de saldos acumulados en el backend y contrastarlo contra los saldos leídos en las tarjetas. De haber discrepancias entre ambos saldos implicaría que hubo un uso de preimagen o bien que fue modificado el saldo de manera fraudulenta.

En cualquiera de estos casos, el servidor puede decidir añadir el UID de la lista negra o gris y/o eliminarlo de la lista blanca para desactivar futuras transacciones.

Implementación de Listas

La infraestructura puede tener una o varias listas de tarjetas y para ello puede utilizarse el UID para identificar las mismas.

Por ejemplo, puede tener una Lista Blanca que corresponda a aquellas tarjetas legítimas, de manera tal que solo aceptará, ya sea en los dispositivos de entrada o en el procesamiento del backend, las tarjetas que pertenezcan a la lista blanca. Una tarjeta fraudulenta debería emular un UID válido para comunicarse con la infraestructura.

También puede tener una lista de tarjetas sospechosas de haber sido manipuladas pero que no se tenga la certeza de que se haya cometido fraude con ellas. Esa lista suele denominarse Lista Gris.

Para rechazar una tarjeta fraudulenta por la infraestructura después de comprobar que fue manipulada se utiliza la Lista Negra. Esta lista negra debe ser remitida a los lectores. Su actualización periódica es más fácil de implementar con los lectores en línea que fuera de línea. Sin embargo, para estos últimos también es factible dicha implementación. Por ejemplo, un lector, ante la detección de una tarjeta fraudulenta, podría proceder a escribir una indicación con una firma en esa tarjeta. El siguiente lector, al momento de identificar la tarjeta, de leer esta indicación, verifica la firma y actualiza su lista negra.

Estas medidas no son totalmente efectivas ante la clonación de una tarjeta válida a un emulador de tarjetas siendo que en este caso el UID se pueden copiar.

Otras medidas:

Adicionalmente, podemos resumir algunas medidas relacionadas al sistema en general:

Comprobar el factor de autenticación en forma física El factor de verificación física incrementa la seguridad. Por ejemplo, los controladores en un tren o en un autobús o guardias de las puertas de control de acceso pueden comprobar el factor de forma física para detectar un emulador de dispositivos. [8]

Leer los datos una vez escritos El lector puede leer y verificar los datos después de que se ha escrito en la tarjeta. Esta contramedida permite detectar un ataque donde el atacante intercepte el comando de escritura y manipule un reconocimiento y respuesta simulada.

Detección de errores de autenticación El lector puede establecer un sistema de detección de las tarjetas fraudulentas cuando falle la autenticación cierto número de veces. En este

[8] Esta medida impide el uso de emuladores pero no impide las tarjetas fraudulentas que tengan la misma forma física como una tarjeta legítima.

caso, el lector puede decidir bloquear la tarjeta agregándola a la lista negra o gris, o bien proceder a la revocación de la tarjeta.

Mantener el estado de entradas y salidas en la infraestructura Para las tarjetas utilizadas en sistemas que utilizan estados de entrada y salida (por ejemplo trenes con check-in / check-out), se puede implementar que el usuario de la tarjeta no pueda entrar en una infraestructura antes de salir de ella. Para implementar estos niveles a nivel sistema central, los lectores del sistema deben estar siempre en línea. Puede ser complementario a las medidas vistas en la seguridad de la tarjeta.

Detección de una tarjeta en la oficina de back-end Una firma (por ejemplo, una firma hash de la UID más relleno posible) se puede almacenar en la tarjeta. La firma se utiliza para verificar si una tarjeta es original o una copia. Esta verificación se puede hacer por el sistema de back-end o de un ambiente controlado y similares. La clave de acceso de lectura a esta firma se diversifica por tarjeta y la clave maestra utilizada para la diversificación de claves sólo está disponible por el sistema de back-end o en otros ambientes controlados sin que la firma sea accesible desde un lector público. Esta contramedida hace más difícil clonar una tarjeta totalmente por el espionaje de la comunicación entre un lector y una tarjeta en un entorno público.

3.2. Evolución de las TISC

NXP, el mayor fabricante de TISC, ha tomado nota de todas estas situaciones y reaccionó sacando al mercado en 2009 la tarjeta Mifare Plus, como la tarjeta sucesora de la TISC Mifare Classic.

> Desde el principio (de la investigación) hemos comunicado al fabricante de NXP estas vulnerabilidades. Dado que el protocolo se implementa en hardware, no prevemos ninguna contramedida definitiva con estos ataques que no requieran sustitución de toda la infraestructura. Sin embargo, NXP está actualmente desarrollando un producto compatible con Mifare Classic, el *Mifare Plus*.[9]

Entre sus virtudes[10] se destacan algunas de las mitigaciones que se nombraron en el punto anterior, pues ofrece:

> Las tarjetas MIFARE Plus soportan una pre-personalización y 3 niveles de seguridad. Son capaces de operar en un determinado nivel de seguridad y sólo evolucionar hacia un nivel superior. Disponen de un mecanismo automático de *anti-rotura* para asegurar la implementación de claves rotativas, es decir, si una tarjeta se quita del campo durante una actualización de clave, o bien concluye la actualización, o automáticamente retoma la clave anterior.

[9] [GvRVS09a]

[10] http://www.nxp.com/documents/leaflet/75016722.pdf

Una de las ventajas a nivel seguridad es que las tarjetas han logrado un nivel EAL4+ en la Certificación del Common Criteria[11].

Pero el beneficio fundamental de esta tarjeta, es su compatibilidad con la infraestructura existente, pues las claves pueden seguir siendo almacenadas con el cifrado de MIFARE Clássic (CRYPTO-1) o como claves AES (2 x 128 bits por sector).

Los niveles de seguridad incluidos[12] son:

Security Level 0 Las tarjetas MIFARE Plus son pre-personalizadas con claves especiales de configuración de tipo CRYPTO-1 y AES.

Security Level 1 En este nivel, las tarjetas son totalmente compatibles con las Mifare Classic. Esto garantiza funcionalidad con la infraestructura existente.

Security Level 2 Este nivel utiliza autenticación mediante el cifrado AES y confidencialidad de los datos almacenados por el sistema CRYPTO-1.

Security Level 3 Este nivel utiliza autenticación y confidencialidad de los datos almacenados mediante el cifrado AES.

[11] [Sem09]

[12] Los niveles 2 y 3 sólo con las tarjetas MIFARE Plus X

Capítulo 4

Conclusiones

Los problemas asociados con el fraude y la recaudación de ingresos no son nuevos en la historia del transporte.

Sin embargo, a medida que la tecnología evolucionó, también se vislumbraron nuevas técnicas para cometer los mismo fraudes de siempre, es decir, las soluciones tecnologías introdujeron fraudes tecnológicos pero el sistema no estaba exento de los mismos.

Cualquier solución o mitigación que quiera adoptarse deberá tener en cuenta que las soluciones de boleto electrónico para transporte público deben ser principalmente: rápidas para permitir el flujo de pasajeros, potencialmente extensibles para su uso en los diversos medios y de costo moderado pero proporcionando un nivel de protección de seguridad suficiente para poder asegurar razonablemente los datos asociados y el valor almacenado.

Dentro de estos límites, si el costo de la protección es mayor que la pérdida de ingresos y el costo de la investigación del fraude, entonces deberá evaluarse la opción de simplemente tolerar o asumir las pérdidas que pueden producirse.

Es mas, hay autores[1] que sugieren que los sistemas de transporte no deberían asumir que los ataques a la seguridad Mifare Classic se traducirán en un fraude a gran escala, citando una serie de factores (técnicos y no técnicos) que podrían ayudar a compensar el problema.

Haciendo extensiva dicha enumeración, se citan entre los elementos *No técnicos* algunos como:

- ◇ La mayoría de las personas son generalmente honestas y no correrían el riesgo de tener antecedentes penales por el solo hecho de viajar gratis en transporte público.
- ◇ Existe una tentación limitada cuando el fraude es pequeño en relación con el esfuerzo y riesgo.
- ◇ Las experiencias de los sistemas de ticket en papel convencional y los controles convencionales son aplicables para contrarrestar el fraude organizado con o sin TISC.

No obstante, es dable entender que si se observa que cualquiera de estas situaciones escalan rápidamente los operadores de transporte deberán tomar determinaciones rapidamente para reaccionar ante esta escalada.

Las posibles soluciones analizadas implican en sí mismas decisiones mayores. Cualquier mitigación o mejora de la seguridad debería ser analizada detenidamente a fin de evaluar la conveniencia de aplicar la mitigación o bien evolucionar hacía otra tecnología que brinde mayor seguridad (como puede ser Mifare-Plus visto en la sección 3.2).

Para ello, la propuesta de NXP a través de Mifare Plus proporciona un roadmap especialmente diseñado que permita contrarrestar muchas de las vulnerabilidades manifestadas en el presente documento y que se relacionan con la debilidad del sistema CRYPTO-1. Su reemplazo ordenado por el estándar AES proporciona un nivel de seguridad adecuado para este tipo de transacciones y debería ser el estándar a adoptar para cualquier implementación nueva.

[1] [MMH09]

Sin embargo, para aquellas soluciones y sistemas ya implementados, de mantenerse dentro de la tecnología Mifare Classic, las mitigaciones y medidas vistas en la sección 3, sin llegar a ser infalibles, dificultan las acciones descriptas y motiva que el fraude se oriente hacia productos de mayor valor y aumenta el nivel de sofisticación y la habilidad de las técnicas de ataque en los que se deben basar para explotar las vulnerabilidades.

Por supuesto, sería mucho mejor poder contar con soluciones que brinden mayor seguridad de uso, por lo que, para los operadores de sistemas de transporte que aún no lo hayan hecho, sería aconsejable planificar el progresivo reemplazo de la *MIFARE classic*.

Aún así prevalecen cuestiones no técnicas, es decir, aún con un sistema de pago electrónico seguro, el sistema de transporte deberá seguir lidiando con evasiones y fraudes, tal cual lo expone el reporte del Metro de Barcelona[2].

Es por todo ello que la seguridad del sistema debe estar planteada del principio al fin y no sólo soportada en la integridad de uno de los elementos como pueden ser las TISC.

[2] [CAS10]

Bibliografía

[CAS10] ANTÍA CASTEDO. Uno de cada tres usuarios del trambesòs viaja sin pagar el billete. *EL PAIS*, 03 2010.

[CDT09] Daniel Ciolek, Lautaro Dolberg, and Pablo Terlisky. Seguridad en sistemas de tarifado electrónico. Technical report, 2009.

[CM03] Nicolas Courtois and Willi Meier. Algebraic attacks on stream ciphers with linear feedback. In Eli Biham, editor, *Advances in Cryptology EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, chapter 21, page 644. Springer Berlin Heidelberg, Berlin, Heidelberg, May 2003. ISBN 978-3-540-14039-9.

[CNO08] Nicolas T. Courtois, Karsten Nohl, and Sean OÑeil. Algebraic attacks on the crypto-1 stream cipher in mifare classic and oyster cards. Technical report, 2008. http://eprint.iacr.org/.

[Cou09] Nicolas T. Courtois. The Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes Anywhere, Anytime. March 2009.

[dKGHG08] Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio Garcia. A practical attack on the MIFARE classic. In Gilles Grimaud and François-Xavier Standaert, editors, *Smart Card Research and Advanced Applications*, volume 5189 of *Lecture Notes in Computer Science*, chapter 20, pages 267–282. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008. ISBN 978-3-540-85892-8.

[dKHG08] Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia. A practical attack on the MIFARE Classic. In *8th Smart Card Research and Advanced Application Workshop (CARDIS 2008)*, volume 5189 of *Lecture Notes in Computer Science*, pages 267–282. Springer Verlag, 2008.

[GdKM+08] Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijrers, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs. Dismantling MIFARE classic. In S. Jajodia and J. Lopez, editors, *13th European Symposium on Research in Computer Security (ESORICS 2008)*, volume 5283 of *Lecture Notes in Computer Science*, pages 97–114. Springer Verlag, 2008.

[GvRVS09a] Flavio D. Garcia, Peter van Rossum, Roel Verdult, and Ronny W. Schreur. Wirelessly pickpocketing a Mifare classic card. *Security and Privacy, IEEE Symposium on*, 0:3–15, 2009.

[GvRVS09b] Flavio D. Garcia, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. Wirelessly pickpocketing a Mifare Classic card. In *IEEE Symposium on Security and Privacy (S&P 2009)*, pages 3–15. IEEE, 2009.

[GvRVWS10] Flavio D. Garcia, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. Dismantling securememory, cryptomemory and cryptorf. In *CCS '10: Proceedings of the 17th ACM conference on Computer and communications security*, pages 250–259, New York, NY, USA, 2010. ACM. ISBN 978-1-4503-0245-6.

[iRV08] ing. R. Verdult. Proof of concept, cloning the ov-chip card. Technical report, Security of Systems at the Radboud University Nijmegen, 2008.

[MMH09] Keith E. Mayes, Konstantinos Markantonakis, and Gerhard Hancke. Transport ticketing security and fraud controls. *Information Security Technical Report*, 14 (2):87 – 95, 2009. Smart Card Applications and Security.

[MMSA08] Konstantinos Markantonakis, Keith Mayes, Damien Sauveron, and Ioannis G. Askoxylakis. Overview of security threats for smart cards in the public transport industry. In *2008 IEEE International Conference on e-Business Engineering*, pages 506–513. IEEE, October 2008. ISBN 978-0-7695-3395-7.

[NEP08] S. Karsten Nohl, David Evans, and H. Plotz. Reverse engineering a cryptographic RFID tag. July 2008.

[Net11] NetCard. What is mifare? 03 2011.

[NS10] NXP-Semiconductors. System level security measures for mifare installations. Technical Report AN10969, NXP Semiconductors, 2010.

[NXP08] NXP. End to end system security risk considerations for implementing contactless cards. Application note AN155010, NXP Semiconductors, 06 2008.

[Pér02] G. Pérez. *Sistemas de cobro electrónico de pasajes en el transporte público*. Serie Recursos naturales e infraestructura. Naciones Unidas ; CEPAL, División de Recursos Naturales e Infraestructura, Unidad de Transporte, 2002. ISBN 9789213220412.

[Sem09] NXP Semiconductors. Security target lit. Technical Report BSI-DSZ-CC-058, Common Criteria, 2009.

[SvdS07] Pieter Siekerman and Maurits van der Schee. Security evaluation of the disposable ov-chipkaart. Technical report, University of Amsterdam, 2007.

[Tan09] Wee Hon Tan. *Practical Attacks on the MIFARE Classic*. PhD thesis, Imperial College LondonDepartment of Computing, 2009.

[Tra07] Anibal Trasmonte. La historia del boleto. *Primer Museo Virtual del Transporte Argentino*, 04 2007. http://www.busarg.com.ar/boletos.htm.

[Wil09] Kyle E. Penri Williams. *Implementing an RFID 'Mifare ClassicÁttack*. PhD thesis, City University London, September 2009.

Índice de figuras

1.1. Boletos y cospeles 4
1.2. Boletera computada DYC Tronic 5
1.3. Usuarios evadiendo molinetes en el Metro de Barcelona 7
1.4. Transporte público 8
1.5. Entrada a un concierto 9
1.6. Entrada a un Evento Deportivo 9
1.7. Diagrama de Bloques Mifare[CDT09] 10
1.8. Memoria Mifare Classic 4K 10
1.9. Estructura de datos en Mifare 1K (Gemalto Datasheet) 11

2.1. Mapping Oyster interpretado en la investigación de Wee Hon Tan 14
2.2. Proxmark 3 haciendo sniffing en la investigación de Wee Hon Tan 15

3.1. Principios de la diversificación de claves 21

Glosario

3DES Algoritmo criptografo simétrico. El Triple DES se llama al algoritmo que hace triple cifrado del DES. También es conocido como TDES o 3DES. 21

AES Advanced Encryption Standard es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos y es uno de los algoritmos más populares usados en criptografía simétrica.. 21, 27, 29

CRYPTO-1 Sistema de encripción propietario de NXP y único disponible para las tarjetas Mifare Classic. 1, 15, 21, 27, 29

e-purse El monedero electrónico o e-purse de una tarjeta es el campo del mapping que proporciona información del saldo cargado en dicha tarjeta.. 10, 11, 14, 15, 21, 22

SAM Módulos de Seguridad o módulos SAM por sus siglas en inglés *Security Acces Module*. 20

TISC Tarjeta Inteligente sin Contacto. 7, 8, 13, 15, 16, 20, 21, 26, 29, 30

UID Unique IDentification Number. Identificador único de tarjeta provisto por el fabricante de chips y que si la tarjeta es NXP original es único. 19–26