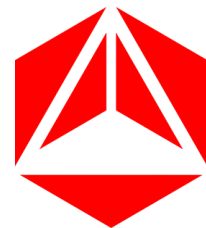


OLD SKEWL HACKING: DVB-T BLACK BUTTON PIVOT



November 2016

Adam "Major Malfunction"
Laurie



Aperture Labs

Who Am I?

Director – Aperture Labs – aperturelabs.com

<http://adamsblog.aperturelabs.com/>

DEF CON Goon – Quartermaster

POC @ DC4420 – DEF CON London

<http://dc4420.org>

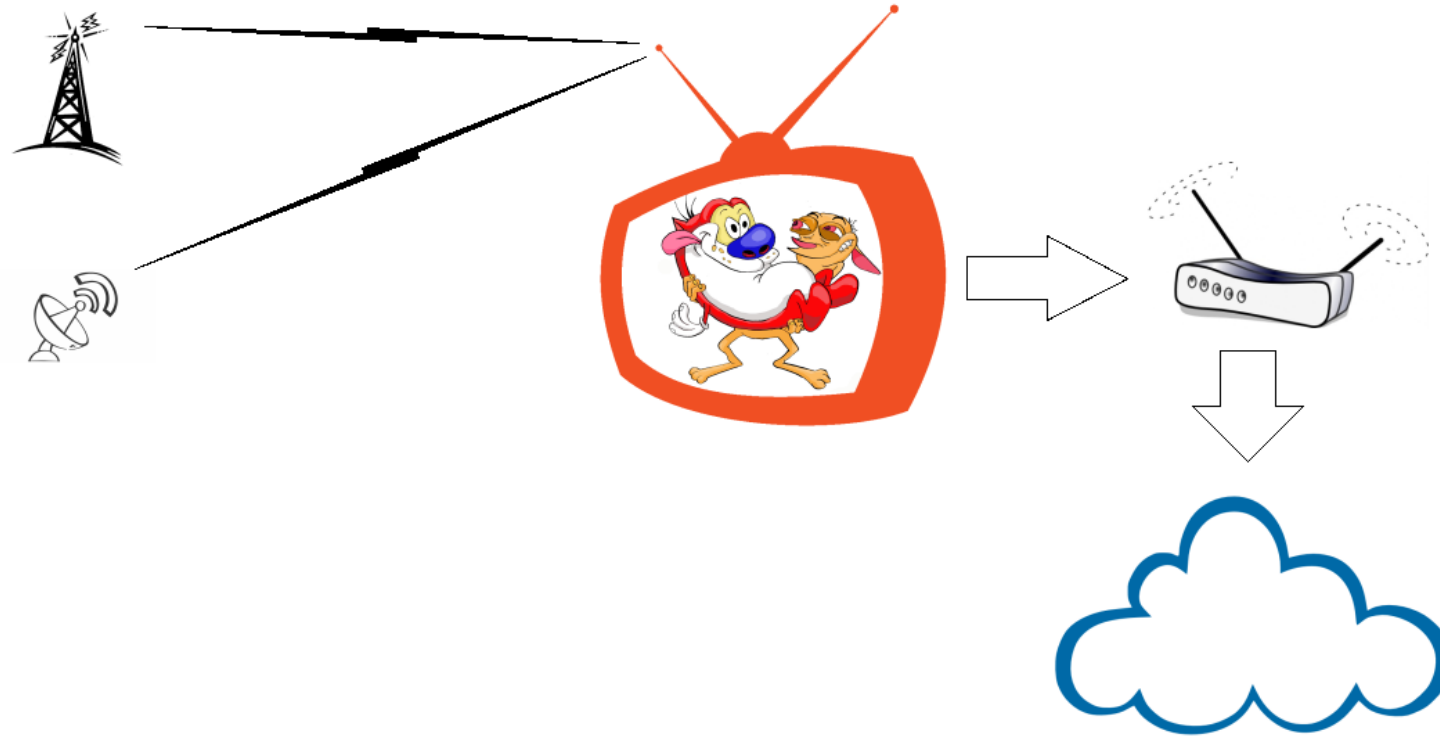
OLD SKEWL HACKING: DVB-T BLACK BUTTON PIVOT

Thanks to Mike Ossman and Dominic Spill for the HackRF hardware!

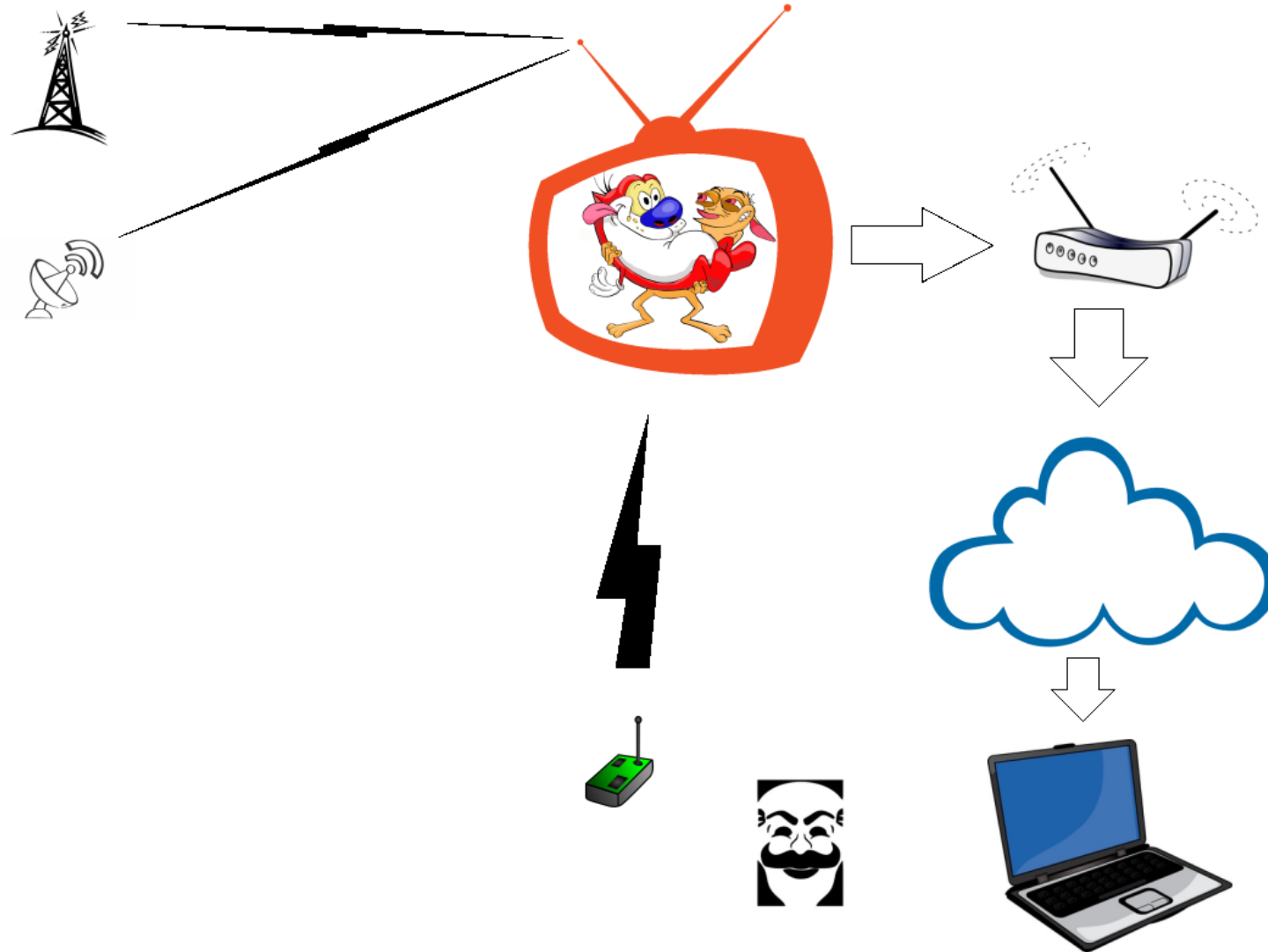
<https://greatscottgadgets.com/>

Just to really show my appreciation, here's what I'm doing with my new toy...

OLD SKEWL HACKING: DVB-T BLACK BUTTON PIVOT



OLD SKEWL HACKING: DVB-T BLACK BUTTON PIVOT



Why?

- TV Hacking

Why?

- TV Hacking
 - In hotels via Infra-Red

Why?

- TV Hacking
 - In hotels via Infra-Red
 - Free Pay Per View
 - Other in-room services
 - Mini Bar
 - Checkout
 - Telephone bills/logs
 - Wakeup Alarm
 - Hotel management servers
 - Billing
 - Info screens

Why?

- TV Hacking
 - In hotels via Infra-Red
 - At home via Satellite

Why?

- TV Hacking
 - In hotels via Infra-Red
 - At home via Satellite
 - Free Pay Per View
 - intercept feed signal from live events
 - Find hidden/interesting streams
 - Data as well as Audio / Video

Why?

- TV Hacking
 - In hotels via Infra-Red
 - At home via Satellite
 - At home via DVB-T

Why?

- TV Hacking
 - In hotels via Infra-Red
 - At home via Satellite
 - At home via DVB-T
 - Free Pay Per View
 - Bypass Premium Rate phone “unlock”
 - MHEG adopted as national standard

Why?

From Wikipedia:

"MHEG-5, or ISO/IEC 13522-5,[1] is part of a set of international standards relating to the presentation of multimedia information, standardised by the Multimedia and Hypermedia Experts Group (MHEG). It is most commonly used as a language to describe interactive television services."

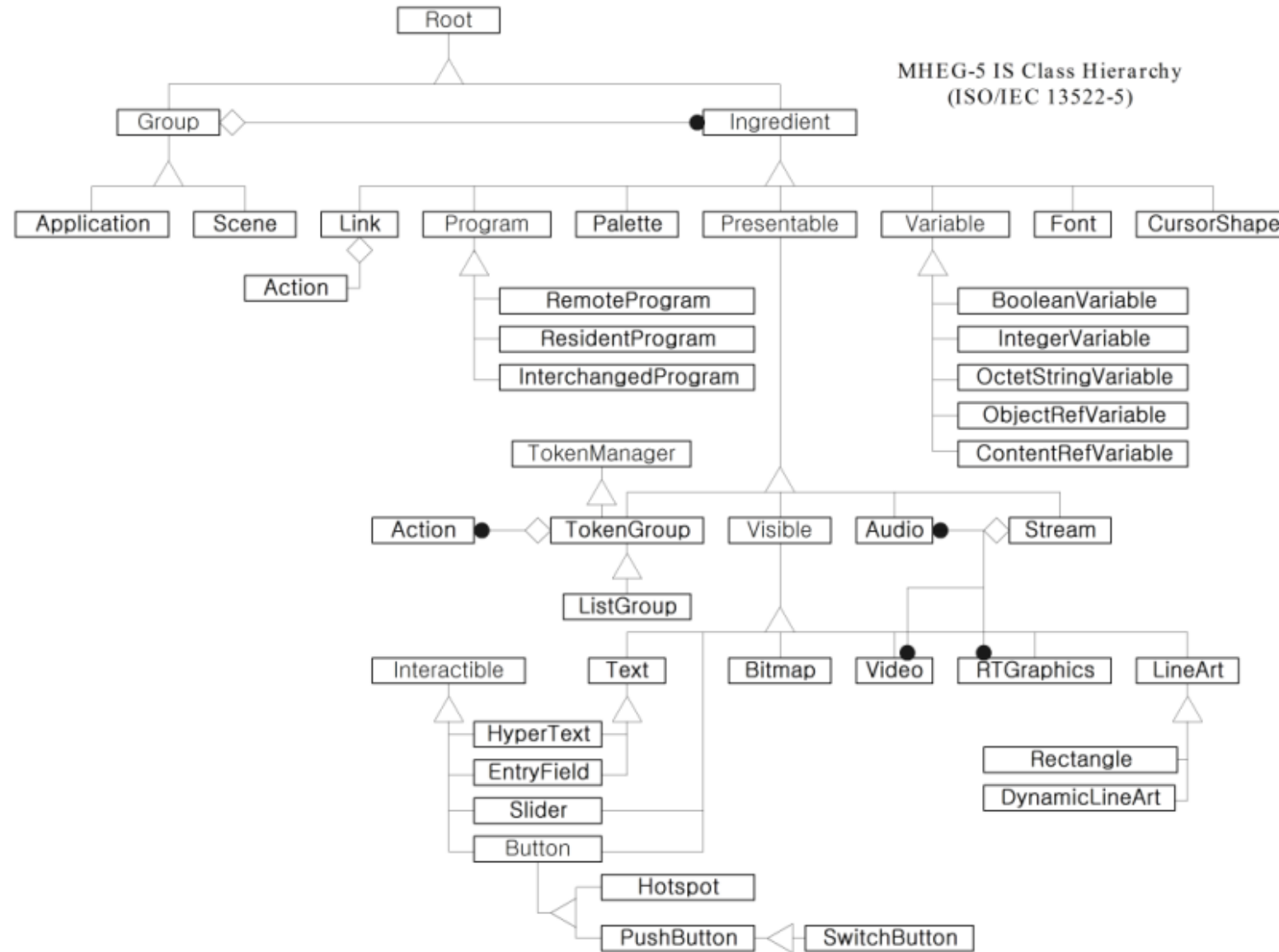
Why?

ALL (compliant) UK TVs are vulnerable to MHEG attacks...



<http://dtg.org.uk/publications/dbook.html>

Why?



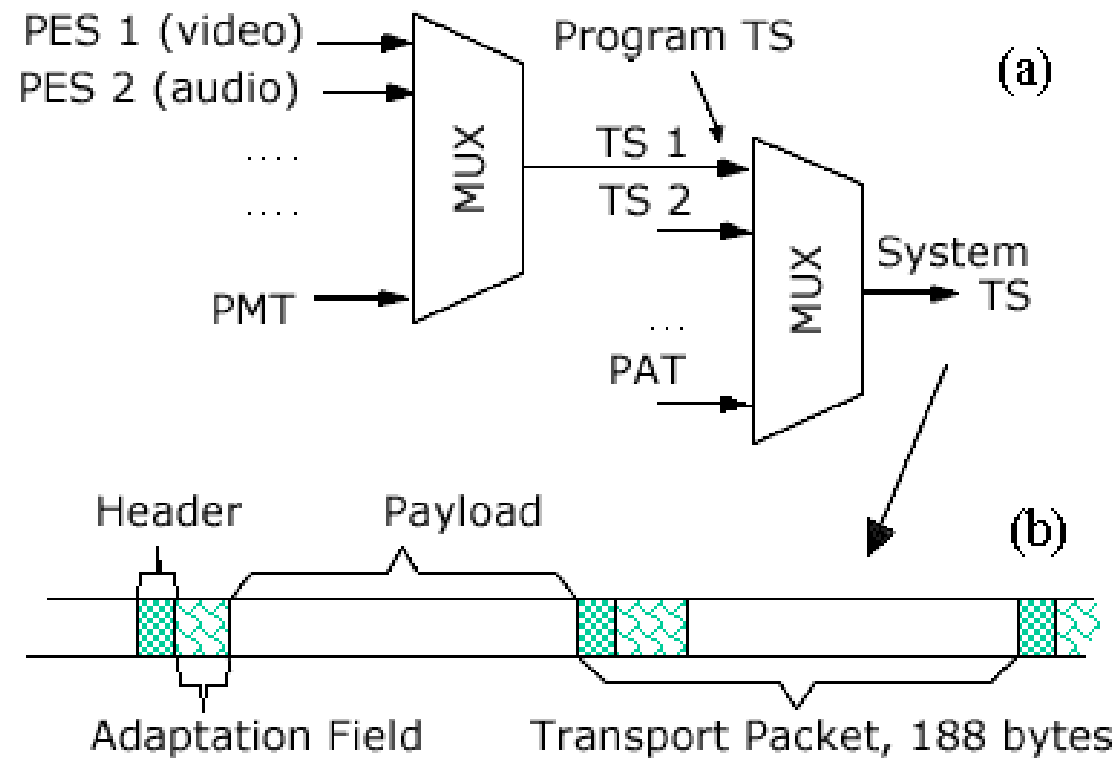
DEF CON talk: Porn Free!

- <https://www.youtube.com/watch?v=1RPmpJi3VRM>



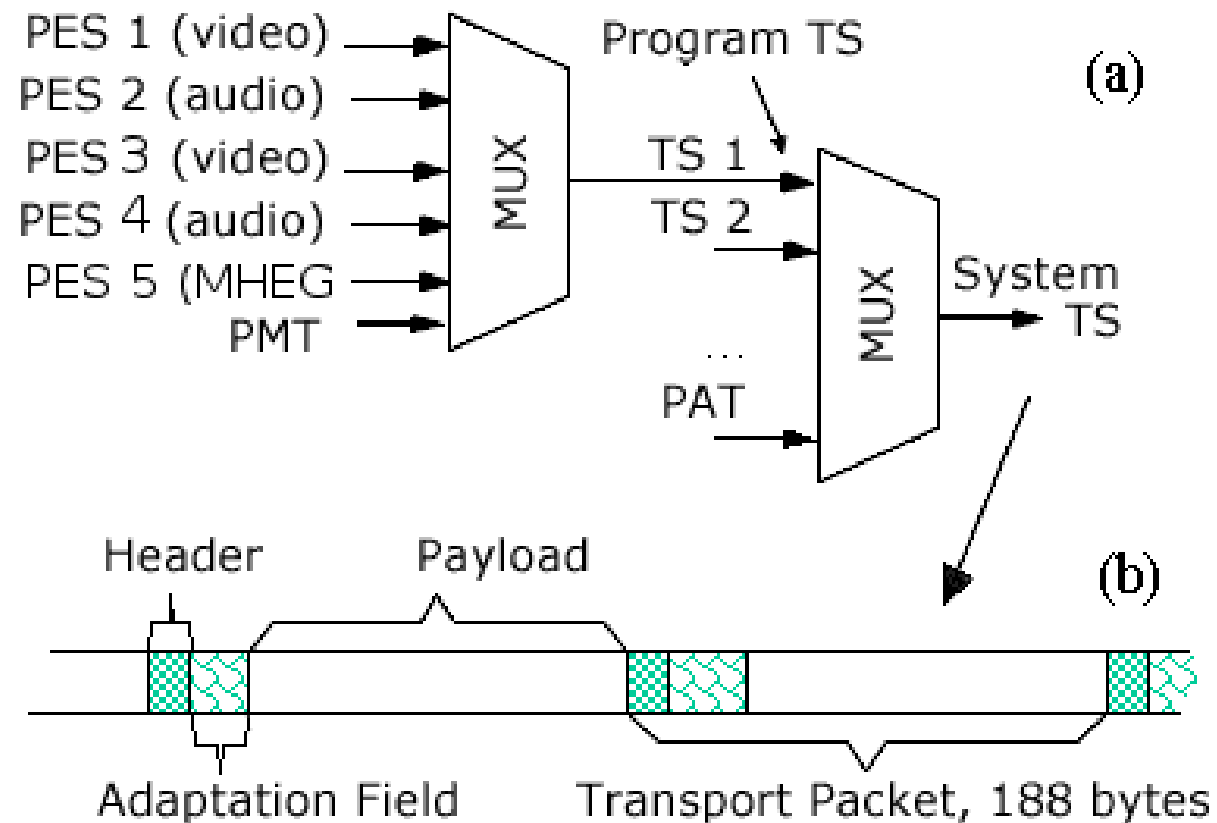
What's going on?

- Pornographer broadcasts blank video & audio streams in PES 1 & 2 (advertised in the PID/PAT etc.)



What's going on?

- MHEG loads and streams PES 3 & 4 only after validation / payment.



Capturing the MHEG

- Standard DVB-T dongle
- rb-download
 - <http://redbutton.sourceforge.net/>

What's there?

- Images
- Certs
- 'binary executable'
 - ASN.1
 - Effectively source code

Data structure

```
addy@blap:rb$ tree services/  
services/  
├── 14576 -> ../carousels/6648/200/srg-0-30303030  
├── 15232 -> ../carousels/6648/200/srg-0-30303030  
├── 4162 -> ../carousels/7201/1/srg-92-01  
└── 4544 -> ../carousels/7201/1/srg-92-01
```

Data structure

```
addy@blap:rb$ tree carousels/
carousels/
├── 6648
│   └── 200
│       └── dir-6-30303235
│           ├── a -> ../../../../../../carousels/6648/200/fil-6-30303130
│           ├── absolute.png -> ../../../../../../carousels/6648/200/fil-15-30303569
│           ├── absolute.txt -> ../../../../../../carousels/6648/200/fil-6-30303073
│           ├── adult.txt -> ../../../../../../carousels/6648/200/fil-6-30303564
│           ├── blank.txt -> ../../../../../../carousels/6648/200/fil-6-30303464
│           ├── capital.png -> ../../../../../../carousels/6648/200/fil-15-30303376
│           ├── capital.txt -> ../../../../../../carousels/6648/200/fil-6-30303164
│           ├── cbsdrama.png -> ../../../../../../carousels/6648/200/fil-15-3030356a
│           ├── cbsdrama.txt -> ../../../../../../carousels/6648/200/fil-6-30303631
│           ├── citv.png -> ../../../../../../carousels/6648/200/fil-15-30303270
│           ├── citv.txt -> ../../../../../../carousels/6648/200/fil-6-30303036
│           ├── heart.png -> ../../../../../../carousels/6648/200/fil-15-30303576
│           ├── heart.txt -> ../../../../../../carousels/6648/200/fil-6-3030336f
│           ├── hudatv_controller.txt -> ../../../../../../carousels/6648/200/fil-6-3030346a
│           └── hudatv_icstatus0.txt -> ../../../../../../carousels/6648/200/fil-6-30303063
```

Data structure

srg-98-01

```
a -> ../../../../carousels/7201/1/fil-26-07
auth.cert.1 -> ../../../../carousels/7201/1/fil-26-08
auth.servers -> ../../../../carousels/7201/1/fil-26-0c
auth.tls.1 -> ../../../../carousels/7201/1/fil-26-09
auth.tls.2 -> ../../../../carousels/7201/1/fil-26-0a
auth.tls.3 -> ../../../../carousels/7201/1/fil-26-0b
b -> ../../../../carousels/7201/1/dir-26-01
boot_state.flg -> ../../../../carousels/7201/1/fil-93-02
c -> ../../../../carousels/7201/1/dir-23-01
d -> ../../../../carousels/7201/1/dir-55-01
e1 -> ../../../../carousels/7201/1/dir-26-05
e2 -> ../../../../carousels/7201/1/dir-26-06
e3 -> ../../../../carousels/7201/1/dir-38-01
enh_gateway.mhg -> ../../../../carousels/7201/1/fil-44-01
g -> ../../../../carousels/7201/1/dir-26-04
r -> ../../../../carousels/7201/1/dir-26-03
radio -> ../../../../carousels/7201/1/dir-2-01
s -> ../../../../carousels/7201/1/dir-26-02
```


Images



Certificates

```
00000000 00 01 00 03 c0 30 82 03 bc 30 82 02 a4 a0 03 02 |.....0...0.....|
00000010 01 02 02 08 0e 65 1a d2 b3 e5 23 c7 30 0d 06 09 |.....e....#.0...|
00000020 2a 86 48 86 f7 0d 01 01 05 05 00 30 81 9e 31 0b |*.H.....0..1.|
00000030 30 09 06 03 55 04 06 13 02 47 42 31 0f 30 0d 06 |0...U....GB1.0..|
00000040 03 55 04 07 0c 06 4c 6f 6e 64 6f 6e 31 29 30 27 |.U....London1)0'|
00000050 06 03 55 04 0a 0c 20 42 72 69 74 69 73 68 20 42 |..U... British B|
00000060 72 6f 61 64 63 61 73 74 69 6e 67 20 43 6f 72 70 |roadcasting Corp|
00000070 6f 72 61 74 69 6f 6e 31 17 30 15 06 03 55 04 0b |oration1.0...U..|
00000080 0c 0e 46 4d 54 20 47 72 65 65 6e 68 6f 75 73 65 |..FMT Greenhouse|
00000090 31 3a 30 38 06 03 55 04 03 0c 31 42 42 43 20 47 |1:08..U...1BBC G|
000000a0 72 65 65 6e 68 6f 75 73 65 20 50 72 6f 64 75 63 |reenhouse Produc|
000000b0 74 69 6f 6e 20 53 65 72 76 65 72 73 20 61 6e 64 |tion Servers and|
000000c0 20 53 65 72 76 69 63 65 73 20 43 41 30 1e 17 0d | Services CA0...|
000000d0 31 35 31 30 33 30 31 31 33 30 30 32 5a 17 0d 31 |151030113002Z..1|
000000e0 38 30 37 32 30 31 31 34 37 30 32 5a 30 81 ab 31 |80720114702Z0..1|
000000f0 25 30 23 06 09 2a 86 48 86 f7 0d 01 09 01 16 16 |%0#..*.H.....|
00000100 42 42 43 52 42 54 65 61 6d 45 78 74 40 62 62 63 |BBCRBTeamExt@bbc|
00000110 2e 63 6f 2e 75 6b 31 1d 30 1b 06 03 55 04 03 0c |.co.uk1.0...U...|
00000120 14 42 72 6f 61 64 63 61 73 74 20 52 65 64 20 42 |.Broadcast Red B|
00000130 75 74 74 6f 6e 31 1a 30 18 06 03 55 04 0b 0c 11 |utton1.0...U....|
00000140 50 72 6f 64 75 63 74 69 6f 6e 20 53 65 72 76 65 |Production Serve|
00000150 72 31 29 30 27 06 03 55 04 0a 0c 20 42 72 69 74 |r1)0'..U... Brit|
00000160 69 73 68 20 42 72 6f 61 64 63 61 73 74 69 6e 67 |ish Broadcasting|
00000170 20 43 6f 72 70 6f 72 61 74 69 6f 6e 31 0f 30 0d | Corporation1.0.|
```

Code (ASN.1)

```
00001560 01 00 0a 01 06 02 01 64 bf 3f 82 01 6d bf 76 2c |.....d.?..m.v|
00001570 30 07 04 02 2f 61 02 01 15 04 21 0d 52 65 64 20 |0.../a....!.Red |
00001580 6b 65 79 20 70 72 65 73 73 65 64 2c 20 6c 6f 61 |key pressed, loa|
00001590 64 20 76 6f 64 20 73 74 72 65 61 6d bf 81 54 25 |d vod stream..T%|
000015a0 02 01 55 bf 81 63 1e 04 1c 2f 69 6d 61 67 65 73 |..U..c.../images|
000015b0 2f 62 75 74 74 6f 6e 73 2f 72 65 64 2d 77 61 69 |/buttons/red-wai|
000015c0 74 2e 70 6e 67 bf 78 2a 30 07 04 02 2f 61 02 01 |t.png.x*0.../a..|
000015d0 22 30 07 04 02 2f 61 02 01 1c 30 16 bf 81 63 07 |"0.../a...0...c.|
000015e0 bf 81 6c 03 02 01 55 bf 81 65 07 bf 81 6c 03 02 |..l...U..e...l..|
000015f0 01 56 bf 81 41 12 02 01 4b 30 0d bf 81 6c 03 02 |.V..A...K0...l..|
00001600 01 56 bf 81 6a 02 05 00 bf 81 54 1d 02 01 55 bf |.V..j.....T...U.|
00001610 81 63 16 04 14 2f 69 6d 61 67 65 73 2f 61 76 61 |.c.../images/ava|
00001620 6c 70 61 39 30 2e 70 6e 67 bf 78 2a 30 07 04 02 |lpa90.png.x*0...|
00001630 2f 61 02 01 22 30 07 04 02 2f 61 02 01 1c 30 16 |/a.."0.../a...0.|
00001640 bf 81 63 07 bf 81 6c 03 02 01 55 bf 81 65 07 bf |..c...l...U..e..|
00001650 81 6c 03 02 01 56 bf 81 41 12 02 01 4a 30 0d bf |.l...V..A...J0..|
00001660 81 6c 03 02 01 56 bf 81 6a 02 05 00 bf 81 3a 0b |.l...V..j.....:|
00001670 02 01 4a 02 02 00 a2 02 02 01 a2 bf 81 54 36 02 |..J.....T6.|
00001680 01 57 bf 81 63 2f 04 2d 68 74 74 70 3a 2f 2f 74 |.W..c/.-http://t|
00001690 72 61 63 6b 65 72 2e 61 76 61 6c 70 61 2e 6f 72 |racker.avalpa.or|
000016a0 67 2f 76 6f 64 2f 6d 68 65 67 74 65 73 74 2f 42 |g/vod/mhegtest/B|
000016b0 42 42 2e 74 73 bf 81 54 0a 02 01 59 bf 81 61 03 |BB.ts..T...Y..a.|
000016c0 01 01 ff bf 73 03 02 01 7e bf 81 5b 0d 02 01 59 |....s...~...[...Y|
000016d0 02 01 01 bf 81 61 03 01 01 ff b4 2d 02 02 00 8a |....a.....-....|
000016e0 bf 3e 09 02 01 00 0a 01 06 02 01 68 bf 3f 1a bf |.>.....h?...|
000016f0 81 32 09 30 07 04 02 2f 61 02 01 0d bf 81 30 09 |.2.0.../a.....0.|
00001700 30 07 04 02 2f 61 02 01 00 9f 33 01 04 bf 34 08 |0.../a....3...4.|
00001710 02 02 02 d0 02 02 02 40 |.....@|
```

Code (Decoded)

```
{ :Link 137
:InitiallyActive FALSE
:EventSource 0
:EventType UserInput
:EventData 100
:LinkEffect (
:Append ( ( '/a' 21 ) '=0DRed key pressed, load vod stream' )
:SetVariable ( 85 :GOctetString '/images/buttons/red-wait.png' )
:Call ( ( '/a' 34 ) ( '/a' 28 )
:GOctetString :IndirectRef 85
:GContentRef :IndirectRef 86
)
:SetData ( 75 :NewRefContent ( :IndirectRef 86 ) )
:SetVariable ( 85 :GOctetString '/images/avalpa90.png' )
:Call ( ( '/a' 34 ) ( '/a' 28 )
:GOctetString :IndirectRef 85
:GContentRef :IndirectRef 86
)
:SetData ( 74 :NewRefContent ( :IndirectRef 86 ) )
:SetBoxSize ( 74 162 418 )
:SetVariable ( 87 :GOctetString 'http://tracker.avalpa.org/vod/mhegtest/BBB.ts' )
:SetVariable ( 89 :GBoolean TRUE )
:Activate ( 126 )
:TestVariable ( 89 1 :GBoolean TRUE )
)
}
{ :Link 138
:EventSource 0
:EventType UserInput
:EventData 104
:LinkEffect (
:Run ( ( '/a' 13 ) )
:Quit ( ( '/a' 0 ) )
)
}
)
:InputEventReg 4
:SceneCS 720 576
}
```

MHEG vulns

TV can connect to remote HTTP/HTTPS to obtain content:

- Reveal IP of victim
- malicious content – images/streams
- **may** be signed/trusted
- other? e.g. buffer overflow etc.

Content can be more MHEG

- **must** be signed / trusted
- trust certs provided in broadcast stream

MHEG vulns:

TV **ALWAYS** trusts broadcast data...

MHEG vulns:

TV **ALWAYS** trusts broadcast data...

The standard says that's OK.

Live Demos

1. Broadcast webcam
2. Broadcast existing transport stream
 - 2a. With data services
3. Capture and replay live TS
 - 3a. With data services
4. MiTM live TS
5. Capture and decode MHEG
 - 5a. Re-use to create own MHEG prog
6. Mux own MHEG data stream with Audio/Video stream
7. Todo: Live TS MiTM re-mux with replaced data stream
 - 6a. Handy wrapper to calculate nasty numbers
8. Test against DVB-S, DVB-C.

Tools

- Hack-RF

- Gnu-Radio Companion
- ffmpeg/avconv
- OpenCaster
- Avalpa
 - <http://www.avalpa.com/>
- Big Buck Bunny
 - <https://peach.blender.org/>



- DVB-T2 dongle

- dvblast, netcat
- mhegc
 - <http://redbutton.sourceforge.net/>



Broadcast webcam

Credit to Clayton Smith for providing example:

<http://www.irrational.net/2014/03/02/digital-atv/>

And for fixing gnu-radio and generally providing help and assistance.

<https://github.com/gnuradio/gnuradio/pull/807>

(should now be in main branch)

Broadcast webcam

Connect HackRF direct to TV receiver to be legal...

Be careful to keep gain low to avoid receiver damage (start low and monitor signal quality with receiver menu system / info)

Broadcast webcam

Get correct mux rate with 'dvbtrate 8':

<https://github.com/drmpeg/dtv-utils>

Start TX python listener script:

`./dvbt-hackrf-receiver.py 1234`

Start webcam muxer:

```
avconv -f alsa -i pulse -f video4linux2 -s 640x480 -i /dev/video0 -vcodec  
mpeg2video -s 640x480 -r 60 -b 4000000 -acodec mp2 -ar 48000 -ab 192000 -ac  
2 -muxrate 6032086 -mpegts_transport_stream_id 1025 -mpegts_service_id 1 -  
mpegts_pmt_start_pid 0x1020 -mpegts_start_pid 0x0121 -f mpegts -y -metadata  
service_name=" <insert channel name here> " tcp://127.0.0.1:1234
```

Broadcast TS

2. Broadcast existing transport stream

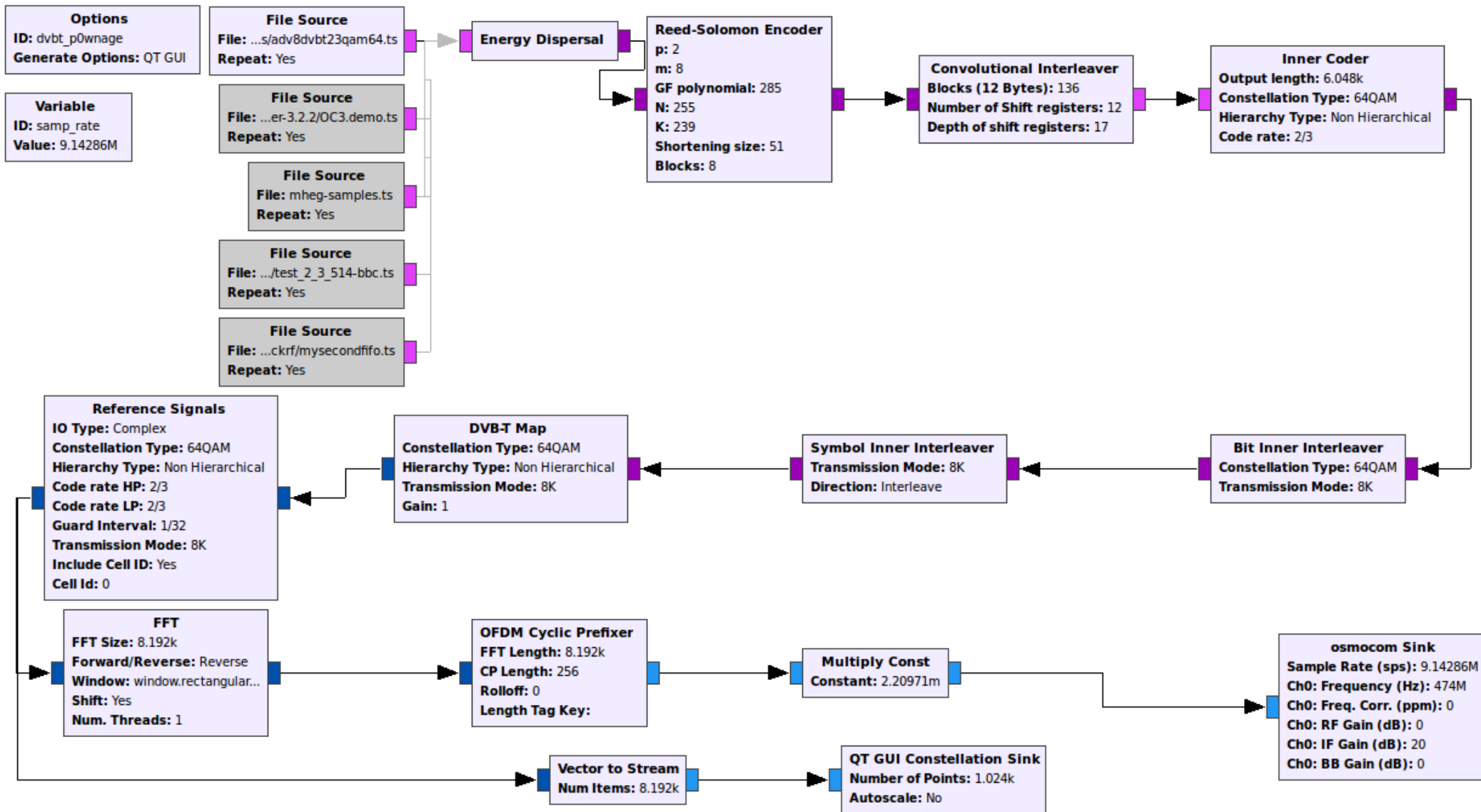
2a. With data services

Broadcast existing transport streams

gnuradio-companion dvbt_mheg-samples.grc

- 1 - single audio/video stream
- 2 – multiple audio/video streams + different data types (TXT / HbbTV / MHEG)
- 3 – multiple complex MHEG services
- 4 – UK full transponder 10 x TV / 16 x Radio plus all data: Red-Button, EPG etc.
- 5 – black-button attack!

Broadcast existing transport streams



Broadcast existing transport streams with my own app...

Input from fifo:

```
gnuradio-companion dvbt_mheg-samples.grc
```

```
tscbrmuxer b:2300000 firstvideo.ts b:188000  
firstaudio.ts b:3008 firstpat.ts b:3008 firstpmt.ts  
b:1500 firstsdt.ts b:1400 firstnit.ts b:1000000  
carousel-ransom.ts b:2000 firstait.ts b:9772084  
null.ts>myfirstfifo.ts &
```

```
tsstamp myfirstfifo.ts 13225001 > mysecondfifo.ts
```


Broadcast existing transport streams

Who needs the BBC?

With just a laptop and an SDR you have the power to broadcast.

Broadcast existing transport streams

Who needs the BBC?

With just a laptop and an SDR you have the power to broadcast.

I love living in the future!