NinjaTV - Increasing Your Smart TV’s IQ Without Bricking It

Felix Leder
About Myself

• Passion:
  • Reverse Engineering (+ tool development)
  • Being out in the snow, being out on a bike, being out in the water

• Fun Projects:
  • Bug hunting in malware
  • Botnet takeovers and countermeasure
  • The Honeynet Project

• $$$ Job:
  • Mobile Threat Research @ Blue Coat Norway
Credits
Western Digital TV (Live Hub)
Inside
Motivation to get other TV stations
Offline Analysis 1
Drive Investigation

- WDTVPriv partition
  - Hauppauge TV app storage
  - Spotify offline storage
  - Last update pkg

- WDTVLiveHub
  - Main media

- Swap
Offline Analysis 2
Updates

WD TV Live Hub Media Center

Product Update

We're pleased to offer the following updates for your WD TV Live Hub Media Center. Updating your media center is simple. Just follow the instructions below, grab your remote and enjoy the show!


- Supports Creepster Channel
- Supports euronews
- Supports MLB.TV closed captioning
- Resolved AccuWeather weekend forecast not displaying the full weekend
Update contents

felix@xxx:$ binwalk wdtvlivehub.bin

<table>
<thead>
<tr>
<th>DECIMAL</th>
<th>HEX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>0x20</td>
<td>Squashfs filesystem, little endian, version 3.1, size: 94877984 bytes, 6913 inodes, blocksize: 131072 bytes, created: Tue Jul 16 05:17:54 2013</td>
</tr>
</tbody>
</table>

| 00000000 | 63 34 32 63 35 34 61 63 | | c42c54ac2f8342ff |
| 00000010 | 38 31 36 65 36 36 65 64 | | 816e66ed6d988310 |
| 00000020 | 68 73 71 73 01 1b 00 00 | | hsqs............. |
| 00000030 | 00 00 00 00 00 00 00 00 | | .................. |
| 00000040 | 00 00 11 00 e0 01 00 62 | | ............b..Q.... |
Firmware signatures

wdtvlivehub.bin

Start Signature (32 bytes)
MD5 of Image I
+ end signature

Image I
root Squashfs 3.1 image

End Signature (16 bytes)
CE FA BE BA
02 00 00 00
Image I size (little endian)
00 00 00 00

wdtvlivehub.b12

Signature
MD5 of Image II
+ end signature

Image II
/opt Squashfs 3.1 image

End Signature (32 bytes)
MD5 of Image I
+ end signature
Update contents 2

Wdtvlivehub.bin

Wdtvlivehub.bi2

- /opt mounted
Which way in?
Vulnerability Finding
Vulnerability finding
SQL injection – here we come

```php
if (isset($_GET['entry_id'])) {
    $get_entry_id = $_GET['entry_id'];
}
if (isset($_GET['lang_id'])) {
    $get_lang_id = $_GET['lang_id'];
}
if (isset($_COOKIE['online'])) {
    $get_online_status = $_COOKIE['online'];
}

<? echo 'Stop'; ?>
```

```
$pdo = new PDO('sqlite:page.db');
$sql = 'SELECT * FROM web_top_tag WHERE entry_id = ? AND lang_id = ? ORDER BY seq_id ASC';
```
Vulnerability finding
RFI – remote file inclusion

```php
$get_language=$_SESSION['lang_id'];
if($get_language==''){
    $get_language=0;
}
include 'local/\$get_language\main.php';
```
Where to place my PHP shell?

Investigating more files:

- `/tmp/media/usb/Local/WDTV LiveHub/` is root of SMB share
- So my videos are in `/tmp/media/usb/Local/WDTV LiveHub/Videos/`
That was only the beginning...
Webserver running as **root** = **woot**
Must remember low hanging fruits...

```
/opt/webserver/htdocs # ls -l
...
-rw-rw-r-- 1 1007 1007 1685 Jun 24 2013 system_password.php
-rw-rw-r-- 1 1007 1007 142 Jun 24 2013 test.php
drwxrwxr-x 3 1007 1007  21 Jul 16 2013 tmp
lrwxrwxrwx 1 1007 1007  32 Dec 12 08:15 user -> /tmp/media/usb/Local/WDTVLiveHub
drwxrwxr-x 8 1007 1007  298 Jul 16 2013 wd_nas
drwxrwxr-x 3 1007 1007  23 Jul 16 2013 wdtvlivehub
drwxrwxr-x 2 1007 1007  102 Jul 16 2013 whatson
```
Approach for HW hackers
Looking for interesting pins

right side of box

RX | TX
GND

Warning: 3.3 Volts
Booting up

+ SMP86xx zboot start ...
+ Version: 3.1.0
+ Started at 0x400ee720.
+ Configurations (chip revision: 1):
  + Enabled checkpoints.

--- PRIMARY_SYSTEM ---

export SYSCONF_BUILD_DATE=2013.07.16-1106
export SYSCONF_BUILD_VERSION=3.12.13
export SYSCONF_NAND_DRIVER=LEGACY
export SYSCONF_FIRMWARE_BIN=wdtvlivehub.bin
export SYSCONF_FIRMWARE=module license 'Proprietary' takes
export SYSCONF_BOOTLOADER_MTD_PARTITION=0 vendor id 0xec...:
export SYSCONF_KERNEL_MTD_PARTITION=/dev/sigblockd
export SYSCONF_FIRMWARE_MTD_PARTITION=/dev/sigblockh
export SYSCONF_FIRMWARE_MTD_SIZE=96468992
export IS_BT=3
export SYSCONF_FIRMWARE_FS=squashfs

--- PRIMARY_SYSTEM ---

-- Boot from /dev/sigblockh --

Mounting application firmware...
Application firmware mounted..
Check the authentication of whole file...
random_number = 7
256+0 records in
256+0 records out
file /dev/sigblockn authenticated
All files have been checked for their integrity...
Launch application firmware...
--- ROOTFS ---

export SYSCONF_BUILD_DATE=2013.07.16-1106
export SYSCONF_BUILD_VERSION=3.12.13
export SYSCONF_NAND_DRIVER=LEGACY
export SYSCONF_FIRMWARE_BIN=wdtvlivehub.bin
export SYSCONF_FIRMWARE_VER=wdtvlivehub.ver
export SYSCONF_BOOTLOADER_MTD_PARTITION=/dev/sigblocka
export SYSCONF_KERNEL_MTD_PARTITION=/dev/sigblockd
export SYSCONF_FIRMWARE_MTD_PARTITION=/dev/sigblockh
export SYSCONF_FIRMWARE_MTD_SIZE=96468992
export SYSCONF_LAST_PARTITION_NODE_NAME=/dev/sigblockk
export SYSCONF_STATIC_CONFIG_MOUNT_POINT=/tmp/static_config
export SYSCONF_PRODUCT_EXT_WDTV_RV=y
export SYSCONF_MOUNT_LOCAL_SATA_DRIVE=y
export IS_DTS=y
export IS_DTCF=n
export SYSCONF_ROOTFS2=y
export SYSCONF_ROOTFS2_DEVICE=/dev/sigblocki
export SYSCONF_ROOTFS2_PATH=/opt

Primary built date: 2013.07.16-1106.
End of boot

41fa4f6ac0b8ebdefb89d443cb6c5ece login:

• What is the password?
Reverse Engineering the boot process (parts of it)

- Password is set by a tool called `gbus_read_serial_num`

- Located in `/usr/local/sbin` (encrypted file system image)

- Original: `/home/file` AES encrypted

- AES key to mount this image retrieved from ROM during boot

- Not visible in raw update bins

```bash
gbus_read_bin_to_file 0x61d00 0x280 /tmp/xosinfo &
genxenv2 g /tmp/xosinfo bc01 |
    sed 's/.*.bc01\(.*/\1/g' |
    sed 's/\ //g' > /tmp/log1 2>&1

echo `cat /tmp/log1` | mymount /home/file /usr/local/sbin -oencryption=aes -p 0
```
Visual

AES Key
What's the root password?

- `REGbus_read_serial_num`

```
echo $SERIALNUMBER | md5sum
```

```
41fa4f6ac0b8ebdefb89d443cb6c5ece
```

```
login: root
Password: <MD5SUM_OF_^> 
```

BusyBox v1.10.0 (2013-06-21 20:40:53 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

#
Where are the Apps?
Many traces on disk

• Logos for all services
• Libraries and DRM files for some
  • Spotify
  • Netflix
  • …
• NO Apps for e.g. redbull.tv, AOL, Bild.de
DMAOSD – the heart of WD TV

- Last process started
- System automatically reboots after process dies (e.g. is killed)
- Located in the encrypted partition
- Uses 75% of available RAM
Services
Service details

- On first connection WD TV uses GeoIP to determine country
- Some services are country specific (e.g. bild.de, ivi.ru)
- Pure web-pages
- Others use pipes to connect to local binaries/libraries (e.g. spotify)
- Crazy jump tables and if-statement
Dmaosd – all in one

- 13 MB (huuge executable for MIPS – even for x86)
- Everything statically linked in
  - QT webbrowser to access the web “services”
  - Libraries for HDMI and codec chips
  - Auto-mounts attached USB sticks, built-in harddrive
  - Controls network shares
  - Update daemon

- Renderer for XML based menus
- Loads all resources (templates, pictures, …) into it’s process space
Debugging Dmaosd live – get GDB up

Step 1: GDBServer on device

• Compile chain for MIPS → create GDBServer
  • http://www.mentor.com/embedded-software/sourcery-tools/sourcery-codebench/overview/
  • LSB, software floating point, shared libraries
    (COMPILEKIND=glibc,softfloat mipsel-linux-gcc -o test.mips test.c)

• Copy GDBServer executable on device
Debugging Dmaosd– attach IDA Pro

• IDA Pro for remote debugging (alternatively MIPS gdb)
• Very sensitive / unreliable
• Don’t be fooled by pipelining in assembly
• You cannot break much 😊 (more on that later)
Tatort

How to get my own services on the box?
Broadcaster “Das Erste” live stream
Browser – lowest hanging fruit

• QT embedded browser started
• Run – time patch the urls
• Windows: OpenProcess, WriteProcessMemory
• Linux: ptrace
  • PTRACE_ATTACH to process
  • PTRACE_PEEKDATA to search
  • PTRACE_POKEDATA to overwrite (in place – size limit)
Supported (HW) codecs?
TV station codec has to fit

NPPVpluginDescriptionString The <a href="http://www.gnome.org/projects/totem/">Totem</a> 0.10.2 plugin handles video and audio streams

Finally 😊
Root but not $\emptyset$wnd

ROM filesystem
root but not 0wnd by me

- All persistent file systems are read-only (from ROM)
- All dynamic parts are copied over to `/tmp` (including shadow, hosts, ...)
- Fresh reset after reboot

```
# mount
...
/dev/sigmblockh on / type squashfs (ro) ← root
...
none on /tmp type tmpfs (rw)
/dev/sigmblocki on /opt type squashfs (ro)
/dev/loop0 on /tmp/static_config type minix (rw)
/dev/loop1 on /usr/local/sbin type romfs (ro)
tmpfs on /opt/webserver/logs type tmpfs (rw)
none on /lib/sigma type ramfs (rw)
/dev/sda3 on /tmp/media/usb/Local/WDTVLiveHub type ufsd (rw,nls=utf8,uid=0,gid=0,fmask=0,...)
```
Persistence

... without the risk of bricking it
Patch firmware conservatively

Want to avoid bricking

• Use clean reset scheme

• Place other tools where they can be removed externally - harddrive (just in case)

• Don’t patch the main image → has several integrity checks (good conditions to run into problems)

• ... patch as little as possible

/init → /bin/run_all → /bin/dmaosd.sh → /opt/qt/bin/run_qt
Challenge: Mount order

- Dmaosd is last process started
  - Mounts the hard drive
  - Race condition: No dmaosd if run_qt blocks $\Rightarrow$ no hard drive $\Rightarrow$ block

Solution:
1. Return control and continue as background process
2. Wait for hard drive to be mounted
3. Continue booting there
Where are the lawyers?

GPL? Linux? ...
GPL Firmware

- Available but ...
  - will lose all DRM keys
  - Potentially WD keys

- ... I haven’t tried what is lost

Warning! This is the GPL source code. This is NOT the firmware for the device. If you use this source code to update the device, it will be treated as a third party user-modified firmware. We recommend using firmware released by Western Digital only. Using third party or user-modified firmware will cause malfunction and will void your product warranty. Once you install third party or user-modified firmware, even if the product is rolled back to the original firmware from WD, access to certain features will be disabled.

Where is the security?
Conspiracy Theory

• Why is WD basically leaving the device open?
Outlook
My situation
Questions?