PLAYING WITH CAR FIRMWARE

(OR HOW TO BRICK YOUR CAR)

@0x222 Paul Such (SCRT)

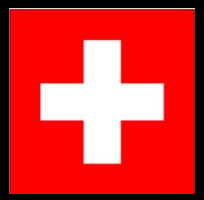
@Agixid Florian Gaultier (SCRT)

SUMMARY

- Who am I ?
- Hacking car firmware , why ?
- Model
- Hidden menu
- Finding the firmware – sources
- Analyzing the firmware
- Some interesting results
- A 2.2 Ton (4400 pounds) brick
- Conclusions

WHO AM I ?

- Name : Paul Such
- Twitter : @0x222
- Life : Security Engineer and founders of SCRT (A Swiss security company specialized in Ethical hacking, IT security, digital forensics)
- Hobbies : Guitarist, mountain biker, fan of motorsport
- Organizer of the Swiss security event : Insomni'hack (security conferences, CTF,…) March 2015



- Research done with Florian Gaultier
- Twitter : @agixid

HACKING CAR FIRMWARE ? WHY ?

- Fun and profit ☺
- A lot of researches have already been done regarding CANBUS, OBD2,…
- Car “entertainment system” can do much more than “entertainment” : you can nearly control everything : lights. central locking , air conditioning, GPS, Bluetooth, phone, Wi-Fi, auxiliary heating, …
- A lot of cars have “built-in” options that are just software-activated : TV, Wifi, auxiliary heating,… sounds interesting

(MAIN) MODEL

- Car : VW touareg 2
- Multimedia : RNS 850 (audi Mmi-3G)

GETTING THE FIRMWARE - SOURCES

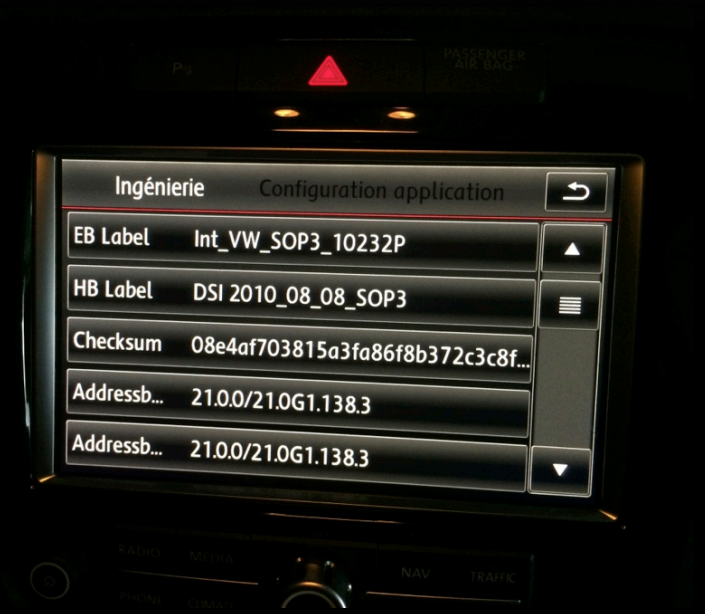
- The hard way : dismount the car , find the disk/flash (in my case -> the drive is inside the glovebox. Note the IDE/PATA interface, not SATA ☺)
- Buy a RNS850 on Ebay
- Social engineering : the VW dealer/mechanic
- For some models : update the GPS => could update the firmware (ex : audi TT)
- Google is your friend : RNS850 firmware ☺

UPLOAD/MODIFY THE FIRMWARE

- No way but the hard way : direct disk access
- Find the magic combo (Press PHONE + SET UP together for 3-5 seconds)

- To reboot the RNS850, you need your 5 fingers (Phone+Climate+Nav+Traffic+Button)

HIDDEN MENUS

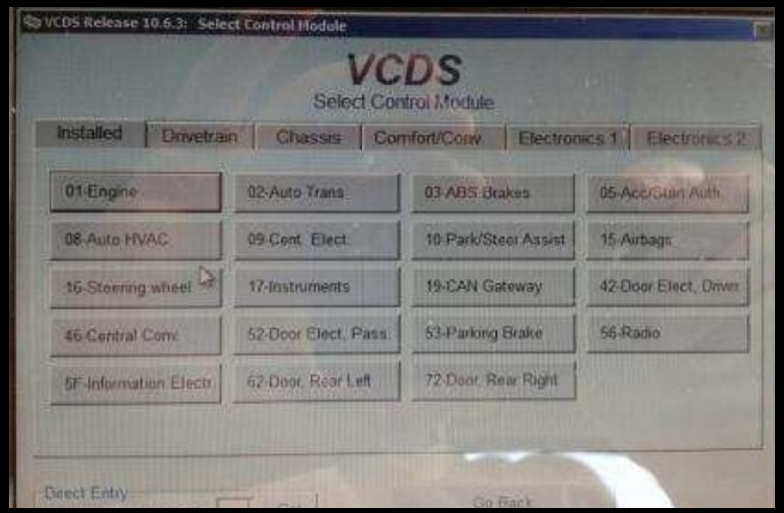


HIDDEN MENUS

HIDDEN MENUS

UPLOAD/MODIFY THE FIRMWARE (2)

- Power-user : OBD2 + VAGCOM + combo



ANALYSING THE FIRMWARE

- Firmware seems to be a mix of EFS & IFS filesystem
- We used the tool dumpefs to dump the filesystem
  - http://www.qnx.com/developers/docs/6.3.2/neutrino/utilities/d/dumpefs
  - We had to create a small Python tool to recreate a filesystem using dumpefs output
- had to deflate some files
  - http://www.qnx.com/developers/docs/6.3.2/neutrino/utilities/d/deflate.html
- … and Dumpifs (but we had to edit the headers of the files so that dumpifs could extract the files)
  - http://www.qnx.com/developers/docs/6.3.2/neutrino/utilities/d/dumpifs.html
- RNS850 is based on QNX ☺
  - Elf header show a SuperH architecture

EXTRACT-EFS.PY

```
import sys
import os
import re
if len(sys.argv)!=3:
        print "Usage: "+sys.argv[0]+" <file> <directory>"
        sys.exit()

f=open(sys.argv[1],"r")
file=f.read()
f.close()
os.system("mkdir "+sys.argv[2])
heads = file.split("---------------------------------------------------------------------------- »)
i=0
while i<len(heads):
        params = {}
        params_raw = heads[i].split("\x0a")
        for j in params_raw:
                if len(j.split("="))==2:
                        params.update({j.split("=")[0]:j.split("=")[1]})
        if params.has_key(".mode") and params.has_key("name"):
                if params[".mode"].find("d")!=-1:
                        directory=params["name"].replace("","")
                        print "mkdir %s"%directory
                        os.system("mkdir -p %s/%s"%(sys.argv[2],directory))
                else:
                        file_name=params["name"].replace("","")
                        dump = heads[i+1].split("data",1)[1]
                        lines = dump.split("\n")
                        dump_hex = ""
                        for k in lines:
                                try:
                                        clear_line = k.split(":",1)[1].split("  ",1)[0]
                                        raw_line = clear_line.replace(" ","\\x")
                                        dump_hex += raw_line
                                        dump_raw = eval('"%s"'%dump_hex)
                                except:
                                        pass
                        print "create %s/%s/%s"%(sys.argv[2],directory,file_name)
                        f2=open("%s/%s/%s"%(sys.argv[2],directory,file_name),"w")
                        f2.write(dump_raw)
                        f2.close()

        i+=1
```

RESULTS

- It is a « unix » filesystem

imageInfo/passwd
root:x:0:0:Superuser:/:/bin/ksh
bin:x:1:1:Binaries Commands and Source:/bin:
daemon:x:2:2:System Services:/daemon:
mail:x:8:40:User Mail:/var/spool/mail:
news:x:9:50:Network News:/var/spool/news:
uucp:x:12:60:Network News:/var/spool/news:
ftp:x:14:80:FTP User:/home/ftp:
nobody:x:99:99:Nobody:/:

ppp/shadow
root:UE/zhLVdRLPk.:19545:0:0

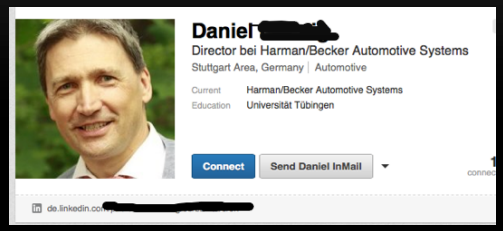
inet.d
#ftp stream tcp nowait root /usr/sbin/ftpd in.ftpd -l
telnet stream tcp nowait root /usr/sbin/telnetd in.telnetd

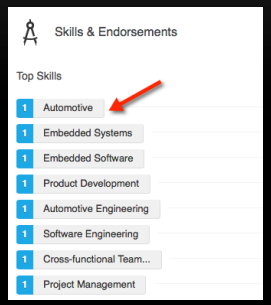
RESULTS

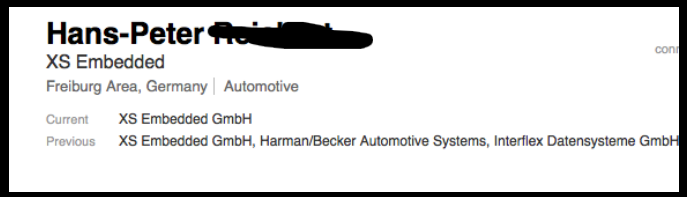
- ..and it leaks a lot of interesting information ☺

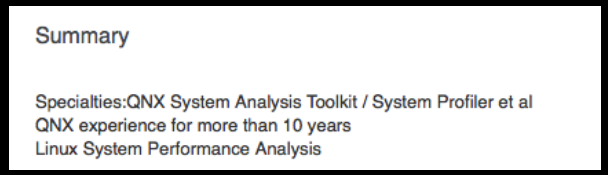
```
root::0:0:Superuser:/:/bin/ksh
bin:x:1:1:Binaries Commands and Source:/bin:
daemon:x:2:2:System Services:/daemon:
mail:x:8:40:User Mail:/var/spool/mail:
news:x:9:50:Network News:/var/spool/news:
uucp:x:12:60:Network News:/var/spool/news:
ftp:x:14:80:FTP User:/home/ftp:
nobody:x:99:99:Nobody:/:
hvo::1007:200:Herbert [redacted]/HBexport/home/hvo:/bin/ksh
hre:x:1009:200:Hans-Peter [redacted]t:/HBexport/home/hre:/bin/ksh
dhu::1012:200:Daniel [redacted]g:/HBexport/home/dhu:/bin/ksh
tsc:x:1017:200:Thomas:/HBexport/home/tsc:/bin/ksh
cjo::1018:200:Claudi [redacted]:/home/cjo:/bin/ksh
ine::1025:200:Ingo [redacted].n:/HBexport/home/ine:/bin/ksh
whe::1026:200:Werner [redacted]r:/HBexport/home/whe:/bin/ksh
jvi::1040:200:Jan Vi[redacted]e:/home/jvi:/bin/ksh
jsh::1035:200:Juergen S[redacted]r:/HBexport/home/jsh:/bin/ksh
hsr::1037:200:Harshit [redacted].a:/HBexport/home/hsr:/bin/ksh
dse::1063:200:Diethard [redacted]th:/HBexport/home/dse:/bin/ksh
tru::1064:200:Thomas [redacted]:/home/tru:/bin/ksh
pre::1065:200:Patric [redacted]rt:/home/pre:/bin/ksh
wzi::1066:200:Werner [redacted]ler:/home/wzi:/bin/ksh
szi::1067:200:Simon [redacted]e:/home/szi:/bin/ksh
```

COOL , YOU CAN FIND THE GUYS ON LINKEDIN









RESULTS

- Leaking internal IP range is also “good practice”, isn’it ?

ifs-root

./proc/boot/server.cfg

```
10.30.158.0/24      10.30.158.73        # Margi Fremont
172.16.42.0/24      172.16.42.10        # von Karlsbad AudiNG3 nach TS Karlsbad
172.16.43.0/24      172.16.42.10        # Next IP Range from Karlsbad
172.16.98.0/23      172.16.99.1  # Ulm
172.16.163.0/24  172.16.160.5    # VS, Roggenbachstrasse
172.16.166.0/22  172.16.166.152 # Hamburg
172.16.177.0/22  172.16.176.117 # Filderstadt
172.16.201.0/24  172.16.201.46  # Hechingen
172.16.206.0/24  172.16.160.5    # VS, Auf der Steig
172.16.216.0/24  172.16.216.24   # Hildesheim
10.42.102.0/24          172.16.102.9   # QSSL Kanata
10.1.180.0/24           10.1.180.27    # 3Soft 192
Erlangen.168.201.0/24         192.168.201.10 # Audi Ingolstadt
192.168.254.0/24   192.168.1.99  # comlet
10.21.13.0/24      10.21.13.47    # nVidia
```

RESULTS

- And yes.. The car can do wifi, so let's pre-configure some SSID

```
##### IEEE 802.11 related configuration #######################

# SSID to be used in IEEE 802.11 management frames
ssid=Audi3gpWLANuAP

# Static WEP key configuration
#
# The key number to use when transmitting.
# It must be between 0 and 3, and the corresponding key must be set.
# default: not set
wep_default_key=0
# The WEP keys to use.
# A key may be a quoted string or unquoted hexadecimal digits.
# The key length should be 5, 13, or 16 characters, or 10, 26, or 32
# digits, depending on whether 40-bit (64-bit), 104-bit (128-bit), or
# 128-bit (152-bit) WEP is used.
# Only the default key must be supplied; the others are optional.
# default: not set
#wep_key0=123456789a
#wep_key1=123456789a
#wep_key2=0102030405060708090a0b0c0d
#wep_key3=00112233445566778899aabbcc
```

OH NO ! HONEY I BRICKED OUR CAR….

- Long story short : I finally managed to brick my car (yeah , a 4400 pound brick)
- I do not know exactly why.. (checksum ? Upload problem ?)
- It happened while trying to replace a dummy text file (SMS pre-configured answers)
- Took 3 months to fix it !
- we are sorry, we had to change the “black box” of your car…

CONCLUSIONS

- Expensive hobby ☺ … and my friends/wife/family do not want me to do tests with their cars (anymore)
- Lot of possibilities.. and work to be done
- Next : the following libs would be very interesting to look at … :
    - ./mmedia/wma9_decoder.so
    - ./mmedia/mpega_parser.so
    - ./mmedia/wma9_parser.so
    - ./mmedia/mp4_parser.so
    - ./mmedia/wav_parser.so

QUESTIONS ?