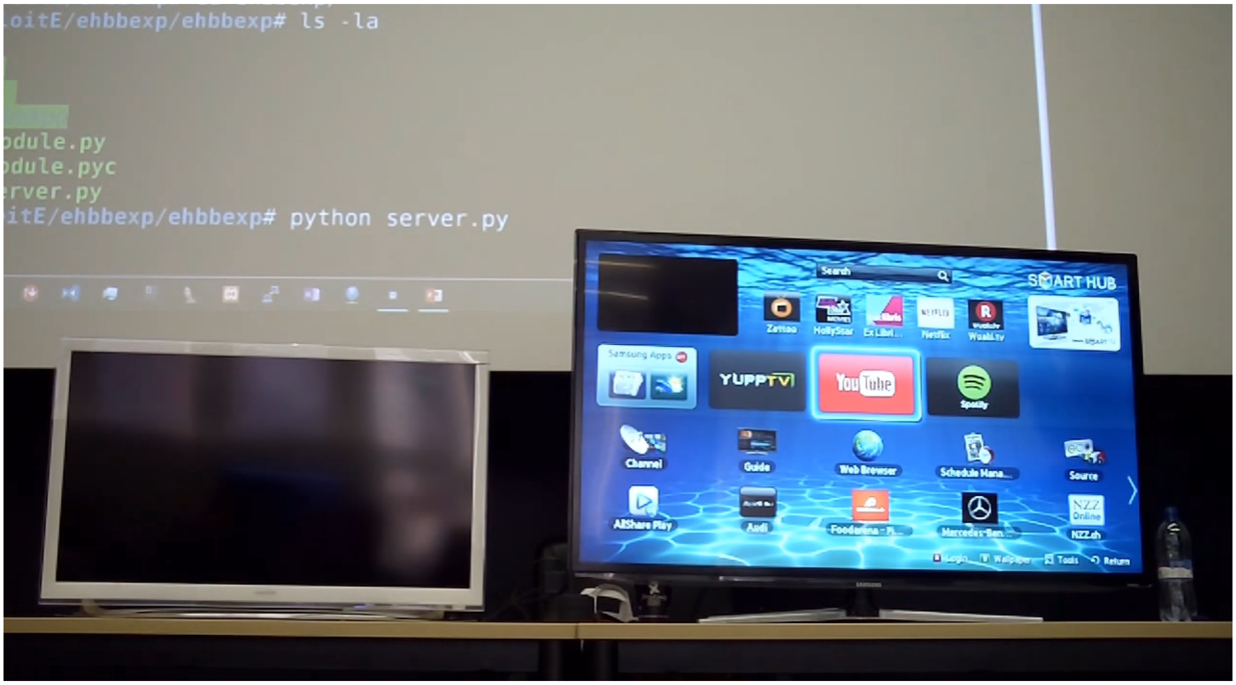
TechXplore

Researcher at security event shows smart TV attack

April 3 2017, by Nancy Owano



```
oitE/ehbbexp/ehbbexp# ls -la
odule.py
odule.pyc
rver.py
itE/ehbbexp/ehbbexp# python server.py
```

(Tech Xplore)—Smart TVs vulnerable to hacks? That is no longer a question but an answer, for researcher Rafael Scheel, with Oneconsult, a cyber security consulting company.

He has demonstrated an attack involving stream signals. The company notes about the presentation said Scheel "gives an introduction to IoT cyber security and shows in a live hacking demo an attack which allows to remotely takeover bulks of smart TVs over the TV stream signal."

Nick Farrell in *Fudzilla* in addition to other technology sites reported on the findings of Oneconsult.

According to the company, "About 90% of the TVs sold in the last years are potential victims of similar attacks."

What has attracted attention is how this type of attack is remote. Catalin Cimpanu in *BleepingComputer*: "Until now, all smart TV exploits relied on attackers having physical access to the device, in order to plug in an USB that executes malicious code. Other attacks relied on social engineering, meaning attackers had to trick users into installing a malicious app on their TV."

The security researcher noted that the attack was possible without a user's interaction and was able to be remotely executed. The stealthy exploit can be run in the TV's background processes, said Farrell in *Fudzilla*. And so the user does not have a clue if an attacker carried out the compromise.

Ars Technica led off with the headline, "Smart TV hack embeds attack code into broadcast signal." Dan Goodin said the attack involved "terrestrial radio signals."

The hacker need only turn on a transmitter within range of a large number of sets, say, in a densely populated apartment building or from a balcony that's near a TV of interest, wrote Goodin.

"Scheel's exploit relies on a transmitter that's based on digital video broadcasting—terrestrial, a transmission standard that's built into the vast majority of TVs. TVs that are connected to the Internet, are currently tuned to a DVB-T-based station, support the hybrid broadcast broadband TV standard, and contain at least one critical vulnerability that can be exploited without showing any outward signs anything is amiss."

An HbbTV website defines the term.

"Hybrid broadcast broadband TV (HbbTV) is a global initiative aimed at harmonising the broadcast and broadband delivery of entertainment services to consumers through connected TVs, set-top boxes and multiscreen devices. The HbbTV specification is developed by industry leaders to improve the video user experience for consumers by enabling innovative, interactive services over broadcast and broadband networks."

Scheel made his presentation, "Hacking a Smart TV," to the European Broadcasting Union (EBU).

Goodin reported that the researcher's proof of concept demo used a transmitter to embed commands into a rogue TV signal.

Goodin quoted Scheel. "Once a hacker has control over the TV of an end user, he can harm the user in a variety of ways," he told *Ars*. "Among many others, the TV could be used to attack further devices in the home network or to spy on the user with the TV's camera and microphone."

Goodin highlighted some key points about the findings. "The infection was also able to survive both device reboots and factory resets." Also, Scheel's approach can work against many TVs at once.

Last but not least, "The hacks underscore the risks of so-called "Internet of Things" devices, the vast majority of which are given network access and computing functionalities without being adequately secured."

[Scheel had said, as stated earlier, that "Among many others, the TV could be used to attack further devices in the home network."]

More information: www.oneconsult.com/en/smart-tv-hacking/

Citation: Researcher at security event shows smart TV attack (2017, April 3) retrieved 9 April 2024 from https://techxplore.com/news/2017-04-event-smart-tv.html