Open Access License Notice

Smart TV Upgrade, Privacy Downgrade?

Abdifatah Abdi-Nur
hirsi018@umn.edu

Michele Azar
ararx013@umn.edu

Chueyee Fang
fangx264@umn.edu

Cindy Hoffman
hoff0262@umn.edu

University of Minnesota Technological Leadership Institute
Distinguished Advisor - Dr. Faisal Kaleem
Minneapolis, MN U.S.A.

Abstract - The purpose of this paper is to create public awareness for privacy and to better protect consumers from Smart TV vulnerabilities. The analysis highlights many of the seemingly harmless Samsung preloaded applications that offer consumers little privacy. With the skyrocketing sales of Smart TVs, comes a critical challenge to protect customers' Personally Identifiable Information (PII). The need to educate and drive security awareness falls on both the private and public sector. Manufacturers, retailers, customers, and legislators need to help define the scope of protection required to mitigate the risk. This paper looks at the need to create public awareness for privacy and explore possible mitigation strategies to better serve and protect consumers from Smart TV vulnerabilities.

Categories and Subject Descriptors

K.3.2 [Computers and Education]: *Computer and Information Science Education*

General Terms

Privacy, Security

Keywords

CISSE, Education, IoT, Internet, Privacy, Regulation, Security, Smart Home, Television, TVs, University of Minnesota.

1 INTRODUCTION

There has been a rapid increase in Smart TV ownership and vulnerabilities. This accelerated growth began in December 2012 when news outlets reported that Smart TVs were the next untapped frontier for data theft [1]. Three years later, in February 2015, Samsung admits to spying on consumers by enabling the TV's microphone [2]. Moving forward to late 2015 and early 2016, a Symantec employee infects his TV with ransomware [3]. Most Smart TVs are shipped with default applications, such as Amazon, Hulu, and Netflix. That said, there are concerns over the details of what user information is sent and where it goes. When default applications were launched, and executed, several conversations to external entities occurred. Two important points were discovered during this analysis: 1) the chatter was not always specific to the launched application; and 2) the privacy agreement did not clarify what information was considered private. This paper covers data transmissions under the Obama administration and the Federal Communications Commission's legal authority to restrict manufacturers from a privacy free-for-all. However, there's been a change in elected officials with Donald Trump sworn in as the 45th president of the United State on January 20, 2017 [4]. Since the change in political office, President Trump signed a bill on April 4, 2017 repealing the Federal Trade Commission's authority to restrict consumer privacy and enable manufacturers to obtain and sell individual's data to the highest bidder [5]. It is imperative consumers learn and practice digital citizenship skills in order to navigate "the digital world safely, responsibly, and ethically" [6].

2 BACKGROUND

The Smart TV came into existence late 2005 as a method to standardize web content for Consumer Electronics (CE) devices [7]. The focus was to establish a way for consumers to have a lean-back Internet experience on CE devices without major effort by the content industry. This benchmark quickly accelerated into CE-HTML standard. In 2007, the Netherlands implemented a pilot program to test the market's appetite for the newly created Internet TV. The following year, Philips Electronics company matured the digital web technology and introduced the Smart TV as part of its LED TV collection in spring of 2009. This introduction was followed by an increase in production and became a magnet for content providers around the world who coined the new discovery as the "Smart TV" invention. Since 2009, the Smart TV industry has grown toward its current position with hundreds of applications available and a wide variety of Smart TV - enabled products including the Samsung brand which was tested in this paper.

2.1 A Smart TV is more powerful than a traditional TV

Not long ago, traditional TVs were used as a medium to watch news broadcasts, children's programming, and commercial shows and movies [8]. Families would make a point to be home in time to watch the latest miniseries or favorite programs. Today post-millennials, also known as Generation Z, are considered "first to have technology available at a young age" or said another way - bathed in bits [9]. This generation is accustomed to accessing media-on-demand and watching their favorite show while texting on their mobile device. The Smart TV is only one portion of the smart device sector. By the year 2009, the number of smart devices had surpassed the number of people on the planet [10]. This equates to 22.9 billion machines connected to the Internet [11]. The reason people should care about all these interconnected devices is that each device serves as a doorway for hackers to gain access to home or work networks. That said, while consumers may view their Smart TV as a medium for entertainment, Smart TVs actually pose a threat to the home - similar to a computer running out-of-date software that translates to known vulnerabilities.

3 APPROACH

The approach included the use of free open source software tools to discover abnormal traffic patterns and risky protocols destined to third parties. Software applications and devices utilized in this analysis included the following four components: 1) a network protocol analyzer tool (Wireshark 2.2.1) [12]; 2) Samsung Smart TV; 3) MacBook Air; and 4) a network capture investigator tool (Netwitness).

Samsung uses a Linux-based operating system named Tizen [13]. This architecture is an open-source software development system utilized by several different types of devices, such as, smartphones, tablets, home appliances and fitness trackers [14]. The outcome of utilizing the same software platform across several types is devices it to create a user-friendly and seamless user experience. Samsung's Tizen architecture. See Figure 1.

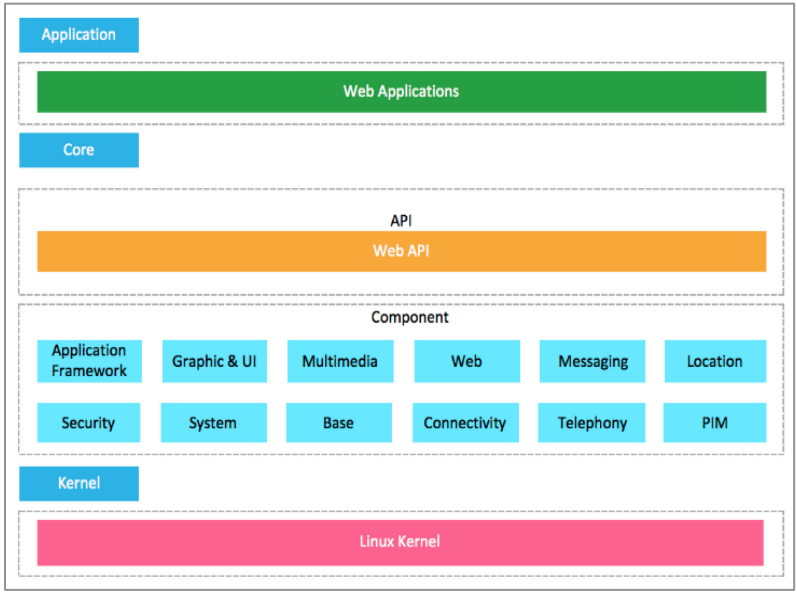

Figure 1: Tizen Operating System [14]

Our goal was to capture traffic between the Smart TV and Internet by examining six popular applications - Amazon Prime Video, Netflix, Hulu, YouTube, Fandango, and HBO GO preloaded by the manufacturer. The analysis was performed using Wireshark Version 2.2.1 to monitor wireless traffic sent between the Smart TV and the Internet as each preloaded application was individually launched. After the wireless traffic had completed for each default application, the traffic analysis was imported into a Netwitness software program to analyze each capture or log for inspection. The benefit of using Netwitness to examine packet captures was that Netwitness provides a detailed map of data as it travels between the application and the internet; whereas, Wireshark provides only a list of data transmitted between the Smart TV and the internet but does not include a way to filter or analyze the log.

4 ANALYSIS

The packet captures (.pcap files) taken from Wireshark were imported into Netwitness; which allowed us to narrow down the conversations between the Samsung Smart TV and the public internet to prove that information was being sent to third parties. It is unclear whether this information was used for malicious intent or to enhance the user experience.

4.1 Distinct exploit techniques utilize different skills and technologies

Smart TVs are vulnerable to Man-in-the-Middle (MitM) Attacks. MitM attacks likely occur in the following three user scenarios: 1) connecting to an OPEN network; 2) receiving application updates through non-secure sites; or 3) visiting an unsecure site through an application browser [15]. Intercepting wireless traffic with an open source network analyzer (Wireshark) as known as "sniffer" was simple. Even on a secured wireless network, the Smart TV was seen using a peer-to-peer protocol for screen mirroring; this is a default feature which means it is enabled right out of the box. Peer-to-Peer networking is dangerous because it can rapidly spread infected malware horizontally from one device to another without detection. Data captured in our analysis included clear text of the information shown in Figure

2 and appeared to be destined to a server located in Korea with the IP address: <http://www.sec.co.kr/dlna>.

Information shown in clear text:

- **Smart TV's Make/Model:** Samsung, LED 48 size screen
- **Model Name:** UN48J5200
- **Model Number:** 1.0
- **Screen Resolution:** 1920 x 1080
- **Serial Number:** 20090804RCR
- **UUID:** 08f0d180-0096-1000-bf66-fcf136df320e

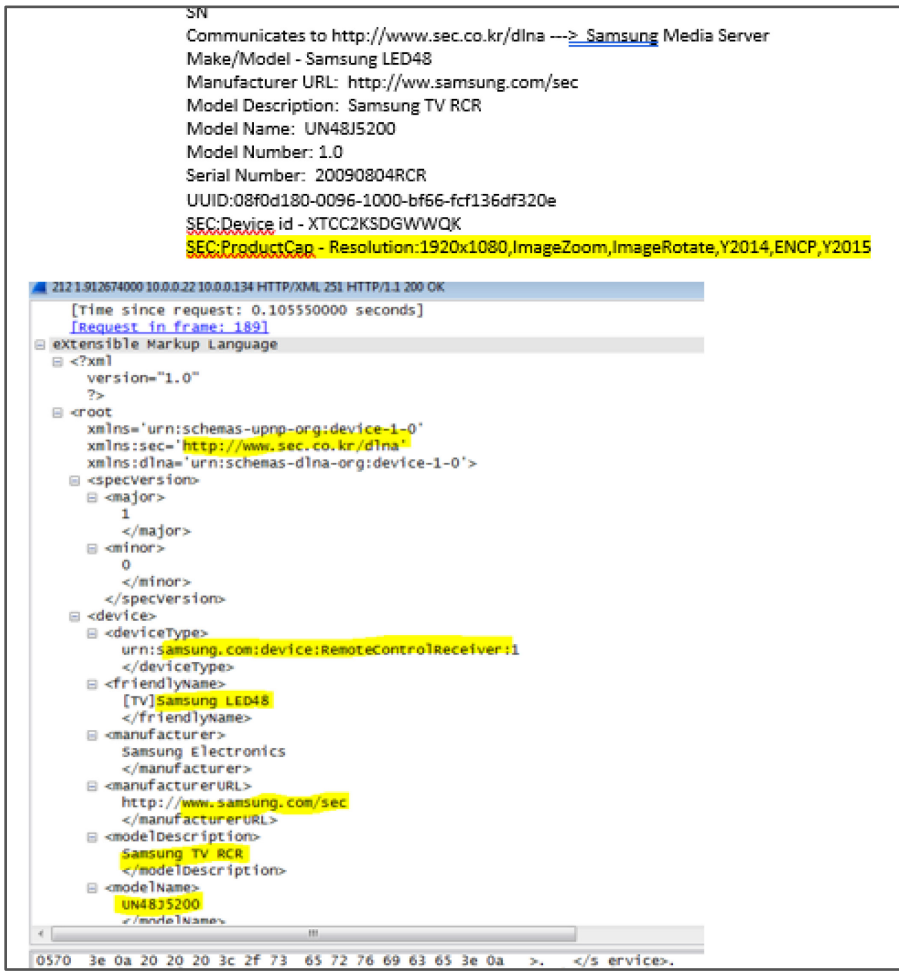

Figure 2: Samsung TV Make/Model, SN, UUID and Screen Resolution details

Smart TVs are susceptible to Ransomware attacks where an attacker could install malicious code via the web; installing an infected application through a website redirects the information to a non-SSL site, local install (with a USB) or remote access management protocol (such as telnet and SSH) [16]. Tools like the SamyGO firmware patcher demonstrate how easy it is to enable remote management tools for potential malicious intent.

Summary Steps to Enable Telnet on Smart TV [17]

1. Download Firmware (i.e. T-CHU7DEUC.exe)file for your TV and unpack
2. Unpack it wine, unrar or pZip
3. Decrypt exe.img.enc in the T-CHU7DEUC/image directory using xor decryptor with key of firmware filename. Rename exe.img
4. Change contents of the rc.local in the decrypted exe.img file
5. Recalculate the CRC32 checksum and update the validinfo.xt
6. Update T-CHU7DEUC/image directory with new CRC information
7. Encrypt exe.img using xor encryption and copy into T-CHU7DEUC/image directory. Rename to exe.img.enc
8. Flash to TV with USB following firmware wizard

List of Components shown in Figure 3:

- Samsung LED 48 Smart TV model UN48J5200
- MacBook air running OS X Yosemite version 10.10.5
- Comcast Wireless Modem/Router
- Wireshark Network Protocol Analyzer version 2.2.1
- RSA Netwitness Investigator

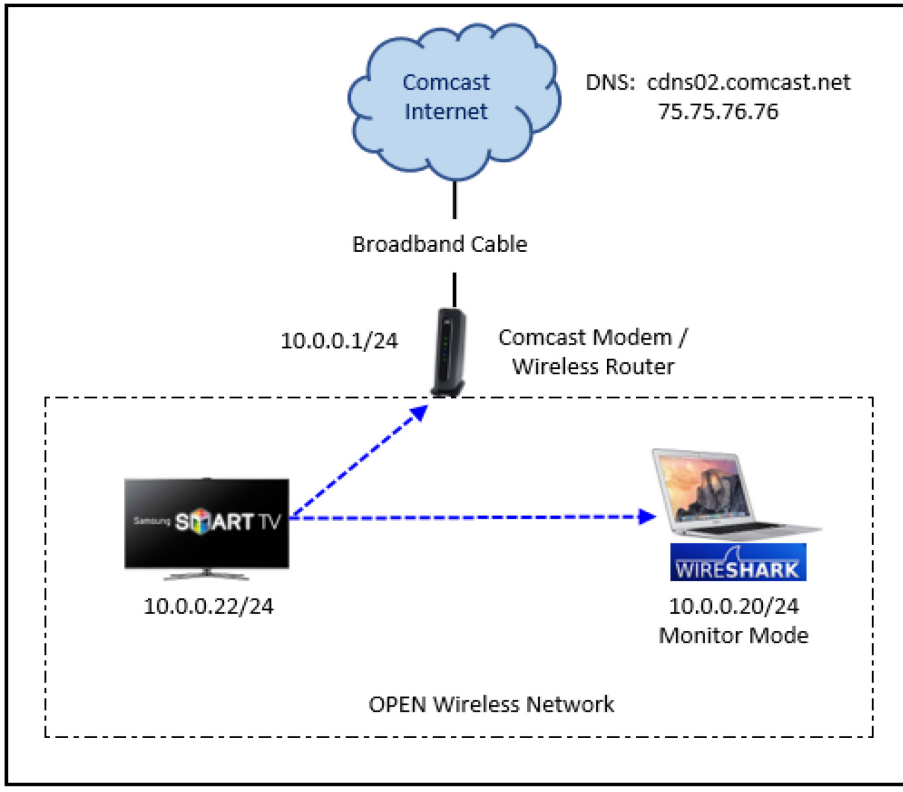

Figure 3: Network Diagram

Samsung Preloaded Applications:

- Amazon Prime Video
- Netflix
- Hulu
- YouTube
- Fandango
- HBO GO

From the analysis, it is highly likely that there were conversations to third party applications. Specifically, services hosted by Amazon AWS - 52.40.47.226 ec2-52-40-47-226.us-west-2.compute.amazonaws.com sent queries back to Navy Network Information Center (NNIC) - Virginia Beach domain name navy.mil, DoD Network Information Center – Nashville domain name army.mil, and the Commonwealth Scientific and Industrial Research Organization (CSIRO). Also, Figure 4 shows noticeable communications routed to China and the Russian Federation. Packets sent to these countries were encrypted; the data was not seen in clear text.

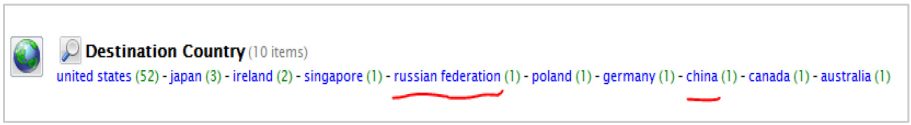

Figure 4: Amazon AWS communications sent to the U.S. and outside the U.S.

Several preloaded apps queried the applications website via non-Secure Socket Layer (SSL). The non-SSL website was eventually redirected to a secure SSL website; however, Figure 5, some of the preloaded apps like Fandango pulled images from non-SSL sites where the images were seen unencrypted and clearly visible.

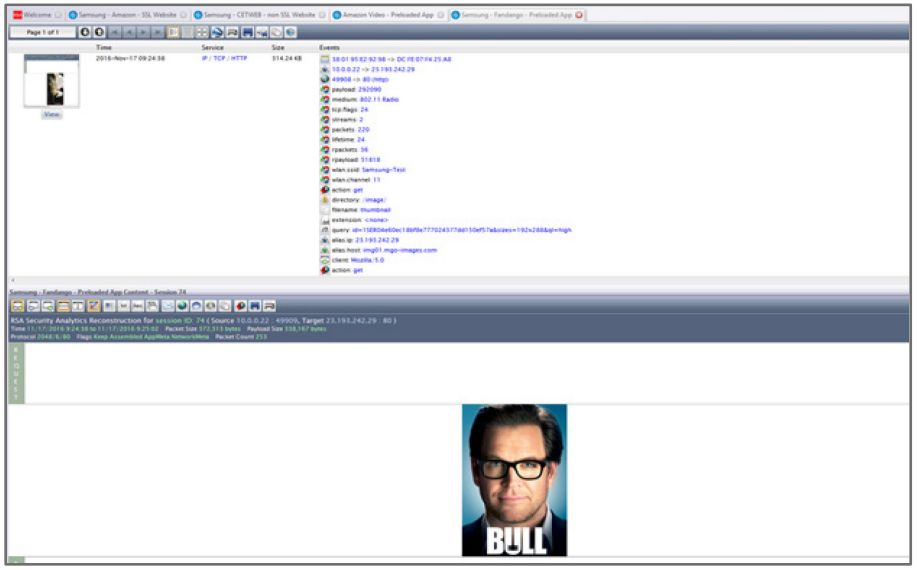

Figure 5: Fandango image from non-SSL site

To further support the analysis, additional testing was conducted to discover if traffic patterns were the same without launching any applications. From the discovery using Netwitness there were no risky protocols observed nor were there any queries to third party entities. The only traffic observed was to legitimate Samsung sites shown in Figure 6. Samsung websites shown in the screen capture include the following:

- <log-ingestion.samsungacr.com>
- <samsungcloudsolution.com>
- <upu.samsungelectronics.com>
- <noticeprd.cloudapp.net>
- <noticedn.samsungcloudsolution.com>
- <notice.samsungcloudsolution.com>
- <dpu.samsungelectronics.com>

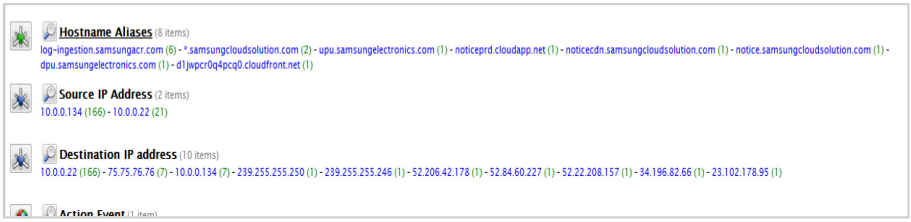

Figure 6: Traffic captures without any applications launched

Additional testing was performed in an attempt to capture usernames and passwords in clear text when logging into external sites like yahoomail.com and amazon.com. Since both yahoo mail and amazon use SSL for tunneling and data encryption, the captured packets did not reveal usernames and password information in clear text. An interesting outcome from this analysis, was the use of higher-level port numbers in all Netwitness reports. Higher level port numbers can be used by an attacker to open ports for remote access or backdoors and can also serve as a pathway for a hacker to deliver malware. In this example, the use of higher ports numbers is used to open a temporary data connection between the client and server for a specific service such as accessing the amazon application. Higher port numbers are also known as ephemeral or uncommon port number assignments. Figure 7 shows port numbers ranging from the commonly used port 80 up to less common port number of 55226.

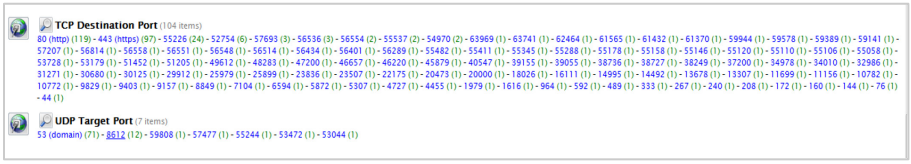

Figure 7: Destination ports used between external sites and Smart TV

5 THREAT ASSESSMENT / VULNERABILITY

For context, there are more devices connected to the Internet than there are people on the planet. This equates to 7.2 billion people worldwide with 25 billion

devices for an average of 3.47 connected devices per person [10]. This is not necessarily a problem until hackers start exploiting these devices to gain access to home or work networks. Therefore, the risks of Smart TVs should not be understated. Smart TVs that connect to home or work networks often times contain out of date software and known vulnerabilities.

The television is the latest in a long line of devices to receive "smart" enhancements which make them operate like a computer rather than a display device. Smart TVs offer consumers web browser capabilities, increased network support and enhanced user convenience; however, unbeknownst to the consumer, Smart TVs introduce potential security vulnerabilities. There are three ways a hacker might infiltrate a home television: 1) through a JavaScript / HTML flaw, 2) through a Man-in-the-Middle attack or 3) IoT's expanded attack surface.

5.1 JavaScript / HTML flaws

All Smart TVs sold today, regardless of their underlying operating system, can run JavaScript and/or HTML. This should not be a surprise, "as compatibility with such standards is necessary for any modern device that wants to serve as a portal to the Internet. Unfortunately, these standards are vulnerable to attack," which arguably hasn't been widely understood by the public and private sectors [18]. Researchers SeungJin Lee and Seungjoo Kim, demonstrated a variety of attacks against the Samsung TV's operating system at the Black Hat USA 2013 conference [19]. These attacks included stealing a local user credentials, reading consumer's browser history and infiltrating the TV's built-in application architecture so that the system would crash; this wasn't the first report. In 2012, another pair of researchers "posted a video showing they had learned to remotely take control of a Samsung television," but the researchers failed to unveil their method [18].

Smart TV devices are vulnerable to many of the issues that haunt android systems. Google's operating system is the most targeted mobile Operating System (OS) in the world, which means there's no shortage of malware for users to avoid. Threats range from simple advertising (ad) injectors that plague users with unwanted content

to full-blown Trojans that can track browsing habits and log every move including passwords entered through Smart TVs.

5.2 The Man in the Middle

Hybrid Broadcast Broadband (HBB) is a popular standard for television because it is user-friendly. Customers can view previously played programs, take interactive content polls and shop on the Internet. In short, HBB is an emerging market worldwide with the highest rate of adoption being in Europe. However, the problem with HBB transmission is that they do not require a verified origin, which makes Smart TVs vulnerable to man-in-the-middle attacks [8]. To deploy this attack, a hacker would inject a malicious data packet via HBB's over-the-air transmission signal to infect the user's Smart TV or other devices connected to the same network.

5.3 IoT additions expand the threat landscape

Each "Smart" device that goes online open another path for hackers to infiltrate business and home networks. As noted in Europol's 2014 Threat Assessment with more objects begin connected to the Internet and the creation of new types of critical infrastructure, we can expect to see (more) targeted attacks on existing and emerging infrastructures, including new forms of blackmailing and extortion schemes (e.g., ransomware for smart cars or smart homes), data theft, physical injury and possible death, and new types of botnets" [20] In the words of Chairman and Former CEO of Cisco, "it's no longer a question of if you'll be breached, it's a question of when" [21].

6 ACTIONABLE STEPS TO INCREASE THE SECURITY OF YOUR SMART TV

As the number of IoT devices increase, there are ways consumers can protect against attacks to the privacy of their Smart Home gadgets and personal network [22]. Similar to locking a car or front door to a house to protect valuables, smart device security awareness and education must be added to that list. Table 1 outlines

twelve steps all users can implement within their home network architecture to safeguard them from malicious attacks. Users who are more technically savvy, can go a step further and Segment normal "user" traffic from your Smart TV by creating separate VLAN (Virtual Local Area Networks). The hope is to have manufacturers and legislators work together to provide and promote the education of technical devices the same way physical security measures are publicized.

12 Ways to Increase the Security of Your Smart TV	
1	**Inventory Devices** Inventory all devices within your network. Disable or remove devices that are unknown or no longer used.
2	**Direct Connect** If possible, plug your TV directly to your Ethernet connection.
3	**Router Settings** If you choose to connect your TV to your home network: ▪ Use a router with an enabled firewall ▪ Hide your SSID ▪ Select a secure password
4	**Automatic Updates** Set your TV to automatically update its software. Double-check to ensure that you have the latest update.

12 Ways to Increase the Security of Your Smart TV	
5	**Enable Smart Security Options on Samsung TVs** This is a new and critical option, available for the open source operating system (Tizen) which may pose more risk than other operating Systems.
6	**Careful What You Say or Do in Front of your TV** Cover the webcam and disable voice-activated controls.
7	**Limit Web Browsing** Keep web browsing to a minimum and do not perform banking activities from your Smart TV. Use your home computer or mobile device.
8	**Disconnect from the Internet** If you don't use its online features or are away for an extended length of time.
9	**Screen Mirroring Feature** Caution when using the screen mirroring feature, because your TV communicates with your nearby devices and may spread malware to all items within your home network.
10	**Limit Use of the Remote Management Technical Support Option** Remote management is used for technical support and by default should be disabled. If this option is enabled, it could leave your TV vulnerable to malware.

12 Ways to Increase the Security of Your Smart TV	
11	**Raise Public Awareness on IoT Crime Prevention & Safety Tips** Public awareness through community and local government websites for citizens to conveniently access; start youth programs to teach digital literacy where students can earn certificates or badges.
12	**Private Sector and Public-Sector Partnerships** Establish new partnerships to promote consumers from potential exploits of personal or financial data accessible through their Smart TV; an ideal partnership would be for Manufacturers to issue mandatory password change from its default setting on all devices
	**Create a Separate Network for your Smart TV** Segment normal "user" traffic from your Smart TV by creating separate VLAN (Virtual Local Area Networks).

Table 1: 12 Ways to Increase the Security of Your Smart TV

Digital Citizenship must be taught now and not further down the road as a reaction to loss of privacy and security. Furthermore, in addition to cyber awareness, digital literacy curriculums must be created and taught to children starting in kindergarten and to not only focus on middle and high school students [23]. There should be free Cyber Security events such as the one offered yearly at Metro State University in St. Paul, Minnesota each October [24]. Activities include workshops on internet and social media safety, computer and mobile device maintenance and education, how to secure your home network and electronic devices. IoT devices like the Smart TV should be included as part of the event curriculum [25]. These events provide local citizens with the tools necessary for cyber security while providing a no-cost option to individuals who may not be able to afford this expense because "attackers know no age' [23].

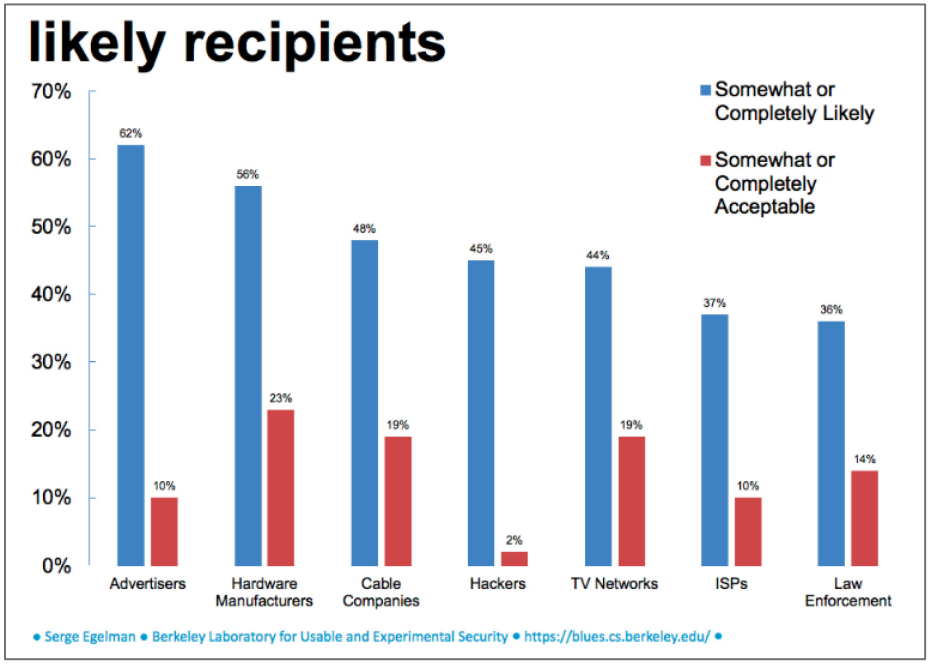

Figure 8: Survey to Gauge Comprehension of Risks Pertaining to Smart TV Data Capture

7 CONCLUSION

In conclusion, CE manufacturers and retailers alike forecast exponential growth in interconnected devices within the next few years; furthermore, the bullish projections of TVs connected to the internet will soar to 319 million by the year 2020 [26]. The next source of attacks will occur on consumers' Smart TVs. This paper underscores the need to heighten the awareness on Smart TV privacy concerns; specifically, there's a need to be more transparent with what information is disclosed without the user's knowledge and what precautionary steps need to be taken before agreeing to the Smart TV terms and conditions. Albeit small strides forward, these proactive steps serve as a way to help consumers enjoy their new Smart TVs and mitigate potential consumer privacy concerns or vulnerabilities to

cyber exploits. In light of the recent announcement in which "VIZIO has agreed to pay $2.2 Million (to the Federal Trade Commission (FTC) and the State of New Jersey) as part of a settlement because VIZIO collected viewing histories on 11 million Smart TVs without users' consent" [27]. Table II shows the likely recipients who may obtain data from their Smart TV and whether or not it is "somewhat or completely acceptable" for advertisers, manufacturers, cable companies, hackers, networks, ISP and law enforcement to use that information [28]. "Many people incorrectly believe privacy laws prevent certain uses of their data. Others understand that the data can be shared, are opposed to it, but do not believe they can do anything about it" [28]. The need to educate and drive security literacy and awareness falls on both the private and public sector. Manufacturers, retailers, customers, and legislators need to help define the scope of protection required to mitigate the risk.

8 ACKNOWLEDGEMENT

The authors would like to thank our distinguished advisor, Dr. Faisal Kaleem for his guidance and expertise throughout this project. We would also like to thank the Technology Leadership Institute's faculty and board members at the University of Minnesota for the opportunity to contribute towards the success of bridging the gap between business and technology.

REFERENCES

[1] R. Wong, "Samsung Smart TVs: The next frontier for data theft and hacking [video]," a4 December 2012. [Online]. Available: http://bgr.com/2012/12/14/samsung-smart-tv-hack-security-exploit-discovered/. [Accessed 14 December 2016].

[2] M. Kumar, "The Hacker News," 8 February 2015. [Online]. Available: http://thehackernews.com/2015/02/smart-tv-spying.html. [Accessed 14 December 2016].

[3] C. Wueest, "How my TV got infected with ransomware and what you can learn from it," Symantec Security Response, 24 November 2015. [Online]. Available: https://www.symantec.com/connect/blogs/how-my-tv-got-infected-ransomware-and-what-you-can-learn-it. [Accessed 14 December 2016].

[4] New York Times, "Trump Sworn In as President," 20 January 2017. [Online]. Available: https://www.nytimes.com/video/us/politics/100000004863329/trump-swearing-in-ceremony-2017.html. [Accessed 23 April 2017].

[5] H. Neidig, "Trump signs internet privacy repeal," 3 April 2017. [Online]. Available: http://thehill.com/homenews/administration/327107-trump-signs-internet-privacy-repeal. [Accessed 22 April 2017].

[6] Common Sense Media, "Common Sense Media EdTech Glossary," [Online]. Available: https://www.commonsensemedia.org/educators/1to1/glossary. [Accessed 23 April 2017].

[7] Consumer Technology Association, "Consumer Technology Association - About Us," [Online]. Available: http://www.ces.tech/about-us. [Accessed 22 April 2017].

[8] M. Niemietz, J. Somorovsky, C. Mainka and J. Schwenk, "Not so smart: On Smart TV Apps," in International Workshop on Secure Internet of Things (SIoT), Vienna, 2015.

[9] Wikipedia, "Generation Z --- Wikipedia{,} The Free Encyclopedia," [Online]. Available: https://en.wikipedia.org/w/index.php?title=Generation_Z&oldid=764662907. [Accessed 11 February 2017].

[10] Evans, Dave; Cisco Internet Business Solutions Group (IBSG), "The Internet of Things: How the Next Evolution of the Internet is Changing Everything," Cisco, San Jose, 2011.

[11] Statista, "Statista - Internet of Things (IoT): number of connected devices worldwide from 2012 to 2020 (in billions)," [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. [Accessed 10 February 2017].

[12] Wireshark, "Wireshark 2.2.1 Release Notes," [Online]. Available: https://www.wireshark.org/docs/relnotes/wireshark-2.2.1.html. [Accessed 22 April 2017].

[13] Wikipedia contributors, "List of smart TV platforms and middleware software," 16 April 2017. [Online]. Available: https://en.wikipedia.org/wiki/List_of_smart_TV_platforms_and_middleware_software. [Accessed 22 April 2017].

[14] International Institute of Cyber Security, "International Institute of Cyber Security - How to Hack your Smart TV," [Online]. Available: https://iicybersecurity.wordpress.com/2015/07/07/how-to-easily-hack-your-smart-tv-samsung-and-lg/. [Accessed 22 April 2017].

[15] N. Sidiropoulos and P. Stefopoulos, "Smart TV Hacking," University of Amsterdam, Amsterdam, 2013.

[16] M.-A. Russon, "International Business Times UK," 12 January 2016. [Online]. Available: http://www.ibtimes.co.uk/its-official-your-smart-tv-can-be-hijacked-malware-holding-viewers-ransom-1537533. [Accessed 14 December 2016].

[17] SamyGO Wiki, "How to enable Telnet on samsung TV's," [Online]. Available: https://wiki.samygo.tv/index.php?title=How_to_enable_Telnet_on_samsung_TV%27s. [Accessed 15 February 2016].

[18] J. Lee, "Make Use Of," 24 May 2014. [Online]. Available: http://www.makeuseof.com/tag/smart-tvs-are-a-growing-security-risk-how-do-you-deal-with-this/. [Accessed 14 December 2016].

[19] S. Lee and S. Kim, "Hacking, Surveilling, and Deceiving Victims on Smart TV," in Black Hat USA, Las Vegas, 2013.

[20] European Cybercrime Centre (EC3), "The Internet Organised Crime Threat Assessment (iOCTA)," European Police Office, 2014.

[21] Cisco, "Cisco Advanced Malware Protection Solution Overview," 3 January 2017. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html. [Accessed 22 April 2017].

[22] S. Tiongco, "Tech Times," 20 June 2016. [Online]. Available: http://www.techtimes.com/articles/165859/20160620/how-to-protect-your-smart-tv-from-hackers-here-are-some-tips.htm. [Accessed 14 December 2016].

[23] M. Patane, "ISU rolls out cybersecurity curriculum for Iowa schools," 25 April 2015. [Online]. Available: http://www.desmoinesregister.com/story/tech/2015/04/26/isu-cybersecurity-curriculum/26282593/. [Accessed 23 April 2017].

[24] Metropolitan State University, "Think Safe, Be Safe: Cyber Security Awareness Month event," 22 October 2016. [Online]. Available: http://www.metrostate.edu/events/old-events/2016/october-2016/think-safe-be-safe-10-22-16. [Accessed 22 April 2017].

[25] Metropolitan State University, "Think Safe. Be Safe, Conference Agenda," 22 October 2016. [Online]. Available: https://metrocatalyst.files.wordpress.com/2016/10/conference_agenda-public.pdf. [Accessed 22 April 2017].

[26] The Digital TV Consultancy, "Connected TV set boom continues," 2016. [Online]. Available: http://www.digitaltvnews.net/?p=26270. [Accessed 15 December 2016].

[27] Federal Trade Commission, "VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent," 6 February 2017. [Online]. Available: https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it. [Accessed 6 February 2017].

[28] Egelman, Serge - Berkeley Laboratory for Usable and Experimental Security, "Privacy perceptions surrounding smart TVs," 7 December 2017. [Online]. Available: https://www.ftc.gov/system/files/documents/public_events/942763/smart_tv_workshop_-_serge_egelman_research_slides.pdf. [Accessed 15 February 2017].

[29] Cyber Security, "How to easily hack your Smart TV: Samsung and LG," 7 July 2015. [Online]. Available: https://iicybersecurity.wordpress.com/2015/07/07/how-to-easily-hack-your-smart-tv-samsung-and-lg/.