RFID/NFC

. . . A QUICK TOUR . . .

Nahuel Grisolía
Cinta Infinita Founder / CEO

nahuel@cintainfinita.com.ar

@cintainfinita

Agenda

Motivaciones…

Definiciones Básicas y Ejemplos

Diversidad de Transponders…

Algo de Hardware, Algo de Software

Algunos Ataques e Ideas

Cierre

nahuel@cintainfinita$ whoami

- Cinta Infinita Founder and CEO

- (Web) Application Security specialist & enthusiast

- Many vulnerabilities discovered in Open Source and Commercial software: Vmware, Websense, OSSIM, Cacti, McAfee, Oracle VM, etc.

- Gadgets and Electronics Lover (RFID!)

- http://ar.linkedin.com/in/nahuelgrisolia
- http://cintainfinita.com
- http://www.exploit-db.com/author/?a=2008
- http://www.proxmark.org/forum/profile.php?id=3000

MOTIVACIÓN

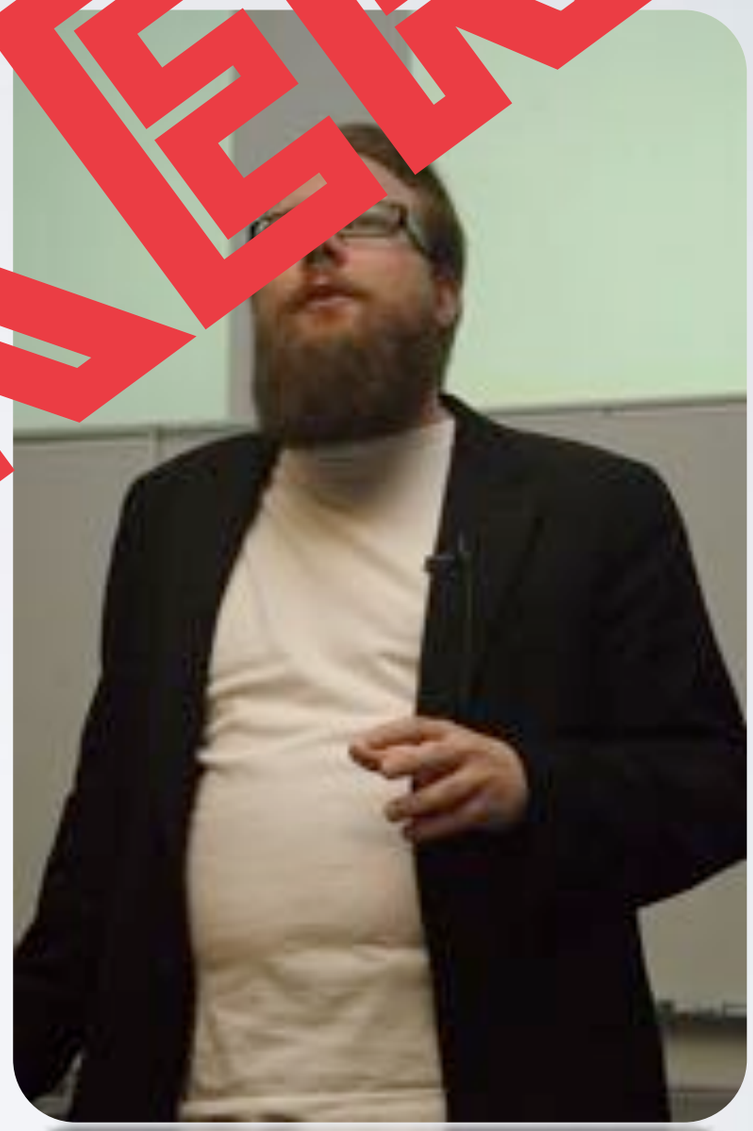
del libro "The Hacker Ethic and the Spirit of the Information Age"

Entusiasta
actitud pasional con el trabajo que realiza

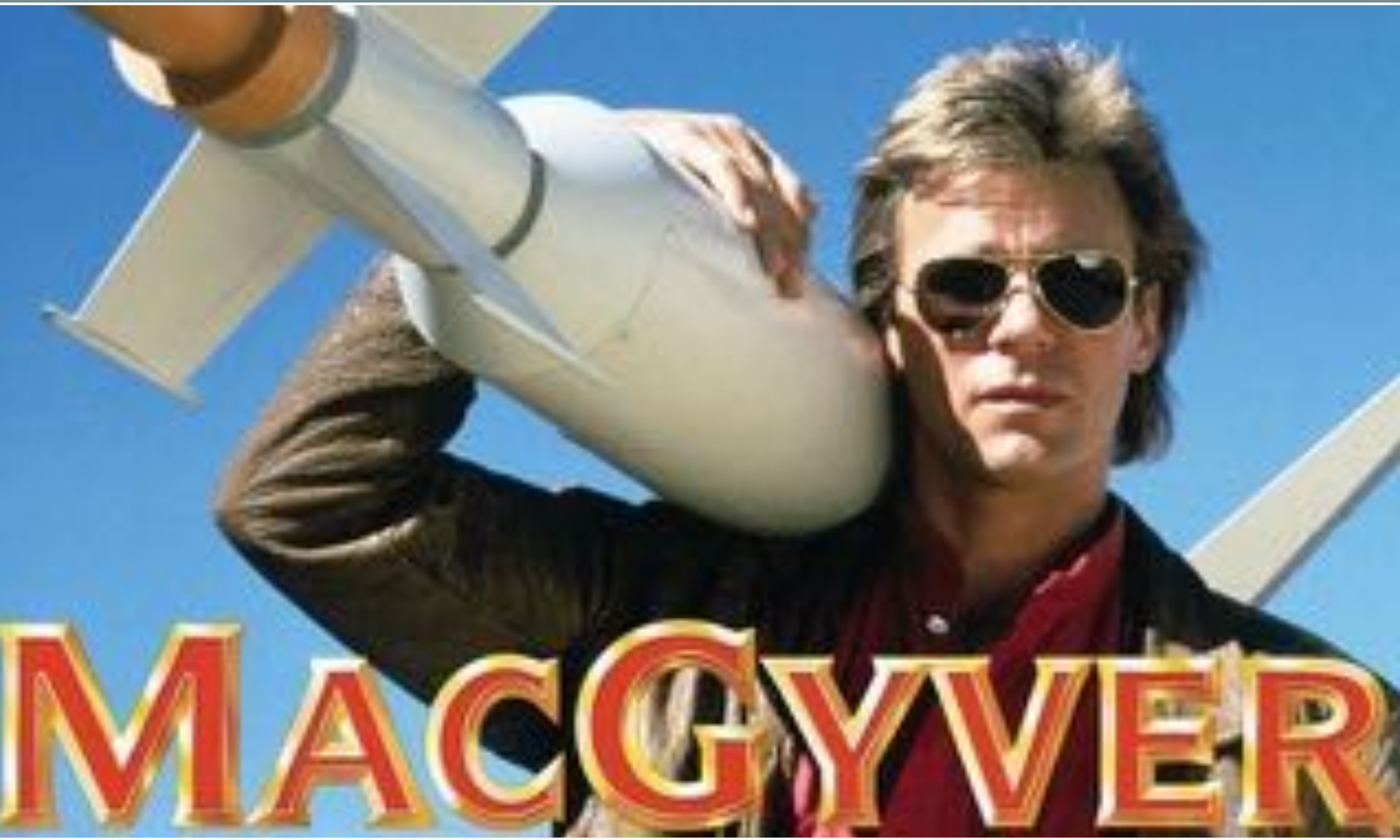
Creativo
deseo de desarrollar creatividad propia en equipo

Ganas de Compartir
los conocimientos con una comunidad

HACKER



Pekka Himanen


MACGYVER

Motivation++...


CON LA SUBE, SUBIMOS TODOS!


RECARGA
SUBE


MONEDERO


tripadvisor
AMERICAN EXPRESS
VISA
VISA
monedero
MasterCard

DATOS TÉCNICOS EN LIC. PUB.

- Año 2009
- Datos técnicos *bastante* completos (lo que nos importa!):

  CHIP PHILIPS MIFARE STANDARD IC MF1 S50 (NXP) 1k. — MIFARE CLASSIC! ;-)

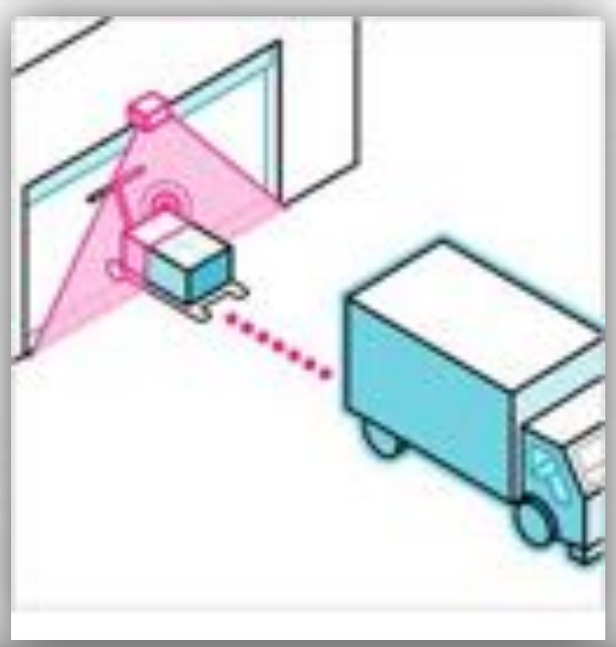
  Módulos SAM

  Equipos Lectograbadores (validadores) y algunos detalles de comportamiento del Firmware

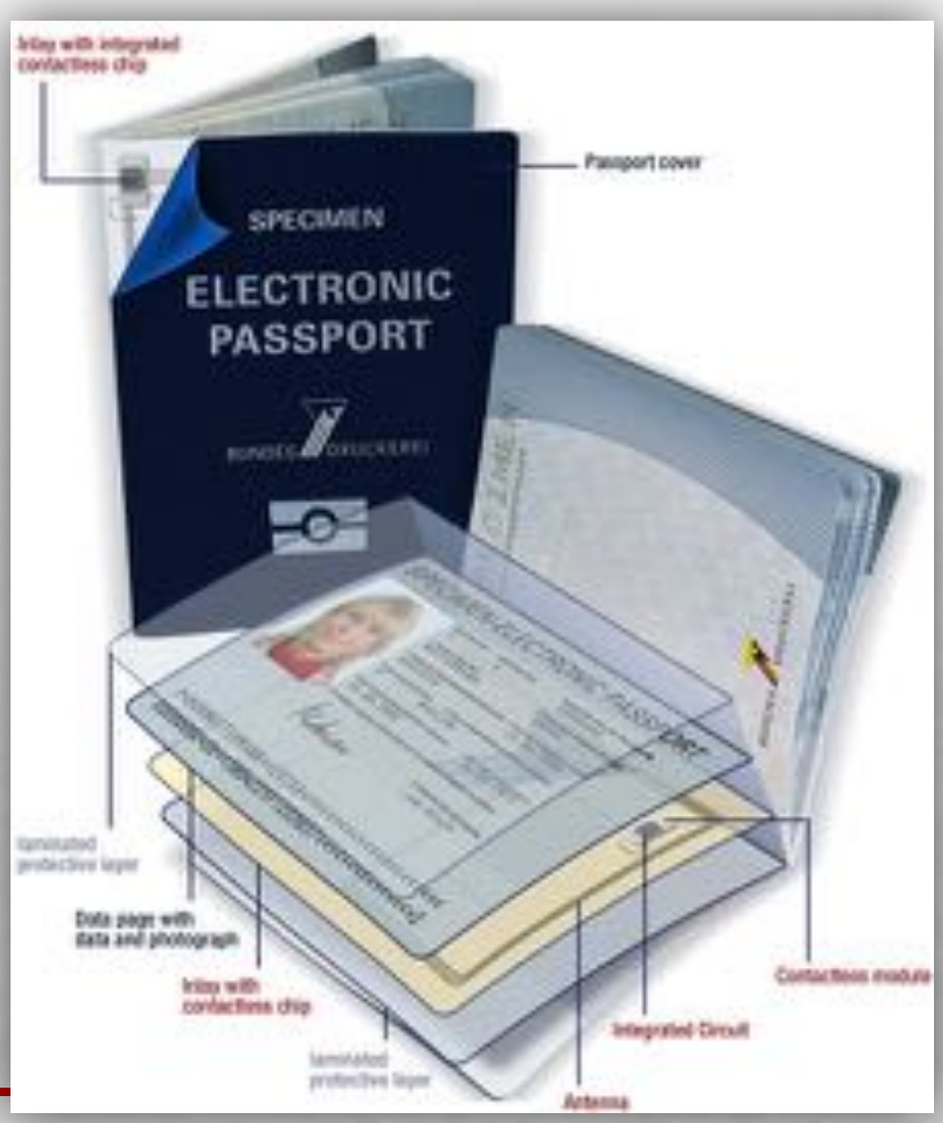
- Ya existían sistemas funcionales muy similares a éste, caso San Pablo, Brasil. Se “escucharon” reportes de vulnerabilidad en la implementación de este sistema.

Real Motto...

Real Life Examples?



Electronic Payments, Physical Access to buildings, Tolls, Passports, Medical Supplies and Equipment Tracking, Clothes, **almost everywhere**!



Real Life Examples?

Electronic Payments, Physical Access to buildings, Tolls, Passports, Medical Supplies and Equipment Tracking,
Clothes, **almost everywhere**!

Real Life Examples?

Santiago de Chile, Chile

Real Life Examples?

Frankfurt, Germany

Real Life Examples?

Moscow, Russia

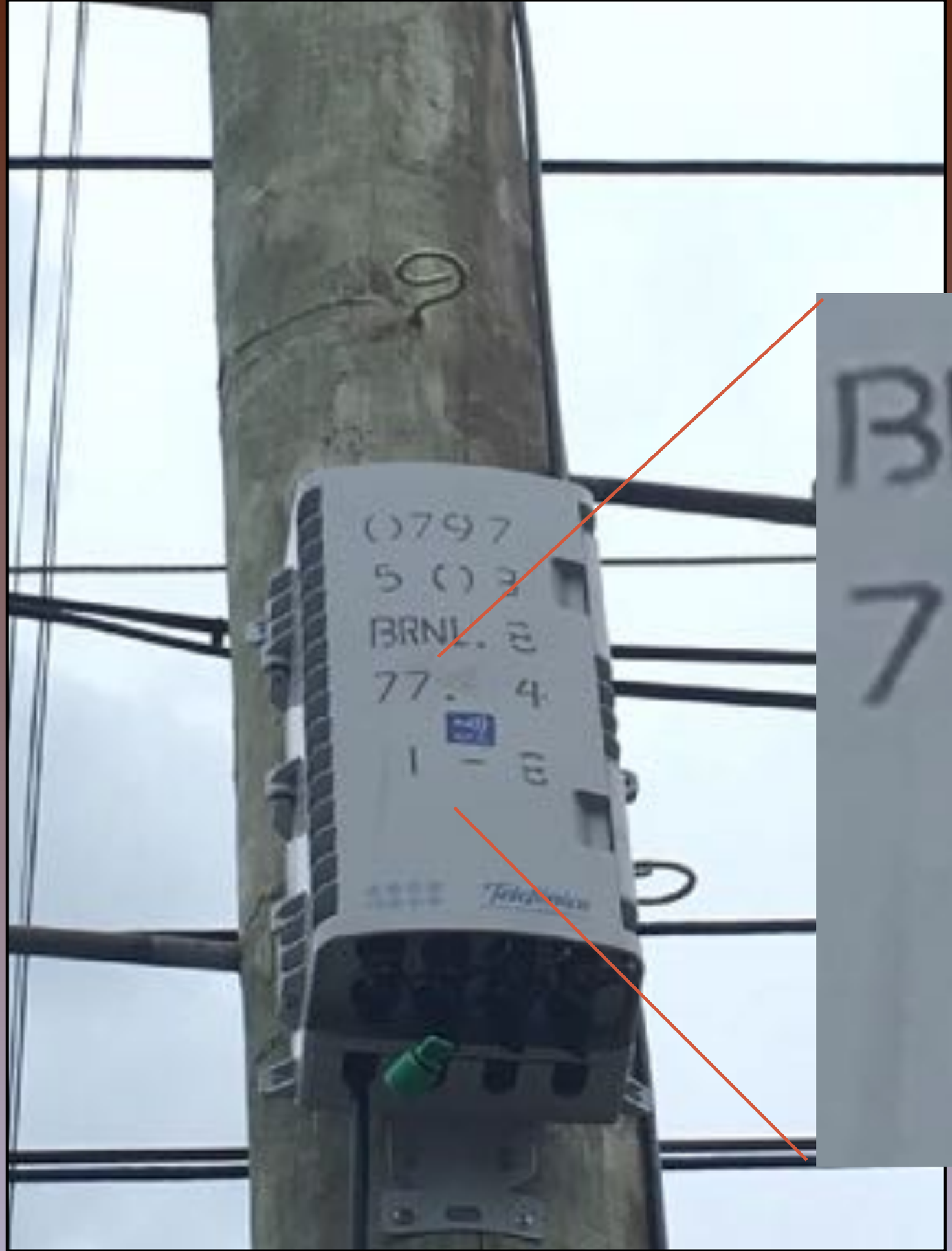
Real Life Examples?

Delhi, India

NEUQUEN!

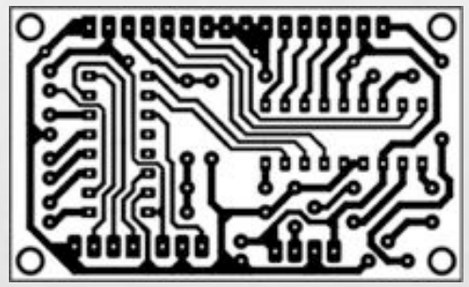

ESTACIONE AQUÍ
Retire su Tarjeta
TASEM-2
Ellnpark
NEUQUÉN FOTOS


SeIN
Terminal de Autoservicio de Estacionamiento Medido (TASEM)
TASEM-1
Ellnpark


BRNL.
77.
4
NFC

RFID Hardware

How does RFID work?



A Radio-Frequency IDentification system has three basic parts:

- A **transponder** - the RFID tag - that has been programmed with information.
- A scanning **antenna**
- A **transceiver** with a decoder to interpret the data

The scanning antenna puts out radio-frequency signals in defined a range.

The RF radiation does two things:

It provides a **means of communicating** with the transponder (the RFID tag) **AND**
It provides the RFID tag with the **energy to communicate** (in the case of passive RFID tags).

What is true about NFC?

NFC (Near Field Communication) is an open platform technology **standardized** in some ISO specs, specifying modulations schemes, coding, transfer speeds, data exchange methods (NDEF – sort of MIME - by NFC Forum), etc.

Form/subset of RFID (Radio Frequency IDentification) given that is uses radio waves for identification purposes.

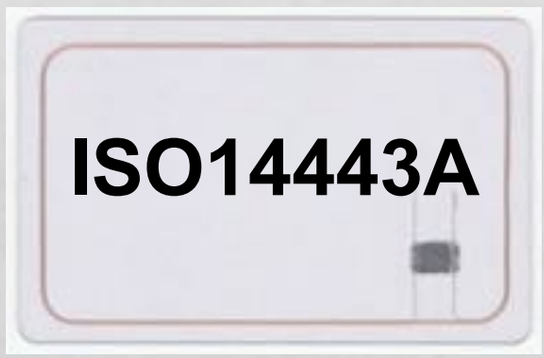
NFC **works at 13.56 MHz** in accordance with inductive coupling principles and allows communications at very short ranges (a few cm).

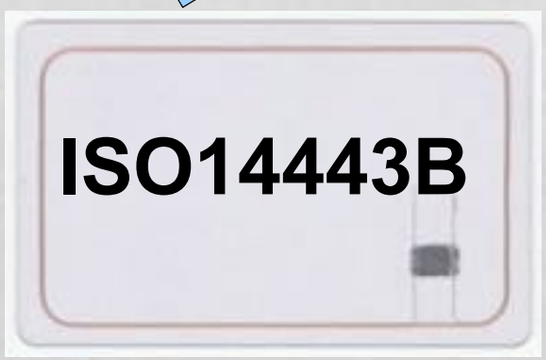
It provides **Card Emulation, Peer-to-Peer and Reader/Writer mode**.

What is true about NFC?

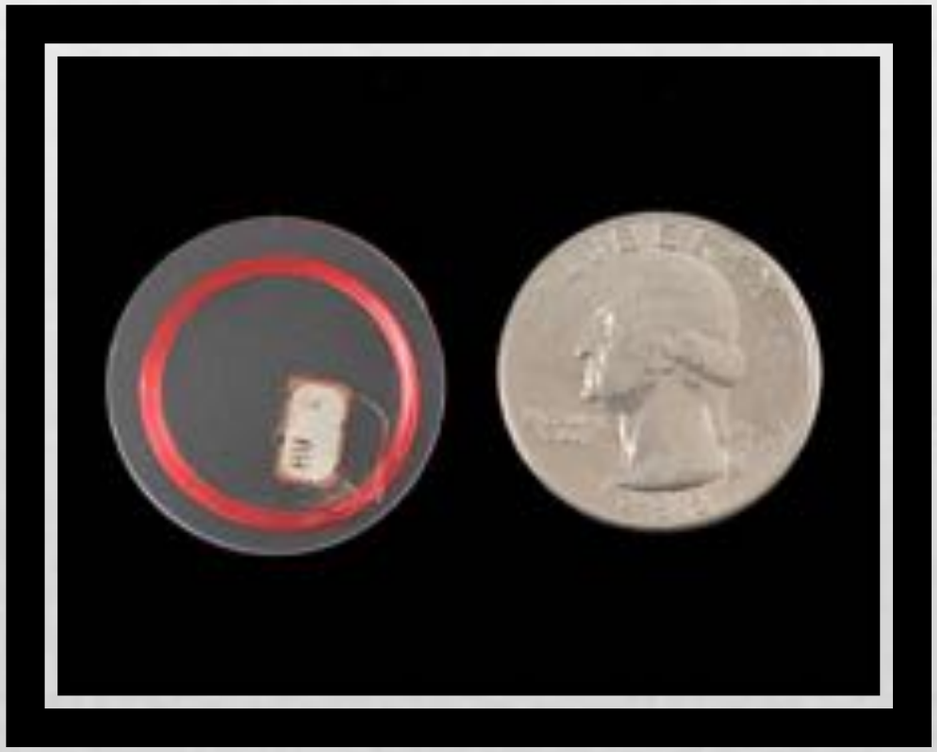
emul

p2p





It’s all About Tags…



TIPOS (HAY DE TODO) . . . VAMOS A CONOCERLOS . . .

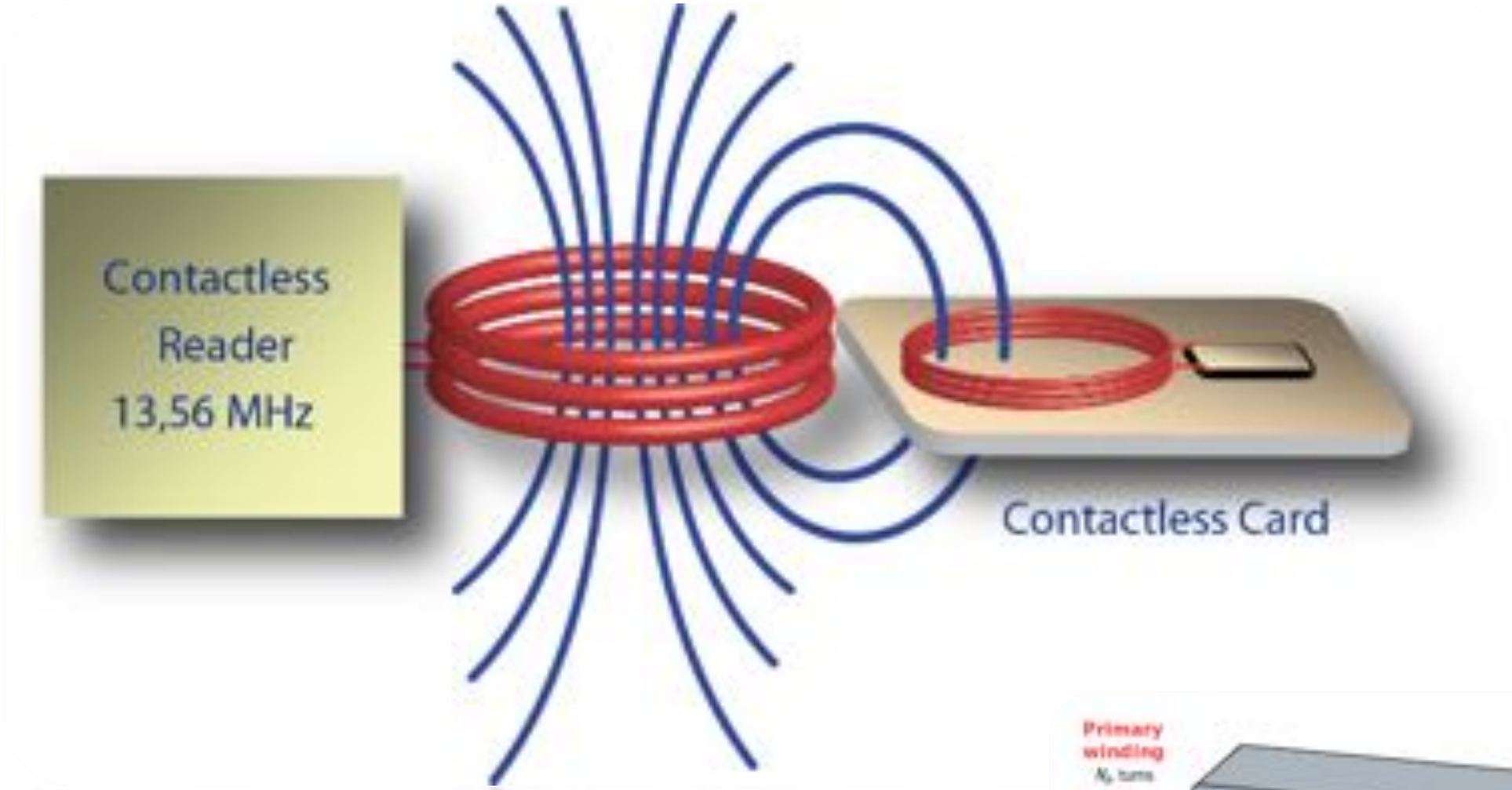
- *TRANSPODERS ACTIVOS*
- *TRANSPONDERS PASIVOS*

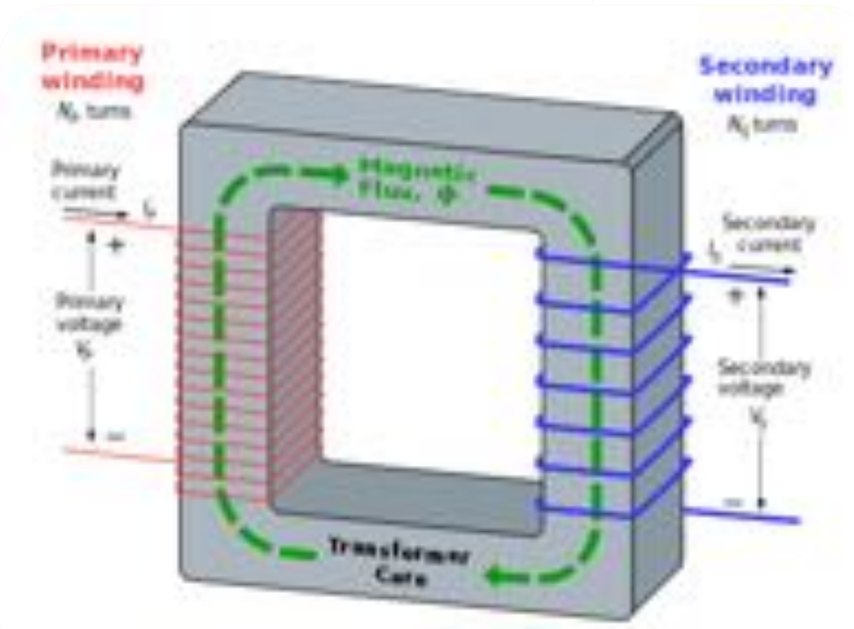
- *EN ALTA FRECUENCIA*
- *EN BAJA FRECUENCIA*
- *EN ULTRA ALTA FRECUENCIA & +*

- *SÓLO UID*
- *CON MEMORIA*
  (protegida - 1 a n claves - o sin clave)
  (con contadores, bits OTP)
- *CON ESTRUCTURA TIPO FileSystem*
- *SMARTCARD!*

ACTIVO

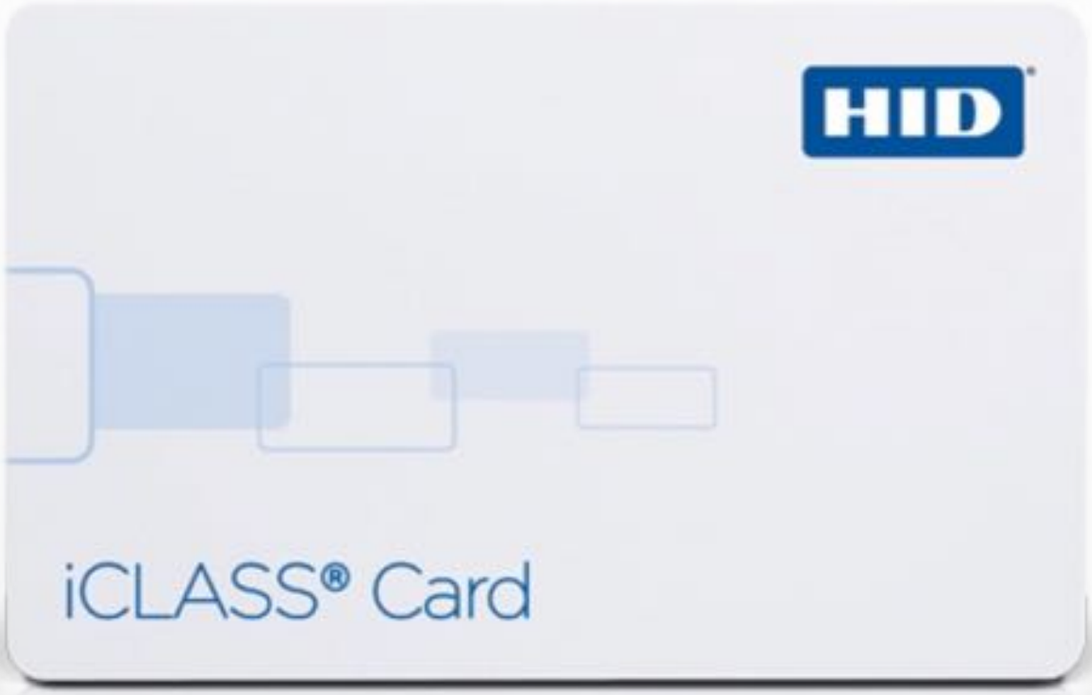
PASIVO


Contactless
Reader
13,56 MHz
Contactless Card


Primary winding
Secondary winding
Magnetic Flux, Φ
Primary current
Secondary current
Primary voltage
Secondary voltage
Transformer Core

Low Frequency Tags, Passive

High Frequency Tags, Passive



y ahora… cómo rompo todo???? daaaale!

Omnikey CardMan 5321

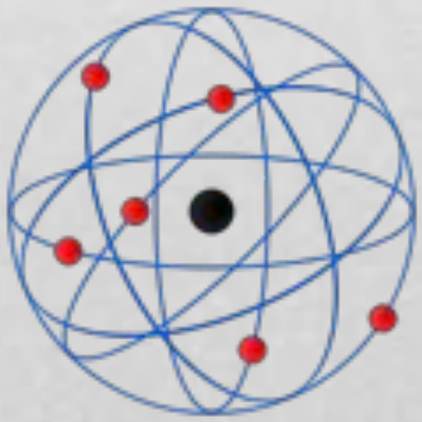
LibNFC

What?

Open Source library for Near Field Communication (NFC)

“libnfc is the first libre low level NFC SDK and Programmers API released under the GNU Lesser General Public License.”

It provides complete transparency and royalty-free use for everyone.



http://nfc-tools.org/index.php?title=Libnfc

LibNFC

What?

All major operating systems are supported, including **GNU/Linux**, **Mac OS X** and **Windows**. Compilation should work out of the box on POSIX-systems. (YEAH! TRUE! :)

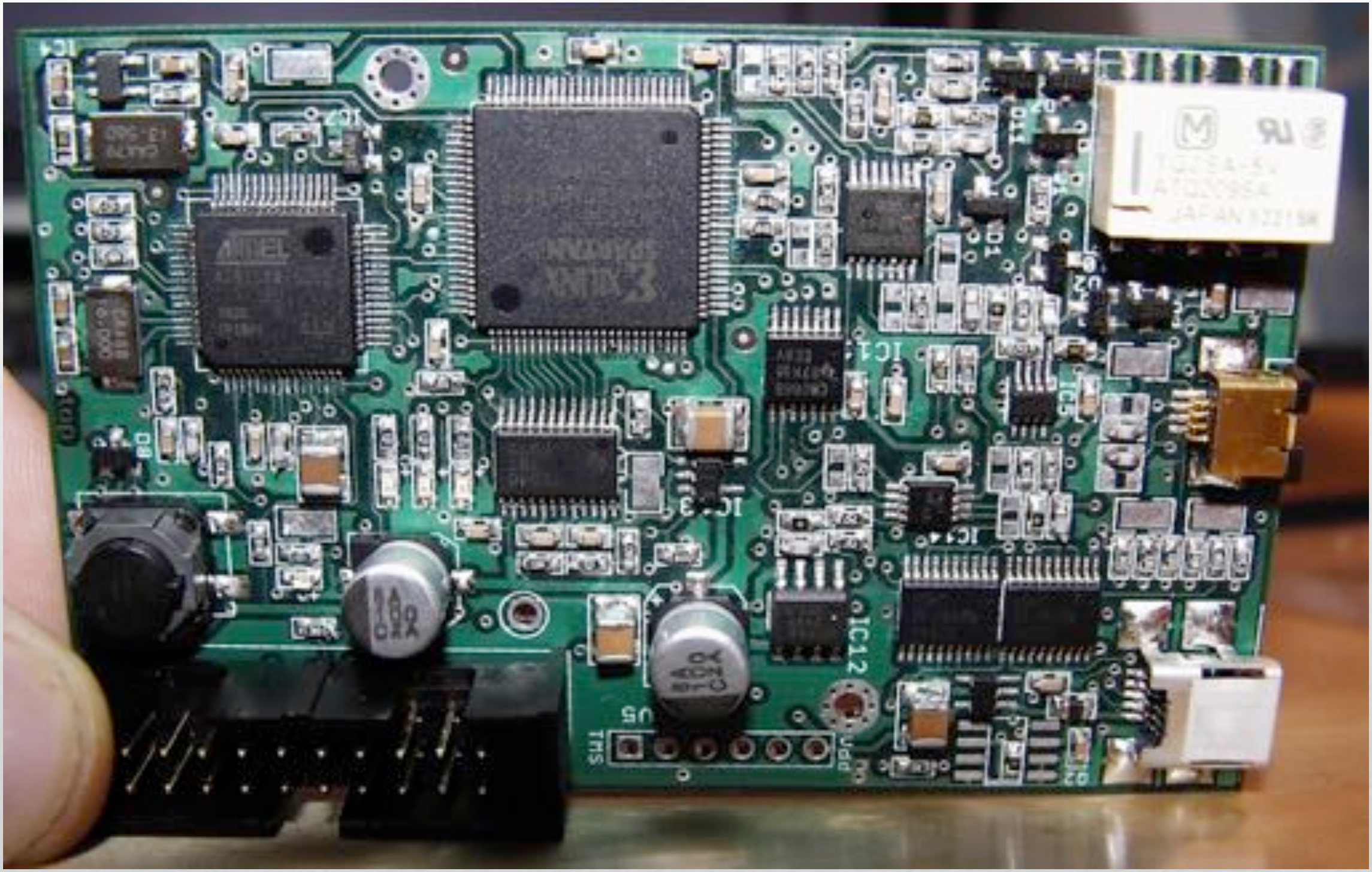
Supports various NFC hardware devices based on PN532 and PN533 chips: dongles, flat and OEM devices.

Supports connection via libusb, PC/SC, UART, SPI and I2C.

Supports modulations for ISO/IEC 14443 (A and B), FeliCa, Jewel tags and Data Exchange Protocol (P2P) as target and as initiator and card emulation (somehow).

Proxmark3

Board



http://cq.cx/proxmark3.pl

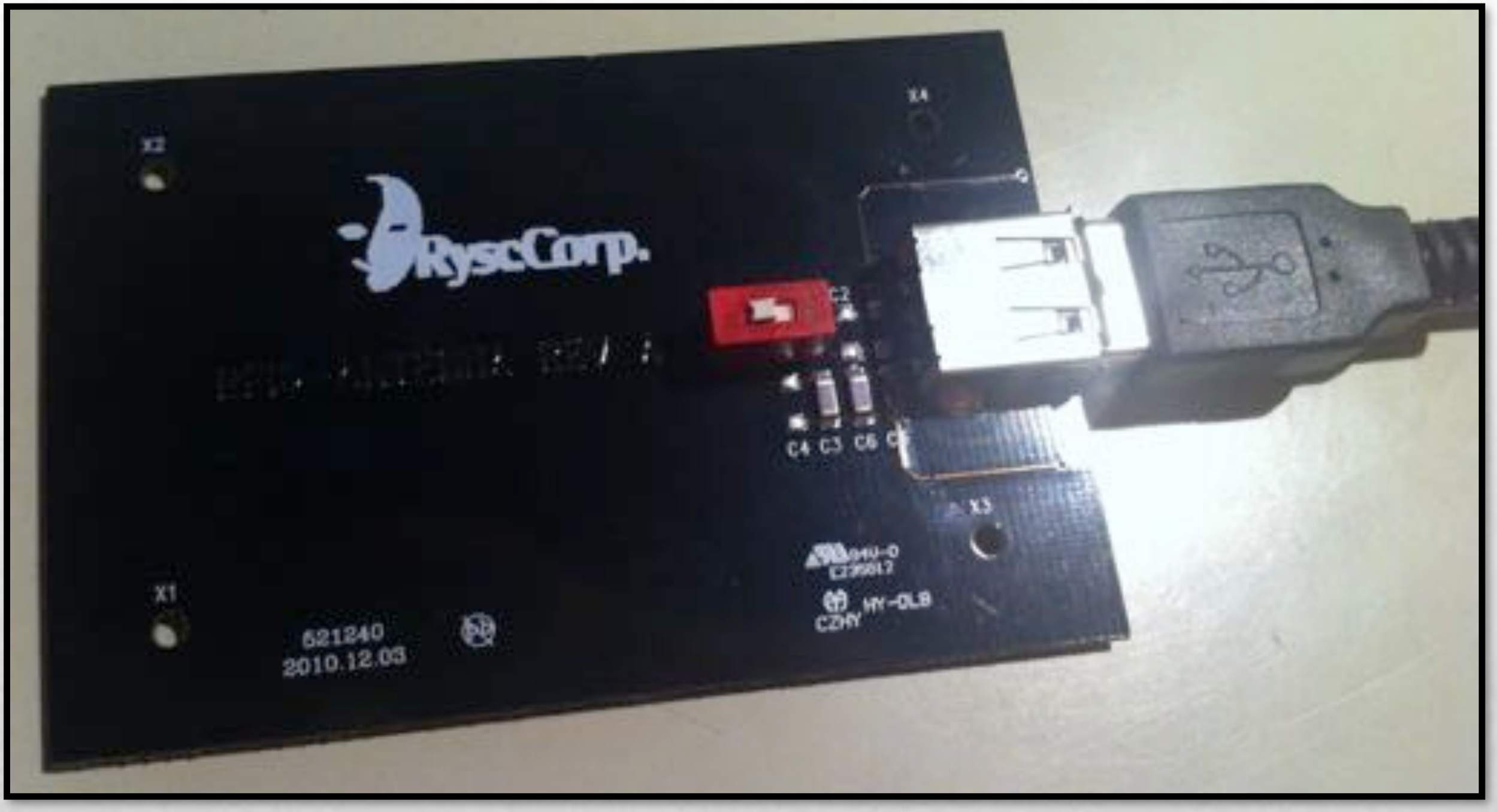
Proxmark3

Low Freq Antenna

http://proxmark3.com/

Proxmark3

Hi Freq Antenna



http://proxmark3.com/

Proxmark3

Board
Chinese “Easy V3”

Y HAY MÁS!!!!!


KASPER OSWALD
Embedded Security Engineering
SMART COSMOS

ALGUNOS ATAQUES!

Y QUÉ ES **EMULAR**?
Y *CLONAR*?

PUEDO EMULAR Y CLONAR TODO ENTONCES CHE??????

PARA **EMULAR** DEBERÍA REPRODUCIR EL MISMO COMPORTAMIENTO DESDE OTRA PIEZA DE HARDWARE. MOSTRAR **VIDEOS!**

PARA **CLONAR** -OPCIONES-:

A) UNA TARJETA "VIRGEN"

B) UNA TARJETA "VIRGEN ESPECIAL"

C) TARJETAS TIPO T55X7 O Q5

Mifare Classic

MIFARE is a trademark of **NXP Semiconductors**.

Became the most successful platform within the automatic fare collection industry.

MIFARE Classic 1K is primarily used in closed systems as fixed value tickets (e.g. weekly or monthly travel passes) or as tickets where **value is extracted from the card** by the service provider.

- ✓ Automatic Fare Collection & Micropayments
- ✓ Access Management
- ✓ Student Cards
- ✓ Loyalty Cards
- ✓ Road Tolling & Parking
- ✓ Event Ticketing
- ✓ Membership Cards & Points to exchange for prizes

Mifare Classic memory

Sector	Block	Byte Number within a Block 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Description
15	3	Key A						Access Bits				Key B						Sector Trailer 15
	2																	Data
	1																	Data
	0																	Data
14	3	Key A						Access Bits				Key B						Sector Trailer 14
	2																	Data
	1																	Data
	0																	Data
:	:																	
:	:																	
:	:																	
1	3	Key A						Access Bits				Key B						Sector Trailer 1
	2																	Data
	1																	Data
	0																	Data
0	3	Key A						Access Bits				Key B						Sector Trailer 0
	2																	Data
	1																	Data
	0																	Manufacturer Block

Mifare Classic

Well-known attacks...

1. Sniff a valid trace (Proxmark!) and use **Crapto1**
2. Default keys? Got one key? Get the others! – **Nested**! (mfoc)
3. No default keys? Get a key! - **DarkSide attack** (mfcuk)
4. Any legit reader in the neighborhood? **Reader-Only attack**

Full Disclosure

OV-Chipkaart.me
Hackers website voor de OV-Chipkaart

In March 2008 the Digital Security research group of the **Radboud University Nijmegen** made public that they performed a complete reverse-engineering and were able to clone and manipulate the contents of a **OV-Chipkaart** (The Netherlands) which is a MIFARE Classic card.

October 2011 the company **TLS**, responsible for the OV-Chipkaart announced that the new version of the card will be better protected against fraud

Full Disclosure

The researchers say their security flaw can be used to copy cards. They claim to have even been able to adjust the amount of credit stored on a pre-pay card.

Shashi Verma, director of fares and ticketing at Transport For London, told the BBC **its system spotted the security breach**.

"We knew about it before we were informed by the students," said Mr Verma

He stressed that the Mifare Classic chip in the Oyster card is **only part of a larger system**. "A number of forensic controls run within the back office systems which is something that customers and these students have no ability to touch."

"We will carry on making improvements to the security of the Oyster system."

Use Case

Buenos Aires, Argentina, using Mifare 1K

Often used as a piece of evidence…

There is a lot of information that you can check in Gov's RFP's ;)

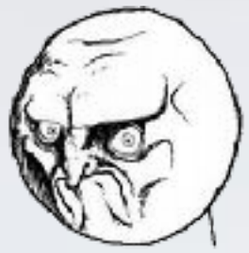
Use Case

Buenos Aires, Argentina, using Mifare 1K

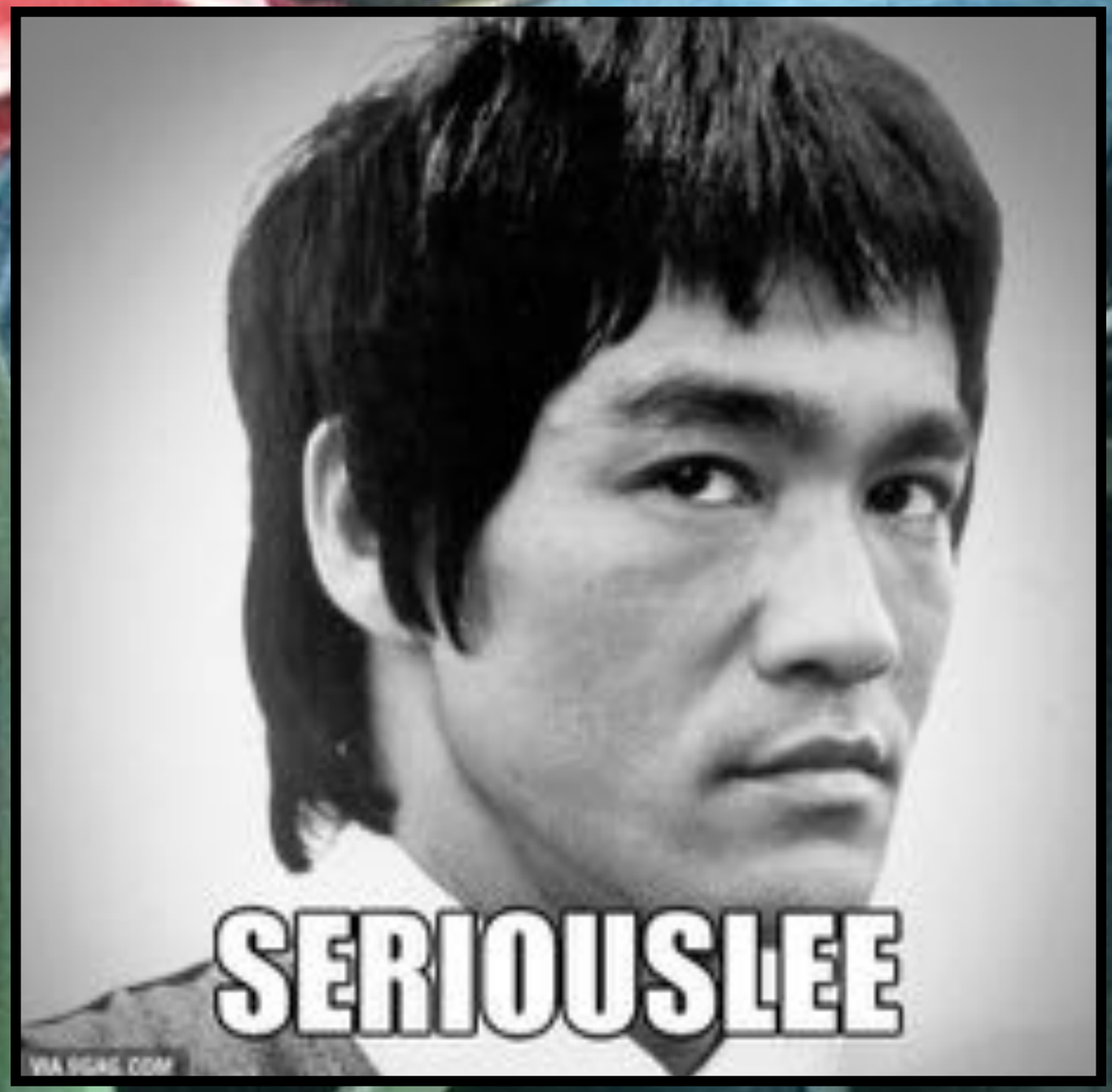
RFID Pedestrian Barriers Tripod Turnstile

CONCLUSIONES Y PENSAMIENTOS…

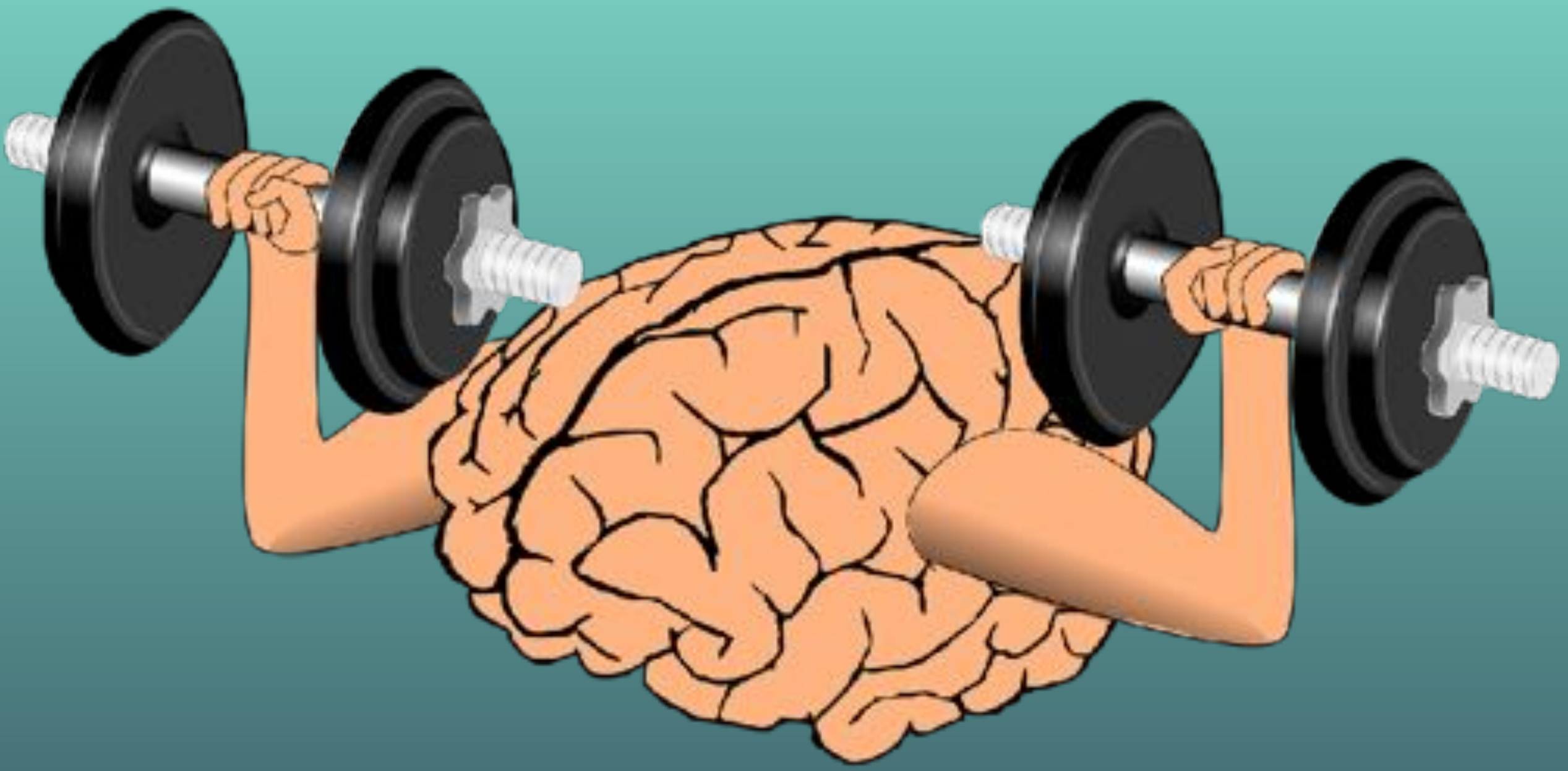
- Dale cargame la SUBE



- NFC es seguro porque es "de campos cercanos"?
- Muchos tipos de sistemas e implementaciones
- Y con los Pasaportes y Tarjetas de Crédito!?
- Hay mucho por aprender! LENGUAJES, OS, ELECTRÓNICA!, UNICORNIOS…
- Ser curioso y autodidacta es lo principal!
- Pensar como el atacante!
- Además, es divertido romper cositas! ¿o no? ;)


SERIOUSLEE
VIA 9GAG.COM

#HaganLío



DUDAS? COMENTARIOS? SENSACIONES?

RFID/NFC

. . . A QUICK TOUR . . .

OWASP
PATAGONIA

Cinta Infinita
Information Security