UNIVERSIDAD
DE GRANADA

Seguridad y Protección de los Sistemas de Información

Análisis de seguridad en tarjetas sin contacto. El caso de Mifare Classic

Criptosistema CRYPTO1 y aplicaciones prácticas

Pedro Bonilla Nadal
Pedro Parrila Navarro
Javier Sáez de la Coba

Curso 2019-2020

27 de noviembre de 2019

Índice

1. Introduccion

En los últimos años, cada vez más sistemas han adoptado la RFID (identificación por radiofrecuencia), en particular las tarjetas sin contacto. Estas tarjetas, más comúnmente llamadas tarjetas contactless han sustituido a los códigos de barras, las tarjetas de banda magnética y los billetes de papel en una amplia variedad de aplicaciones. Las tarjetas contactless consisten en una pequeña pieza de memoria a la que se puede acceder de forma inalámbrica, pero a diferencia de las etiquetas RFID, también tienen algunas capacidades computacionales. La mayoría de estas tarjetas implementan algún tipo de criptografía de clave simple simétrica, haciéndolas adecuadas para aplicaciones que requieren control de acceso a la memoria de la tarjeta inteligente.

Varias aplicaciones a gran escala utilizan tarjetas contactless. Por ejemplo, se utilizan para el pago en varios sistemas de transporte público como la tarjeta utilizada en los buses o metros de Granada, en diferentes locales de hostelería, o en supermercados entre otro tipos de comercios. Muchos países ya han incorporado una tarjeta inteligente sin contacto en sus documentos oficiales, como pasaportes y tarjetas de identidad. Muchos edificios de oficinas e incluso instalaciones seguras, como aeropuertos y bases militares, utilizan tarjetas inteligentes sin contacto para el control de acceso. Se diferencian en tamaño, carcasa, memoria y potencia de cálculo. También difieren en las características de seguridad que proporcionan.

En este trabajo se van a analizar las tarjetas Mifare Classic, explicando el criptosistema utilizado y un ejemplo de como realizar un ataque a este tipo de tarjetas. Se ha escogido este modelo debido a que es el más utilizado a nivel mundial, con millones de unidades vendidas.

Se puede añadir más respecto a nuestra contribución, explicando los pasos que vamos a realizar en el ejemplo de manera muy breve

2. Tarjetas Mifare Classic

MIFARE es una tecnología de tarjetas inteligentes sin contato (TISC), de las más ampliamente instaladas en el mundo, con el 70 % de cuota de mercado en el caso de la variante MIFARE Classic.

El MIFARE Classic es un dispositivo de almacenamiento de memoria, donde la memoria se divide en segmentos y bloques con mecanismos de seguridad simples para el control de acceso. Están basados en ASIC[1] y tienen una potencia computacional limitada.

Este modelo tiene una memoria que ofrece 1.024 bytes de almacenamiento de datos, divididos en 16 sectores de 64 bytes; cada sector está protegido por dos claves diferentes, llamadas A y

[1]ASIC: Circuito integrado diseñado para una aplicación específica

B. Cada clave puede ser programada para permitir operaciones tales como lectura, escritura, incrementar contadores, etc. Las hay con memoria de 4KB ofreciendo 4.096 bytes divididos en cuarenta sectores, de los cuales 32 son del mismo tamaño que el de 1K con ocho más que son sectores de tamaño cuádruple. Para cada uno de estos tipos de sistemas, se reservan 16 bytes por sector para las claves y las condiciones de acceso, y normalmente no se pueden utilizar para los datos de usuario. Además, los primeros 16 bytes de la tarjeta contienen el número de serie de la tarjeta y algunos otros datos del fabricante y son sólo de lectura. Esto reduce la capacidad de almacenamiento de estas tarjetas a 752 bytes para MIFARE Classic con 1K de memoria y 3.440 bytes para MIFARE Classic con 4K de memoria.

MIFARE Classic cumple con las partes 1 a 3 de la norma ISO 14443-A [3], especificando las características físicas, la interfaz de radiofrecuencia y el protocolo anticolisión. El Mifare Classic no implementa la parte 4 del estándar, que describe el protocolo de transmisión, sino que utiliza su propia capa de comunicación segura. En esta capa, Mifare Classic utiliza el cifrado de flujo propietario CRYPTO1 para proporcionar confidencialidad de datos y autenticación mutua entre la tarjeta y el lector. Esta cifrado ha sido desmantelado utilizando ingeniería inversa.

3. El sistema Crypto1

Crypto1 es un algoritmo de cifrado privativo creado por NXP Semiconductors específicamente para las etiquetas RFID de Mifare, incluido por ejemplo en las tarjetas Consorcio Público de Transportes de Andalucía, que son las que van a ser analizadas en este trabajo.

En 2009, la investigación criptográfica realizada en la Universidad Radboud de Nijmegen (Paises Bajos) [1], demostró que "la seguridad de este cifrado es cercana a cero". Crypto1 es un cifrado de flujo muy similar en su estructura a su sucesor, Hitag2. Crypto1 se compone de:

- Un registro de desplazamiento de retroalimentación de 48 bits para el estado secreto principal del cifrado
- Una función lineal
- Una función no lineal de dos capas de 20 a 1
- Un LFSR[2] de 16 bits que se utiliza durante la fase de autenticación (que también sirve como generador de números pseudo aleatorios en algunas implementaciones de tarjetas).

Puede funcionar como un NLFSR[3] y como un LFSR, dependiendo de sus parámetros de entrada. Las salidas de una o ambas funciones lineales y no lineales pueden retroalimentarse al estado de cifrado o utilizarse como filtros de salida. La operación habitual de los

[2] LFSR: Linear feedback shift register o registro de desplazamiento con retroalimentación lineal
[3] NLFSR: Nonlinear

cifrados Crypto1 e Hitag2 utiliza retroalimentación no lineal sólo durante la etapa de inicialización/autenticación, cambiando a la operación LFSR con un filtro de salida no lineal para encriptar las comunicaciones de la etiqueta en ambas direcciones. En esta tarjeta las operaciones criptográficas se realizan en hardware. La seguridad de la tarjeta se basa en parte en el secreto del algoritmo CRYPTO1, que se conoce como como "seguridad por ocultación". Las tarjetas Mifare Classic se utilizan normalmente para la autenticación.

Para el acceso, el objetivo es que dos partes demuestren quiénes son. Ambas partes, en este caso la tarjeta Mifare y el lector de tarjetas, realizan ciertas operaciones y se comprueban mutuamente los resultados para asegurarse de con quién están tratando.

Los investigadores y estudiantes del grupo de seguridad digital de la Universidad Radboud de Nijmegen descubrieron el 7 de marzo de 2008 un grave defecto de seguridad en Mifare Classic. Anteriormente, los investigadores alemanes Karsten Nohl en Henryk Pltz señalaron las debilidades de seguridad de estas tarjetas.

Debido a que algunas tarjetas pueden ser clonadas, en principio es posible acceder a edificios e instalaciones con identidad robada, habiendo sido demostrado en un sistema real. En muchas situaciones en las que se utilizan estas tarjetas habrá medidas de seguridad adicionales; es aconsejable reforzarlas siempre que sea posible.

El grupo de seguridad digital encontró debilidades en el mecanismo de autenticación del Mifare Classic. En particular:

- El funcionamiento del algoritmo de encriptación CRYPTO1 ha sido reconstruido en detalle.
- Hay un método relativamente fácil para recuperar claves criptográficas, que no depende de costosos equipos. En caso de que no existan medidas de seguridad adicionales, esto permitiría el acceso no autorizado de personas con malas intenciones.

La autenticación exitosa es también un requisito previo para leer o escribir parte de la memoria del Mifare Classic. El manejo correcto de las claves es otro tema en si mismo. Por encima, hay dos opciones:

- Todas las tarjetas y todos los lectores de tarjetas utilizados para alguna aplicación tienen las mismas claves de autenticación. Esto es común cuando se utilizan tarjetas para el control de acceso.
- Cada tarjeta tiene sus propias claves criptográficas. Para comprobar las claves de una tarjeta, el lector de tarjetas debe determinar primero con qué tarjeta está hablando y, a continuación, buscar o calcular la(s) clave(s) asociada(s). Esto se llama diversificación de claves.

Se afirma que el segundo enfoque se utiliza para el transporte público neerlandés. Y para el andaluz?

En este sistema el LFSR el polinomio generador $p(x) := x^{48} + x^{43} + x^{39} + x^{38} + x^{36} + x^{34} + x^{33} + x^{31} + x^{29} + x^{24} + x^{23} + x^{21} + x^{19} + x^{13} + x^9 + x^7 + x^6 + x^5 + 1$ y una función de filtro f. En cada tick del reloj, 20 de los bits del LFSR se pasan por la función filtro, generando un bit de salida. Después se hace un shif hacia la izquierda de un bit, y se utiliza el polinomio generador para crear un nuevo bit a la derecha.

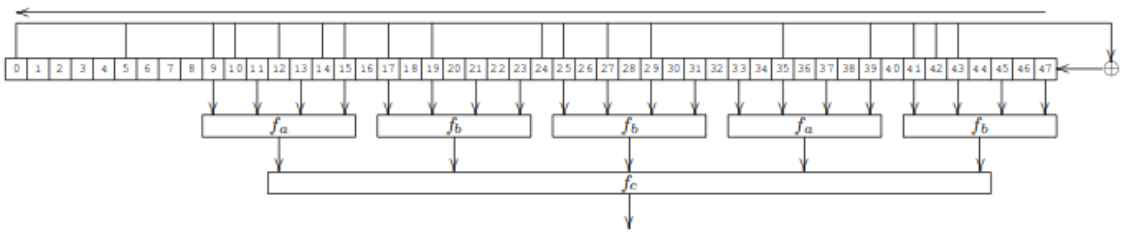
Nota. *Denotaremos como $\mathbb{F}_2$ al cuerpo de dos elementos. Además, dado un cuerpo F, se denotará como $F^n := \times_{i=0}^{n} F$ donde $\times$ representa el producto cartesiano de cuerpos.*

Definition 3.1. La función de feedback es $L : \mathbb{F}_2^{48} \to \mathbb{F}_2$ definida como

$$L(x_0...x_{47}) := x_0 \oplus x_5 \oplus x_9 \oplus x_{10} \oplus x_{12} \oplus x_{14} \oplus x_{15}$$

$$\oplus x_{17} \oplus x_{19} \oplus x_{24} \oplus x_{25} \oplus x_{27} \oplus x_{29} \oplus x_{35} \oplus x_{39} \oplus x_{41} \oplus x_{42} \oplus x_{43}$$

Además las funciones de filtro se aplican como se muestra en la figura posterior:



Definition 3.2. La función feedback $L_{16} : \mathbb{F}_2^{16} \to \mathbb{F}_2$ del generador pseudoaleatorio es definida por:

$$L_16(x_0x_1...x_{15}) := x \oplus x_2 \oplus x_3 \oplus x_5$$

A partir de esta, definimos la función sucesor suc que computa la siguiente secuencia del LFSR como

$$suc(x_0...x_{31}) := x_1, ..., x_{31}L(x_{16}, ..., x_{31})$$

Porque el periodo del generador de números pseudoaleatorios es solo de 65535, y por lo tanto al cambiar cada 9.44μs, cicla cada 618 ms.

4. Protocolo de autentificación e inicialización

El proceso de lectura de una tarjeta desde fuera parece simple, únicamente acercar la tarjeta al lector y ya se realiza la operación con la que ha sido destinada casi de manera instantánea.

Detrás de esto hay un proceso de identificación y comienzo de envío de mensajes que será explicado a continuación, ya que vendrá bien conocerlo para el resto del trabajo redactado.

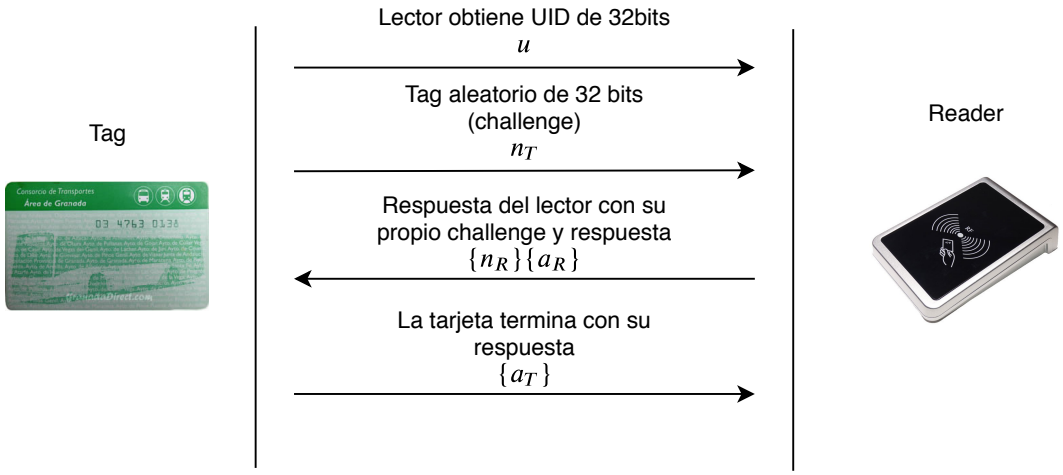


Figura 1: Protocolo de autentificación

- En primer lugar, el lector y la tarjeta participan en el protocolo anticolisión de acuerdo al estándar ISO/IEC 14443-3 [3], en el que el lector aprende el ID (u) único de la tarjeta y selecciona la tarjeta.
- El lector emite un comando '60 XX' o '61 XX' mediante el cual inicia el proceso de autenticación simétrica mutua entre la tarjeta y el lector, con la clave correspondiente al bloque número XX.
- La tarjeta responde con un n_T aleatorio de 32 bits.
- El lector envía un criptograma de 64 bits que es: $a_R := suc^6 4(n_T)$.
- La tarjeta finaliza con la respuesta $a_T := suc^9 6(n_T)$
- A continuación, se encriptan todas las comunicaciones y datos subsiguientes y la tarjeta aceptará ahora los comandos de lectura, escritura e incremento para el bloque XX.

Durante el protocolo de autenticación, se inicializa el estado interno del cifrado de la secuencia. Comienza como la clave del sector k, entonces $n_T \oplus u$ es desplazado y n_R también. Debido a que la comunicación se encripta desde n_R en adelante, la encriptación de los bits posteriores de n_R se ve influenciada por los bits anteriores de n_R. La autenticación se logra alcanzando el mismo estado interno de la cifra después de cambiar en n_R.

5. Debilidades

En esta sección explicaremos las debilidades de diseño de Mifare Classic.

5.1. Debilidades de Paridad

El estandar ISO 14443-A especifica que cada byte es seguido de un bit de paridad. Mifare Classic computa el bit de paridad sobre el texto plano, en lugar que sobre el texto cifrado. Además, el bit de keystream es usado para encriptar el bit de paridad es reusado para encriptar el siguiente bit de texto plano. Esto rompe la confidencialidad del sistema de encriptación.

Hay una consecuencia más de la paridad de bits. Durante la autenticación de protocolo, cuando el lector envía un nonce, el lector comprueba la paridad antes de la respuesta del lector. Si al menos un bit de paridad está mal el lector no responde. Si todos estan correcto pero la respuesta está mal, se responde con un código de error 0x5 *encriptado*. Esto sucede cuando el lector no se ha identificado aún y se asume que no debe ser capaz de descifrar.

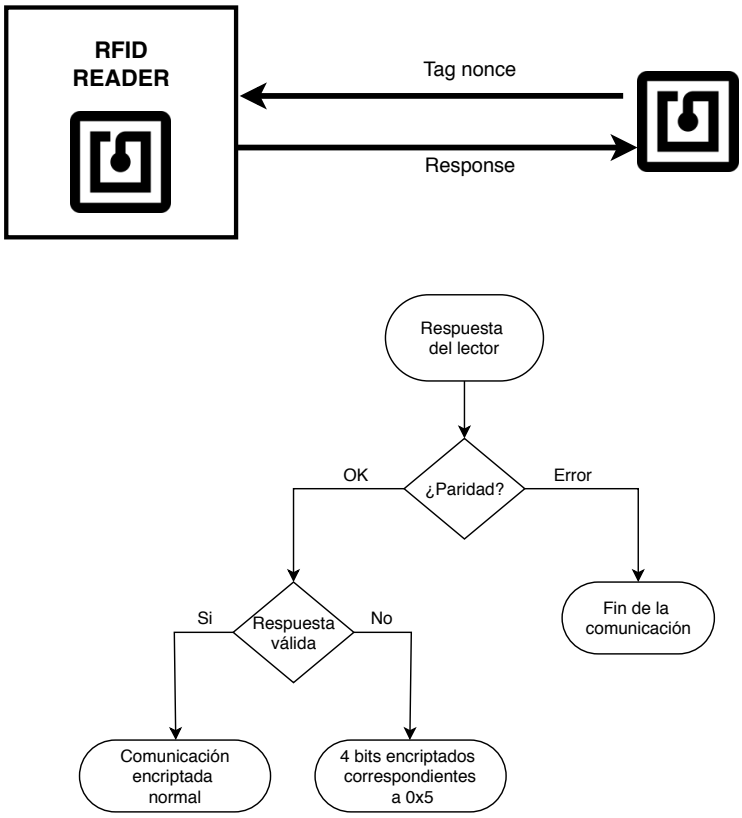


Figura 2: Diagrama de respuestas de la tarjeta ante la debilidad de paridad

5.2. Autenticaciones anidadas

Un atacante solo necesita conocer una clave de un sector, ya que existe una vulnerabilidad que permite al adversario conocer las demás con esa clave. Cuando un lector está comunicando con una tarjeta, un subsecuente comando de autenticación subsiguiente para un nuevo sector

también tiene que ser enviada encriptado. Después de esta autenticación el estado interno del cifrado se establece en el comando para el nuevo sector y el protocolo de autenticación comienza de nuevo.

Esta vez, sin embargo, el de la etiqueta también se envía cifrada. Como sólo hay 2^{16} posibles nonces, un atacante puede simplemente trata de adivinar los 32 bits de clave.

También aquí, la información que se filtra a través de los bit de paridad pueden utilizarse para acelerar el ataque. Aunque hay 216 marcas. Algunos investigadores han probado que contando esta información sólo hay 2^{13} nonces posible.

6. Ataques

Es importante darse cuenta de que para recuperar la clave es suficiente con recuperar el estado interno del cifrado, ya que el atacante conoce el id de usuario, el nonce de la tarjeta y el nonce del lector, puede deshacer los cambios temporales hasta el estado inicial, donde la clave es la configuración interna de cifrado.

6.1. Ataque de fuerza bruta.

El atacante juega el papel de un lector y trata de autenticarse para un sector de su elección. La tarjeta responde con un challenge con ocho bytes aleatorios (y ocho bits de paridad aleatoria). Hay una probabilidad $1/256$ de que los bits de paridad sean correctos y el tag responda con el código de error de 4 bits cifrado. A el éxito filtra 12 bits de entropía (de 48). esto que significa

Repetir el procedimiento anterior con suficientes veces veces determina de manera única la llave he leido que seis es suficiente pero bueno en verdad ni idea . Dado que la longitud de la clave es de sólo 48 bits, el atacante ahora puede aplicar fuerza bruta en la clave: puede comprobar cuál de las 2^{48} claves produce las seis veces la correcta paridad corregir los bits de paridad y la respuesta recibida. Esta última línea no se como redactarla

En la práctica, reuniendo una cantidad sesiones de autenticación con la información correcta los bits de paridad sólo toman un promedio de $6 - 256 = 1536$ intentos de autenticación que se pueden hacer en menos de un segundo. El tiempo que se tarda en realizar la operación offline el ataque de fuerza bruta, por supuesto, depende en gran medida de los recursos que el atacante tiene a su disposición.

6.2. Variando el nonce del Lector

Teniendo la capacidad de variar el nonce del lector, podemos accelerar un poco el proceso. Cuando conseguimos al final un nonce con la paridad correcta, tenemos una pareja (n_R, α) donde n_R es el nonce que ha utilizado el lector, y α el estado interno de cifrado. Una vez hecho esto, procederemos a crear otro nonce de lector n'_R que mantendrá igual los primero 31 bits, y cambiará el último, y variará aleatoriamente el resto hasta que la paridad sea correcta. De este modo el estado resultante será $(n'_R, \alpha \oplus 1)$. La encriptación de estos sucede que es la misma un 9.4 % de la veces.

Podemos acelerar nuestro ataque buscando n_R con estas propiedades, que de media conseguiremos al 11 intento con éxito en la paridad, y subsecuentemente poder buscar la clave en un espacio más de 10 veces menor.

6.3. Variando el nonce de la tarjeta

6.4. Ataque de autenticación Nested

En este ataque se asume que se conoce al menos una clave del sector, que será donde se le aplique el exploit.

El tiempo entre las dos autenticaciones puede variar de una tarjeta a otra, pero es constante para cada una. Aqui un atacante puede estimar este tiempo después de haber sido autentificado dos veces para el sector donde se presenta el exploit. Con esto puede conocer la distancia δ entre el primer y segundo nonce.

El atacante puede autentificarse para el sector que tiene el exploit y de manera subsecuente para otro sector. En la autentificación del exploit la tarjeta envia un nonce n_T^0, y durante la segunda autentificacion el nonce n_T es enviado de manera encriptada como n_T. Computando $suc^i(n_T^0)$ para i cercano a la distancia δ. Con esto se pueden reducir las posibilidades para n_T usando los 3 bits de información de la paridad de los bits.

7. Ejemplo de ataque al sistema del Consorcio de Transportes de Andalucía

Referencias

[1] Wirelessly Pickpocketing a Mifare Classic Card,
https://www.cs.ru.nl/~flaviog/publications/Pickpocketing.Mifare.pdf

[2] Identification cards — contactless integrated cir-cuit cards — proximity cards (ISO/IEC 14443) 2001, Radboud University Nijmegen.

[3] ISO Standards,
https://www.iso.org/standards.html

[4] Fco. Javier Rodríguez Navarro, RFID http://www.pinguytaz.net/M_Archivos/RFID/RFID.pdf

[5] A 2018 practical guide to hacking NFC/RFID https://smartlockpicking.com/slides/Confidence_A_2018_Practical_Guide_To_Hacking_RFID_NFC.pdf