Protecting TV Receivers Against Attacks via the Broadcast

Jon Piesing

Chair DVB TM-MIS

Background

- Several security researchers have experimented with attacks on TV broadcast
  - Intercept broadcast TV signal, modify & re-transmit
  - Demonstrations given to HbbTV and DVB audiences
- Experiments focus on interactive elements of the broadcast
  - Theoretical possibility of modifying video, audio or subtitles
    - Likely to be more complex and with a range of counter-measures
  - Some attacks on interactive elements don't need active involvement of the viewer
    - Autostart apps run on changing to a channel just like video and audio
- DVB and HbbTV worked together to define requirements for a solution for interactive services
  - DVB is now working on a solution that meets those requirements

Why Now?

- Attacks via broadcast have been discussed for at least 15 years
  - Initially called “man in a van attack”
- Several things have changed in the last few years
  - Price and size of DVB-T modulators has fallen
    - E.g. UT-100Cfor US$170 - $230 http://www.hides.com.tw/product_cg74469_eng.html
  - Price & size of equipment to modify streams has fallen
    - Can now be done in software on a Raspberry Pi
  - TV sets now use commodity software
    - Exploits for bugs in open source software (e.g. libraries and/or browsers) can be aimed at TVs

Example Terrestrial TV Attacks

Transmission mast

MITM drive-by re-transmission

Urban / suburban DTT receivers

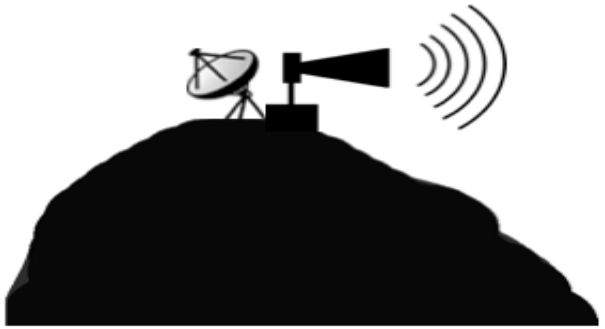
Terrestrial Transmitter

MITM Static Retransmission

Multiple Dwelling Unit (MDU)
Or Cable/IPTV/Relay Station ingest point

Example Satellite TV Attacks

Satellite broadcast



Static satellite re-transmission

Urban / suburban DSAT receivers

Satellite broadcast

(persistent vs transient)

Multiple Dwelling Unit (MDU)

How Many People Might an Attack Reach?

- Densely populated urban area might have up to 5900 people per square km
  - Mobile attack with 60m radius would therefore cover 67 people or 29 households
    - TV reception on the attacked multiplex would also be blocked for a much larger area around the 60m attack radius
- Degree of success depends on proportion of TVs that are;
  - Both smart (i.e. connectable) and actually connected?
  - In use at the time?
  - Tuned to a channel on which the attack is happening?
  - Vulnerable to the exploit(s) selected by the attacker?
- Making assumptions and multiplying these out suggest 30 attacks might be needed to get a single victim
  - If 10-second attacks are performed every 30 seconds and are limited to 4.5 hours each day of peak viewing time, then 540 attacks can be performed in each session and should yield about 14 victims

Source: DVB CM-SEG calculation based on publicly available statistics

Work in DVB

- Detailed threat analysis
  - Far more detail than is included in this presentation
- Solution in 2 parts
  - Mechanics of how to authenticate data in the interactive broadcast
    - See next slide for some details
  - How to establish trust
    - E.g. Broadcasters issue certificates to themselves which become trusted over time as they are seen by a TV
    - E.g. Broadcasters issue certificates to themselves which are cross-sponsored by others so as to become trusted without any delay
    - E.g. Platform operator or network operator issues certificates to broadcasters
    - Still a work in progress
      - Searching for solution that is adaptable between markets where service providers can be expected to cooperate and other markets where this cooperation is less likely. Unfortunately the protection that can be provided may not be the same in all markets

Some Technical Details

- Authentication messages are added to the broadcast
  - Contain hash values for AIT and object carousel sections
  - Also contain a signature to validate the hash values
    - See “how to establish trust” for how a certificate would be obtained to verify this
- Authentication messages can be carried either
  - in the PID carrying the AIT and/or carousel they authenticate or
  - in another PID, e.g. for a carousel spread across multiple PIDs
- Receivers cache validated hash values and match them with incoming AIT and object carousel sections
  - Incoming AIT and carousel sections are kept in a quarantine buffer until a matching hash value is found or the buffer becomes full

What Comes Next

- Finishing the specification
  - Making good progress
- Test descriptions and test material
  - DVB does not do testing – this will be up to HbbTV and other users of the specification
- Deployments
  - This work is an insurance policy & Insurance policies have a premium
  - Participants in each market will have to evaluate the risks and decide if the premium is worth paying

Thank You