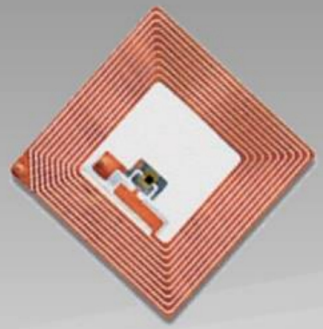
RFID Insecurity

陈 华 江

Kevin2600@gmail.com



XCon2011 安全焦点信息安全技术峰会

Legal Disclaimer

All my actions have been authorized by related College and Company.

I do not take any responsibilities for any public misuse of any type of RFID system in People's Republic of China.

This presentation is only for a research purpose. Not a manual that can be misused for committing crimes.

WHO AM I ?

Fans of open source software/hardware

Gain my degree at Dundalk I.T Ireland

BLOG: http://hi.baidu.com/kevin2600

2002-2011

Beijing

The 10th

Why you here ?

1）RFID History & Security ;

2）RFID Proxmark3 Introduction & Usage ;

3）Breaking Mifare classic;

4）Mifare classic Data analysis;

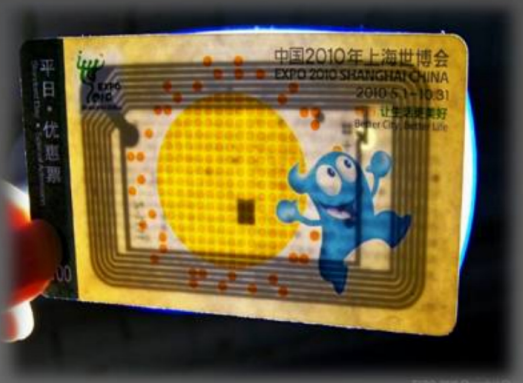
5）RFID System Design Conclusion.

2002-2011

Beijing

The 10th

RFID are everywhere



2002-2011

Beijing

The 10th

RFID（Radio Frequency ID）

Two major tag types:

- **Passive: No internal power source or transmitter, shorter range**
- **Active: Power source (battery) and transmitter, longer range**

RFID (Frequency Ranges)

2002-2011

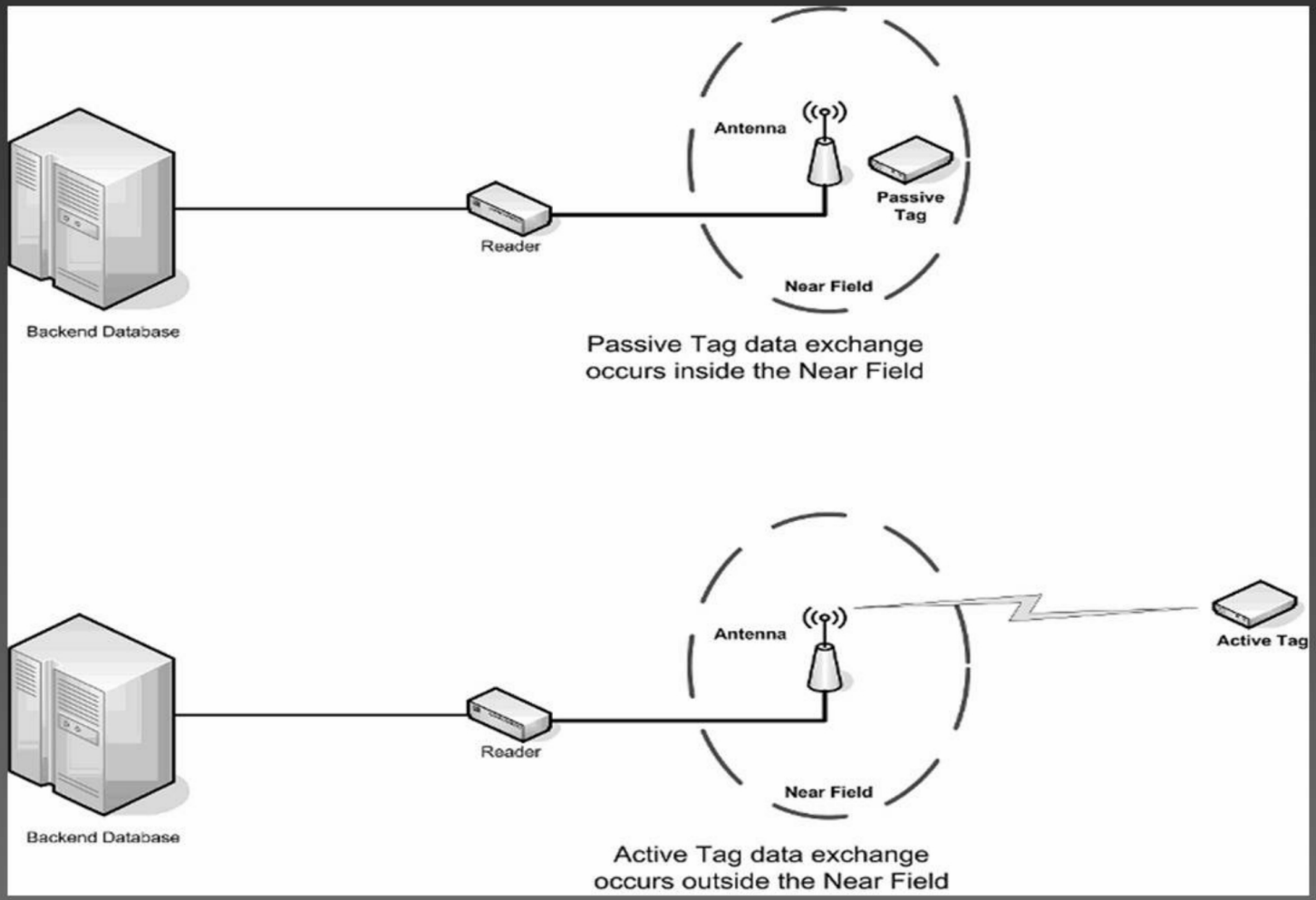
Beijing

The 10th

Different types of RFID transponders

Short range	Mid range	Long range
<= 15 centimeter	<= 5meter	Up to 500 meter
ISO 14443 A+B	ISO 15693	ISO 18000-xx
13.56 MHz, 125-134.2kHz	13.56 MHz, 125-135kHz	860-956 MHz (UHF) 2.4 GHz (Microwave) 5.8 GHz (Microwave)
E-field, magnetic field	EM-field	EM-field

RFID (System layout）



Philips NXP Mifare series

The most popular RFID Card types (Mifare Ultralight; Mifare Classic; DESFire). Use ISO 14443A & operating on 13.56mhz. Mifare Classic series 1K; 4K.

Mifare classic has been implemented in many types RFID systems around the world. Bus tickets; Access contorl etc.. The cryptographic oprations it can Perform, are implemented in Hardware, using “Linear feedback shift register (LFSR)” The algorithm called Crypto1.

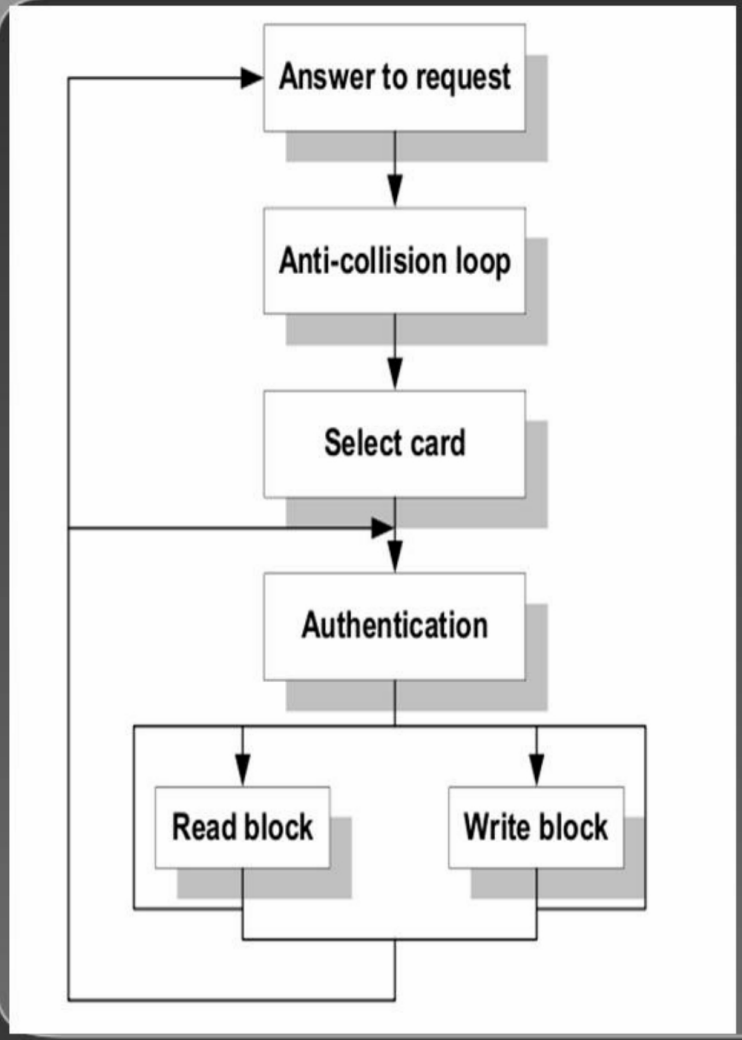
However, in year 2007, Karsten Nohl from CCC, has cracked the "Crypto 1“, by analyzed on chip directly. In Year 2008, researchers and students from Radboud University Netherlands, has also found weakness of Mifare classic protocol.

2002-2011

Beijing

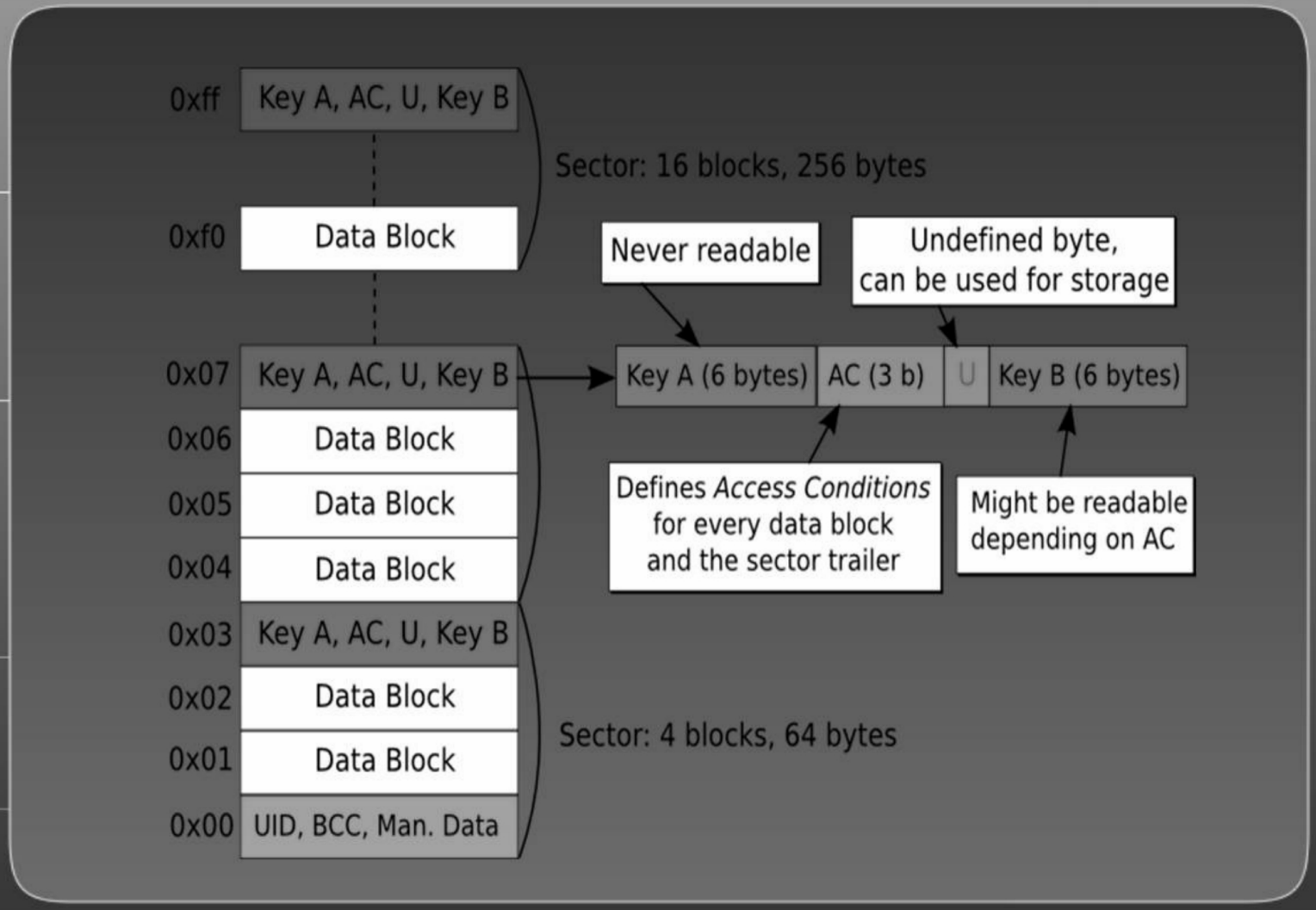
The 10th

Mifare Classic Access method




```
+  30402:    :     26
+     66:   0: TAG 04  00
+    854:    :     93  20
+     64:   0: TAG 1c  39  2e  d1  da
+   2367:    :     93  70  1c  39  2e  d1  da  69  83
+     64:   0: TAG 08  b6  dd
+  13439:    :     60  00  f5  7b
+     88:   0: TAG 91  08  e3  b3
+    976:    :     23  39  a2  7b  1e  60  fa  fd     !c
+     64:   0: TAG f0  ce! 84  39!
+   6990:    :     00  f5  e9  87     !crc
+     66:   0: TAG 3f! ab  19! f5  08! 4f  e4  f1  63! 8
+  13253:    :     af  ad  16  a7     !crc
+     88:   0: TAG 06! f0! c1  b4
+    977:    :     ad  6d  8d  63  83  13  ae  af     !c
+     64:   0: TAG 08  57! 96  4e!
+   6742:    :     11  41  21  7e     !crc
+     64:   0: TAG 1f! 46  21! 51! d6! 78! 23  b5! b8! 3
+  13150:    :     2c  fd  47  4e     !crc
+     90:   0: TAG f5! 6b  f2  93
+    974:    :     8c  09  69  03  d1  c1  d6  ac     !c
+     66:   0: TAG ae! cf  89! 42!
+   7598:    :     ed  48  74  b2     !crc
+     64:   0: TAG c5  40! 4a! 22  04! fe  0d! 00! 99  e
+  13102:    :     44  38  fe  da     !crc
+     88:   0: TAG 7e! df! 1a! b5
+    977:    :     ec  ea  ad  5a  be  da  46  0d     !c
+     64:   0: TAG 34  c4  97! 39
```

Mifare Classic Data structures 1



Mifare Classic Data structures 2

2002-2011

Beijing

The 10th

Why you here ?

1）RFID History & Security ;

2）RFID Proxmark3 Introduction & Usage ;

3）Breaking Mifare classic;

4）Mifare classic Data analysis;

5）RFID System Design Conclusion.

RFID Swiss knife Proxmark3

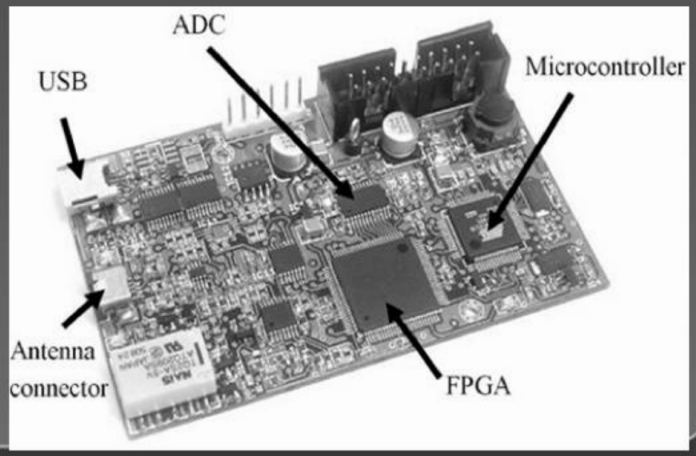
The Proxmark III is the most powerful open source device available for performing RFID research, designed by Jonathan Westhues.

Can be use for reading; Sniff and emulate High and low frequency tags, almost behind every RFID security research projects.

RFID Swiss knife Proxmark3

- CPU : ARM, 256kB of flash memory, 64kB of RAM
- FPGA : Xilinx Spartan-II
- Two independent RF circuits, HF and LF
- Power : through USB port
- Connectivity : mini-USB port
- User interface : one button, four LEDs.

- Fully open-source design, both HW and SW



Proxmark3 HF Antenna DIY

PCB Made HF Antenna costs 59 dollar online. But we can build one for only 2.50 EU, use a Hirose USB cable.

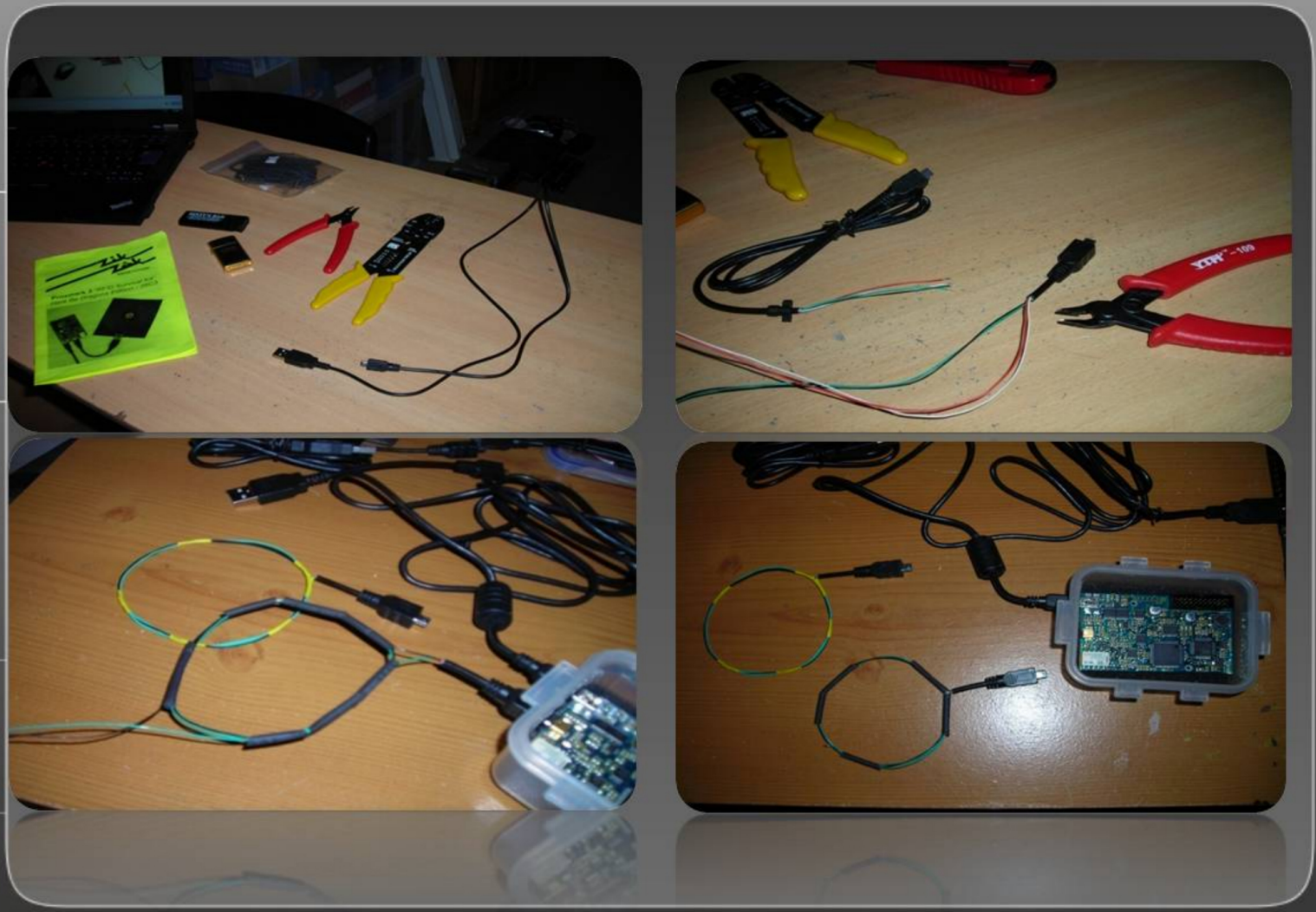
```
proxmark3> tune
> tune
#db# Measuring antenna characteristics, please wait.
proxmark3>

# LF antenna:  0.00 V @   125.00 kHz
# LF antenna:  0.00 V @   134.00 kHz
# LF optimal:  0.00 V @ 12000.00 kHz
# HF antenna:  8.35 V @    13.56 MHz
# Your LF antenna is unusable.
proxmark3> tune
> tune
#db# Measuring antenna characteristics, please wait.
proxmark3>

# LF antenna:  0.00 V @   125.00 kHz
# LF antenna:  0.13 V @   134.00 kHz
# LF optimal:  0.00 V @ 12000.00 kHz
# HF antenna: 12.05 V @    13.56 MHz
# Your LF antenna is unusable.
```

2002-2011

Beijing

The 10th

Proxmark3 HF Antenna DIY



2002-2011

Beijing

The 10th

Now What ?

Frequency determine 125khz or 13.56mhz ?

```
proxmark3> tune
> tune
#db# Measuring antenna characteristics, please wait.
proxmark3>

# LF antenna:  0.00 V @   125.00 kHz
# LF antenna:  0.00 V @   134.00 kHz
# LF optimal:  0.00 V @ 12000.00 kHz
# HF antenna:  8.35 V @    13.56 MHz
# Your LF antenna is unusable.
proxmark3> tune
> tune
#db# Measuring antenna characteristics, please wait.
proxmark3>

# LF antenna:  0.00 V @   125.00 kHz
# LF antenna:  0.13 V @   134.00 kHz
# LF optimal:  0.00 V @ 12000.00 kHz
# HF antenna: 12.05 V @    13.56 MHz
# Your LF antenna is unusable.
```

Proxmark3 VS HID Proxcard2

“HID 在非接触式门禁卡市场占据主导地位，在全球的用户超过 2 亿，公司在全球享有盛誉。 HID 感应卡被认为是物理门禁的业界标准。 采用 125 kHz RFID 技术的 HID prox 产品可靠，价格适中，可以无缝集成到门禁” -- 广告摘取自Internet

Proxmark3 VS HID Proxcard2

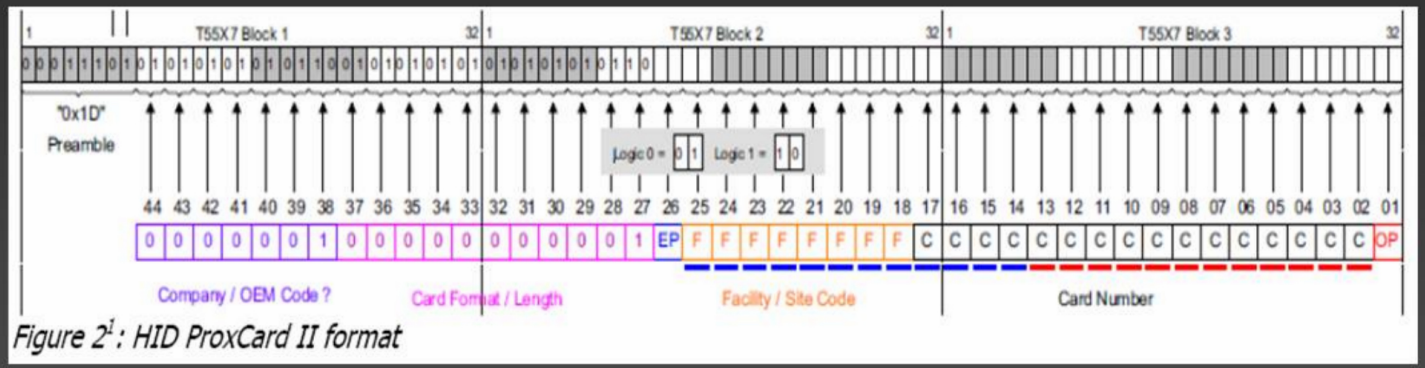


Figure 2[1]: HID ProxCard II format

The passive card simply stores a 44bit value which is read then sent to the backend systems which decides whether or not that value has access to the specific door the tag was presented at. If it does, the system triggers the door to open and the card holder gains access. This 44 bit value is split up in a number of different fields. The most important fields are the facility or site code, and the actual card number.

Of this 44-bit value, only 26-bits are actually used to identify the card holder and so if you're able to obtain that value, then you'll be able to impersonate that user. Additionally it should be noted that no authentication, encryption, or any other real security mechanism is used to protect the card's value or to validate the card to the reader, all that's there is a 26-bit value.

Proxmark3 VS HID Proxcard2

ProxBrute is simply a modification to the available firmware of the proxmark3. It enable functionality so that one can capture a valid card and using the facility/site code from that card brute force another valid card number.

let's say you're able to read one person's card and have the ability to access a common area, but need to access a more privileged area. You can use ProxBrute to read a user's card, then brute force another valid tag ID.

Proxmark3 VS HID Proxcard2

```
#db# [ProxBrute] In Mode Red, Copying read tag to Ora
#db# Playing
#db# Red is lit, not entering ProxBrute Mode
#db# 0 950 14720127
#db# Stopped
#db# Done playing
#db# Playing
#db# Entering ProxBrute Mode
#db# brad a. - foundstone
#db# Current Tag: Selected = 1 Facility = 00000950 ID
#db# Trying Facility = 00000950 ID 14720126
#db# Stopped
#db# Trying Facility = 00000950 ID 14720125
#db# Stopped
#db# Trying Facility = 00000950 ID 14720124
#db# Stopped
#db# Trying Facility = 00000950 ID 14720123
#db# Stopped
#db# Trying Facility = 00000950 ID 14720122
#db# Trying Facility = 00000950 ID 14720121
#db# Stopped
#db# Trying Facility = 00000950 ID 14720120
#db# Stopped
#db# Trying Facility = 00000950 ID 1472011f
#db# Stopped
```

2002-2011

Beijing

The 10th

Why you here ?

1）RFID History & Security ;

2）RFID Proxmark3 Introduction & Usage ;

3）Breaking Mifare classic;

4）Mifare classic Data analysis;

5）RFID System Design Conclusion.

Mifare-Classic-Mistakes

- Mifare Classic's KeyA length only 48bits. Brute-force attack? PC 3 years; FPGA days…
- There are "Default keys" left behind in the developers datasheet (Somehow, developers often forget to change). → Nested Attack
- Once we cracked KEYS, we able to clone 99% of contents into another blank cards, except the Sector 0. However, we can use Proxmark3 to emulate one (include sector 0)

ffffffffff	a0a1a2a3a4a5
D3f7d3f7d3f7	aabbccddeeff
b0b1b2b3b4b5	000000000000
4d3a99c351dd	1a982c7e459a

Breaking Mifare Classic – 3 PASS authentication 1

1: The reader accessed the sector use Key A or Key B

2: After reads KEY & AC. The tag sends Nonce AS challenge.

3: Reader response using KEY & AC, also the Nonce challenge.

4: The card verifies the response & challenge, and then send it own response.

5: The reader verifies the tag response with its own Challenge

Breaking Mifare Classic – 3 PASS authentication 2

- Reader: 26: Request, Any tag out there ?
- Tag: 04 00: Hello! Here I am!
- Reader: 93 20: Select card, Anti-Collisions
- Tag: Here is my UID
- Reader: 93 70 UID
- TAG: 08 b6 dd: Type Mifare classic

- 3 Pass Authentication

- Reader: 60 00 f5 7b: 60 KeyA: 61 KeyB.

- TAG: 91 08 e3 b3: Nonce Tag

- Reader: 23 39 a2 7b: Nonce Reader
- Reader: 1e 60 fa fd : Answer Reader

- Tag: f0 ce 84 39

```
+  40452:     :      26
+     64:    0: TAG 04  00
+    855:     :      93  20
+     64:    0: TAG 1c  39  2e  d1  da
+   2366:     :      93  70  1c  39  2e  d1  da  69  83
+     66:    0: TAG 08  b6  dd
+  30402:     :      26
+     66:    0: TAG 04  00
+    854:     :      93  20
+     64:    0: TAG 1c  39  2e  d1  da
+   2367:     :      93  70  1c  39  2e  d1  da  69  83
+     64:    0: TAG 08  b6  dd
+  13439:     :      60  00  f5  7b
+     88:    0: TAG 91  08  e3  b3
+    976:     :      23  39  a2  7b  1e  60  fa  fd     !crc
+     64:    0: TAG f0  ce! 84  39!
```

2002-2011

Beijing

The 10th

Breaking Mifare Classic –Proxmark3 Sniffing Demo 1

2002-2011

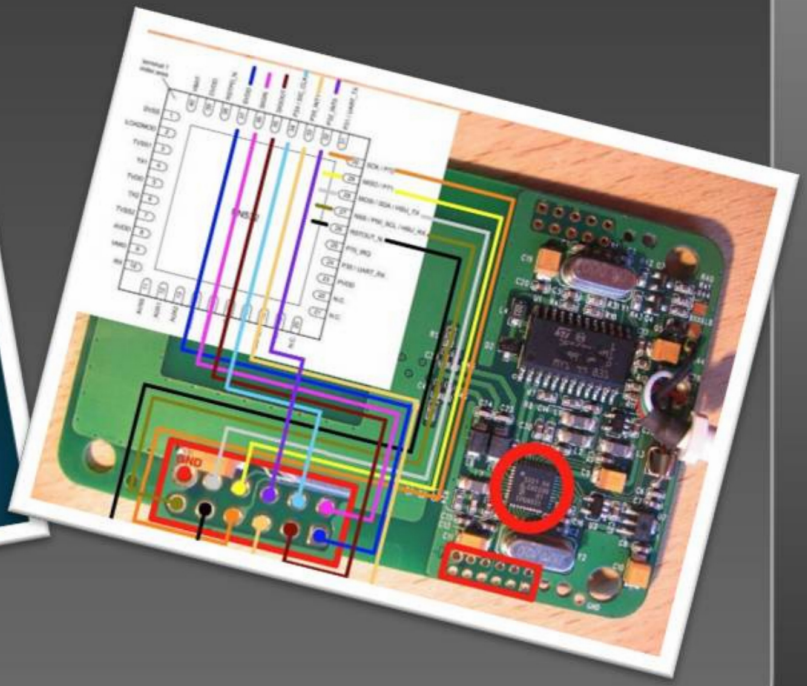
Beijing

The 10th

(Live demo Proxmark3 Sniffing)

Breaking Mifare Classic -- Hardware

Touchatag Reader (PN532 Chipset)



Breaking Mifare Classic-- Software

RFIDiot (http://rfidiot.org/)
python library for reading/writing/ RFID cards

LIBNFC (http://www.libnfc.org/)
libnfc is a library for communicating with ISO14443 RFID tags. libnfc works with NXP PN53x series chipsets

NFC Tools
- MFOC (Mifare Classic Offline Cracker)
- MFCUK (Mifare Classic Key Recovery - "Dark Side)
- NFC-MFClassic (Dumping data into other cards)

Breaking Mifare Classic– Demo 2

(Live Demo & touchatag)

CASE STUDY — DKIT Student card (Default keys !)

2002-2011

Beijing

The 10th

```
[Key: d3f7d3f7d3f7]  -> [x.xxxxxxxxxxxx]
[Key: 000000000000]  -> [x.xxxxxxxxxxxx]
[Key: b0b1b2b3b4b5]  -> [x.xxxxxxxxxxxx]
[Key: 4d3a99c351dd]  -> [x.xxxxxxxxxxxx]
[Key: 1a982c7e459a]  -> [x.xxxxxxxxxxxx]
[Key: aabbccddeeff]  -> [x.xxxxxxxxxxxx]
[Key: 714c5c886e97]  -> [x.xxxxxxxxxxxx]
[Key: 587ee5f9350f]  -> [x.xxxxxxxxxxxx]
[Key: a0478cc39091]  -> [x.xxxxxxxxxxxx]
[Key: 533cb6c723f6]  -> [x.xxxxxxxxxxxx]
[Key: 8fd0a4f256e9]  -> [x.xxxxxxxxxxxx]

Sector 00 -  FOUND_KEY    [A]  Sector 00 -  UNKNOWN_KEY [B]
Sector 01 -  UNKNOWN_KEY  [A]  Sector 01 -  UNKNOWN_KEY [B]
Sector 02 -  FOUND_KEY    [A]  Sector 02 -  UNKNOWN_KEY [B]
Sector 03 -  FOUND_KEY    [A]  Sector 03 -  FOUND_KEY    [B]
Sector 04 -  FOUND_KEY    [A]  Sector 04 -  FOUND_KEY    [B]
Sector 05 -  FOUND_KEY    [A]  Sector 05 -  FOUND_KEY    [B]
Sector 06 -  FOUND_KEY    [A]  Sector 06 -  FOUND_KEY    [B]
Sector 07 -  FOUND_KEY    [A]  Sector 07 -  FOUND_KEY    [B]
Sector 08 -  FOUND_KEY    [A]  Sector 08 -  FOUND_KEY    [B]
Sector 09 -  FOUND_KEY    [A]  Sector 09 -  FOUND_KEY    [B]
Sector 10 -  FOUND_KEY    [A]  Sector 10 -  FOUND_KEY    [B]
Sector 11 -  FOUND_KEY    [A]  Sector 11 -  FOUND_KEY    [B]
Sector 12 -  FOUND_KEY    [A]  Sector 12 -  FOUND_KEY    [B]
Sector 13 -  FOUND_KEY    [A]  Sector 13 -  FOUND_KEY    [B]
Sector 14 -  FOUND_KEY    [A]  Sector 14 -  FOUND_KEY    [B]
Sector 15 -  FOUND_KEY    [A]  Sector 15 -  FOUND_KEY    [B]


Using sector 00 as an exploit sector
Sector: 1, type A, probe 0, distance 21837 .....
Found Key: A [5017faeb6544]
Sector: 0, type B, probe 0, distance 21837 .....
Sector: 0, type B, probe 1, distance 21797 .....
```

Why you here ?

1）RFID History & Security ;

2）RFID Proxmark3 Introduction & Usage ;

3）Breaking Mifare classic;

4）Mifare classic Data analysis;

5）RFID System Design Conclusion.

2002-2011

Beijing

The 10th

Raw data investigate -- DKIT Student card

Cracking Mifare classic keys, is only 1st step of break down entire RFID system.

Is this RFID system operated online or offline?

Option 1: Use UID? Not able to clone entirely, But can be emulated use PM3.

Option 2: Use Card number? Very easy to dump to a blank card. User detail abused.

2002-2011

Beijing

The 10th

Breaking Mifare Classic – Emulate UID Demo 3

(Emulate UID Live demo)

Raw data investigate -- DKIT Student card

2002-2011

Beijing

The 10th

Raw data investigate -- DKIT Student card Demo 4

(Clone student card VIDEO DEMO)

2002-2011

Beijing

The 10th

Raw data investigate – Water-Card– Clone Demo 5

(Water card Clone: Video Demo)

2002-2011

Beijing

The 10th

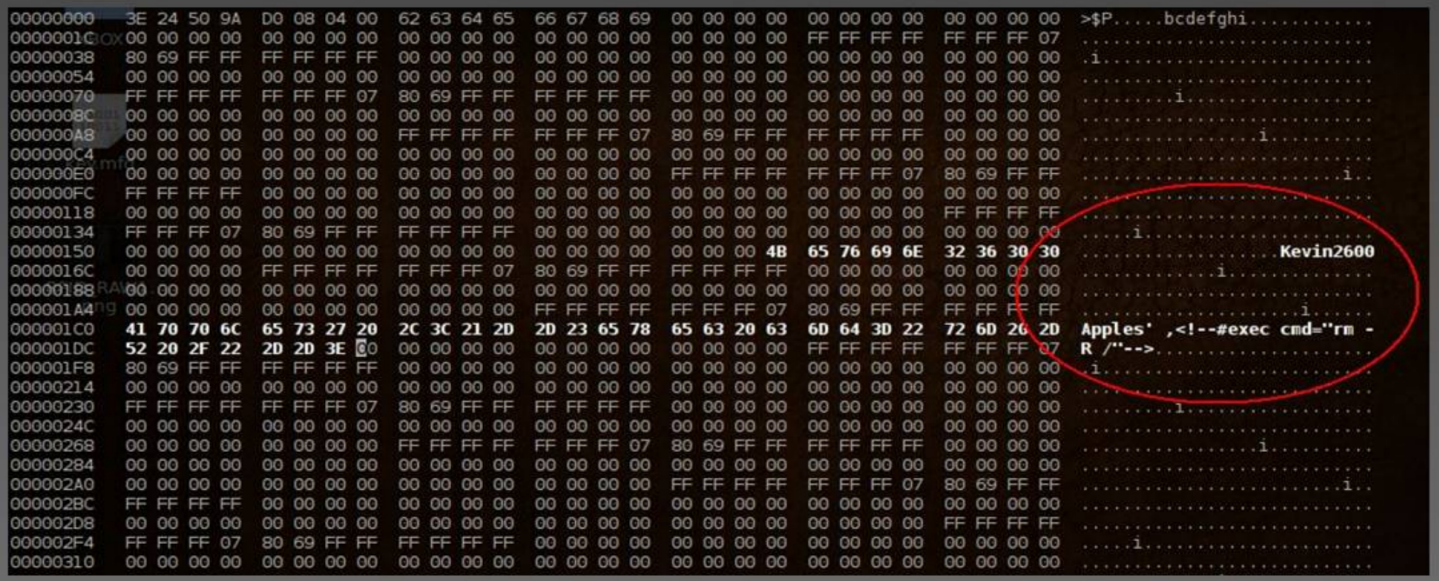
Raw data investigate -- SQL Injection?

Old stuff New use → Select id from Staff where id = '$value'

SQL Inject → '1' ='1 OR 1f:31:1f:20:3d:1f:31:20:20

OR 72:6d:20:2d:72:20 !?

More details → www.rfidvirus.org



Why you here ?

1）RFID History & Security ;

2）RFID Proxmark3 Introduction & Usage ;

3）Breaking Mifare classic;

4）Mifare classic Data analysis;

5）RFID System Design Conclusion.

Conclusion

HID Proxcard2 access card -- replace it ASAP.

Mifare classic -- Extending a Mifare classic to public payment system is a very bad idea. Use strong cryptography instead (Mifare DESfire, CPU card).

Keep in mind: Security by obscurity really doesn't work!!!

What's Next?

There are many more RFID & Others to play with ....

- Some high class car keys (Hitag2?)
- Research on GSM Network with USRP?

Links

http://www.libnfc.org/

http://hi.baidu.com/kevin2600

http://code.google.com/p/proxmark3/

THANK YOU ……

Kevin2600@gmail.com

XCon2011 安全焦点信息安全技术峰会