Watch and be Watched: Compromising All Smart TV Generations

Benjamin Michéle, Andrew Karpow

Security in Telecommunications
TU Berlin and Telekom Innovation Laboratories
Berlin, Germany

CCNC’14
Motivation
Interesting novel target on Smart TVs

Media players!
Interesting novel target on Smart TVs

Media players!

Scope and impact

- Contain complex media parsers
  ⇒ Very promising target
- Present on virtually every Smart TV since 2009
- Regardless of vendor
- Actually used by many TV owners
- Camera + microphone + network connectivity
  ⇒ Privacy nightmare
Attack overview

1. Compromising All Smart TV Generations
   Benjamin Michéle (SECT)
   CCNC'14 4 / 12
Media player overview

- FFmpeg / libav for format detection
- Samsung, LG, possibly others
- Result passed back to proprietary SW player
- SW player provides HW playback with data
Media player pseudocode

```c
av_register_all();
av_open_input_file();
puts("open successful");
dump_format();
seek(begining_of_file);
start_playback_natively();
```
PoC attack: Malicious movie file

1. Compromise FFmpeg’s probing function
2. Spawn new process for malicious payload
3. Seek in media file to benign video
4. Overwrite results of media format detection
5. Pass benign movie data to SW player
6. Stealthy pwning done :)

Benjamin Michéle (SECT)
Example: Samsung B650

- 4xm media format
- CVE-2009-0385: Integer signedness error
Example: Vulnerable code in 4xm

```c
1 int cur = -1; // current track
2 int track_count = 0; // total tracks
3 AudioTrack *tracks = NULL;
4 for (i=0; i<header_size - 8; i++) {
5   if (fourcc_tag == strk_TAG) {
6     cur = RL32(&header[i+8]);
7     if (cur+1 > track_count) {
8       track_count = cur + 1;
9       tracks = av_realloc(tracks, track_count*20);
10      }
11     tracks[cur].adpcm = RL32(&header[i+12]);
12     tracks[cur].channels = RL32(&header[i+36]);
13     tracks[cur].rate = RL32(&header[i+40]);
14     tracks[cur].bits = RL32(&header[i+44]);
15   }
16 }
```
Potential payloads

- Tap into built-in camera and microphone, send over the Internet
  ⇒ See demo at 13:00 :)

- Attacks on local network
  - Steal files from USB or file servers
  - Steal private content displayed on TV
  - Attack systems on local network
    ⇒ Likely no further firewall, TV is inside the private network

- Valuable resources: computing power, energy and bandwidth!
  - Botnets
  - Bitcoin mining
Conclusions

- Media parsers are very complex, leads to vulnerabilities
- Present on all Smart TVs since 2009, regardless of vendor
- We built a PoC that works on virtually all Samsung Smart TVs
- Vendors have to be made aware of risks
- We propose effective countermeasures
  - Execute media parsers in unprivileged, sandboxed environment
  - Remove parsers for unsupported formats
Watch and be Watched: Compromising All Smart TV Generations

Benjamin Michéle, Andrew Karpow
ben@sec.t-labs.tu-berlin.de
www.fgsect.de

Security in Telecommunications
TU Berlin and Telekom Innovation Laboratories
Berlin, Germany

CCNC’14