Security Issues with Hybrid Broadcast Broadband TV (HbbTV)

Watching TV suddenly is fun again!
Agenda

• HbbTV Introduction
• Current Adoption
• Possible Attack Vectors
• Mitigation
• HAL – HbbTV Access Limiter
• Recommendations

... no pr0n ;)
Who am I

- Martin Herfurt
- Security Consultant working with n.runs
- Co-founder of trifinite.org
- Bluetooth security expert
- Based in Salzburg/Austria
- @mherfurt  +MartinHerfurt
**SmartTV Security Overview**

- December 2012: ReVuln - USB/Local attacks on SAMSUNG Smart TV
- March 2013: CanSecWest – Smart TV Security (great talk, but excluding HbbTV stuff) (SeungJin Lee, Seungjoo Kim)
- May 2013: (TU Darmstadt) HbbTV Privacy issues (Marco Ghiglieri, Florian Oswald, Erik Tews)
- June 2013: Security Issues with HbbTV
- August 2013: Attacking Smart TVs via apps (Aaron Grattafiori, Josh Yavor)
- November 2013: LG TVs transmit personal info
HbbTV Background

- Pan-European effort
- HbbTV = H4TV(fr) + HTML Profil(de)
- ETSI TS 102796 (published in June 2010)
- Adopts existing specifications
  - HTML-CE (Web for Consumer Electronics)
  - OIPF (Open IPTV Forum)
- Goal is to combine broadcast content with online content
HbbTV – Intended Use-Cases

- enhanced teletext
- catch-up services
- video-on-demand
- interactive advertising
- Personalization
- Voting
- Games
- social networking
Plain Old DVB

DVB Stream

DVB Stream
HYBRID BROADCAST BROADCAST TV

Augmented DVB Stream

Data Exchange via HTTP

Press Red Button for more!
The Red Button
SevenOne Media

Unique Devices - SAT.1, ProSieben, kabel eins
Anzahl Benutzer (=Devices) nach Monaten

© 2013, n.runs professionals GmbH – Security Research Team
Martin Herfurt
What you think you see
What you are really seeing
How is the Red Button displayed?

- TV has a DAE (Browser)
- Content from URL within DVB-Stream
- Overlay on actual TV image
- Mostly transparent web page
Data Collection

• Extraction of channel list
• Transparent proxy setup
• Script for switching channels via IP
• Script for saving proxy-log per station
Astra 19.2E Statistics

- 680 TV/HD channels
- 119 with HbbTV
- Only 40 hosts
- No SSL in use
- Maybe 15 entertainment providers

Data acquired on 23.12.2013 (no CI+ modules except HD+)
Use of Ad-Servers

- OpenX – now called Revive (2 stations)
  - Anixe
    - Used as frame for current program
    - Geo-IP to locate the viewers
    - First banners date back to October 2011 (directory listings enabled ;)
  - RTL2
    - Used for ads within HbbTV portal page
Use of 3rd Party Tracking

- Google Analytics (22 channels)
  - ARTE, DAS VIERTE, Kabel1, Pro7, Sat.1, SIXX, sonnenklar.TV, n-tv, VOX, RTL

- Other tracking services (4 channels)
  - RTL2 (etracker.com)
  - TVP Polonia (gemius.pl)

- Cookie with unique IDs (7 channels)
  - TecTime TV, Kinowelt TV, ORF1, ORF2, RTL2
Legal Aspects

• Telemediengesetz (TMG)
  – §15 collection of usage data – current use of tracking could be considered illegal
  – Missing opt-out
  – [Link](http://www.gesetze-im-internet.de/tmg/)
Not Only Big Brother is watching
Possible Attack Vectors

Augmented DVB Stream

Data Ex

HTTP

Press Red Button for more!
Attacking Playout System
Attacking Satellites

...ask Travis Goodspeed about this.
Watering Hole Attacks – sometimes very likely

Apache/1.3.27 (Unix) (Red-Hat/Linux)
mod_ssl/2.8.12 OpenSSL/0.9.6b DAV/1.0.3
PHP/4.1.2 mod_perl/1.26
mod_gzip/1.3.26.1a
Attacks on DNS

Current Efforts - HbbTV
Content Injection
What Would Dr. Evil Do?
Rogue Video Display
• Brand-new trifinite.project
• Overlays news tickers from
  – Tagesschau24
  – n-tv
• Thanks for the permission/support to
  – www.der-postillon.com
  – Stefan Sichermann
> Putzfrauenstreik im Speicherkraftwerk: Zu viele Staubecken

FUSSBALL-BUNDESLIGA
Slomka in Hannover vor dem Aus

Computer gehackt: Holzfäller verliert sämtliche Daten
Botnet Activities

• JavaScript
  – Network scans ... maybe router-XSRF
  – BitCoin mining
  – Hash cracking
  – DDoS attacks
  – You name it!

• Generation of new TV formats ;}
Resistance is Futile
Countermeasures
Disconnect SmartTV

The chart shows the percentage of respondents who own a smart TV, are connected to a smart TV, and the share of connected smart TVs by age group. The data is categorized into four age groups: All, 18-34, 35-54, and 55+. The graph indicates a decrease in the percentage of respondents owning a smart TV and being connected to a smart TV as the age group increases. The share of connected smart TVs remains relatively consistent across all age groups.
Use a Proxy/Firewall
Filter/Block DNS
HAL – To Serve & Protect
How HAL works

• Virtual Server in Germany
  – ServerBiz

• DNS Server
  – tinyDNS

• Webserver with catch-all
  – nginx
  – Document tree with symbolic link structure
    • Some TVs perform HEAD request before GET
HAL Stages
HAL Stages

• Stage 1 – Collecting Data
  – HbbTV application Data
  – Smart TV Data

• Stage 2 – Data Analysis
  – Definition of criteria for HbbTV apps

• Stage 3 – HbbTV app auditing

• Stage 4 – White-List Generation

... in iterating repetitions ...
HAL Units
Data Collection Unit

3sat|1.1079.28007|Samsung|http://hbbtv.zdf.de/zdfstart/index.php

• Station name
• DVB Triplet
• TV Manufacturer
• Red Button URL
Good morning, Dave!

Shortly, I am going to check your device for certain properties. The outcome of these checks is transferred to one of my external storage units (an external server) for later analysis. I hope you are not concerned about this.

Hit the red button whenever you are ready to start!

Waiting for you to start!
SmartTV Auditing Unit

• Checks for
  – Available HTML5 objects
    • WebSockets, WebWorkers, AppCache, SessionStorage, LocalStorage, WebSQL
  – Objects from Open IP TV Standard (OIPF)
    • ApplicationManager, VideoBroadcast, DownloadManager, DownloadTrigger, ParentalControlManager, CodecManager, DRMMManager, GatewayInfo, InternetMessagingService, RecordingScheduler, SearchManager, MulticastDeliveryTerminatingFunction, StatusView, Configuration
  – Personalized Data
HbbTV App Auditing Unit

• Use of HTTrack Website Copier
  – http://www.httrack.com/

• Static code analysis
  – Very basic
  – Mainly manual
  – A lot of room for improvement 😊
HAL Goal

• DNS Server for SmartTVs
  – Only clean service endpoints get resolved
• Security relevant info about SmartTVs
  – without having to buy all of them
• Overview of HbbTV services (worldwide)
  – Along with a classification info
How to use HAL

• Just use the following IP as the DNS server for your TV
  109.230.231.222

• Also Spooofticker® will be visible then

• Also check
  trifinite.org/hbbtv/
Upcoming FS1 Co-Operation

http://fs1.tv/
OpenCaster

http://www.avalpa.com/
MitXP HbbTV-Testsuite

MIT-xperts HBBTV testsuite

- About / Imprint
- Get and set channel
- Channel list
- Video swapping and scaling
- Video controls
- Streaming video playback events
- Streaming video/audio formats
- AVComponents in video/broadcast
- DOLBY video format / AVComponents
- Memory audio
- Broadcast in background
- Application manager
- EIT events

Testsuite release: 1.7.3 (20131204)

HBBTV testsuite project initiated/maintained by:

MIT-xperts

Instructions:
Please select the desired test using the cursor keys, then press OK. After that, test-specific instructions will appear. More information is available under "About / Imprint".
In case you have questions and/or comments, you can reach us at info @ mit-xperts.com

Test description:
Displays more information about this testsuite (this is no test).

https://github.com/mitxp/HbbTV-Testsuite
TV Application Layer

http://fmtvp.github.io/tal/index.html
Credits to...

- Collin Mulliner
- Emerson Tan
- Eva
- Graf Zahl
- Lukas Grunwald
- Matthias Zeitler
- Michael Schäfer
- Roger Klose
- trifinite.group

- BerlinSides Conference
- n.runs professionals GmbH
- Der Postillon – Stefan Sichermann
- IF WE DON'T, REMEMBER ME.
  iwdrm.tumblr.com
Thank You!

More: mherfurt.wordpress.com

GooglePlus Community: HbbTVSecurity
blog.nruns.com trifinite.org/hbbtv/