ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 22-24

Compromising Smart Television

Mohan Kumar, Manoj Mishra, Bhavin Shah, Nilesh Gode & Kunal Shriwas
Electronics & Telecommunication Engineering Department, Atharva College of Engineering, Mumbai, India

Abstract: *Smart Televisions are offering an ever-growing number of features such as Internet access, media player's built-in cameras and microphones. They are physically placed in sensitive locations and connected to trusted home and business networks. Smart Televisions use the same operating systems and software as regular Personal Computers, leaving them vulnerable to attacks. Security updates are provided less frequently. As these systems are closed, it is difficult for users to find out and examine if the TV has been compromised. This paper shows us that Smart Televisions must not be considered trust worthy. They pose a severe security and privacy threat. We show that the integrated media player is highly vulnerable.*

Keywords: *Smart Televisions, Apps, Web Browser, Media player and Attack*

I. Introduction

Televisions have started incorporating additional features, turning them into Smart TVs. While conventional TVs were only capable of displaying broadcasted programs, Smart Televisions added features such as direct media playback, Internet access, and built-in cameras.

Smart Televisions have introduced new risks to users' security and privacy. Users are not aware of the associated risks. Smart Televisions are a valuable target for unlawful activities.

II. Smart TV Features And Risks

Televisions have been posing threats to safety due to high voltage and implosion rather than to security or privacy. This changed when Televisions were connected to the Internet. Smart Televisions have various features that could become valuable targets for attackers.

1. Apps

Numerous functions are provided through social network , shopping or streaming apps. They can be installed from online app stores or from storage device. Apps run in a sandbox and are not easily exploitable. They can store information which an attacker may steal once the Television has been compromised.

2. Web Browser

Nowadays Smart Televisions are equipped with web browsers and built-in WiFi. Users find it more convenient to surf the web on tablets, smart phones, or notebooks. It is unlikely that criminals will target browser vulnerabilities in Smart TVs unless the user base increases.

3. Media Playback

All vendors have a built-in media player for music, photos, and videos in their Smart Televisions. Files can be played from attached USB mass storage or from network storage. A movie player feature has been added in nearly all Smart TV models . This feature is used extensively by the users. In general, videos are downloaded from the web or received from friends, placed on USB disks or network storage, and played back directly on the TV using the built-in player and interface. Every movie player is vulnerable.

4. Skype, Voice Commands, and Motion Sensing

Numerous models of Smart Televisions feature built-in or add-on cameras and microphones. They can be used for Skype conversations and for controlling the TV via voice commands and gestures. By having access to conversations in personal spaces/homes, conference rooms or offices are a privacy threat.

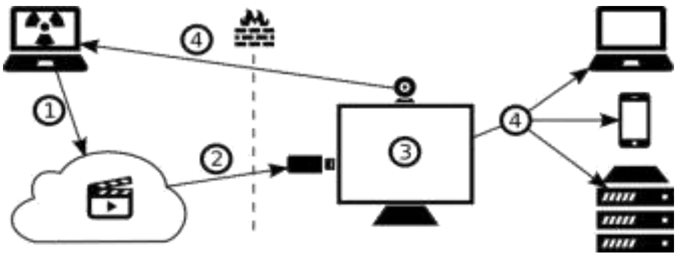

Fig. 1. Attack scenario: (1) Distribution (2) download of exploit video, (3)compromise of TV and (4)execution of payload

III. Payload

This section presents some interesting payloads that can be executed after exploiting a vulnerability in the media player.

1. Camera

In 2010, Samsung added camera support for their Smart TV that allows users to make Skype calls or control the TV by physical gestures..

The video stream cannot be captured directly using the Linux camera device, as it is used exclusively by the exe DSP process for gesture recognition. To capture the video stream unnoticed by the user, the full feature set of the TV has to be maintained.

2. Microphone

Alongside the gesture support, Samsung introduced a voice control feature. The TV continuously captures the surrounding sounds, even if the voice control feature is deactivated by the user.

3. Reflash

In many cases an attacker will be interested in installing his payload permanently on the victim's TV, so that it survives a power cycle. After compromising the TV, the attacker's code runs with root privileges and is therefore able to reflash the TV's software. Samsung has built in a protection mechanism, a process called authuld. During startup, authuld reads a kernel-supplied random value and starts to hash each flash partition using this value as a NONCE. The resulting hash value is written back to the kernel. The kernel compares this value with the expected value and, if they don't match, reboots the TV. The expected value is read from a flash partition that contains values for all partitions. If no value is reported back to the kernel before a timeout occurs, the TV is rebooted.

4. Various

Having a compromised Smart TV in a network enables the following attacks, extending the list.

I .24/7 Permanent Backdoor: The malware can be made permanent by writing a modified image to flash. The TV will then execute the attacker's payload only while the user has it turned on; however, a malicious firmware can ignore shutdown requests and instead simulate them by turning off the screen and setting the power LED appropriately.

II. Spy: A remote attacker is able to receive a live A/V stream from Smart TVs with built-in or add-on cameras and microphones.

III. Attack Local Systems in a Trusted Network: Since the Smart TV is normally attached to a trusted local network, all systems on the same network can be attacked.

IV. Offer Malicious Services: Some of the services offered by the TV are used by Smart phones, e.g., Airplay or Allshare, to send content from the phone to the TV or vice versa. If the TV is compromised, these services can exploit vulnerabilities on the smart phone using the service.

V.Exfiltrate Data: The TV has access to connected USB drives, file shares offered on the local network, and media files sent via Airplay/Allshare. Sensitive data can be collected and sent to the attacker, possibly over a long period of time.

.

IV. Conclusion

In this paper we have discussed serious threats for Smart Televisions. By using malicious media files as an attack vector we can exploit a widely used Smart TV feature. From an attacker's point of view, this approach is very promising, as nearly all Smart Televisions sold in the last half decade offer a built-in media player. The attack can be launched from far of places and does not require physical proximity to the target.

References

[1]. FFmpeg. FFmpeg security. http://www.ffmpeg.org/security.html.

[2]. M. Ghiglieri, F. Oswald, and E. Tews. HbbTV - I know what you are watching. In 13. Deutscher IT-Sicherheitskongress. SecuMedia Verlags-GmbH, May 2013.

[3]. A. Grattafiori and J. Yavor. The outer limits: Hacking the Samsung smart tv. In BlackHat USA, July 2013. https://www.blackhat.com/us-13/ archives.html#Grattafiori.

[4]. T. Klein. FFmpeg type conversion vulnerability. http://www.trapkit.de/ advisories/TKADV2009-004.txt.

[5]. M. Melanson. 4xm format. http://wiki.multimedia.cx/index.php?title= 4xm_Format.

[6]. C. Mulliner and B. Michéle. Read it twice! A mass-storage-based TOCTTOU attack. In Proceedings of the 6th Workshop on Offensive Technologies, WOOT '12. USENIX Association, 2012.

[7]. SamyGO. SamyGO, Samsung firmware on the go. http://wiki.samygo.tv.

[8]. SCO. System V application binary interface. http://www.sco.com/ developers/devspecs/gabi41.pdf.

[9]. L. SeungJin and S. Kim. Smart tv security - #1984 in 21st cen-tury. In CanSecWest, March 2013. http://cansecwest.com/slides/2013/ SmartTV%20Security.pdf.

[10]. Strategy Analytics. Global smart tv vendor market share Q1 2013. http: //www.digitaltvnews.net/content/?p=22852, July 2013.

[11]. The NPD Group Blog. Internet connected tvs are used to watch tv, and that's about all. https://www.npdgroupblog.com/ internet-connected-tvs-are-used-to-watch-tv-and-thats-about-all.

[12]. Twice.com. IHS: Smart tvs rise to 27% of tv shipments. http://www. twice.com/articletype/news/ihs-smart-tvs-rise-27-tv-shipments/105108.