Простая инструкция по сбросу пароля на видеорегистраторе NBD6904T-F через UART

Исходные данные:
- видеорегистратор на платформе XM. Для примера, рассмотрим NBD6904T-F V2.01 (NVR);
- регистратор полностью рабочий (загружается), но утрачен пароль администратора;
- доступ к регистратору по протоколу TELNET закрыт;
- текущая версия прошивки регистратора неизвестна;
- известные генераторы паролей не подходят;
- задача – сбросить пароль администратора (сохранить текущую конфигурацию цели не стоит).

Идеология решения задачи предполагает удаление во флеши (ИМС SPI-флэшпамяти) с прошивкой конфигурационного раздела регистратора целиком. В конфигурационном разделе хранятся все пользовательские настройки. Если удалить этот раздел, то при последующей перезагрузке регистратор пересоздаст его с настройками по умолчанию.

Задача декомпилируется следующим образом:
- выяснить **смещение** конфигурационного раздела в адресном пространстве флэши (*смещение – это число байт, которое необходимо отступить относительно начала флэша, чтобы попасть в начало раздела*);
- выяснить **размер** конфигурационного раздела;
- аккуратно **удалить** раздел, не затерев соседние.

Решение (на примере NBD6904T-F):

1. подпаиваем штыри UART на плате регистратора, подключаемся PuTTy, останавливаем загрузку U-boot по Ctrl-C и вычитываем переменные окружения U-boot командой **print**. Видим:

U-Boot 2010.06-svn198 (Nov 26 2014 - 14:38:43)

Check spi flash controller v350... Found
Spi(cs1) ID: 0xEF 0x40 0x18 0x00 0x00 0x00
Spi(cs1): Block:64KB Chip:16MB Name:"W25Q128B"
envcrc 0x62c57050
ENV_SIZE = 0x3fffc
In: serial
Out: serial
Err: serial
USB: scanning bus for devices... 1 USB Device(s) found
0 Storage Device(s) found
Press CTRL-C to abort autoboot in 0 secondshisilicon # <INTERRUPT>
hisilicon # <INTERRUPT>
hisilicon # print
bootcmd=sf probe 0;sf read 84000000 e80000 40000;logoload 84000000;decjpg;sf read 84000000 80000 400000;fload 84000000;bootm 0x82000000
bootdelay=1
baudrate=115200
bootfile="uImage"
restore=1
da=mw.b 0x82000000 ff 1000000;tftp 0x82000000 u-boot.bin.img;sf probe 0;flwrite
du=mw.b 0x82000000 ff 1000000;tftp 0x82000000 user-x.cramfs.img;sf probe 0;flwrite
dr=mw.b 0x82000000 ff 1000000;tftp 0x82000000 romfs-x.cramfs.img;sf probe 0;flwrite
dw=mw.b 0x82000000 ff 1000000;tftp 0x82000000 web-x.cramfs.img;sf probe 0;flwrite
dl=mw.b 0x82000000 ff 1000000;tftp 0x82000000 logo-x.cramfs.img;sf probe 0;flwrite
dc=mw.b 0x82000000 ff 1000000;tftp 0x82000000 custom-x.cramfs.img;sf probe 0;flwrite
up=mw.b 0x82000000 ff 1000000;tftp 0x82000000 update.img;sf probe 0;flwrite
tk=mw.b 0x82000000 ff 1000000;tftp 0x82000000 zImage.img; bootm 0x82000000
dd=mw.b 0x82000000 ff 1000000;tftp 0x82000000 mtd-x.jffs2.img;sf probe 0;flwrite
ipaddr=192.168.1.10
serverip=192.168.1.1
netmask=255.255.255.0
gatewayip=192.168.0.1
ethaddr=00:0b:3f:00:00:01
appVideoStandard=PAL
bootargs=mem=82M console=ttyAMA0,115200 root=1f01 rootfstype=cramfs
mtdparts=hi_sfc:512K(boot),4M(romfs),5632K(usr),1536K(web),3M(custom),256K(logo),1280K(mtd)
appSystemLanguage=Russian
stdin=serial
stdout=serial
stderr=serial
verify=n
ver=U-Boot 2010.06-svn198 (Nov 26 2014 - 14:38:43)

2. Анализируем строку:

mtdparts=hi_sfc:512K(boot),4M(romfs),5632K(usr),1536K(web),3M(custom),256K(logo),1280K(mtd)

Здесь, конфигурационный раздел имеет имя: **mtd;** размер: **1280K** (килобайт); расположен в **конце** адресного пространства флэши. Проверяем в скачанной и распакованной, например, отсюда: https://pan.sohu.net/f/MTY3OTQsaGRpeG0.htm прошивке для этого регистратора наличие образа раздела конфига: **mtd-x.jffs2.img.** Такого раздела в прошивке нет. Если бы он был, можно было бы залить его по TFTP командой **run dd** и оценить результат.

3. Анализируем строку сведений о примененной в регистраторе флэш-памяти:

Spi(cs1): Block:64KB Chip:16MB Name:"W25Q128B"

Нас интересует объем памяти и размер блока. Обычно размеры разделов во флэши кратны размеру блока – 64KB (килобайт) – «берем на ум», как говорится. Объем флэша, как видим, составляет 16MB (мегабайт) или 16x1024= 16384K (килобайт) в десятичной системе счисления. Проверим суммарный размер разделов на флэши (в килобайтах):

512(boot)+4096(romfs)+5632(usr)+1536(web)+3072(custom)+256(logo)+1280(mtd)=16384(full) - Зер гут.

4. Вычисляем **размер** конфигурационного раздела в байтах:
   1280x1024=**1310720** (байт)

5. Вычисляем полный размер флэша в байтах:
   16384x1024=16777216 (байт)

6. Вычисляем **смещение** (помним, что раздел конфигурации находится в конце адресного пространства флэша):
   16777216-1310720=**15466496** (байт)

7. Теперь, любым online калькулятором, например, этим: http://www.calculator.net/hex-calculator.html конвертируем полученные десятичные значения в шестнадцатиричные:

- **размер** конфигурационного раздела в байтах: 1310720 → h**140000**
- **смещение** конфигурационного раздела в байтах: 15466496 → h**EC0000**

8. Удаляем конфигурационный раздел (формат команды: sf erase <смещение><размер>) – в командной строке загрузчика вводим:

sf probe 0
sf erase ec0000 140000

В других регистраторах формат команды может быть такой:
sf erase 0xec0000 0x140000

Получаем:

hisilicon # sf probe 0
16384 KiB hi_sfc at 0:0 is now current device
hisilicon # sf erase ec0000 140000

Erasing at 0xed0000 -- 5% complete.
Erasing at 0xee0000 -- 10% complete.
Erasing at 0xef0000 -- 15% complete.
Erasing at 0xf00000 -- 20% complete.
Erasing at 0xf10000 -- 25% complete.
Erasing at 0xf20000 -- 30% complete.
Erasing at 0xf30000 -- 35% complete.
Erasing at 0xf40000 -- 40% complete.
Erasing at 0xf50000 -- 45% complete.
Erasing at 0xf60000 -- 50% complete.
Erasing at 0xf70000 -- 55% complete.
Erasing at 0xf80000 -- 60% complete.
Erasing at 0xf90000 -- 65% complete.
Erasing at 0xfa0000 -- 70% complete.
Erasing at 0xfb0000 -- 75% complete.
Erasing at 0xfc0000 -- 80% complete.
Erasing at 0xfd0000 -- 85% complete.
Erasing at 0xfe0000 -- 90% complete.
Erasing at 0xff0000 -- 95% complete.
Erasing at 0x1000000 -- 100% complete.
hisilicon # reset
resetting ...

9. Перезагружаем регистратор командой **reset**. Регистратор загружается на китайском (кнопочка «ОК» – справа.). Пароль пустой. Конфигурация заводская (дефолтная).

10. Все ваши действия – на ваш риск. «Мойте руки перед едой» - делайте резервные дампы разделов перед началом ремонтных работ. Если для вашего регистратора местоположение конфигурационного раздела не в конце флэша, то пересчитываете смещение с учётом его местоположения. Естественно, все расчёты можно сделать другим, удобным вам способом.

    P.S. Естественно, инструкция применима для решения аналогичных задач в отношении другого оборудования (видеорегистраторов и камер) производства **Xiong Mai Tech**. Главное, - включить «думательный аппарат» (с), понять принцип и внимательно рассчитать необходимые параметры для команды **sf erase.**

Kosyak_kpol
январь 2018г.