Contents: [Dobrica PavlinuÅ¡iÄ 's random unstructured stuff]

Cheap(er) China Proxmark

- http://www.xfpga.com/e_products/?big_id=17&small_id=7
- http://www.proxmark.org/forum/viewtopic.php?id=863

Mifare sniff/crack

http://code.google.com/p/crapto1/

http://www.youtube.com/watch?v=kTvb7tjbSTI
http://www.fuzzysecurity.com/tutorials/rfid/3.html

Proxmark firmware comparison on emulated Mifare 4k

r	command	note
590		USB HID
	hf mf rdbl 0 A a0a1a2a3a4a5	OK
	hf mf chk 0 A a0a1a2a3a4a5	Can't select card
617		USB HID
	hf mf rdbl 0 A a0a1a2a3a4a5	OK
	hf mf chk 0 A a0a1a2a3a4a5	Can't select card
	hf mf mifare	2 red, needs power cycle
	hf mf nested o 0 a a0a1a2a3a4a5 4 t	Can't select card
672		proxendian.h:22:4: error: #error Define BYTE_ORDER
756		USB CCID
	hf mf rdbl 0 A a0a1a2a3a4a5	Auth error
	hf mf chk 0 A a0a1a2a3a4a5	Can't select card
	hf mf mifare	red, yellow, red, needs power cycle
	hf mf nested o 0 a a0a1a2a3a4a5 4 t	Can't select card
840		latest

cell=0x9f55348 [16,0] cell=0x9f55488 [16,1]	hf mf rdbl 0 A a0a1a2a3a4a5	cell=0x9f55700 [16,2] Can't select card
cell=0x9f55508 [17,0] cell=0x9f55a00 [17,1]	hf mf chk 0 A a0a1a2a3a4a5	cell=0x9f55c78 [17,2] Can't select card
cell=0x9f55a38 [18,0] cell=0x9f55f78 [18,1]	hf mf mifare	cell=0x9f560f8 [18,2] Can't select card
cell=0x9f562b8 [19,0] cell=0x9f563f8 [19,1]	hf mf nested o 0 a a0a1a2a3a4a5 4 t	cell=0x9f56760 [19,2] Can't select card

Usage

```
proxmark3> hw version
#db# Prox/RFID mark3 RFID instrument
#db# bootrom: svn 816 2013-10-11 22:09:42
#db# os: svn 816 2013-10-11 22:09:43
#db# FPGA image built on 2012/ 1/ 6 at 15:27:56
uC: AT91SAM7S256 Rev B
Embedded Processor: ARM7TDMI
Nonvolatile Program Memory Size: 256K bytes
Second Nonvolatile Program Memory Size: None
Internal SRAM Size: 64K bytes
Architecture Identifier: AT91SAM7Sxx Series
Nonvolatile Program Memory Type: Embedded Flash Memory

proxmark3> hw tune
#db# Measuring antenna characteristics, please wait...
#db# Measuring complete, sending report back to host

# 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:  7.28 V @    13.56 MHz
# Your LF antenna is unusable.

proxmark3> hf 14a read
ATQA : 02 00
 UID : ?? ?? ?? ??
 SAK : 38 [1]
TYPE : Nokia 6212 or 6131 MIFARE CLASSIC 4K
 ATS : 0d 78 f7 b1 02 4a 43 4f 50 76 32 34 31 27 cc
       -  TL : length is 13 bytes
       -  T0 : TA1 is present, TB1 is present, TC1 is present, FSCI is 8
       - TA1 : different divisors are NOT supported, DR: [2, 4, 8], DS: [2, 4, 8]
       - TB1 : SFGI = 0, FWI = 8
       - TC1 : NAD is NOT supported, CID is supported
       -  HB : 4a 43 4f 50 76 32 34 31
```

brute force 26-bit proxcard

- https://github.com/brad-anton/proxbrute

firmware version

According to
http://wiki.radiowar.org/Proxmark3%E5%9B%BA%E4%BB%B6%E5%88%97%E8%A1%A8
firmwares newer than 617 have problems.

Google translated version

> Please do not upgrade your firmware to the CDC Proxmark3 version r617 ~ r830 driver's! We found that because the problem will lead to Proxmark3 code appears unable to identify high-frequency card, and 816 will appear after Nested number of keys for 000000000000.

flashing update

```
dpavlin@blue:/blue-zfs/FPGA/proxmark/proxmark3$ make flash-all
```

Compile new version of firmware

All instructions below this are for old version of software see
http://www.proxmark.org/forum/viewtopic.php?id=1668

http://code.google.com/p/proxmark3/wiki/Compiling je strgan
http://www.proxmark.org/forum/post/3244/#p3244

```
sudo apt-get install build-essential libreadline5 libreadline-dev libusb-0.1-4 libusb-dev libqt4-

dpavlin@t61p:/tank/proxmark3$ svn co http://proxmark3.googlecode.com/svn/trunk proxmark3
```

Boot loader

```
dpavlin@t61p:/tank/proxmark3/proxmark3$ ./client/flasher -b ./bootrom/obj/bootrom.elf
Loading ELF file './bootrom/obj/bootrom.elf'...
Loading usable ELF segments:
0: V 0x00100000 P 0x00100000 (0x00000200->0x00000200) [R X] @0x94
1: V 0x00200000 P 0x00100200 (0x000017a8->0x000017a8) [R X] @0x294

Waiting for Proxmark to appear on USB...
Connected units:
        1. SN: ? [004/013]
 Found.
Entering bootloader...
(Press and release the button only to abort)
Waiting for Proxmark to reappear on USB....
Connected units:
        1. SN: ? [004/014]
 Found.

Flashing...
Writing segments for file: ./bootrom/obj/bootrom.elf
 0x00100000..0x001001ff [0x200 / 2 blocks].. OK
 0x00100200..0x001019a7 [0x17a8 / 24 blocks]......................... OK

Resetting hardware...
All done.
```

```
Have a nice day!


^


dpavlin@t61p:/tank/proxmark3/proxmark3$ ./client/flasher ./armsrc/obj/fullimage.elf
Loading ELF file './armsrc/obj/fullimage.elf'...
Loading usable ELF segments:
0: V 0x00102000 P 0x00102000 (0x0000a4bc->0x0000a4bc) [R  ] @0xb4
1: V 0x00110000 P 0x00110000 (0x0000ba8c->0x0000ba8c) [R X] @0xa570
2: V 0x00200000 P 0x0011ba8c (0x00000004->0x00000004) [RW ] @0x15ffc
Note: Extending previous segment from 0xba8c to 0xba90 bytes

Waiting for Proxmark to appear on USB...
Connected units:
        1. SN: ? [004/015]
 Found.
Entering bootloader...
(Press and release the button only to abort)
Waiting for Proxmark to reappear on USB....
Connected units:
        1. SN: ChangeMe [004/016]
 Found.

Flashing...
Writing segments for file: ./armsrc/obj/fullimage.elf
 0x00102000..0x0010c4bb [0xa4bc / 165 blocks].....................................................
 0x00110000..0x0011ba8f [0xba90 / 187 blocks].....................................................

Resetting hardware...
All done.

Have a nice day!
```