# HbbTV and Security

HbbTV takes security very seriously. Security researchers who wish to disclose vulnerability in an HbbTV specification should contact info@hbbtv.org in order to enable a constructive engagement. Vulnerabilities associated with a specific manufacturer's implementation of HbbTV should be reported to the manufacturer concerned but HbbTV can assist in facilitating this.

## Tampering with Broadcast Transmissions

Tampering with the broadcast transmissions is currently an area of interest for security researchers. Whilst HbbTV does not define the specifications for broadcast transmission, we take this topic very seriously and work actively with the other standards organisations responsible such as the DVB project on such matters, as well as making revisions to our own specifications to protect users.

Relevant publications include the following;

- Technical University of Berlin (April 2015)
  Benjamin Michéle, Smart TV Security. Media Playback and Digital Video Broadcast, Springer Verlag, 2015

- Columbia University (May 2014)
  www.cs.columbia.edu/~angelos/Papers/2014/redbutton-usenix-sec14.pdf

Although a number of aspects of the Columbia University paper are challenged by the TU-Berlin paper, HbbTV acted promptly to correct a vulnerability that could have allowed misuse of HTTP cookies from a broadcast-delivered application. This vulnerability was corrected in the August 2014 errata to our HbbTV 1.5 specification and was also addressed in our HbbTV 2 specification before publication. For more technical details, please see below (1).

The research underlying the TU-Berlin paper was first disclosed to HbbTV in autumn 2014. This research does not identify a feature or bug in HbbTV. Instead, it highlights the possibility for someone tampering with the broadcast to use HbbTV as a vehicle to exploit bugs in TV implementations. Although this is not a feature or bug in the HbbTV specification, we are working on a solution to enable TVs to identify and reject broadcasts that have been tampered with. At the time of writing, we have developed a detailed set of requirements for such a solution and have identified a preferred approach. For more technical details, please see below (2). We are working closely with DVB on this matter and hope a solution can be included in one of their specifications in time to meet market expectations. This work has been done in co-operation with the author of the paper with exchanges of information and feedback throughout the process. We would like to express our thanks to the author for his constructive participation.

Outside of the laboratory, the level of threat from tampering with the various types of broadcast transmissions is not yet fully known. For example, the TU-Berlin paper points out that an attempt to target a whole area would likely cause loss of TV reception to a much wider number of people, aiding detection. Also, for an attack on a vulnerability in a particular TV model, only people with that specific TV would be affected and only if viewing the tampered channel. Nonetheless, users have a right to expect that their televisions are secure and HbbTV recognises that attacks continue to advance.  Therefore, specifications and test materials will be updated to provide additional protection for users. Actually deploying the updated specification will require receiver manufacturers, broadcasters and network operators to be convinced that it is a threat in the real world.

## Technical Details

Here is a simple high level description of the technical details of the recently reported threats and their solutions. This section is aimed at engineers at companies using HbbTV rather than security experts and does not cover the attacks and remedies in full detail.

(1) A key component of the web security model is the origin of an HTML document (https://tools.ietf.org/html/rfc6454). Various features and APIs are only available when two pages come from the same origin (http://en.wikipedia.org/wiki/Same-origin_policy). Protocols like XMLHttpRequest use a technology called CORS (http://www.w3.org/TR/cors/) to enable web servers to reject connections based on the origin. Origins in the web are an http or https URL.

One extension of HbbTV compared to the web is the ability to deliver HTML documents through the broadcast. The HbbTV specification prior to August 2014 allowed a broadcaster to specify the origin to be used for these documents, e.g. http://broadcaster.com/a/b/c/d. The Columbia University paper pointed out that if an attacker could tamper with the broadcast, they could use this feature to connect to other web sites (e.g. social media) using cookies stored from previous user interaction with those sites, allowing the attacker to perform cross site request forgery (CSRF) attacks. Although in practice many TV implementations would limit the opportunity for such attacks due to using different browsers for SmartTV (more likely to be used for access to social media) and for HbbTV, still HbbTV promptly addressed the issue.

The HbbTV specification was changed in August 2014 - see (http://www.hbbtv.org/pages/news_events/pdf/140819_HbbTV15_Errata2.pdf) – to define the origin for an HTML document delivered through the broadcast as a “dvb:” URL constructed from information in the broadcast signal. By doing so, even if an attacker were to tamper with the broadcast stream, the TV set will always use a “dvb:” URL for the origin of a broadcast delivered document, thus blocking the ability for such an attacker to forge a request with an “http” or “https” URL as the origin.

This same change was included in the HbbTV 2 specification under development at that time. The HbbTV test suite will include tests checking that the new behaviour is supported and that the former behaviour is not supported.

(2) The TU-Berlin paper describes an attacker tampering with the broadcast in order to use HbbTV to cause a TV set to play a malformed media file. The malformed media file then exploits a bug in the media player component used in a particular make and model of TV set, ultimately allowing the attacker to take control of that TV. HbbTV decided that it would enable TV sets to detect and reject tampering with the broadcast hence preventing the use of HbbTV as a delivery mechanism for attacks on the internal software of a TV set. A wide variety of different approaches for this were evaluated. In the end we reached a preference for an approach based on authentication of the

MPEG-2 ‘section’ structures in which HbbTV applications and their associated signalling are delivered.

Our preferred approach is to add extra tables to the elementary stream(s) containing the AIT and the DSM-CC object carousel (and perhaps those carrying DVB-SI). These tables would contain both signatures for the existing sections in these streams and certificates containing keys to validate those signatures. The certificates can either be i) anchored by regular certificates from a PKI if a country or operator organises one of these or ii) persistent broadcaster self-signed certificates. For the second of these, we have decided on an approach for deriving trust based on the certificates having been seen in the broadcast for some time.

We are working closely with DVB and hope that an updated specification including a solution for this type of attack can be completed by the end of the year.