RfidResearchGroup / **proxmark3** Public

<> Code ⊙ Issues 84 Pull requests 12 ▷ Actions Projects Wik

master ▾ proxmark3 / doc / **ext_flash_notes.md** Go to file ···

[redacted]

[redacted]

129 lines (97 sloc) | 4.58 KB <> Raw Blame

External flash

External 256kbytes flash is a unique feature of the RDV4 edition.

Table of Contents

Addresses

^Top

Flash memory is

- 256KB (0x40000= 262144)
- divided into 4 pages of 64KB (0x10000 = 65536)
- 4 pages divided into 16 sectors of 4KB (0x1000 = 4096), so last sector is at 0x3F000

Therefore a flash address can be interpreted as such:

```
0xPSxxx       e.g. 0x3FF7F
  ^ page             ^ page 3
   ^ sector           ^ sector 0xF
    ^^^ offset         ^^^ offset 0xF7F
```

Layout

^Top

Page 0:

- available for user data
- to dump it: `mem dump f page0_dump o 0 l 65536`
- to erase it: `mem wipe p 0`

Page 1:

- available for user data
- to dump it: `mem dump f page1_dump o 65536 l 65536`
- to erase it: `mem wipe p 1`

Page 2:

- available for user data

- to dump it: `mem dump f page2_dump o 131072 l 65536`
- to erase it: `mem wipe p 2`

Page 3:

- used by Proxmark3 RDV4 specific functions: flash signature and keys dictionaries, see below for details
- to dump it: `mem dump f page3_dump o 196608 l 65536`
- to erase it:
  - **Beware** it will erase your flash signature so better to back it up first as you won't be able to regenerate it by yourself!
  - edit the source code to enable Page 3 as a valid input in the `mem wipe` command.
  - Updating keys dictionaries doesn't require to erase page 3.

Page3 Layout

^Top

Page3 is used as follows by the Proxmark3 RDV4 firmware:

- **MF_KEYS**

  - offset: page 3 sector 9 (0x9) @ *30x10000+90*x1000=0x39000
  - length: 2 sectors

- **ICLASS_KEYS**

  - offset: page 3 sector 11 (0xB) @ *30x10000+110*x1000=0x3B000
  - length: 1 sector

- **T55XX_KEYS**

  - offset: page 3 sector 12 (0xC) @ *30x10000+120*x1000=0x3C000
  - length: 1 sector

- **T55XX_CONFIG**
  - offset: page 3 sector 13 (0xD) @ *30x10000+130*x1000=0x3D000
  - length: 1 sector (actually only a few bytes are used to store `t55xx_config` structure)
- **RSA SIGNATURE**, see below for details
  - offset: page 3 sector 15 (0xF) offset 0xF7F @ *30x10000+150*x1000+0xF7F=0x3FF7F (decimal 262015)
  - length: 128 bytes
  - offset should have been 0x3FF80 but historically it's one byte off and therefore the last byte of the flash is unused

RSA signature

^Top

To ensure your Proxmark3 RDV4 is not a counterfeit product, its external flash contains a RSA signature of the flash unique ID. You can verify it with: `mem info`

Here below is a sample output of a RDV4 device.

```
[usb] pm3 --> mem info

[=] --- Flash memory Information ---------
[=] ID................... 25AD99A782A867D5
[=] SHA1.................
67C3B9BA2FA90AD4B283926B70017066C082C156
[+] Signature........... ( ok )

[=] --- RDV4 RSA signature ---------------
[=]
C7C7DF7FA3A2391A2B36E97D227C746ED8BB475E8766F54A13BAA9AAB29299B

[=]
37546AACCC29157ABF8AFBF3A1CFB24275442D565F7E996C6B08090528ADE25
```

```
[=]
ED1498E3089C72C68348D83CBD13F1247327BDBC9D75B09ECE3E051E19FE19B

[=]
98CB038757F2EDFD2DC5060D05C3296BC19A6F768290D555DFD50407E0E13A7


[=] --- RDV4 RSA Public key --------------
[=] Len.................. 128
[=] Exponent............. 010001
[=] Public key modulus N
[=]
E28D809BF323171D11D1ACA4C32A5B7E0A8974FD171E75AD120D60E9B76968F

[=]
4B0A6364AE50583F9555B8EE1A725F279E949246DF0EFCE4C02B9F3ACDCC623

[=]
9337F21C0C066FFB703D8BFCB5067F309E056772096642C2B1A8F50305D5EC3

[=]
DB7FB5A3C8AC42EB635AE3C148C910750ABAA280CE82DC2F180F49F30A1393B


[+] RSA public key validation.... ( ok )
[+] RSA private key validation... ( ok )
[+] RSA verification..... ( ok )
[+] Genuine Proxmark3 RDV4 signature detected
```

backup first!

^Top

To make a backup of the signature to file:

`mem dump p f flash_signature_dump o 262015 l 128`