Instructions for use

This card uses private commands to modify internal data. The data supported for modification are:

- ATQA modification

The user can customize ATQA with a length of two bytes, which is the opposite of the result read by Pm3. It should be noted that if the card byte length> 4 bytes, then it must be 004X (Pm3 order)

- SAK modification

Users can customize SAK, one byte

hf 14a raw -s -c -t 1000 cf0000000035<ATQA><SAK>

*ATQA may be reversed on Pm3

Example: hf 14a raw -s -c -t 1000 cf0000000035440028

Modify ATQA=00 44 SAK=28 (note that ATQA on Pm3 is reversed)

- ATS modification

The user can customize the ATS of any length, or not open the ATS. It should be noted that when SAK=20,28, ATS must be turned on, otherwise the card will not be recognized!

Set up ATS:

hf 14a raw -s -c -t 1000 cf0000000034<length><ATS>

*The length is set to 0, which means that ATS is not sent

*When SAK is 20 or 28, ATS must be set, otherwise the card cannot be read

*The last two digits of ATS are CRC and cannot be counted as length

Example: hf 14a raw -s -c -t 1000 cf000000003406067577810280

Modify ATS to 0606757781028002F0

- Byte length modification

Users can switch between 4, 7, and 10 byte lengths at will

hf 14a raw -s -c -t 1000 cf0000000068<Param>

Param=00: 4 bytes 01: 7 bytes 02: 10 bytes

Example: hf 14a raw -s -c -t 1000 cf000000006801

Modify the card number length to 7 bytes

- 14443A/B-UID modification

Modifying block 0 in area 0 means modifying the UID of the card. It should be noted that this area cannot be read and written by password, and must be written through backdoor instructions! See below for details: Read and write any block

- Ultralight protocol switch

Turning on this switch allows to read and write each block without a password. In this mode, if SAK=00 ATQA=0044 (Pm3 sequence), it can become an Ultralight card

Set Ultralight mode

hf 14a raw -s -c -t 1000 cf0000000069<00>

01: UL agreement opened

00: UL agreement closed

- Rolling code restore switch

This mode is divided into four states: off (pre-write), on (on restore), don't care, and high-speed read and write. If you don't need it, please set it to "don't care" to avoid affecting performance. If you use it, please enter the pre-write mode first. At this time, write the full card data. After writing, set it to on. At this time, after writing the data, the first time you read the data just written, the next time you read It is the pre-written data. All modes support this operation. It should be noted that using any block to read and write in this mode may give wrong results.

If it is an Ultralight card, in order to improve the response speed, please set it to "High Speed Reading and Writing".

hf 14a raw -s -c -t 1000 cf0000000032<parameter>

Parameter	Description
00	Closed, shadow data can be written at this time
01	Open, start restore
02	Turn it off completely, as a normal card
03	High-speed read and write mode

●Any block read and write

Using the backdoor command can read and write any area without password, similar to UID card, it should be noted that this command must be used to modify UID.

Backdoor card reading:

hf 14a raw -s -c -t 1000 cf00000000CE<block number>

Backdoor write card:

hf 14a raw -s -c -t 1000 cf00000000CD<block number><single block data>

●Fast card issue

This operation can directly write all the configurations into the card (except the card number) with one instruction. It is valid in Recovery mode or when the card is issued by the machine.

<Refer to the attached code for this mode>

It is recommended that you use this mode.

●Backdoor password setting

All backdoor operations are protected by passwords. If the password is incorrect, the card will not reply to any information. The user can set the backdoor password to avoid possible card tracking. It should be noted that once the password is forgotten, the card will be scrapped and can only be returned to production again.

Modify the backdoor password

hf 14a raw -s -c -t 1000 cf00000000feaabbccdd

Modify the original password 00000000 to aabbccdd

Attention

Description of Recovery Mode

The card number becomes: 01023304 and it enters Recovery mode. In this mode, you can only pass

☆Quick issue

To repair the card.

Code

```
1.  private string generateSendChangableData()
    {
        string bkdat = "CF00000000"+(cmb_fuse.Checked?"F1":"F0");
        bkdat += chk_ul_en.Checked ? "01" : "00";
        if (rb_10b.Checked)
            bkdat += "02";
        else if (rb_7b.Checked)
            bkdat += "01";
        else
            bkdat += "00";
        bkdat += txt_bk_pwd.Text;
        this.Invoke(new Action(() =>
        {
            bkdat += "0" + cmb_shadow.SelectedIndex;
        }));
        this.Invoke(new Action(() =>
        {

            if (cmb_ats_len.Text == "No ATS")
                bkdat += "00";
            else
                bkdat += cmb_ats_len.Text;
        }));
        bkdat += txt_ats_dat.Text;
        bkdat += txt_atqa.Text.Substring(2, 2);
        bkdat += txt_atqa.Text.Substring(0, 2);
        bkdat += txt_sak.Text;
        this.Invoke(new Action(() =>
        {
            bkdat += "0" + cmb_ul_mode.SelectedIndex;
        }));
        return bkdat;
    }
```

Demo Program

1. FuseTool fast card issuance routine

2. PyPm-Proxmark3 Python Write Sample Code