Hacking (Hybrid) into Broadband and Broadcast TV system

How to setup and use a quick and dirty testbed for security evaluations

P. Barre, C. Kasmi, T. Sabono

26 November 2018

xen1thLabs
A DARKMATTER COMPANY

SMART AND SAFE DIGITAL

Content

Who we are

- Pierre Barre, Senior Security Researcher, Mobile and Telecom Lab
- Chaouki Kasmi, Lab Director, Mobile and Telecom Lab
- Thomas Sabono, Lead Security Researcher, Software Lab

- Tests and Validation Labs, Xen1thLabs, DarkMatter LLC
- www.darkmatter.ae

01

Smart TV…
not so smart when talking about security

What is a Smart TV

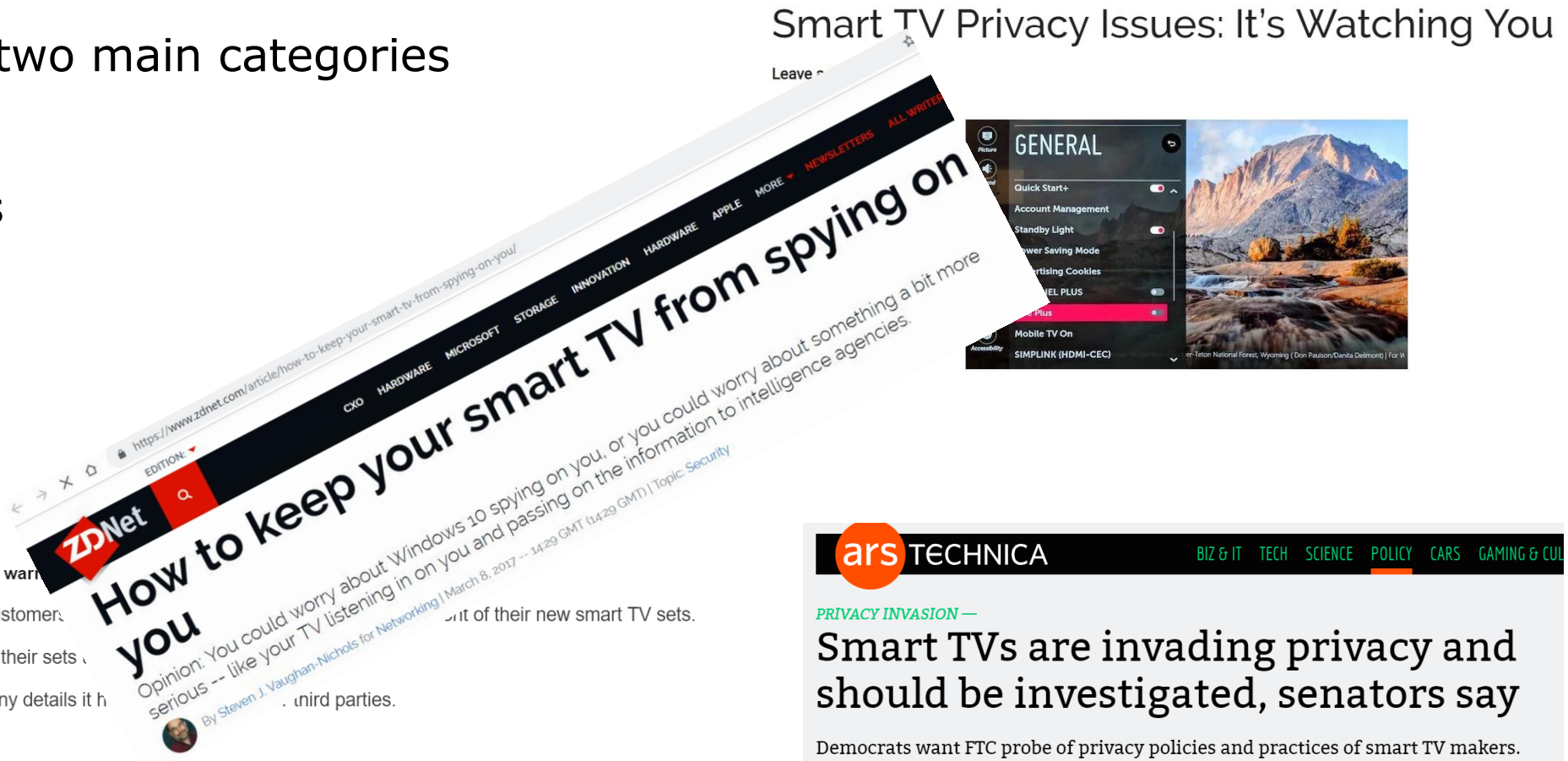
Smart TV = TV + multiple network interfaces + a “smart” Operating System

- Integration of web technologies
- Integration of applications (like smartphones…)
- Increasing entertainment with HbbTV
- Wireless parts
  - IR/DVB-T/DVB-S/ and Bluetooth/3G/4G
  - Built-in or additional dongles

What could go wrong?

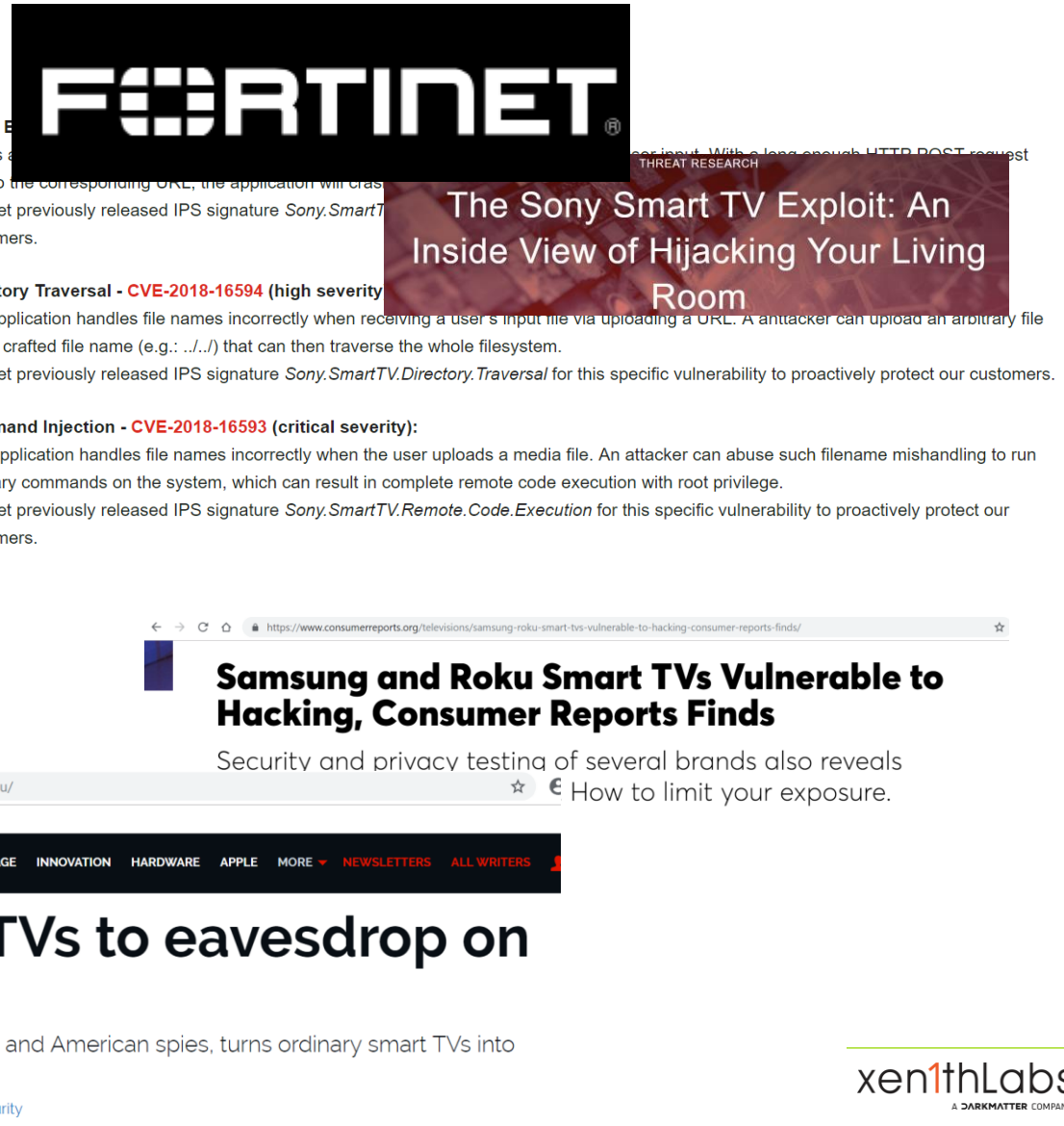
What has been done

- Many studies – two main categories
  - Privacy
  - Many studies



What has been done

- Many studies – two main categories
  - Security
  - Many papers
  - Multiple attack vectors
  - Computer security level in 2000s

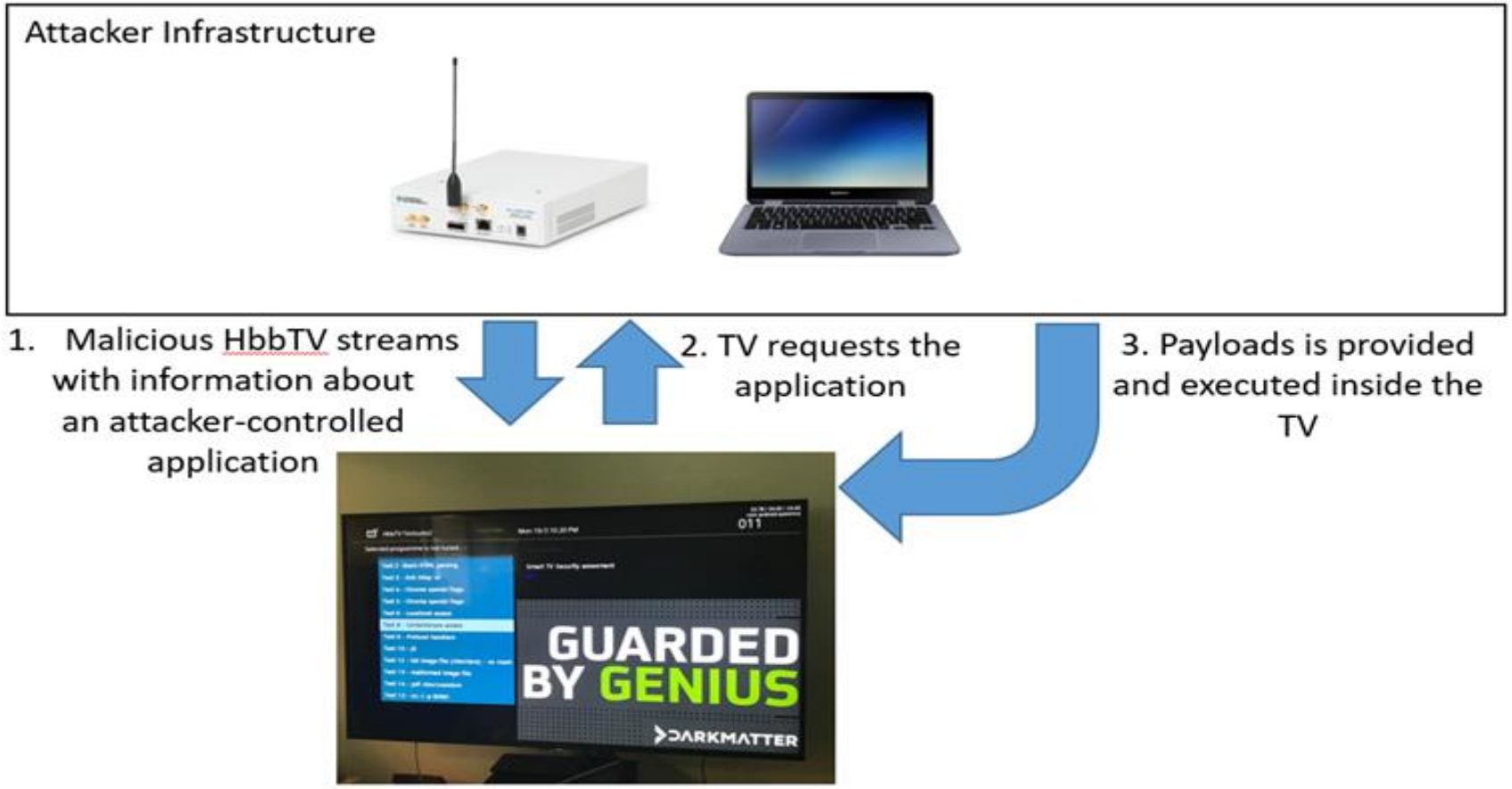


Why a new Talk on this topic

- Most studies:
  - Highlight findings
  - Nice vulnerabilities and demos
  - Few covering the testbeds for the community
  - Quick combinations can lead to big findings
  - Blogpost to be released describing the platform

What we have built

- HbbTV Testsuite [1]
- DVB-T – gr-dvbt [2]
- USRP/HackRF [3]
- A Target
- Multiple payloads
- 0 days – CVEs



What's Next

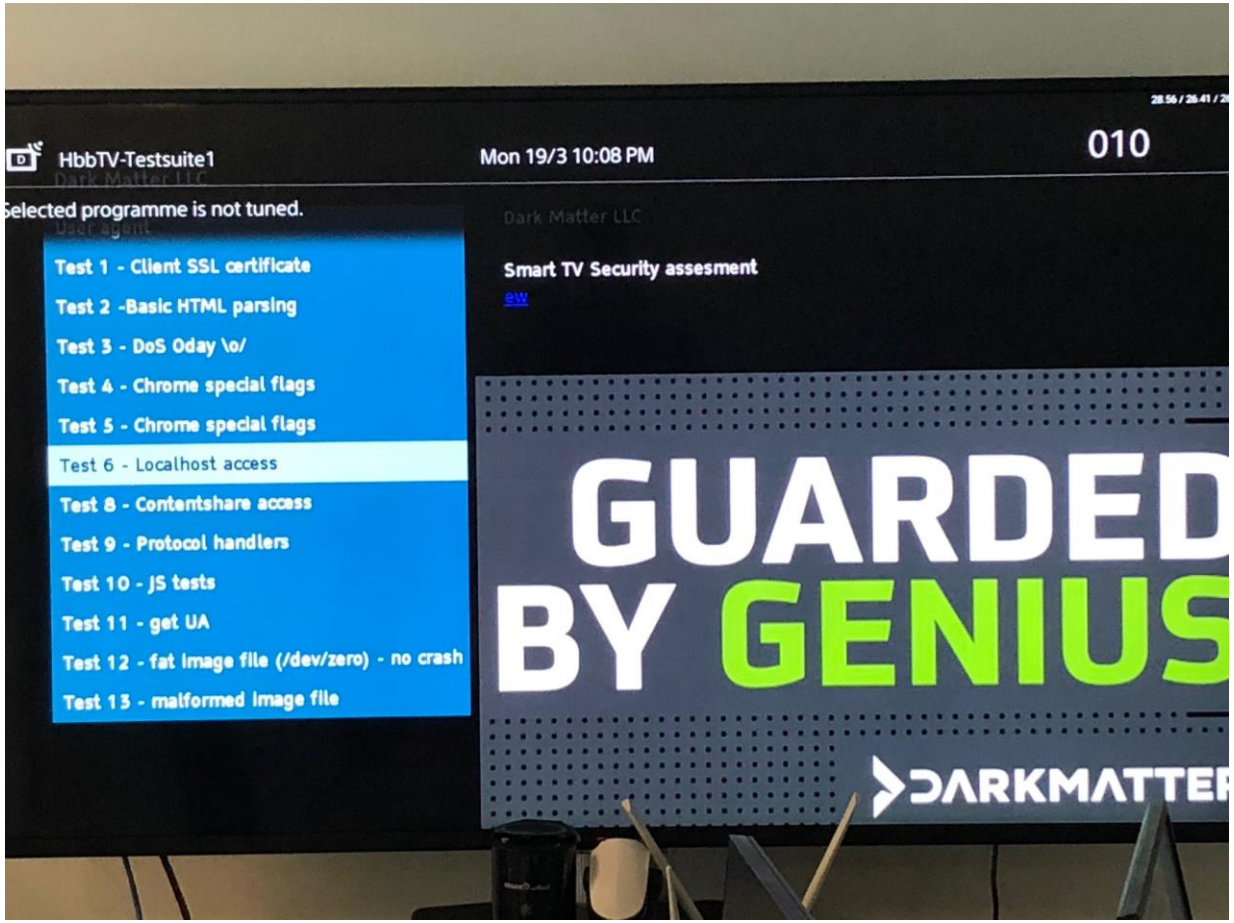
- Targeting the Smart TVs
  - Daemons on (W)LAN
  - Miner
  - Exploits
  - Malicious Applications
  - Ransomware
- Targeting networks
- Targeting devices

02

Target 1: The Smart TV

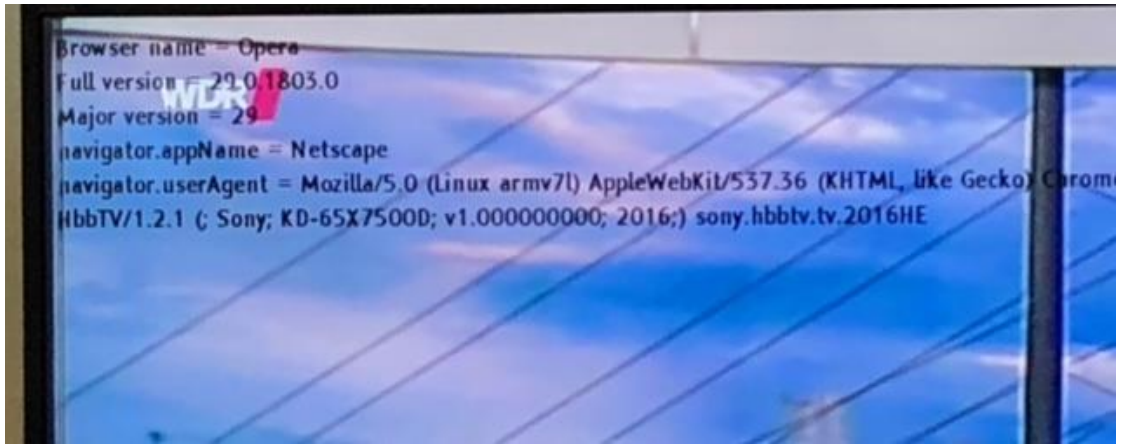
Attack Surface

- Category
  - Applications
  - APIs / Libraries
  - Network



Attack Surface - Applications

- Outdated applications
  - Opera browser
    - version 29.0.1803 (2015)
    - Rendering engine – Chromium (v.42)
    - JavaScript engine – v8
- Debug applications
  - Android Debug Bridge (ADB) 5555/tcp
- Targeted attacks
  - Browser based attacks
    - Headers
    - URLs
    - Schemes



Attacks Surface – API / Libraries

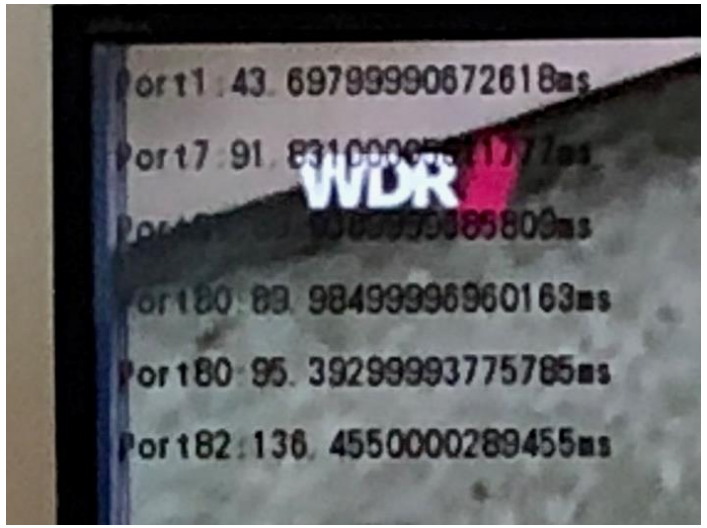
- API / Libraries
  - Outdated libraries (parsing)
    - WebM / MP4 / JPEG / PDF / SVG
  - Custom libraries / APIs
    - JavaScript
    - Electronic Program Guide (EPG)
    - XML AIT (Broadcast independent applications)

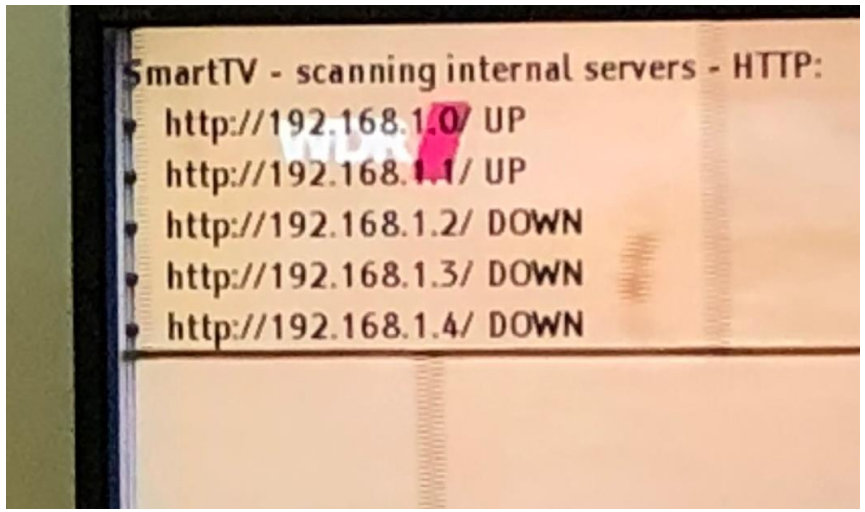
Attacks Surface – Network

- Network
  - WebSockets / XMLHTTP requests
    - Reach others process inside Smart TV
    - Reach others devices in (W)LAN
  - Metadata inside streams
    - Service Description Table (SDT)
    - Fake news – Live demo

Attacks Surface - Pivot

- Pivot
  - Relay to voice-enabled assistant devices
  - Crypto-mining
  - Port scanner
  - Stage X payload on other devices on LAN





03

Target 2: Expanding the attack Surface

Expanding the Attack Surface

- Hacking TVs is cool but what about other devices ?
- Using the TV as a relay to attack the (W)LAN:
  - LAN (in)security – routers, NAS, cameras, IP Phones, network appliances
  - WLAN (in)security – routers, AP
  - We can execute code (JS, WebSocket, WebAssembly - depending of the television models)
- Masterplan
  - Network Scanning using JS or WebSocket
  - Service enumeration
  - Writing exploits in JS – based on public CVEs/0days
  - RCEs against daemons exposed on the LAN (UPNP, httpd of routers, custom daemons), everything TCP related (limitations of JS and websocket)!

TV as a relay

- Reality VS Masterplan
  - First PoC – DDoS using Televisions – live demo
  - JS parsing is BAD
  - Browser security anyone ?
  - Debugging a lot – tcpdump, adb, luck
- Results
  - Network Scanning using JS and websocket
  - Exploiting CVEs and 0-days against devices
    - Camera – pre-auth RCE as root, live demo
    - Router – pre-auth RCE as root, ~~live demo~~
  - Huge success!

TV as a relay

- Websocket and JavaScript are very powerful
- Future:
  - ADB in JavaScript
  - Scanning + implementation of CVEs in JavaScript
- Television are complete toolkits for attackers
- Very hard to defend against attacks from TVs, even in a closed network

Conclusions

Conclusion

- 2014 – full of vulnerabilities
- 2018 – still full of vulnerabilities
- **Use your SmartTV as a CRT monitor…**
  - Deactivate HbbTV option (software…)
  - No Wifi
  - No Bluetooth
  - No HbbTV
  - No RJ45
- Security assessment of devices
- Risk evaluation

Q/A

Thank you

References

[1] Hbbtv Test Suites, https://github.com/mitxp/HbbTV-Testsuite
[2] gr-dvbtv, https://github.com/BogdanDIA/gr-dvbt
[3] USRP, ettus.com, https://www.ettus.com/
[4] GNURadio, Signal processing and RF , https://www.gnuradio.org/