Active and Passive Privacy Issues in Current Smart TVs

Pubudu Gayan Buddhika

A thesis submitted to the graduate faculty of Design and Creative Technologies

Auckland University of Technology

In partial fulfilment of the

Master of Information Security and Digital Forensics

School of Engineering, Computer and Mathematical Science

Auckland, New Zealand

2020

Declaration

I hereby declare that this submission is my own work and that, to best of my knowledge and belief, it contain no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a university or other institution of higher learning, except where due acknowledgement is made in the acknowledgements.

Pubudu Gayan Buddhika

Acknowledgements

First, I would like to thank Auckland University of Technology for the opportunity given me to improve my knowledge and skills regarding Information Security and Digital Forensics. Secondly, I am eternally indebted to my mother who is behind me all the time and encouraged me when difficulties came. She went through many struggles to raise me to the person I am today, ever since the death of my father at a young age.

Further I would like to express my deepest gratitude to my supervisor Prof. Brian Cusack for all the guidance and support he gave me during the thesis work. His tireless guidance and advice has greatly helped me in completing this thesis successfully.

In addition, I would like to take this opportunity to thank Dr. Alastair Nisbet who accepted my application for the MISDF program in the Auckland University of Technology.

Finally, I give thanks to my wife and loving daughter Oshi for being patient with me during my studies.

Abstract

The convergence of electronics and Internet connectivity has transformed the consumer application market, and added the word “smart” ahead of every device and gadget. The present smart world produces thousands of products that enhance people’s daily lives. The smart televisions (STVs) are one of the leading products that modern homes have, and individuals have smart phones. In recent years STVs have gained a considerable amount of computing power with the help of low-cost electronic manufacturing. The voice recognition remote controllers, motion recognition cameras, scheduled programme records, and other smart features have added great experiences to the STVs and value, that has attracted more consumers.

When a device is connected to the Internet everyone has to pay attention to security and privacy as a first priority. The fact is that the moment a device is connected to the Internet, it starts exchanging data with servers. However, most people are not concerned with security and privacy of STVs, and simply want the enhanced experiences and conveniences. This inconsiderate behaviour of STV users could open the door for perpetrators to get into their home networks and invade user privacy by connecting not only to STVs but also to other devices such as smart phones, home security systems and automobiles. In the first instance it is the responsibility of STV manufacturers to pay attention to the security of their products and develop enhancements and security improvements continuously. They have to protect from cyber attacking methods, tools that can compromise a STV, and continuously improve the user protection as well as their experiences.

The purpose of this research is to analyse modern STV security vulnerabilities and possible privacy issues that can occur. These can happen due to one of data communication exposure, open operating system implementation methods, or the collecting of data on watching the habits of users. This can be carried out by the manufacturers by using the STV as a sensor

network and data feeds to subscribing agents. Hence, the chosen research question is: “What are the active and passive privacy issues of current smart TVs?”. In comparison with previous generations of technology, modern smart TVs have some security enhancements for data communications and internal system protection. These improvements show the influence of government regulations and policies to protect their citizens. Awareness of the need to protect personal identity information (PII) and security researchers’ findings on STV security breaches, are driving security improvements.

In this research several government policies are reviewed in relation to PII data. The New Zealand new privacy Bill is compared with the European GDPR and the Australian Privacy Act. The findings of this research show that both the tested STV brands have enhanced their system security to protect data. However, their data collection behaviour and use in advertising campaigns can lead to social engineering of an STV user, and the possibility of privacy issues. Further potential issues that can happen in the future are noted that relate to STV security implementations and weak cypher exchanges. Further research is required into the data collection processes in STVs and the potential use to influence users to purchase goods and services.

Table of Contents

List of Figures

List of tables

List of Abbreviations

- ACR Automatic Content Recognition
- AIT Application Information Table
- BA British Airways
- BBC British Broadcasting Corporation
- CIA Central Intelligence Agency
- COPPA Online Privacy Protection Act
- CVE Common Vulnerabilities and Exposures
- DHCP Dynamic Host Configuration Protocol
- DNS Domain Name System
- DoS Denial-of-service
- DSM-CC Digital Storage Media – Command and Control
- DVB Digital Video Broadcast
- EPG Electronic Program Guides
- FTC Federal Trade Commission
- GDPR General Data Protection Regulation
- HbbTV Hybrid Broadcast Broadband TV
- HTTP Hypertext Transfer Protocol
- ICMP Internet Control Message Protocol
- IoT Internet of things
- IPG Interactive Program Guide
- IPTV Internet Protocol television
- LCD Liquid-crystal display

- MIPS Microprocessor without Interlocked Pipeline Stages
- MITM Man-In-The-Middle
- NIST National Institute of Standards and Technology
- OTT Over the Top
- PII Personally identifiable information
- PMT Program Map Table
- RCA Radio Corporation of America
- RFID Radio-frequency identification
- SOAP Simple Object Access Protocol
- SSL Secure Sockets Layer
- STV Smart TV
- TLS Transport layer security
- TOCTTOU Time-Of-check, Time-Of-Use
- UDP User Datagram Protocol
- UPnP Universal Plug and Play Vulnerability
- USB Universal Serial Bus
- VOIP Voice over Internet Protocol
- VPPA Video Privacy Protection Act
- WPA Wi-Fi Protected Access

Chapter 1

Introduction

1.0 BACKGROUND

About 20 years ago consumer privacy and household television units were not interrelated. People were concerned about program content and the potential indirect influence of content on human behaviours. However, STVs have introduced concerns over the collection of user data and the unauthorised use to influence human behaviour. The jump from black and white television to colour television, enhanced human experience but was never a threat to a users' privacy until STVs were developed. The cheap broad band Internet and fast growing streaming industry made huge demands on STVs to collect data. The switch from analogue transmission to digital transmission gave the capability to directly collect a wide range of user data. Nearly 50 Countries Switched off Analogue TV, and boosted the STV industry (Whittaker, 2019). The consumer had two options, either to buy a converter which converts digital signals to analogue or buy a new STV. The STV comes with inbuilt functionality to support local channels and uses other functionalities based on the Internet, such as streaming, Internet browsing, VOIP and scheduled recordings. The STV related privacy issues were raised based on data communication related matters, such as plain text user credentials sent to servers to get authentication to access applications or websites. However, privacy issues arose since STVs gained more features such as webcams, voice recognition, and smart remote file sharing and cloud connectivity.

After STVs became popular more cyber-criminal lawsuits and privacy breach issues were raised against STV manufacturers and government agencies. Thus, the data collection processes improve user experiences on STVs but also increases STV related privacy issues. Also attackers targeted STVs for financial credentials and personal information gained through open applications and built in functionalities such as cameras, microphones, and logs (Michéle & Karpow, 2014). A

vulnerability of any of these devices can open remote access to a STV internal environment which leads to a compromise of the entire network. As the STV industry expanded, security researchers began to take an interest in the risks associated and the related privacy issues. Based on those findings, governments were encouraged to implement laws to protect consumer privacy. Therefore, eventually STV manufacturers had pressure to improve the security of STVs. STV manufacturers, related application developers and other related service providers started to implement more sophisticated security methods and vulnerability management systems compared to the previous versions of the technology.

The data collection process from smart devices became a more sustainable income for smart device manufacturers. Gilbert (2019) described this is one of the major reasons that STVs are getting cheaper. On the other hand, this is an unfair trade as STV manufacturers receive income without giving any benefit to the users. However, to prevent this unfair data use from user's perspective, several counter measure products are available at present that a user can easily deploy to a STV to prevent sending their data to data collection centres, even though a STV is programmed to collect the data.

In this research the literature review addresses several privacy acts that are currently in use in different judicial systems. Some acts focus on child protection and some are deeply concerned about offshore companies that collect onshore citizen data, including that of minors. STV privacy policies are crucial as they make a legal agreement between the user and the STV manufacturer. Therefore, several STV privacy policies are reviewed in this research, including related lawsuits where consumers litigated against STV manufacturers. In addition it is important to disclose how attackers can attack STVs to breach security. Consequently, in the literature review several attack models and vulnerabilities that researchers have published, are summarised. These reviews and similar studies guided the development of the research hypothesis and the main research question including the three sub questions. The proposed main research question is:

"What are the active and passive privacy issues in current smart TVs?"

1.1 MOTIVATION

The above section elaborated the background used to determine the scope of the research topic. This section discusses the motivation to do the research in terms of covering two major sections. They are consumer privacy of IoT and the strength of the STV security. Furthermore, by combining these areas the researcher was motivated to address the specific area of active and passive privacy issues in current STVs.

It is significant to recognise what is consumer privacy and why it is important to protect consumer privacy when using STVs. As addressed in the introduction, in this modern era it is hard to ignore the STVs or STV box as the whole world is switching from analogue transmission to digital transmission. The available solution for citizens is to move with the new technologies and have the right to enjoy entertainment in the way they prefer, either via STV or STV box. Nevertheless, does that mean consumers need to sacrifice their privacy for the new technologies? Most times people assume that STVs cannot harm or disturb their privacy like smart phones have. Due to these false beliefs people put their own privacy at risk. STVs can harm consumer privacy the same as or more than smart phones. Current day STVs are loaded with several input items including built in cameras, microphones that are capable of voice recognition, and other sensors. Therefore, if an attacker gains the access to STV via those input sensors and mechanisms, attackers can acquire user's authentication data such as session cookies. STVs are found from private bedrooms to hotel rooms, therefore it is clear why consumers need to think about their privacy concerns regarding STVs.

Other motivation for choosing this research was to find the ways that a STV collects data, who can access data in the STV, and the range of data that is collected from a STV. Obviously, big companies do not want to get sanctioned with the banning of their products in any country or have extra taxes on top their consumer electronic goods. Due to the huge competition in the STV market if anyone loses an existing market share it is challenging to get it back. When third parties request user behaviour data, and will pay, what would be the STV brand response to those requests? According to Whittaker (2019) it is quite a mixed response, as some companies give data to

governments, some collect data anonymously, and some companies never get any requests from third parties. The data can be used for legitimate solving of crimes, but in contrast it can be used for illegal spying on users regarding what they are doing in their homes and lives. Therefore, it is necessary that people should care and be aware of STV data collection.

In 2019 the New Zealand government announced that a new privacy bill will be enacted in April 2020. However, it is postponed to November 2020 due to the COVID -19 pandemic. In Europe they have the GDPR, and Australian citizens are covered by Australian Privacy Act. Yet the New Zealand privacy protection Act is old compared to the rest of the nations. As explained above, with modern technology it is hard to expect companies will protect consumer privacy, and in that case there should be controls to protect citizens' privacy from exploitation. Most of the data collectors are based offshore and New Zealand does not have law to protect consumer privacy regarding offshore company actions. On the other hand, until 2019 there are no protocols, regulations, or guidelines regarding the security features of IoT devices. To address this issue NIST has introduced six new recommendations concerning the security features for IoT devices. Hence, by knowing the above issues, I was encouraged to do research on how the New Zealand privacy Bill can effect STV privacy issues.

1.2 RESEARCH APPROACH AND FINDINGS

The main approach for the research thesis was decided by reviewing related literature on STV and privacy. Then peer research reviews and publications were helpful in identifying the methodologies, tools, and technical guidance, to find the answer for the main research question. In addition, by reviewing the literature the privacy issues on current STVs and how those issues can arise, were established. Furthermore, by highlighting the privacy issues and the related vulnerabilities, the sub questions were formed to answer the main research question.

Four phases were used to execute the research. In the first phase the attack methods and tools were identified. In the second phase, the test environment to execute the identified attack methods

against tested STVs, was structured. In the third phase the identified attack types were executed and recorded for the analysis process. In the fourth and last phase, the acquired data was analysed to find the answers for the sub questions and the main question. During the first phase the literature reviewed guided the testing. In the second phase the scope for the test environment and setup hardware and software were defined. At the beginning of the third phase two attack types were executed on two selected STVs that are currently in the market. The collected outcomes were analysed in phase 4.

This research shows that current STV manufacturers are genuinely concerned about data protection and data communication. Furthermore, they seriously find ways for restricting the inside file system access and encryption cypher details, which are promising improvements for STV security compared to 7 years ago. However, this research shows that the collected data were used to influence other users in the same network. By using the influence of advertising attackers can do social engineering on the user behaviour gained from a STV.

1.3 STRUCTURE OF THE THESIS

This research thesis contains six chapters. They are chapter 1: Introduction, Chapter 2: Literature Review, Chapter 3: Methodology, Chapter 4: Research findings, Chapter 5: Discussion of Findings and Chapter 6: Research conclusion.

Chapter 1 provides the introduction for the overall research, and the interests and motivation for doing this research. Plus, it outlines the expected research findings.

Chapter 2 reviews literature related to STVs and privacy issues for smart and IoT devices. Furthermore, several methods are identified that are used to extract data from STVs. Also privacy and the related Acts that are available to protect consumer privacy, are reviewed. To conclude the chapter, STV privacy policies and attack types that cyber attackers use against STVs are listed.

In chapter 3 the research methodology is built from four previous published studies that are related to STV privacy matters. The main research question including three sub questions and three

hypotheses are also defined. In addition, the chapter describes the data generation process and analysing processes for acquired data.

Chapter 4 has the setup of the test cases and testing for the built test cases. Furthermore, the captured data with evidence is presented in screen shots.

Chapter 5 discusses the research findings by answering the research question and sub questions. The three hypotheses based on the research findings in chapter 4 are also tested.

Chapter 6 concludes the thesis by reflecting on the findings and discussions. In the second part of the chapter several recommendations are made for future research based on gaps in the findings.

The appendix is at the end of the thesis and contains supplementary information. Moreover, it contains the data collection record about advertisements that popped up, time records, and fixture resistance while conducting one test attack method.

Chapter 2

Literature Review

2.0 INTRODUCTION

The literature was selected by carrying out keyword searches via the Google search engine and Google Scholar. The Electronic Library Portal of Auckland University of Technology was used to find more specific details related to STVs and the privacy issues. Initially started to search for more generic keywords such as “Smart TV” and “privacy issues”. After referring to the contents of the findings, new collections of search criteria were defined to narrow the topics, such as “Smart TV privacy issues, threats and vulnerabilities”, “Data protection mechanisms in current Smart TVs". Then many literature resources were reviewed, and the selected items were saved to a google document for further review. Moreover, white papers and security review websites helped in understanding the latest privacy issues as well as trends in the STV industry and other related areas such as broadcasting, IoT and HbbTV.

The rapid development of cloud computing and embedded technology have changed the entire computing world. Today, most devices from coffee machines to automobiles are connected to the cloud and exchange data to improve their services. In the same manner the STV manufacturers have improved their end products aggressively with the help of embedded electronic systems, hence many new features such as human gesture recognition, online gaming, conference calling via the Internet and web browsing, are included. Speed, inexpensive Internet connectivity, and applications make STVs popular among consumers. As a result everyone gathers around modern STVs without age limits and often a single house owns one or more STVs.

Generally, most of the STV users are non-technical or have limited knowledge about an STV’s back-end operations. The STV has an operating system, an advanced hardware system and software applications to process user requests. It also has backend processes to capture user activity

and send data back to data collection centers which helps to improve user experiences. This collected data set and inbuilt sensors may give some serious privacy issues for consumers. Since STVs have fewer enforced security methods than computers, then conceivably hackers can convert device sensors to spyware and monitor the people who live in a house or any other location. Collectively these matters have made more problematic issues for the users, comparatively to smartphones and personal computers.

2.1 SMART TV ARCHITECTURE

STVs or connected TV's architecture can be explained using two separate modules. That is the hardware and the software modules. The manufacturers provide two types of hardware units. One is inbuilt in the monitor panel which comes as a single unit and the other one comes in a separate STV box. Occasionally people get confused about IPTV or Internet TV which is similar to STV. Fundamentally IPTV is a technology and STV is a device that includes all the related technologies. (IPTV receives the video stream via the network protocol which can be either cable or wireless media.) The following sections describe the general overview of STV hardware and software architecture.

The Internet of Things (IoT) acts as a critical element in STVs. It is the core technology that converts normal TVs to STVs. Various STV manufacturers use different IoT architectures and components. However, the foundation is based on a high performing IoT platform. To operate any STV it needs an operating system and at present the leading STV operating system is Android, followed by Tizen. The majority of well-known STV brands use Android OS in their STVs as most of the Google functionalities are easy to integrate with an Android OS. As Tizen OS only supports a limited number of applications it is still not widely used in STVs. This is a crucial issue when it comes to security and privacy provisions, which will be discussed in section 2.2. Figure 2.1 shows STV market share in 2018.

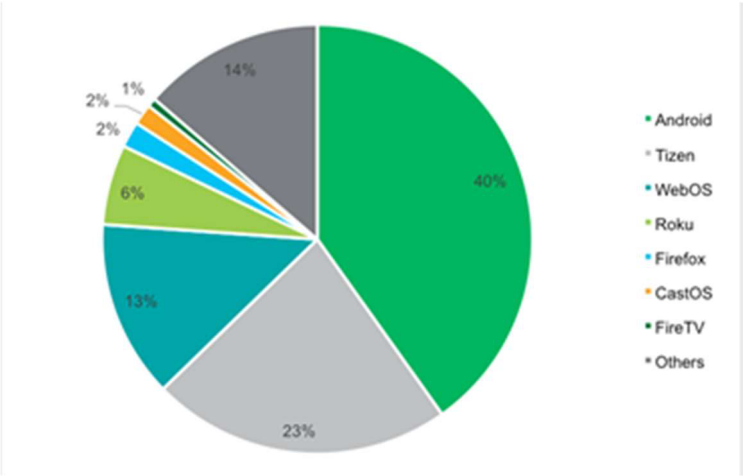


Figure 2.1 2018 STV Operating System market share

(Kinsella, 2018)

Based on its functionalities, STV components can be divided into several subcategories (Kumar & Vembu, 2017). They are,

- User Interface
- Apps
- Electronic program guide and Interactive program guide
- Hybrid Media System content playback
- Extended media format support
- DLNA and Input control framework

The following paragraphs discuss individual components and their importance to the STV functionality.

The user interface plays a major role in any smart device regardless of the size and the purpose. Hence, smart device application developers and product manufacturers are seriously concerned about their smart device user interfaces. For STVs, developing user interfaces is a significant mission as they have different platforms and screen sizes plus optimal distances for

interfaces. However, all STVs have their own development methodologies and guidelines such as fonts, layouts and panel navigation layout.

Similar to smartphones, STVs need applications to establish communication between users and devices. Nearly every STV comes with pre-loaded applications for basic usage such as Netflix, YouTube, Facebook, Skype and others. On the other hand, it is the user's responsibility to keep these pre-loaded applications functional or install only the necessary applications as it might affect the performance of the STV. For example, social media applications have background threads to check notifications and messages and they listen to the server continuously, hence they can generate unnecessary Internet traffic.

In the past, users only had a few channels in their TVs or radios and the program guides were commonly provided within newspapers. For STVs they use the same method although in different ways. That is instead of printed program guides STVs have Electronic Program Guides (EPG). These EPGs will show broadcast scheduling information or upcoming events on each channel. The Interactive Program Guide or IPG is the new generation or the advanced version of EPG. The benefit of IPG is that users can interact with the guide by searching, recording or adding reminders. There are three types of EPG menus that can be found in modern STVs. They are This Channel, Multiple Channel and Full EPG version (Kab, 2019).

2.1.1 Automatic Content Recognition (ACR)

There is no clear evidence of who the inventors of ACR technology might be. However, in 2011 an online music recognition application known as Shazam had implemented a similar technology to recognize sound tracks. At present it is a common technology that is available in any smart device and enables manufacturers to eavesdrop on users viewing habits on smart devices. The ACR can capture distinctive data regarding a user's viewing behaviour such as genre, time, frequency, and so on. The consumers conceivably can assume this technology can only monitor their online streaming, nonetheless it can collect all the activities including cable connection, air broadcasting and any disk

media (CD,DVD, Blu-ray) (Newman, 2019). The ACR technology has a positive impact on the advertisement industry as advertising companies can use this technology to understand the user behaviour in smart devices. The next two sections will examine the ACR technologies and how they works in STVs.

2.1.1.1 Digital fingerprinting method

In the world each biological animal has a unique identification. As an example, each zebra has different stripe patterns on its skin. The same theory applies to tigers, leopards, giraffes. Humans have unique fingerprint patterns and eye pupil patterns. When it comes to digital video and audio files, every single file has its own unique fingerprint. This fingerprint can either be based on the audio file decibel level mix, background noises, background brightness of video files, colour patterns, camera angles, object movement speed and directions, and so on. To generate a fingerprint for video and audio files needs several frames from the specific file and the metadata of that file has to be stored in a database. However, this process does not modify the original file to get the digital fingerprint which is a great advantage when compared with other ACR technologies. By using the captured fingerprint, the host can monitor various sources such as radio broadcasting, YouTube, STV or else can identify whether the original content file has changed.

The ACR publishers use digital fingerprinting technology to identify copyright violations, measure audience size, version controlling, advertisements. The Central and Local matching methods are used to match the fingerprints with the file that a publisher wants to check. In the Central matching system, the hosting devices connect with the central process machine via an API, and compare the fingerprint that is sent by a local device either a STV, smartphone or any other smart device. In the Local matching process, the central server distributes several fingerprints to local devices, and the local devices only get the matching result according to the publisher setup (Automated Content Recognition creating content aware ecosystems, 2012). Finally, by using fingerprints it is not possible to build the original video or audio file. Moreover, this technology cannot be guaranteed in use with

modern technologies, hence, it is an unstable factor to use for forensic processes or as a tool for evidence collection (Nitin, 2012).

2.1.1.2 Digital watermarking method

The second method that ACR uses to capture the user behavior is the digital watermarking method. In the past publishers used this method for audio files. However nowadays it is widely used for video files as well. In digital watermarking, publishers insert different tags that contain publisher ID, audio file ID, or any other unique ID that ACR can send to the publisher. These added tags will not change the quality and are undetectable as they are dynamically embedded into the files. Another important advantage of a watermarking method is that it is unnecessary to search the tags or references in the database as the fingerprint process does (Stojancic, 2011). For the detection process chip, manufacturers or embedded system developers cooperate with TV manufacturers to insert detection process embedded systems into appropriate end user systems.

This technology can collect video and audio metadata and send them back to data collectors for marketing purposes. The data collections may include online user behavior patterns and consequently if these data are compromised, it would breach consumer privacy. If someone hacks a STV connected network then they can collect all the data that the STV has collected.

2.2 PRIVACY

The researchers, scientists, philosophers, and sociologists have defined privacy in different ways before people were attached to this modern data driven world. It is stated that according to Alan Westin who is a Philosopher of Privacy, there are four main states in privacy (Jordan, 2018). They are Solitude, Intimacy, Anonymity and Reserve. The right to be let alone, limited access to the self, secrecy, control over personal information, personhood (again this is divided into another two subsections: a. Individuality, Dignity and Autonomy b. Anti-totalitarianism), and Confidence are the six different concepts of privacy differentiated by Daniel Solovet (Solovet, 2002). In contrast Mike

Chapple, James Michel and Darril Gibson have described privacy as protecting personal information from unauthorized access from individuals or systems (Chapple, Michel, & Gibson, 2018). Correspondingly, there are other authors who have defined, and categorized privacy based on race, culture, geographical facts, and social truths. In general, these definitions are not useful due to the constant changing nature of technology. Consequently, there is no assurance that people's privacy will be protected in a data driven world.

It is generally a known fact that strong definitions provide correct guidance in making decisions. In terms of privacy, there is a need for a precise definition to illustrate privacy. As mentioned in the first paragraph various people try to define privacy depending on their environment and influences. On the other hand, no one can declare a single definition for privacy as it can be misguided for some situations. For example, privacy can be restricted for prisoners and cannot be expected that the same privacy definition covers suspects who are not yet convicted. Similarly, in some situations, the definitions can be questionable as an example a patient who is recovered from a serious mental illness, and after rehabilitation, he/she can live a normal life. In that case should authorities inform neighbours? and if the answer is yes then how would be the reactions of the neighbours impact the patient?, and by what means would that disclosure result in the patient's productive life changing? Therefore, giving a proper definition for privacy is not a simple task. It is important to define privacy based on situations or areas such as law, government, civil society, and so on.

Consumer behavior is a well-known term that economists use to explain consumer activity with a product or a service, especially when it has a commercial value or can produce a commercial value for an existing product. Therefore, vendors may not consider consumer privacy as a first priority. Furthermore, as people have different personalities, they may respond differently about the value of their own privacy. Particularly when the world is focused on new technologies and society moves rapidly towards cloud and Internet. The next section will discuss the crucial acts that people

need to be aware of and sample cases that victims have used to prosecute the vendors for violating their privacy rights.

2.2.1 Children's Online Privacy Protection Act

In 1998 the US Congress passed a Children's Online Privacy Protection Act (COPPA) to protect the privacy of children aged under 13 years of age. However, it took two years to feel the effect of this Act. It is managed by the Federal Trade Commission (FTC) in the United States. Basically, this act applies to all the businesses that operate within the US. If any business organization operates outside the US and collects personal information of someone who aged under 13 years living in the US, then this Act applies to them as well. According to the FTC website they have stated four major requirements before a person collects data related to children. They are,

- Notify parents before collecting the data.
- Must get parent's verifiable consent before collecting person information about their children.
- Must have the availability for parents to review the content and the collected data of their children.
- Reasonable security enforcements to protect children's personal information.

(Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business, 2017). Since the COPPA came into force, in 2012, the FTC introduced major amendments to the Act to resolve the conflicts and to cover the challenges from new technologies. In this amendment the FTC has redefined the term "Operator" and included services and plug-ins that can collect personal information from children (Children's Online Privacy Protection, 2012). According to Gadbaw (2016) the COPPA is concerned about the application security. For an example, in the COPPA Act section 312.8 it highlighted application firewalls, and security about employee accessibility to data. Furthermore, it strictly prohibits any motivation of users to expose personal information by giving prizes (bribing) (Gadbaw, 2016).

The reviews two prominent lawsuits against companies that violated the COPPA are now summarized. They further discuss how these cases influence STV and consumers privacy outlined in the next chapters.

Electronic games commonly known as video games, are broadly used by any age group. The majority of people download these applications to their smartphones, smart watches and STVs. When these games applications are downloaded to devices, the application hosting companies can collect data without any acknowledgement from the users. The Walt Disney Company allegedly violated COPPA in some of their game applications. The victim's parents claimed that Walt Disney Company violated COPPA in 42 applications. As stated in the lawsuit these applications did not collect children's personal information, however they have collected hidden data which were exclusive to smart devices (Posses, 2017). By using these exclusive identifiers, the companies are capable of tracing user activity combined with gathering geo location, audio, and video and image files. More notably as Shayna Posses mentioned in her report, the Walt Disney Company paid a massive $3 million of money as a civil penalty for violating the COPPA. This was not the first time that Walt Disney violated the COPPA law (Posses, 2017).

The key problem of the above lawsuit is, who can access the data that was collected by Walt Disney from smart devices, and who will take the responsibility if someone uses that data in criminal activities. In that claim, the victimized parents proved to the court that Walt Disney Company had connections with other advertisement companies such as TapJoy, Vungle and Flurry (Sortor, 2019). Technically, it is an accurate fact that personal identification data was not in the collected data, however with the help of new data analysis and mining tools, the specialists can locate specific child behaviour patterns and routings. Even modern STVs can provide a platform to collect data in the same way that the Walt Disney application did. Only the device has changed but the outcome is similar. Therefore governments, law enforcement agencies, parents and technology researchers are concerned about the privacy of anyone using the devices.

The FTC recently call for another interesting investigation that relates to Amazon Echo Smart Speaker. This device is a cloud connected smart assistance device featured by natural voice interactions, music playback, alarm setup and real time information, such as road traffic and flight schedules. Using the default configuration of this device, Amazon can listen to all conversations in range and without the acknowledgment of users. The application keeps track of the conversation related keywords. Additionally, this smart speaker can keep sensitive details, like allergic foods to specific people who live in a house. The CBS News reported that even when parents try to delete the files still Amazon Echo can remember these sensitive details (Amazon's Echo Dot Kids puts kids at risk, the complaint alleges, 2019).

Most recently Amazon released another device which is similar to Echo. The device has a screen and a camera called Echo Show. It can see the person and has wider capability to collect personal behaviour data than the Echo Speaker, and hence create more privacy concerns (Goode, 2019).

Finally, Governments cannot preclude or restrict research and developments which can cause privacy damages for children. Still, governments have the capability of identifying potential threats that can harm children and cover those threatening situations under the COPPA law. The respective actions taken by the governments to alleviate the disturbing situations make companies, investors, and developers that are involved in the smart world, be more vigilant about the boundaries of their work. On the other hand, some diagree how governments balance the companies and the parents interests.

2.2.2 General Data Protection Regulation (2018)

The United Kingdom passed the first Act in 1984 to address the privacy issues of data (Foulsham, Hitchen, & Denley, 2019). At that time, the Internet was not an entity and the public were not seriously concerned about personal information. However, after the introduction of personal computers, the public began to be concerned about their privacy and personal data. Therefore, the British government introduced additional data protection principles to that Act in 1998 (Foulsham, Hitchen, & Denley, 2019). Similarly, European law enforcing bodies recognized that they ought to introduce further laws and regulations to protect the European Union citizen's privacy. In May 2018, the European Parliament implemented the General Data Protection Regulation to overcome risk areas of citizen's privacy.

A government can fine up to 4% of company's annual global turnover by using this Act (Kho, 2018). The European Parliament has given a two-year grace period for companies that are affected by the new Act. During this two-year grace period they need to declare what type of personal data that they process and implement security tightening to prevent data breaches. Additionally, this Act covers extra general identity information. For example, the data that can be used to locate a user's physical location, biometric data, religious beliefs, political support, views and even RFIDs are considered as personal data. The significant key roles in this Act are as follows: Data Protection Officer, Data controller, Data processor and Sub-Processor (Foulsham, Hitchen, & Denley, 2019). These predefined roles provide an advantage to non-technical people like lawyers and judges in identifying the actual scenario (Data breach).

The following paragraph discusses the first time that the Information Commissioner Office (ICO) used GDPR Act to fine a company that breached GDPR regulations.

British Airways is the national carrier of the United Kingdom and holds a vast amount of data of European passengers that use their services. In 2018 British Airways reported an incident that directed their website to a fake site and compromised approximately 500,000 bio data, travel details , credit card details and logins (Intention to fine British Airways £183.39m under GDPR for data

breach, 2019). The Information Commissioner Website stated, the incident happened due to a poor security implementation (Intention to fine British Airways £183.39m under GDPR for data breach, 2019). Furthermore, the ICO decided to impose a penalty on BA with a staggering amount of 183 million pounds. At that occasion BA agreed to cooperate with the ICO investigation and they faced a penalty of 1.4% of BA global turnover. If BA did not cooperate for the investigation then the penalty could be 489 million pounds (Sweney, 2019).

However, it was a debatable factor why that whole penalty was credited to the government treasury. Moreover, during their investigations ICO found credit card details and CVV pins also compromised. Therefore, who is to take responsibility for victimized customers and what assurance the government or BA can provide regarding the ramifications that can happen using the stolen data.

This case made a statement for all business organizations to care about the privacy of people and data they share with other business organizations. Consequently, in relation to IOT devices or any other smart devices, the GDPR regulation can be used to fine inappropriate practices on EU citizens' data.

After the introduction of GDPR, many STV manufacturers cared about the terms and conditions in the agreements with their consumers. For example, Samsung announced they pay attention to GDPR when they compiled the new privacy policy. As a result of the GDPR strong regulations, Samsung declared that they are collecting user behaviour data for Internet based advertisements (James, 2018).

2.2.3 Video Privacy Protection Act (VPPA)

In 1988 the USA passed the VPPA legislation Bill to protect the rental information (including personal identification information) of video, audio, and visual arts. The background that caused the VPPA bill was that Ronald Reagan's administration nominated Judge Robert Bork for United States Supreme Court. However, most senators and public service administrators did not like the appointment of Judge Robert Bork. Consequently, they started media propaganda by publishing

Judge Bork's video rental details that included extremist pornography to damage his character (Lambe, 2017). As a result, he was not elected for the US Supreme Court. This event directed the Washington administration to bring a new Act to prevent similar incidents in the future.

The VPPA stated that people who engaged in rental, sale or providing services of audio, video or any kind of similar visual material cannot disclose any information related to the consumers who rented, purchased or viewed the media (Lambe, 2017). However, there are exceptions to this law under certain circumstances. As an example, if law enforcement agencies have an appropriate warrant or court order for criminal investigations then the other party must release the required information. As the boundaries of the media and video industry extended, in 2012 VPPA was amended to provide more protection for electronic communications and online video streaming services. This is vital for STV privacy issues.

In recent years online TV streaming services like Netflix, Amazon Prime, Hulu, YouTube, and HBO revolutionized the video and audio rental industry. At present online video streaming is a huge industry and consequently companies constantly compete to supersede each other. These companies try to be proactive rather than being reactive hence they perpetually attempt to forecast the online streaming viewer habits. Concerning this, Netflix announced an open challenge to improve their video streaming recommendation algorithm. Netflix offered 1 million US dollars cash prize and a database that contains information of Netflix subscribers (Lambe, 2017). According to the original lawsuit Netflix has taken necessary actions to remove the identification of particulars and provided a unique ID to identify data (Amended order granting motion for preliminary approval of class action settlement [Netflix Privacy Litigation], 2012). However, the two scientists who are the plaintiff of the case proved that they backtracked two potential users via the unique ID that was provided in the Netflix database. To defend this, Netflix argued that they do not operate under the VPPA and that the unique ID cannot be considered as a personal identification of information. The court denied the argument of Netflix as it did not contain direct information. However, the information that Netflix has provided can expose the PII details (Newman, 2009).

There are some other cases that are based on VPPA where defenders tried to pronounce that their businesses do not relate to video or audio rental and tried to convince the court that businesses are service providing companies via Internet. An example is the Hulu Privacy Litigation case. In this case Hulu shared their customers' video preferences with another party. Essentially, Hulu was not a video tape service rental or service-related company. However, they provided materials that can described as text, printed, electronic form, etc. according to the Oxford Dictionary (The Video Privacy Protection Act as a Model Intellectual Privacy Statute, 2018). Therefore, the court has rejected Hulu's argument and stated that there was no requirement to pay money to service providers to be the subscriber (At that time Hulu provided their services free of charge).

The VPPA generally considers PII details and covers a broad range of matter that relates to audio and video materials. Further the consumers and law professionals have argued with the 2012 amendment, that large online streaming companies can gather data of people's watching behaviour and handover the collected data to third parties. Before the alteration (HR. 6671), VPPA has stated that users can decide whether they permit to share their PII data with streaming companies or not. However, with the new alteration users do not have an option to defend themselves and companies can collect PII data without the user consent (Lambe, 2017). Video streaming or other large entertainment companies have expanded their capacities to collect and analyze people’s behaviour via STVs. With a combination of law, policies, technical, and research, authorities can focus more on controlling the actions and behaviour of large companies with regards to collecting consumer information.

2.2.4 New Zealand New Privacy Bill (2020)

The upcoming Privacy Bill comes into operation in 2020 and replaces the 25 years old Privacy Act of 1993. The Privacy Bill had its second reading on 7th of August 2019 and after the third and last reading it will be sent for the royal assent. According to the Minister Andrew Little the new Bill will treat peoples’ personal information as a higher priority plus it will cover both local and foreign

business operations that keep personal information for commercial purposes (Little, 2019). Conversely, the new Act will apply if foreign organizations only operate in New Zealand. For an example if businesses use New Zealanders' personal information to perform their business tasks and do not operate in New Zealand then the Act cannot be used for any privacy violation cases. In addition, if any organization makes any monetary payment to supply goods or services the act will apply to them (CIO upfront: Privacy Bill update, 2019).

Secondly when comparing the new Act with the old Act, the new Act will give more power to the Privacy Commissioner to do investigations on incidents of breach or privacy violation. Importantly this act will introduce a new criminal offence to the New Zealand juridical system. The New Zealand Ministry of Justice website has stated that:

> "It will be an offence to mislead an agency in a way that affects someone else's information, and to destroy documents containing personal information if a request has been made for it. The proposed penalty is a fine up to $10,000"
>
> (Key Initiatives , Privacy, 2019).

Compared with the GDPR and other jurisdiction privacy Acts the fine may be a very small penalty and offer little deterrence. The other amendment made by the Act is, it will give some sort of independence to the media. In detail, this Act will give an exception to public media including electronic media and radio. However, they have to follow appropriate guidance and regulations. Other than that, there are no significant changes that New Zealand citizens can expect from the upcoming privacy Bill in 2020.

The following section will discuss how the current privacy Acts are involved to investigate the event that happened in Christchurch on March 15, 2019.

After the Christchurch attack the New Zealand police requested Facebook to give a social media account details and the network details for further investigation (especially the account details of people who shared the videos and details). By refusing that request Facebook argued that their

operations are not counted under the existing Privacy Act of New Zealand. Google also stood with Facebook and even refused a New Zealand court order to remove incident contents from its search engines. This behavior was sufficient to open the eyes of the New Zealand Parliament and Judiciary for concern for changing the laws. As a result, the new privacy Bill has introduced new regulations including that overseas companies cannot deny providing information if they operate in New Zealand.

2.3 ANALYSIS OF SAMSUNG, VIZIO, LG SMART TV'S PRIVACY POLICIES AND POTENTIAL PRIVACY VIOLATIONS

This section will review and discuss Samsung, Sony and Panasonic STV privacy policies. These three names are the dominant brands of the STV market. The privacy policy information was fetched from their latest publications on their websites. This section will explore the default privacy settings in each STV plus examine the potential privacy threats that could arise because of these default privacy settings.

Technically a privacy policy is a legal document or an agreement between the consumer and the service or product provider. Therefore, it is a consumers' responsibility to read the agreement fully before giving consent. On the other hand, it is the responsibility of corporate bodies to provide a policy that is easy to understand by its users and avoid obfuscating clauses. Most of the electronic media and system privacy policies are encapsulated as part of terms and conditions. Therefore, when users/consumers accept mandatory terms and conditions, they automatically agree to the privacy policy. It is then that consumers legally grant permission to collect data, to share and to be stored by the merchants. Hence accepting terms and conditions is a crucial legal bond that users blindly accept without giving proper attention to the contents of policies. From the user's point of view, it is unfair that no one can read this kind of legal document in a few minutes or hours. The research conducted by two researchers in Carnegie Mellon University has discovered it may take an average of 76 working days to read modern terms and conditions completely (Wagstaff, 2012).

Government and consumer protection agencies have a responsibility to review those terms, agreements, and privacy policies. Most commercial actors try to make obligations desirable and force

users to share their data indirectly (David, 2019). For example, hacking a system is a lawfully punishable offense, however if you agree with someone to take your data or information, then it is not punishable as you already agreed to that activity when you agreed with the privacy policy. In contrast both activity outcomes may be similar. Therefore, if the government cannot look after its citizens then they are disadvantaged. In New Zealand, the privacy commissioner has indicated the principles to follow under the privacy act, especially when business organizations handle personal information. The following section will analyze four STV privacy policies and default settings and how they could affect a consumer's privacy.

2.3.1 Samsung STV privacy policy analysis

Samsung is a well-known brand that invests billions of dollars in smart technology. Chinese STV brands are also coming into the market, but the Samsung STV was the biggest share in the STV market (2019). Some of the new Samsung smart technologies urge government policy makers to rethink existing laws and policies regarding people's privacy. On the Samsung website, their privacy policy mentions that they will collect almost everything that the user does on a smart TV including the watching details, time, IP address, network details, search history, purchase history and much more. Conversely, Samsung privacy policy tells users to choose the default settings and what they collect. However the Samsung's policy statements are made in favor of themselves. The next paragraph will discuss one potential privacy policy violation incident.

In 2015 the U.S Federal Trade Commission received a complaint about a Samsung STV. According to Steven (2015) in CNET, Samsung has introduced a new voice recognition technology to the STV remote control. This smart remote control collects all the voice recordings of whoever talks nearby to it and sends those details back to Samsung. Furthermore, this data is processed by a third-party company known as "Nuance". Samsung has covered this third-party involvement in a section in their policy.

> "Please note that when you watch a video or access applications or content provided by a third party, that provider may collect or receive information about your Smart TV (e.g. its IP address and device identifiers), the requested transaction (e.g. your request to buy or rent the video), and your use of the application or service. Samsung is not responsible for these providers' privacy or security practices. You should exercise caution and review the privacy statements applicable to the third party websites and services you use."

(Samsung,Privacy, n.d.)

As it states, Samsung will not take any responsibility for third party privacy or security practices. This is a serious concern as consumers do not directly purchase services or goods from the subcontracting companies to Samsung. The other issue in the privacy policy is that they have mentioned that they will collect voice details via voice recognition technology. Hence, Samsung STV users cannot expect a primary level of privacy when they speak in front of their STV. Samsung claimed that they certainly take users' privacy seriously when they send captured data to Nuance. Nonetheless, penetration testing partners have published the evidence that Samsung did not encrypt data that they sent to Nuance. Furthermore, Samsung accepted that they did not encrypt voice recognition data when they uploaded it to Nuance (Kelion, 2015).

The Electronic Privacy Information Center had complained to the FTC that Samsung violated the COPPA Act and FTC Act (Samsung "SmartTV" Complaint, n.d.). These charges forced Samsung to amend their privacy policy to be simple and covering default settings. By default, Samsung STVs enabled their voice recognition feature and "Agree" to send the Voice recognition data to Nuance. However, the default setup of the smart hub Terms and Policy, is to agree to give data for marketing purposes. These default values do not change unless experts point it out. Therefore, these practices are highly debatable in terms of the ethical side of the businesses, as these default settings expose opportunities for attackers to get details from users. The best example is the "Weeping Angel" attack that was demonstrated by the CIA.

2.3.2 VIZIO STV privacy policy analysis

With a predatory pricing strategy, VIZIO STV managed to capture a big portion of the STV market share. VIZIO mainly manufactures smart devices including TVs, tabs, and sound solutions. Their STV platform is known as SmartCast and it is developing capability as a STV platform. As a result VIZIO STV has a limited number of applications compared to other STV brands. However, this SmartCast platform is free from commercial advertisement, hence it became a popular STV brand (Katsaounis, 2019). When compared with other STV privacy policies, VIZIO STV privacy policy statements are clear and do not have any tricky patterns or complex statements that are hard to understand by normal users.

In 2015 the FTC received complaints regarding VIZIO STVs, stating that they were spying on customers and collecting information. The company had agreed to pay a $2.2 million settlement fee and the FTC estimated that 11 million VIZIO STV consumers were affected by this (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, 2017). According to the FTC report (2017) VIZIO, Inc., VIZIO has collected data about consumer activities on cable, DVD, broadband and streaming devices. The collected data was then sold to marketing companies and consumer data analysis brokers to analyze consumer behaviour for marketing campaigns. The company has also collected sensitive data such as income level, household size, home ownership details plus the household value. The Commission then decided that VIZIO has violated the FTC Act and New Jersey consumer protection law as well.

> "This Privacy Policy does not apply to the practices of any company or individual that VIZIO does not control. This Privacy Policy does not cover information on non-VIZIO applications, web services or tools that you download or access from a VIZIO product. It does not, for example, apply to any third party services or applications (such as Google Cast or Netflix) that you may access from VIZIO products. You

should review the privacy policies of these applications and services to learn more about their privacy practices, which may differ significantly from VIZIO's."

(www.cn.vizio.com, n.d.)

The above section is taken from the VIZIO STV privacy policy that is displayed on the company website. According to that statement VIZIO will not be responsible for other applications' data collections via their platform in the STV. In simple terms they will not be responsible for what others do in their environment. On the other hand, it is reasonable to accept the disclaimer that it is not a VIZIO issue rather the application creators' issue. However the applications run in VIZIO's environment and follow their protocols to be built. Hereafter it is VIZIO's responsibility to turn off or alert consumers if any application collects data that can be a threat to consumer privacy.

To conclude, VIZIO has clearly stated that if a user does not want to send their data to VIZIO then they can disable that option without interfering with other smart options. Further they added a direct customer care number and an email if users want to get any assistance to disable the viewing data feature. Essentially this is a signal for other corporate companies to show that they respect consumer rights.

2.3.3 LG STV privacy policy analysis

The Lucky Goldstar or commonly known as LG is another South Korea based electronic manufacturing company that does mass production of STVs. Similar to Samsung, LG correspondingly struggled with STV privacy protections. The main architecture of LG STV is based on a Google Android system and it comes with the Google assistant. Therefore, the LG privacy terms have influence from Google services' terms and conditions. The LG smart devices will ask users to create a LG SmartWorld account to use some of the smart functionalities of their products. The LG privacy terms and conditions do not specifically state the kind of data that they collect from the end users. However, LG's rival Samsung, mentioned in their privacy policy that they collect user network, search and viewing data to improve end user experiences. Therefore, LG undoubtedly overlooks

consumer rights. On the other hand, this behaviour of LG is an abuse of user rights as they have access to any information through their STV products.

LG has received a lot of complaints about their data collecting approach from the users. The researchers and authors have pointed out that LG will aggressively stop the services from their STVs if users do not accept sending data to them. For example, if users do not agree to LG's privacy policy, then they cannot use Skype, BBC Iplayer (Smith, 2014). It is understandable that LG could stop their own applications or services when users do not accept the terms and conditions. In contrast discontinuing essential applications that consumers regularly use such as Skype does not make common sense. This kind of action requires clarification as LG did not mention the kind of services that buyers cannot use if they do not accept terms and conditions. On the other hand, LG indirectly forces the users to compromise their living room privacy to get the smart features they thought they already paid for when they purchased the STV. Government agents should closely monitor these unpleasant commercial behaviors and intervene to alter the policies that will be fair for both parties.

Further the researchers have reported another disconcerting practice from LG STVs. That is LG was acquiring data from USB devices that were attached to LG STVs. This incident was publicized when a LG TV sent collected data to a nominated server as plain text for all to read. Cushing (2013) has published an article based on this issue and he stated that LG STV does not care about what kind of data is stored in those devices. In simple terms, users have not been informed that the data in the attached devices were not LG devices. Therefore, this issue is highly debatable how LG can access external device data without user permissions and under what circumstances that they send data out from the user's network.

The LG SmartWorld account is a compulsory feature if users want to use special features of LG STV as mentioned earlier. Through the SmartWorld account LG collects all the payment details, play stores and passwords that users use for different systems or services via STV. LG has plainly declared this data collection process in the terms and conditions agreement, therefore permitting the collecting of data. However, in the same section they state:

> "You do not have to agree to the Privacy Policy but if you do not, not all Smart TV Services will be available to you. In that case, we will still receive certain non-identifying information from your Smart TV that we need to provide the basic functions that will be available."

(Cushing, LG Will Take The 'Smart' Out Of Your Smart TV If You Don't Agree To Share Your Viewing And Search Data With Third Parties, 2014)

It shows that LG does not care about whether users accept terms and conditions and they will collect the data from STVs in either case. In simple terms even if users do not agree to share the information LG still compromises user privacy as much as they want.

To conclude this analysis, the evidence suggests that LG STVs do more than they claim in taking user data through third parties. When children use STVs, LG requires a filter for child use and have a child lock enabled. Additionally, the governments and consumer protection authorities should closely monitor what STV manufacturers are collecting particularly when the users do not accept the terms and conditions.

2.4 PRIVACY ISSUES IN STVS

To understand how STVs can be a source of creating security and privacy issues in people's private and social life, a researcher needs to find out how it can happen, from where and how. The following paragraphs will review and discuss how ACR technology, built in cameras and microphones can compromise, and importantly how spy agencies can use STVs as spy agents.

As described in section 2.1.1 the ACR facilitates manufacturer capability to spy on users' watching behaviour in STVs. Perhaps consumers assume this technology can only monitor their online streaming, nonetheless this technology can collect all the activities including cable connection, air broadcasting activities, and any disk media (CD,DVD, Blu-ray) (Newman, 2019). ACR technology can collect audio and video metadata and send it back to data collectors for marketing purposes. This data collection may include online user behaviour patterns and consequently if these

data get compromised then it would breach consumers' privacy. If someone hacks a STV connected network then they can acquire all the data that STV collects.

According to the Symantec Corporation, outdated software is a major risk for STVs (Schubert, n.d). The reason is that most manufacturers do not update firmware regularly as it is not profitable to do so. Symantec indicated therefore hackers can easily get access to Samsung STVs via its insecure Wi-Fi connection. Another news article in the International Association of Privacy Professional stated that LG STVs search all shared files on the STV connected network and send them to LG (Brookman, 2013). This practice has more issues as they send files without any encryption. It is understandable that collecting information related to what users watch on TV is helpful, but why STV manufacturers want to scan the connected network shared files can breach privacy.

Hacking cameras and microphones are not a new thing in the technology world. The STV contains both these components and buyers need to be more careful about what kind of security enforcements that manufactures have implemented to protect inbuilt cameras and microphones in STVs. It is true that Voice recognition is a delightful feature, however this feature can be overturned to get unauthorized access to STVs by recording the original person's actual voice and activating the voice application for access.

Many times, security researchers have demonstrated how STVs can be used as facilitators to enter connected networks and implant malware to target personal information or other valuable data. Michele (2015) demonstrated several ways that STVs can be compromised including Time-Of-Check-To-Time-Of-Use (TOCTTOU), USB Storage Emulation and Block Cache byPass (Michéle, 2015). Hybrid Broadcast Broadband TV (HbbTV) is a technique that is used to provide on demand videos to STVs (Michéle, 2015). Two security researchers Youssef Oren and Angelos Keromytis demonstrated a successful attack on Digital Video Broadcast stream which can send countless malicious content loads to STV or TV box (Ghiglieri & Waidner, 2016). All these malicious activities

can trigger without any user interaction, therefore STV consumers should be alert for privacy settings that are set up in their devices.

It is not a secret that spying agencies use mobile phones, computers, tablets and other consumer smart devices to fetch the details about target users. However, two years ago Forbes and Vice magazines have published articles about CIA and MI5 having a joint project to spy on people that use STVs (Franceschi-Bicchierai, 2017 ; Brewster, 2017). The malware that CIA hackers have developed can indicate a "Fake-Off" on a TV power indicator thus it is actually spying on the user (Franceschi-Bicchierai, 2017). Thomas Brewster (2017) explained malware named Weeping angel appears on a TV as a normal application and it can recover the connected Wi-Fi network keys, saved usernames and passwords. This was the first time that public media has exposed the evidence of government spy agencies using STVs as spy tools in public.

To recap briefly, the above-mentioned privacy issues have illustrated that consumers cannot expect full privacy even after turning off the STV power button. Potentially, no one can stop technology development, still governments and standard development organizations can force smart TV manufacturers to improve the security of the devices and provide consumers more flexible options in agreements. More importantly, before it is too late consumers must check regular application updates and if possible, should consider installing smart device firewalls such as Dojo, F-Secure Sense and CUJO (Dickson, 2017).

2.5 VARIOUS SECURITY VULNERABILITIES IN THE SMART TV

As STVs are spread around the world, and available for a distributed attack surface. They lack security enforcement and most importantly can see and hear. Hackers use STVs to spy or steal data from corporate organizations or individual people. Security experts, Forensic examiners and hackers utilize hundreds of methods individually or collectively to breach security barriers in STVs. Section 2.5 considers the most common vulnerabilities that scholars have published about STVs.

2.5.1 Universal Plug and Play Vulnerability

UPnP is a collection of several network protocols that permits connection of devices to available networks. This is an extensive version of Plug and Play architecture. The devices that have UPnP technology can easily connect to the network and obtain IP addresses. In addition, this technology facilitates communication with other devices in the network to share service availability of the newly connected device. It also checks the service availability of other devices in the network so that it can use them. This two-way synchronization process attracted smart device manufacturers to add UPnP technology to their products. The next paragraph will discuss in detail how UPnP works.

Like other network devices, UPnP enabled equipment obtains the IP address from the DHCP server and then broadcasts the services that the device can offer. When a DHCP server is not available in the network it will assign an IP address itself, by using the predefined IP address table. To find other UPnP supported devices the newly joined device broadcasts the discovery message using UDP protocol through port 1900. Then as a response to the search request these UPnP enabled devices send a reply to the first device with location and device details. This description may include a list of services that this device can provide such as serial number, model and version etc. After gathering all device details within the network, the new device starts its actions using a remote procedure call (RPC) model. All the above-mentioned communications are XML formatted data on a SOAP protocol. It is sent via a HTTP request and all the responses, status changes and errors are maintained in the device state table. In some cases, devices can be found on the HTML interface that can communicate with the device control panel for checking the status of a device and status of the services (Device Security and Security Console, 2019).

Generally, message broadcasting is the main cause for UPnP vulnerabilities. The reason is the messages broadcast rapidly to the network and the device accepts the messages without an authentication. This opens a door to Man-in-the-Middle-Attacks and the attacker can command the

device to reconfigure itself to send the data packet through the attacker's computer. Mottalib and Hasib (2010) illustrated these vulnerabilities plus buffer overflow attack and the DDOS attack (Hasib & Mottalib, 2010). In their research they have demonstrated this attack model by sending altered NOTIFY messages to the target computer to download the details for other UPnP device descriptions. Then they acquired the control point in the network and routed other traffic to the attacker's computer. This security vulnerability worsen as UPnP was not checking the error on location URL (Hasib & Mottalib, 2010). Benjamin (2015) discusses in his book how an attacker can get access to MIPS (Microprocessor without Interlocked Pipeline Stages) registers by using buffer overflow attacks (Michéle, 2015). This unethical acquisition helps attackers to control STVs and monitor user activities.

This paragraph identifies several literature examples that discussed the UPnP attacks and their concerns. It was reported in the BBC news (2019) that a hacker group has taken control of Google STV and it affected more than 10,000 STVs (Tidy, 2019). Roku and Sonos hacked STV devices in a similar way that Mottalib and Hasib demonstrated, which means UPnP enabled devices can send commands to another UPnP device and vulnerable devices will execute them without checking for authentication (Wagenseil, 2018). Furthermore, the author has illustrated a snipper can easily setup fake pages to get victims' financial institution details.

2.5.2 Hybrid Broadcast Broadband TV (HbbTV)

In 2012 November, ETSI (European Telecommunications Standards Institute) accepted HbbTV as a broadcast technique (Ghiglieri & Waidner, HbbTV Security and Privacy: Issues and Challenges, 2016) to transmit digital videos and the Internet. The people who do not have Internet could use the media playback functionality with the help of DSM-CC (Digital Storage Media – Command and Control). Another important feature in HbbTV is that commercial advertisers can track user behavior separately and by region. Finally, all the above features are discussed in the following paragraph in detail.

In general, HbbTV signaling method can be divided into two major components. That is Program Map Table (PMT) and the Application Information Table (AIT). The PMT delivers available programs to the STV users with AIT which contains application specific information such as which application should start automatically or what kind of transport method should serve to get the application (Michéle, 2015). As stated in the first paragraph in this section, by using DSM-CC method broadcasters can deliver small applications and their data via TV broadcasting channels. This technique allows fragmentation of application data and prioritize fragments according to the user request (Mattoussi, Crussiere, Helard, & Zaharia, 2019). This method enables an interactive mode between the broadcaster and the STV hence most advertisers advertise in HbbTV channels. However, there is another method available in HbbTV that can broadcast information to STVs. It is to connect the application to a HTTP server via the Internet and deliver the contents to STV. The HbbTV 2.0 which was released in 2015 can handle HTML5, Web sockets, Web storage, Server –Sent Events and Media fragmented URI (Pascale, 2014).

The major disadvantage of HbbTV applications is different vendors produce their own products hence there is no stable standard protocol to make the assurance of security. As HbbTV applications can be triggered by Digital Video Broadcast (DVB), attackers can inject malicious URLs or other applications without the user acknowledgement (Ghiglieri & Waidner, HbbTV Security and Privacy: Issues and Challenges, 2016). Hackers use different attacking matrixes to compromise systems, therefore they will try every possible way to break potential security systems. Ghiglieri and Waidner have explained (2016) due to the data flow within the HbbTV application, perpetrators can deploy side channel attacks to wireless networks that STV is attached. They showed how it is possible to collect data packets' metadata, such as size and location, though the network as enforced by WPA/WPA2.

As defined in the second paragraph of this section HbbTV applications can be delivered via HTTP traffic or as a DSM-CC object. Therefore, attackers can create a small app and send it to the target STV and trigger the application to enable an attack surface. The most dangerous situation is

this attack could occur even when the STV is not connected to the Internet or can bypass security enforcement that is implemented in the device's attached network (Michéle, 2015). Further Ghiglieri and Waidner (2016) explained that incorrectly implemented HTTPS certificates within the STV application can cause security vulnerabilities.

2.5.3 Time-Of-check, Time-Of-Use (TOCTTOU)

The imperfect software applications and inferior software quality assurance can cause unrecoverable problems for end users. From a cyber security point of view these poor practices are the back doors that hackers can use to gain unauthorized access to systems. Therefore, the TOCTTOU problem is an example for products have multithreading and unpleasant software development practices. Regardless of the architecture of the software or hardware, if multithread operations take place, there is a possibility to race these attack conditions. These conditional occurrences are a huge problem for operating systems, especially for the operating systems that use UNIX kernels (Lowery, 2003). According to Jinpeng and Calton (2010), detection of TOCTTOU vulnerabilities is a microscopic operation and crucial task due to the nature of the environment and the development method of the application.

Apart from gaining access to files, in some cases hackers gain access to the root directory. Therefore, TOCTTOU is not limited to one problem. A good example is OpenSSL software. These applications are used to generate the Certificate Signing Request that is commonly known as CSR. Hence, if an attacker can get access to the root, they can get the details of certificate private key information from the compromised OpenSSL application. Table 2.1 illustrates the affected applications by TOCTTOU.

Table 2.1 Affected applications by TOCTTOU

Application Domain	Application Name
Administrative tools	At, diskcheck, GNU fileutils, logwatch, patchadd

Enterprise applications	Apache, bzip2, gzip, getmail, Impwebmail, procmail, openldap, openSSL, Kerberos, OpenOffice, StarOffice, CUPS, SAP, samba
Device managers	Esound, glint, pppd, Xinetd
Development tools	make, perl, Rational ClearCase, KDE, BitKeeper, Cscope

(Wei & Pu , 2010)

It is a controversial factor that a TOCTTOU attack method may not be easy to use against consumer electronic devices to break privacy, as raising the condition in a smart device environment is a tedious task. Nevertheless, Mulliner, Collin & Michéle, Benjamin (2012) had practically proved that this attack method can be used to compromise STV security. In addition, as mentioned in the previous paragraph, a TOCTTOU attack helps attackers to open a back door to the root access as most STVs support single sign on applications and acquire the access token that is kept in the root directory. Hence, if an attacker gets the SSO token, then they can use tokens to access actual user accounts. In real life, security and privacy cannot be simplified or neglected.

With regards to new prospects, future smart devices will be heavily loaded with multiprocessors and large amounts of memory capacity, comparative to current smart devices. When it comes to STVs, they probably will do some serious tasks such as virtual reality, photo and video editing and supporting more wearable devices. It is a well-known fact that these tasks will heavily consume processor power and memory, so in the near future STVs will get bigger multiprocessors. Jinpeng and Calton (2006) practically proved TOCTTOU attack has a bigger success rate in multiprocessor environments rather than in uniprocessor environments. Subsequently, if manufacturers introduce multiprocessors to STVs then TOCTTOU attack methods could have a bigger success rate in those environments.

2.6 CONCLUSION

The literature reviewed in this chapter has provided a comprehensive knowledge of the topic, and identified various privacy concerns in STVs, various legal Acts that relate to privacy issues, and various vulnerabilities in STVs. In addition, renowned STV privacy policies and various issues that customers and governments have to focus on have been discussed. All have to take extra precautions to protect consumer privacy rights. Section 2.2 focused on defining privacy and how philosophers have defined privacy based on culture, country, race, and various other factors. This literature covers three major Acts that are used around the world to prosecute privacy violators. Further it discussed the new privacy Bill that will be introduced into New Zealand legislation in April 2020. Therefore, it justifies the importance of privacy related issues in STVs and the reason that manufacturers need to address those privacy issues.

Each STV manufacturer has their own privacy policy that act as an agreement with the users. The section 2.3 analyzed three privacy policies that belong to Samsung, VIZIO, and LG, respectively.

The current privacy issues and various security vulnerabilities are discussed in section 2.4 and section 2.5. The important factor is the kind of vulnerabilities that STVs have and their consequences. The reviewed literature shows that STVs can be used as spy agents to spy on users and can be used as digital footprints to trackback to the users. However, the various vulnerabilities that were reviewed in section 2.5 illustrated the reasons that STV manufacturers need to rethink their data collection methods and technologies in relation to user privacy protections. Furthermore, as the technical industry is agile in nature, various malicious programs and techniques will come into action to attack STVs. Consequently, it is the STV manufacturers' responsibility to invest in preventing malicious attacks and ensuring the protection of end user privacy.

The chapter 3 will select the research problem and methodologies that are used in this research. In addition, it will discuss related works and introduce the sub questions and hypothesis.

Chapter 3

Methodology

3.0 INTRODUCTION

Chapter 2 critically reviewed a wide range of relevant literature regarding STVs. The reviewed literature assisted in gaining knowledge about various STVs and the privacy policies. In this Chapter a methodology for studying privacy issues that can arise in STVs and the procedures that manufacturers use to collect user behaviour data for various purposes, is developed. Chapter 2 also discussed several legal Acts that are used to prosecute STV manufacturers in regard to violations of consumer privacy. Uncommon attacking surfaces that researchers have overlooked were listed to disclose how attackers commonly gain access to STVs. The main purpose of Chapter 3 is to develop a research specification that identifies the problems and issues, and a way of investigating the reality of these matters in a laboratory.

Parallel and similar studies from previous research and publications are an advantageous start in defining research processes. Section 3.1 is dedicated to analysing five similar studies to advance the knowledge and understanding of applicable research methods to implement in the thesis, such as data collection, selection of tools and setting up an efficient test environment for the research. Section 3.2 explains the research design which incorporates the research hypothesis and sub questions. In subsections 3.2.1, 3.2.2 and 3.2.3 explain previous studies related to this research and respectively reviews of the solutions. The data requirement section (section 3.2) is focused on the outline of the data that should be collected during the data collection process and how data will be sanitized for the analysis process. Finally, section 3.4 discusses the limitations and the obstacles that exist in the proposed methodology.

3.1 REVIEW OF SIMILAR STUDIES

Four previous publications and studies were critically analyzed and reviewed in order to understand and develop the research methodologies for this project. These similar publications and studies guide the selection and design of methods and determine the thesis hypothesis. Correspondingly, the elected studies and publications cover a wide range of products and technologies, since STV technology is fragile and fast paced. Therefore, the publications cover a wide area of STV privacy issues including technical and the legal perspective.

3.1.1 Not so Smart: On Smart TV Apps

Niemietz, Somorovsky, Mainka and Schwenk (2015) have explored and demonstrated various attack models for STVs and the applications that users can install in STVs. In that research paper, the researchers have targeted Facebook, eBay, and other popular streaming applications. Further, the authors are concerned about the way that applications transmit data packets to the destination server and the security mechanisms that manufacturers apply to protect from malicious users (attackers). According to the authors, they planned to acquire single sign on access tokens and use those to compromise other applications that users have used. Therefore, researchers question the privacy issues that can occur after an attacker gains access to a user private account. In terms of security vulnerabilities in STVs, the authors have exposed that some STV applications did not use the basic encryption methods to protect credential data such as username, password, tokens, and so on. In addition the authors have acquired an OAuth token from STVs, Wi-Fi passwords and SSO data (Niemietz, Somorovsky, Mainka, & Schwenk, 2015).

Marcus et al. (2015) tried to cover all the main brand names that produce STVs including the devices that can produce STV functionalities. Moreover, in these tested devices, the research team upgraded all the patches that manufacturers have produced, and this helps get accurate results from the research. The authors have shown that they have employed three types of attacking methods to acquire the user data from STVs. The methods are Eavesdropper, Storage attack (needs to have the

physical access to the device) and Malware attacks. Fundamentally in the second and third attack methods, experimenters assumed that an attacker application had been installed in the target STV. Moreover, physical access research suggests that attackers can implement the application download link in spam mail or instant messages (Niemietz, Somorovsky, Mainka, & Schwenk, 2015). The above eavesdropper attack method and storage attack method are relevant to this research thesis. However, in this research it will not use the code injection attack method due to the limitation of time.

During the eavesdropping attack, Marcus, and the team (2015) have exposed how user privacy can be violated in STVs. Initially the research team discovered that unencrypted data were carrying user information to scorecardresearch.com. That data container had user identification IDs, Samsung SSO usernames, passwords and additional information related to video playlists that a user had accessed (Niemietz, Somorovsky, Mainka, & Schwenk, 2015). As a result of poor security configurations in STVs and its installed applications, users' SSO login data could be compromised to an eavesdropper. This circumstance can create a surface for attackers to gain access to mobile phones, PCs, or other smart devices that users have connected to the SSO account. This is a serious issue of user privacy since it contains all the user details and financial information. Secondly, Marcus et al. (2015) discovered unencrypted OAuth access tokens are used for Facebook and eBay applications in Grunding STVs. This vulnerability can lead to disclosure of user information to the public. As an example, even if a user posts a Facebook post in private mode, an attacker who gains the token can make the post public. Additionally, researchers have explained that even when eBay uses a TLS encrypted channel, attackers can gain OAuth access tokens via the poor security practices within Grundig STVs. My research will not examine Grundig STVs, but these findings lead to reexamining the manner that other STV manufacturers react to the revelations of security vulnerabilities of Marcus and the research team (2015).

The internal storage and cache data keep Wi-Fi, cookies, regular user inputs and occasionally user credentials in STV browsers. Therefore, if an attacker gains access to the internal storage they can gain tokens and other activities that users do on STVs. This discovery opened the doors for

forensic examiners to investigate criminals as STVs are getting popular for a communication device. Importantly the researchers showed that STVs should encrypt internal data to improve the privacy of its users, since in the real-life people sell their STVs to secondhand buyers in order to upgrade to a new STV. Consequently, if the first owner disregards resetting to the factory settings, the secondhand buyers can gain access to saved data and use credentials to hijack the previous owner accounts. Nonetheless if STV manufacturers encrypt the internal storage no one can gain access and the STV user privacy will be improved. With the completion of the study by Marcus et al, the following points will be incorporated into this thesis research method.

Eavesdropping – The Eavesdropping attack method has been selected to intercept the communication between STVs and other parties over the Internet. This method can be easily set up and provides evidence of the destination IP address.

Wireshark- Wireshark is identified as a monitoring tool and by using it the data packets can be examined in-depth.

PCAP Files: These are generated by Wireshark and keep the records of captured network traffic. Therefore, these files contain the network information and the communication data between two network IPs. In addition, the PCAP file will keep the data when Wireshark starts collecting network monitoring traffic.

3.1.2 A Study of Vulnerability Analysis of Popular Smart Devices through their Companion Apps

Mauro Jr, Melo, Lu,d' Amorim and Prakash (2019) researched smart application security vulnerabilities and the sort of privacy issues that can arise due to their companion applications. The research paper focused on four questions for IoT applications. They are:

- "Are encryption key(s) hardcoded"?
- "Does the application use local communication?"
- "Does the application send broadcast messages?"

- “Does the application use any well-known protocol with vulnerabilities?”

(Mauro Junior, Luis , Hao, Marcelo d’, & Atul , 2019)

The first question focuses on the impact if the developers’ hardcode encryption keys in the source code. This is an old security issue though some developers still have neglected it due to the lack of knowledge about security key management or simply ignored security key management principles by thinking that no one can hack their application. The second question focuses on the IoT application communication protocols. Each application needs to communicate with the Internet and with the devices in the local network. Therefore, the study showed the value of the matter when it comes to user privacy concerns. The third and fourth questions are the most important research questions in this study since broadcasting messages are the messages that inform the device information to the other devices in the network. These broadcast messages may contain sensitive data about the host device. Finally, the research questions about the extent that application developers are aware of the Common Vulnerability and Exposure (CVE) issue announcements and the actions that smart application developers take into account in order to recover the issues if they use affected protocols in their build.

The authors have used attacks that include four steps: find an encryption function that smart applications use; explore the exchange messages structure; the protocol that messages use to communicate; and finally monitor the pairing process (Mauro Junior, Luis , Hao, Marcelo d’, & Atul , 2019). To discover the functionalities of network communication and smart application encryption, the authors have used a social engineering technique and reverse engineering methods. For example, to expose the encryption methods in IoT applications they have created a possible encryption function using Java (Mauro Junior, Luis , Hao, Marcelo d’, & Atul , 2019). Many programmers use Java programming language in the Android development environment and by creating similar functionalities programmers can easily understand what methods that original application uses for network communication. Secondly, by using network traffic monitoring, the research team has

acquired the exchanged messages and broadcast messages from the target device. Consequently, Davino and the team (2019) acquired the cipher keys while initiating the pairing process of the application and the target smart device. The poor encryption methods open the door to decrypted exchange keys for attackers and they discovered that initially developers have used hardcoded values for cipher keys (Mauro Junior, Luis , Hao, Marcelo d', & Atul , 2019).

The Mauro Jr et al. (2019) study shows most of the applications that they have researched, used hard coded keys and 19 percent of the applications have not used any encryption, which means plain text communication over the network. 50% of the applications used encryption methods. Some applications have used vulnerable protocols and ports at the time that they conducted the research. Hence, this research paper showed the extent of the security limitations used by developers and the risks to consumer privacy and data protection. Another alarming point is some applications ranked highest in the list of IoT device sellers and they have a security error rating of 4 out of 5 (Mauro Junior, Luis , Hao, Marcelo d', & Atul , 2019). In conclusion, IoT application developers should give more attention to penetration testing and follow information security standards such as OWSAP when they develop smart applications. After the evaluation of the study by Davino et al. (2019) the following topics will be included into the proposed research method:

CVE Vulnerabilities- CVE maintain cybersecurity related vulnerabilities, such as protocols, ports and procedures and methods. Therefore, the proposed research method will be tested for STV to CVE announced vulnerabilities. This practice will help to understand security enforcements that manufacturers have introduced to correct the weaknesses.

Network protocols: It is important to detect the kind of network protocols that different STVs use for communication with the network and to connect with a cloud. Monitoring whether these communications are encrypted or not is important.

Broadcasting messages: The message broadcasting can summon attackers to attack smart devices. Therefore, concerning STV privacy, the details that the selected STVs broadcast to and out of the network require checking. In addition, by studying broadcasting messages, the researchers can be

mindful about the variety of information that a host device expects, such as shared devices or folders in the attached network.

3.1.3 I know what you streamed last night: On the security and privacy of streaming

Nikas, Alepis and Patsakis (2018) had investigated multimedia streaming platforms and various plugins that users widely use in smart devices. Since governments, merchandisers and broadcasting companies take extra measures to stop illegal video sharing practices over the Internet, new demand has risen for streaming videos in media platforms and applications in smart devices. Consequently, to fill the gap of illegal video sharing sites, new content of service sites and platforms are available over the Internet. Netflix, Prime video and Cinemax are good examples for legitimate content of services. However, Nikas et al. (2018) had focused their research on legitimate applications with plugins or add-ons to their platforms. In the research they focused on Kodi, Cuberevo, CCcam, Newcamd, OpenViX, Woosh OpenPLi, Roku MediaTomb and similar systems.

Nikas et al. (2018) highlighted that users can experience security threats subsequently when installing plugins and add-ons to smart devices. First, users can experience security issues that are specifically targeted to individual users or the applications. For example, malicious attacks can disrupt other services in the smart devices or may execute malicious code to execute additional tasks against other devices in the same network. In the second type of threat, targeted devices may contribute to perform attacks to another device, such as a distributed denial of service attack or distribute malware. The third and final threat model is snooping, where the attacker collects user behaviour and patterns (Alexios , Efthimios , & Constantinos , 2018). The authors have illustrated that vulnerable multimedia plugins and add-ons will compromise user privacy. The next paragraph will elaborate what are the possible attack methods that the research team used against the target systems.

Essentially subtitles in films and videos add extra value for non-native speakers, therefore in the present-day there is a huge demand for subtitles. Most smart device media players have plugins to support subtitles and some plugins will automatically download subtitles for the video (Alexios,

Efthimios , & Constantinos , 2018). In that scenario malicious users can send remote execution code via subtitles as plugins and download the text file and execute via the media player plugins. According to the Popcorn Time, the famous media players Kodi, VLC, and Stremio have been affected by the mentioned remote attacks (Hacked in Translation – from Subtitles to Complete Takeover, 2017). When focusing on application history, some applications keep track of user actions in a SQLite database. Nikas et al. (2018) have explained that even after deleting some data from SQLite database still malicious users or forensic examiners can recover considerable amounts of data that can disclose user privacy.

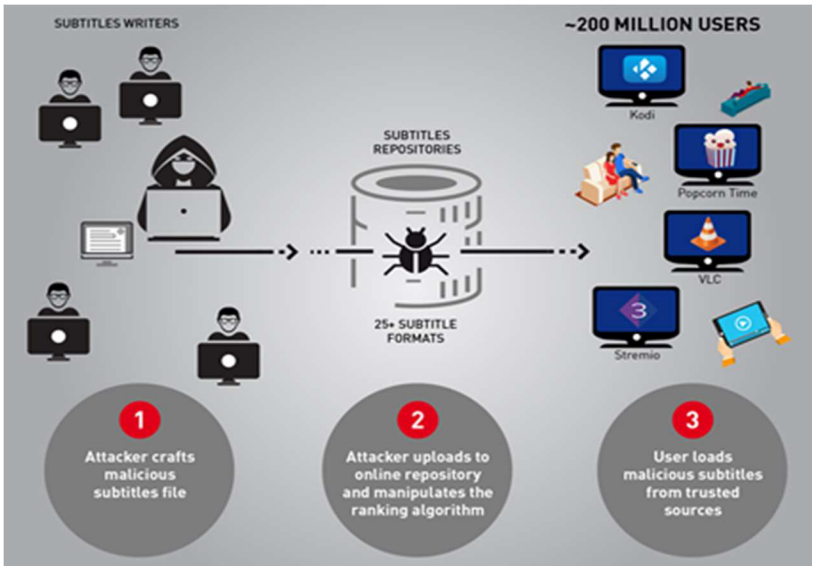


Figure 3.1 Hack via subtitles

(Hacked in Translation – from Subtitles to Complete Takeover, 2017)

Upon the evaluation of the study by Nikas et al. (2018) the following points will be considered for the proposed research methodology:

SQLite database- This is a small database that developers use to store small amounts of data in smart devices. Thus, unencrypted databases can expose data that can compromise the user privacy.

Malicious remote – By using subtitles or other payload, perpetrators can gain access to smart devices remotely. By using a Linux environment, they will try to replicate STV screens remotely without the knowledge of STV users.

3.1.4 Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices

Nikas et al. (2018) focused on the devices that can facilitate STV functionalities and how they trace user activities plus where they send out that information. For their research they selected two OTT platform providers, they are Roku and Amazon fire. Roku and Amazon fire TVs have market share of 59% to 65% globally in the OTT platform industry and the authors pointed out this was the main reason for choosing these two platforms for their research (Mohajeri , et al., 2019). In addition, they found the two OTT Platforms were collecting device serial numbers, MAC addresses and transmitted back to platform providers. The authors have shown the main income of OTT manufacturers was not the sale of the devices but the advertisements over the device that it streams (Mohajeri , et al., 2019). Therefore, Moghaddam et al (2019) argued OTT platform companies will collect user data without concern for the privacy of the users. Thus, platform providers are interested in exploring OTT endpoints and what information they collect from users.

According to the authors there were two major parts in the research project, that are "Triggering Video Playback" and "Collecting Network Data and Intercepting Encrypted communications" (Mohajeri , et al., 2019). They manually triggered video playbacks and collected information such as the number of keystrokes in the remote controller. However, to decrypt encrypted communications, the research team used mitmproxy. In some cases, Moghaddam et al (2019) failed to intercept encrypted communications. To overcome this issue, they gained root access to OTT devices and installed self-signed certificates to the devices. Roku was not allowed to access the root directory, however, Amazon fire TV permitted them to access the root directory. (Mohajeri , et al., 2019).

From the test setup the research team had collected SSL logs that contained SSL keys which were used to intercept the TLS session for each channel. This also included events, time stamps of the channel launch, install or remote-control key press times, TLS artifacts and screenshots. By tracking and collecting user inputs, the research team had expected to monitor the kind of

advertisements they will get back from OTT host companies. With the help of the collected data at the data processing stage, the authors explained several data trackers received data without prior notification to viewers. Additionally, the authors explained all the tracking and data collecting practices that trackers execute can be prosecuted under the VPPA Act. By thinking out of the box, Moghaddam et al (2019) explored the Remote controller API's contribution to compromise user privacy and security. Normally OTT devices use API endpoints to receive user commands. The authors found the Roku remote API can easily be hacked and to gain access to devices for installing malicious applications (Mattoussi, Crussiere, Helard, & Zaharia, 2019).

Finally, this research provided a guideline to monitor and track STV data collection and the tracing of user experiences for advertisements. Therefore, the proposed research will help to understand when trace data may not violate user privacy and when STV violates the privacy laws, also how it affects the VPPA and the upcoming New Zealand privacy Bill. Upon the evaluation of the study by Moghaddam et al. (2019) the following points will be integrated into the proposed research thesis:

TLS – Transport layer security is a protocol that provides end-to-end security for network and Internet communications. Its end to end cryptographic encryption, communication channels can be protected from eavesdropping and message forgery.

Intercepting traffic - It is a tedious task to understand encrypted traffic thus by intercepting traffic via proxy server it may give more chances of exploring the certificate or bypass HTTPS traffic.

3.2 RESEARCH DESIGN

Section 3.1 provides corresponding analysis of four previous research studies that relates to this thesis and provides guidance for this thesis. The individual research illustrated how to design the research methodology and to construct suitable methods for research thesis questions. In addition, it guided directions to fill the gaps in research techniques, and how previous research paper results can be

integrated for this research thesis methodology. Further it helps to elaborate sub questions of the main hypothesis and add more research weight to them.

The section 3.2.1 sums up four studies of the review in section 3.1 in order to build the data requirement for this research thesis and filter unnecessary points from the research papers. Section 3.2.2 illustrates solution selections and will address the relevant selections for the research thesis. The section 3.2.3 defines the research questions and the section 3.2.4 explains the hypotheses respectively. The subsection 3.2.5 explains the research phases and the last part of the section 3.2 (section 3.2.6) illustrates data mapping. Section 3.3 discusses data requirements including data generation, data collection and data processing steps. Section 3.4 provides the overall limitations of this research thesis and finally the section 3.5 concludes Chapter 3.

3.2.1 Summary of Similar Studies

Marcus et al. (2015), Davino et al. (2019) and Moghaddam et al (2019) explained that most of the vulnerabilities and the security breaches of STVs occur due to inappropriate security enforcements on the data packets which are sent from STVs. As STVs are attached to home or office networks, it always allocates IP addresses from a DHCP server. Therefore, attackers need to identify the target device IP address that is to be attacked. To fulfill this requirement the authors used network scanning tools and sniffing tools in their research setups. Hence in this research these two categories of tools cannot be neglected as it provides real time network data communication monitoring plus the ability to analyze sniffed data. Therefore, sniffing tools and network scanning tools will be adopted for this research.

The Time of Check to Time of Use (TOCTOU) attack method and the code reverse engineering method, guess the functionality of the computer source code execution. In the study of Davino et al. (2019), reverse engineering methods to identify the Java class libraries were used. These specify application developer choices show encrypted data communication methods such as which java libraries are defined for a communication protocol (java.net.DatagramSocket), and the API used for cryptographic encryption that finds any hard coded encryption key. These two methods are

disregarded in this research because of the time frame and programming requirements. In addition, more development frameworks are introduced for development such as Xamarin from Microsoft, and it needs to check related libraries of the application development frameworks which are out of the scope in this research thesis.

The three research papers discussed in section 3.1 are focused on malware payload attacks which enable a back door to malicious users to take the control of STVs. Nikas et al. (2018) exposed that malicious payloads can be sent to target devices via subtitles. Moghaddam et al (2019) showed that payload can be injected via media player plugins, and finally Marcus et al. (2015) described executed malicious code via USB drives. All authors stated that they gained access to internal storage of STVs or to authentication tokens of various systems via this method. As this attack method has various approaches and creates various privacy issues for STV users it is considered suitable for the proposed research. Moreover, Nikas et al. (2018) showed by gaining access to the internal storage build, forensic evidence in STVs is accessible. However, this research will not focus on building forensic evidence, in contrast it will consider types of data that can compromise user privacy if an attacker gains access to internal storage.

Finally, the study by Nikas et al. (2018) focused on online data collection from STVs. This proven method is useful as a cross reference for this research to compare who collects data from STVs and types of collected data. This will increase the integrity and the consistency of the research findings since the research is based on privacy issues of STV users.

3.2.2 Research questions and Hypotheses

Chapter 2 discussed various areas that facilitate privacy issues in modern STVs. At the beginning of Chapter 2 the main components of STVs are defined, and then various privacy policies of the STV market leaders are evaluated. In the privacy section, the various meanings of privacy are defined according to several authors who described privacy use in the past. These definitions help to understand various privacy Acts around the world that are used as safeguards against electronic or

online privacy violations for consumers. After, evaluating uncommon thus effective attack methods that hackers use to compromise STV privacy, suggestions are made for protection. Section 3.1 summarized previous research works that are related to this research thesis. This section outlines the research methodologies and identifies various tools that can be used when conducting the proposed research. In addition, some tools and methods have a higher capability to provide evidence of actual attacks against STVs, though some tools may not. Finally, the research question is derived below, and it breaks down to three sub questions in order to answer the main research question.

The Main research question of this research thesis is:

What are the active and passive privacy issues in current smart TVs?

The goal of this research thesis is to explore the kind of privacy issues that can occur in STVs and the ways that it can happen such as due to bad configurations, manufacturing faults or other issues.

To answer the main question, the following sub questions are needed:

(SQ 1) What data and information do STVs send out and to where?

This sub question is expected to find out what sort of data that STVs send out and to where.

(SQ 2) What security mechanisms are used in STVs to protect data?

Here I will execute various types of attacks against selected STVs, explore which attack methods get success, and how far STVs can defend against attacks. Further I will analyze how much data that an attacker can retrieve from a compromised STV, and how those data raise privacy issues for STV users.

(SQ 3) How will the upcoming NZ privacy Bill will help protect STV consumers?

The answer for this will be based on the above two answers, to show how far the new privacy bill covers consumer rights in New Zealand.

Hypothesis 1 (H_1)

Every penetration testing tool that is used to attack STVs will not succeed every time. However, these commonly used and well-established penetration testing tools will be expected to work without any errors in all recommended environments.

Hypothesis 2 (H_2)

When executing attacks against STVs it is expected that attackers might already be in the network or else neutralize the network security enforcement of the STV attached network.

Hypothesis 3 (H_3)

When it comes to network packet capturing tools, it is expected that tools will perform well under a high level of network stress without any errors.

3.2.3 Research Phases

To get the answers for the main and sub-questions, the following research plan was designed. The proposed research plan contains five phases as shown in Figure 3.2. The first phase is for preliminary investigation and identifies attack methods that hackers can use against STVs to breach user privacy. The preliminary investigation will be done in this phase to find the types of attacks that can be used to gain the data from the components in STVs. For example, by sniffing STV network traffic, attackers can gain access tokens as mentioned in the section 3.1.1. The first phase will identify the necessary tools and the software for the selected attack methods. As a preliminary attack map, a combined and setup demo environment will be made to test the tools to verify that they return expected results or expected outcomes in a similar environment. Finally, and importantly I will review the documents and electronic materials to identify and acquire knowledge about selected attack behaviour and possible outcomes, and how acquired data can be evaluated against privacy matters for STV viewers.

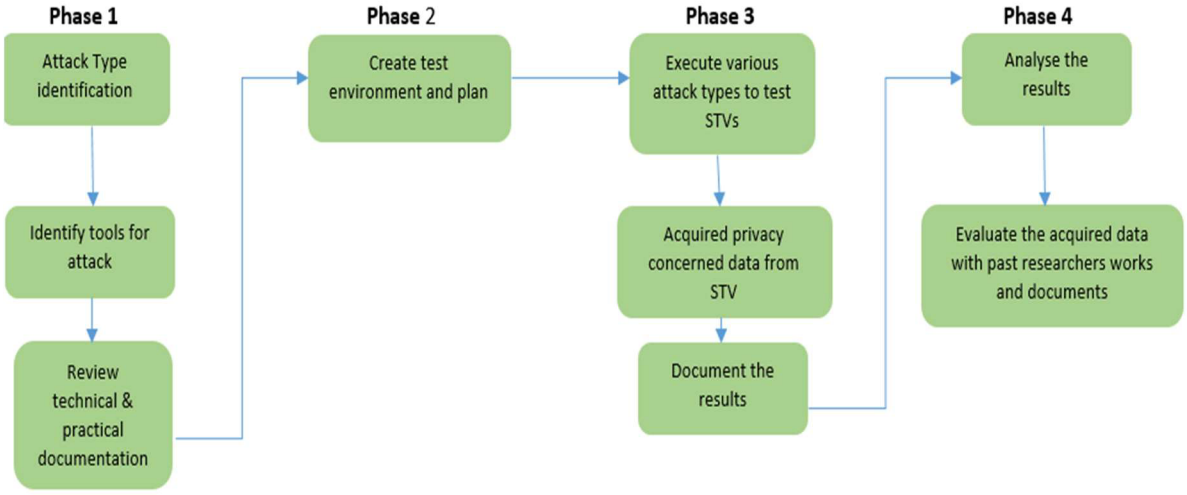


Figure 3.2 Research Phases

The phase 2 is designed to test the environment physically and logically, including a network setup for a typical home STV setup and office STV setup. In addition, it is to create a test plan for each scenario to cover privacy issues in STVs. Therefore, in the test plan each test case should test different brands of STVs that are in the same network. Equally, all the setup and configurations will be done as explained by the manufacturers in the STV user-manuals or latest instructions in the official websites of the manufacturers. Rather than providing binary test results, all the test cases will execute specific tasks and evaluate the level of privacy that can be breached or any other threats that can occur with breached data.

Phase 3 will execute all the attack vectors and the collected data according to the test spectrum that is defined in the phase 2. Furthermore, this phase will capture outbound network traffic from STVs by using network traffic monitoring tools. However, I will not expect that captured data may alarm user privacy issues in this phase. In some cases it will expect some data to expose direct privacy breaches such as unencrypted network traffic, and payload attacks. After executing the test plan, will document all the methods and test results for analysing in the next phase.

Phase 4 is the final phase that will analyze the acquired data and files from the STVs. In this phase I try to interconnect all the acquired data and files, and will discuss how these files and data can make serious privacy issues for STV viewers. Moreover, rather than the dangers I will analyze the severity level of breached data with regards to privacy. The reason is sometimes data may cause serious issues in some areas but not others. After analysing data and the test cases, I will review previous research work and compare the kind of security levels that manufacturers have applied to overcome the exposed vulnerabilities. Finally, in this phase I will combine the sub questions and hypothesis to support the main research question to show the significance of STV privacy issues.

3.3 DATA REQUIREMENTS

This research needs different sources of data to analyze the privacy issues in STVs. It can be either preliminary test data, data collected from network monitoring tools, manual collections of data on Google aderts and reconstructed data that is acquired from STVs. The information gathered in the first phase will be used to create a structured test plan that covers regular attack scenarios that have been discussed in section 3.1. Based on the collected information, test plans will be created in the second phase. The case scenarios are invaluable for this research as various attackers can use different techniques, practices, or collections of attacks. In contrast, these test cases cover the data that manufacturers are trying to collect from STVs.

The implemented test plans will be executed in the third phase within the setup network that is similar to a home network. All the hardware and software environments are similar in this network except the target STV. Therefore, it will help to reduce external factors that could affect the expected results. In the third phase the data collection process will be monitored the in real time within the defined time frames such as hours, days and weeks. In the final stage of the third phase collected data will be documented to define the test cases and the outcomes. All the attack methods defined in the test cases simulate real world attack scenarios in a real-world home network. The following sections

will elaborate in greater detail what data should be generated, which ways they generate, plus how to process, analyze and present the acquired data.

3.3.1 Data Generation

The data generation and collection process are two vital parts in this proposed research. For this process it first needs several email accounts to link with the STV. The STV should operate as a normal home user. It is required to operate popular entertainment applications in all the STVs based on the following main categories:

- Sport
- News
- Weather
- VOIP
- Video streaming
- Internet browsing

Apart from old pictures and videos, dummy files will be used to monitor how STVs behave when external devices are attached. The above-mentioned data generation process will be done manually and will not use any data generation tools.

3.3.2 Data Collection

There are three types of data that need to be collected from STVs for the analysis process. They are:

- Inbound data
- Outbound data
- Stored data

When STVs operate on a home network it receives data from the main host server and sends back data to the nominated server. According to previous studies, this communication traffic generates large amounts of data. By capturing this data I can analyze which data are encrypted and which are

not, and the strength of the security reinforcements that STV manufacturers have implemented. Further, through the analysis I can reveal user activities recorded under the channels, the date, the time, synced email addresses, and the duration of watching a program. This process will ensure the usual home usage of STVs in a home network. However, these experimental data will be collected in a controlled lab environment. To collect network traffic data I will use network monitoring tools in an experimental network.

The extraction of data from STVs will be performed remotely via an experimental network. This research will not cover physical data extractions such as removing the memory EPROM chips and extracting data from them. I will extract stored data from STVs by executing various attack matrix while the STVs operate. Each test case has its own attack model and I will describe its steps and process that applies to generate the data or extract the stored data in STVs. These test cases are not binary type test cases, and show the capacity and the extent that a test case can handle attack. To maintain the consistency, I will record the MD5 hash value as a proof for the acquired data are not altered before analysing.

3.3.3 Data processing

The previous section described the data collection process and the type of data required to be collected for the research analysis. The collected raw data will be entered into a pre-formatted excel sheet for convenience. Then the collected data will be compared with previous research paper outcomes that are reported in section 3.1. I will closely analyze the collected data to find any PII information or any other information that can breach a user privacy.

3.3.4 Data analysis and presentation

This section covers the analysis and the presentation of the processed data that is collected in the data collection stage. Generally, there are four levels of data that will be analyzed in this research project. On level zero there is no harm done. In the first level analyzed data which do not cause serious harm for STV users by compromising them such as channel details and durations of watching, are reported.

In the second level analyzed data that causes considerable damage to STV users if compromised is found. At the last level is the data that can cause serious damage. The findings of this level report to CVE.

Table 3.1 Damage level analysis

Effective Level	Damage
Level 0	No Harm
Level 1	It may not affect heavily even this information leaked, such as email, programme watching time
Level 2	Considerably affect but not heavily such as data of birth, bank account number
Level 3	Will do heavy damage and can be big loose, passwords, access tokens, pins

In addition, I will do a comparative analysis for each level of data with the tools that have been used to produce or capture data. If an attacker uses an expensive process to attack a STV in order to acquire level one data then it will not be feasible if the attacker uses simple tools and methods to compromise the STV system and acquired a third level of data. This will be a serious privacy issue from the STV consumer’ s point of view. Finally, the main purpose of this analysis phase is to find what data that compromises a STV user privacy and how it will affect New Zealanders in the future.

3.4 LIMITATIONS

This proposed research focuses on evaluating the privacy issues that can occur in STVs and its applications. There are several tools and scenarios that should be used to extract data from STVs and several tools that need to be used to execute attacks on STVs. Therefore, each of these tools and scenarios have their own limitations and, in this section, I will discuss the general limitations. Furthermore, these limitations can be the starting points for future research.

In penetration testing and the dark web there are many tools available to execute cyber-attacks against IoT devices and smart devices. Some tools state they have great success rates in smart devices. However, none of these tools are specifically designed to make cyber-attacks on STVs and they are not tested against STVs. Due to the time constraints, I will not check all the different tools for one STV. When tools are selected for the attack I will refer to previous work and recommendations from the industry experts. Therefore some attacks can either be successful or partially so, and some can be unsuccessful.

Secondly, this research will not cover all the applications that can be installed in STVs. Consequently, the result may not be complete since untested applications can have security holes. Therefore, the end results of this research will not reflect the entire picture about STV privacy issues. As mentioned in Chapter 2, STV manufacturing is profitable in various ways. Lots of Android based operating systems are developed for new STV sets and this project will not cover new STVs and their application systems, architectures and so on. Similarly, the test environment of the STV is setup with minimum facilities and services, and may result in limited data or fault alarming.

Finally, this research has the influence of some legal constraints based on the data privacy and online privacy laws. Some of the related topics are discussed in the chapter 2. However, I did not take legal guidance to analyze the research findings. Therefore, when combining data breaches and legal factors will require further scrutiny to clarify the knowledge gap between them.

3.5 CONCLUSION

Chapter 3 provides a comprehensive outline of the designed research methodologies, data collection methods, research question, and hypothesis of the proposed research. The section 3.1 discussed the similar works done by other researchers which are relevant to this research. By evaluating previous related works, readers can get a clear idea about the relevant technology to use in the research and necessary methodologies that need to integrate. Equally, STV privacy issues are a new topic in Information Security. Most of the vulnerabilities probably have not been exposed previously, hence

data extraction can be challenging, as penetration tools may not completely perform in the STV environment.

Throughout the research I will collect research data by developing relevant test cases and executing them according to the test plan. Each phase of the data collection process reflects the strength of the privacy concerns if miscellaneous users get access to data in STVs or data generated by STVs. The data generation process will be manual as it cannot be automated in the STV environment at the moment. Therefore, this research setup has attempted to cover all the aspects of a home environment and the usual user behavior, but in a test environment.

Finally, the limitations of this project are discussed in the section 3.4 including the technical limitations and the legal limitations. The limitations are discussed in order to give a clear picture about the research findings and guidance to future research topics for STVs. The next chapter presents the research findings and the analysis as defined by the methodology specification in this chapter.

Chapter 4

Research Findings

4.1 INTRODUCTION

The previous Chapter 3 has defined the research methodologies and reviewed similar studies that are related to the research questions and sub questions for this study. Section 3.2.3 also described the research phases for this research. Section 3.3 described the experimental data generation processes and data collection processes that are implemented to analyze privacy issues in STVs.

The objectives of chapter 4 are to demonstrate the test cases and to present the research findings of the privacy issues in STVs. The data findings are compared with each selected STV brand in the research. In summary this chapter contains four major parts. The first part, section 4.1 discusses the variations including data generation, data processing and data analysing. The subsection 4.2 explains the test environment setup for data generation. Subsection 4.3 illustrates the test cases and the test results followed by the subsection 4.4 which is the chapter conclusion.

4.2 VARIATIONS ENCOUNTERED IN RESEARCH EXPERIMENT

Moderated variations were made after implementing the pilot experiments according to the methodology that is explained in section 3.3. These changes are not significant, however, variations provide a broader view of how STV data can raise privacy issues in areas such as user interests, time frames, suggestions, and exposure to other network users via advertisements. Therefore, it is an important matter to describe in detail, what are the changes for the test phases. The following subsections outline the changes made during the research.

4.2.1 Test Environment

Initially the test environment was designed only to monitor STV activity, however after doing several pilot test runs, it was concluded that the research needed an additional third-party smart device

(mobile, tablet) to reflect how merchandisers use data that is fetched from users. Without this extra modification it was a difficult task to identify how it affects other smart devices in the home network.

4.2.2 Data Collection

In the data collection process, changes were made to get a better result rather than just using true false test cases. The reason is that when answering the questions and sub questions of this research, binary answers will not give a clear picture of the research outcomes. Therefore, two different Gmail addresses were setup in smart devices. One email address is for the STV and the other one is for another smart device that is connected in the test home network.

4.3 RESEARCH TEST ENVIRONMENT SETUP

Principally this research is focused on household STVs as most office environments have installed Deep packet inspections or other security measurements to protect outbound data. Therefore, when setting up the test environment it is focused on a simple home network. The Figure 4.1 shows the physical environment that is used in the research project.

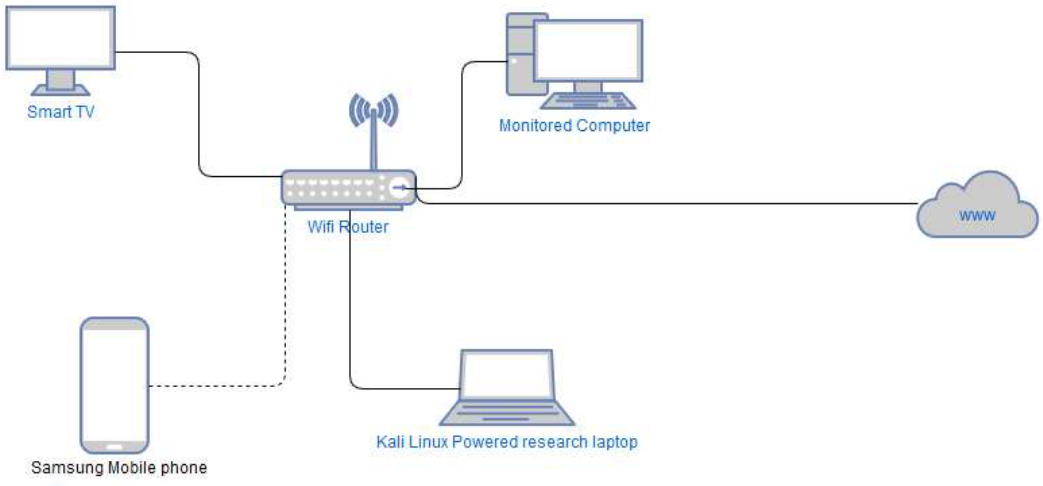


Figure 4.1 Network diagram of the test environment

The physical equipment is connected to each other as shown in Figure 4.1. The main penetration testing computer is powered by an Intel (R) Core i7-5500 CPU with a clock speed of 2.4 GHz and

has 16GB RAM plus HDD of 1TB. Kali-Linux is used as the operating system platform for this project. To capture data traffic from the specific device Wireshark is used.

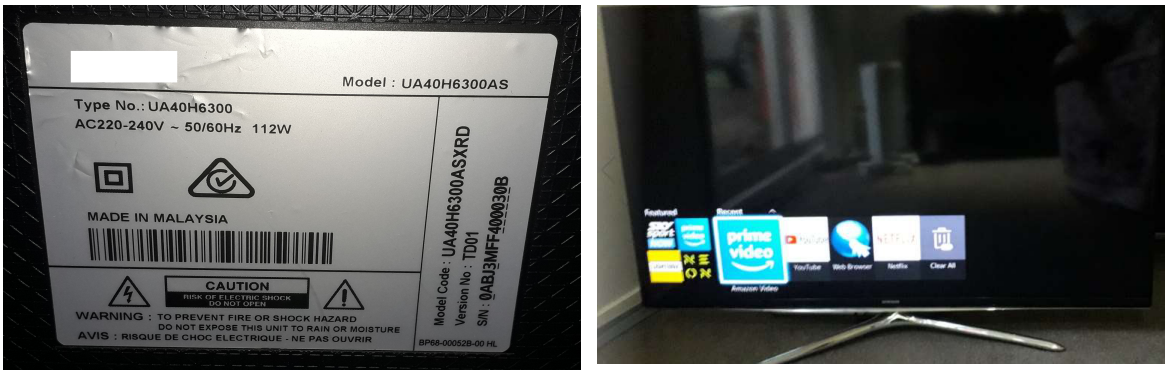


Figure 4.2 Tested STV A

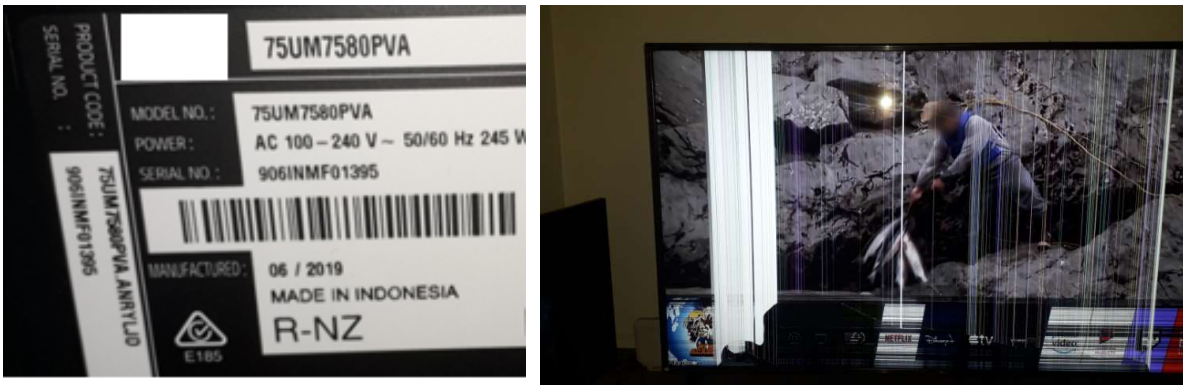


Figure 4.3 Tested STV B

A Samsung J3 is used as a third-party smart device for advertisement monitoring. This phone is operated by an Android version 9 operating system. The mobile phone has installed a Samsung Internet browser and Chrome Internet browser. The following figure shows the phone and kernel version of the system.

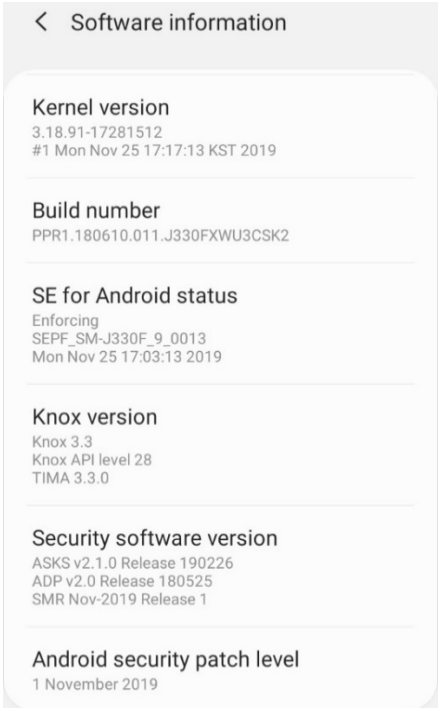


Figure 4.4 Samsung J3 Kernel details

To connect with the Internet a 10/100 ethernet router is used that is provided by the Internet Service Provider. This router has a browser-based administration configuration interface. However, the router is configured with recommended basic security settings for home use.

4.3.1 Test Cases

The section 3.3.1 explained seven categories of TV programs that a usual household STV stream. The section 3.3.2 illustrated three sections that monitor data in STVs. Each test case has a unique expectation and coverage such as what attack methods are used to compromise privacy. The following Table 4.1 illustrates the summary of the test cases plus the next section explains the test cases in detail and its expected outcomes.

Table 4.1 Test cases for STVs

Test Case	Category	Iterations	Attack type	Expected results
T0001		3	DoS Attack	STV works normal without any disturbances.

T0002		3	MITM Attack	All inbound and outbound data should be encrypted.
T0003		3	Social engineering	STV attached network users should not get any clue on what users watch on STV.
T0004		3	Acquire root access	STV should not allow to get root access.

The above test cases are tested 3 times. The reason is if it is tested only once then it may not give a clear picture, and similarly if it is tested 2 times it may give a binary result. Therefore, to balance the test outcome, each test case is tested 3 times. The test cases shown in Table 4.1, focus on sniffing inbound and outbound data, and to capture any data that can be harmful for STV viewer privacy.

4.4 TEST RESULTS

This section presents the test results obtain through the test cases showed in Table 4.1. Section 4.4.1 shows the DoS attack outcomes against the tested STV. Section 4.4.2 shows the results of a MITM attack. The third section presents the social engineering result of each tested STV. The final section shows the result of root access attempts and the outcomes.

4.4.1 Test Case T001

This test case is designed to test the Denial of Service attack against the test STV. The main purpose of DoS attacks is to block or shutdown the service or functionality of the system or device. Flooding the network traffic and crashing the services are two major types of DoS attacks. Therefore, most of the time attackers use Buffer overflow attacks and ICMP floods. Buffer overflow attack types generate traffic over the network for more than the initial system is designed to handle, hence eventually the system will be stuck or shut down. On the other hand an ICMP flood generates traffic to the misconfigured network endpoint until it shutdowns (What is a denial of service attack (DoS) ?, 2020).

The above test cases have employed the ICMP flood attack type. To generate an ICMP attack, one python script is used that finds the CVE-2013-4890 vulnerability (Mesellem, 2013). (Initially this script was in python 2. However, I modified the script for python 3 as it suits the kali Linux environment.)

When an attacker does not have the physical access to a STV they sniff the home network to get the IP address and the device information. In the test environment I used Zenmap to get the IP address and the details of the HTTP supported ports within the STV. The following two sections show how attacks are executed against STV A and STV B.

CVE-2013-4890 vulnerability script against STV B

The figure 4.5 shows the Zenmap results of the IP addresses, and the open ports in the STV B (which are port 3000 and 3001). The figure 4.6 shows the graphical visualization of the traffic generated against the IP when an attack script is executed in the STV B.

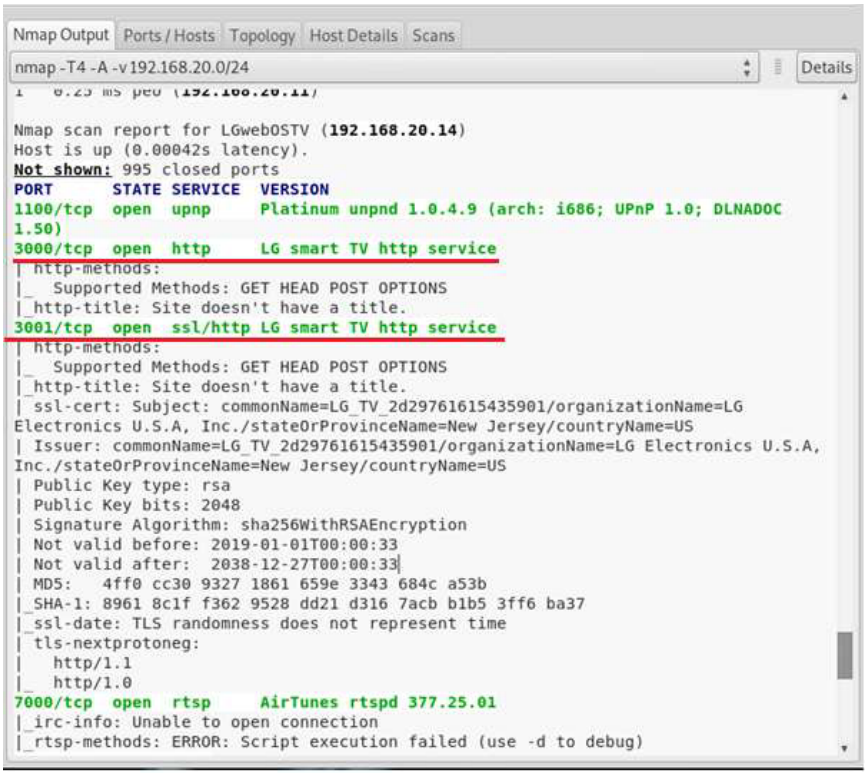


Figure 4.5 Zenmap sniffing report of targeted STV B and ports

The script says that the targeted STV is down, however it was working perfectly without any disturbances. However, as a proof for the traffic generation EtherApe was used to show the graphical view of the attack packet generation.

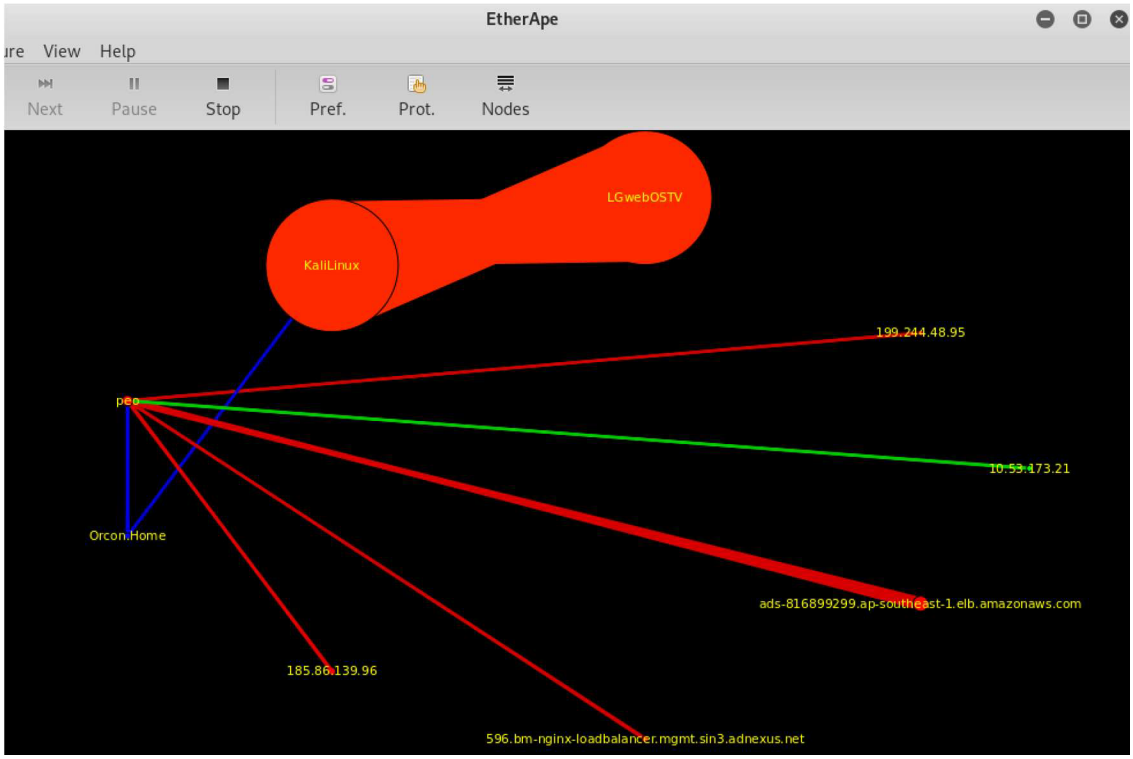


Figure 4.6 EtherApe tool shows the graphical view of the attack when executed against STV B.

The following Table 4.2 illustrates the result of T001 against STV B. It is interesting that even with the heavy load of traffic at specific ports, the STV works perfectly without any service interruptions.

Table 4.2 T001 Findings for STV B

Test Case	IP Address on STV	Targeted Ports	Service Down
T001-1-1	192.168.20.14	3000,3001, 8080	No
T001-1-2	192.168.20.14	3000,3001, 8080	No
T001-1-3	192.168.20.14	3000,3001, 8080	No

CVE-2013-4890 vulnerability script against STV A

The Figure 4.7 shows the result of Zenmap. The ports that are underlined in red are identified as targeted ports for DoS attack in scenario one. The Figure 4.8 shows actual IP address of the STV at that time for the Zenmap report. After gathering all the necessary information, the executed Samsung_D0s.py script against all the ports is mentioned in the Zenmap report. It is expected that the STV A functions properly without any disturbances. The script ran 3 times and the targeted STV A functioned properly all 3 times.

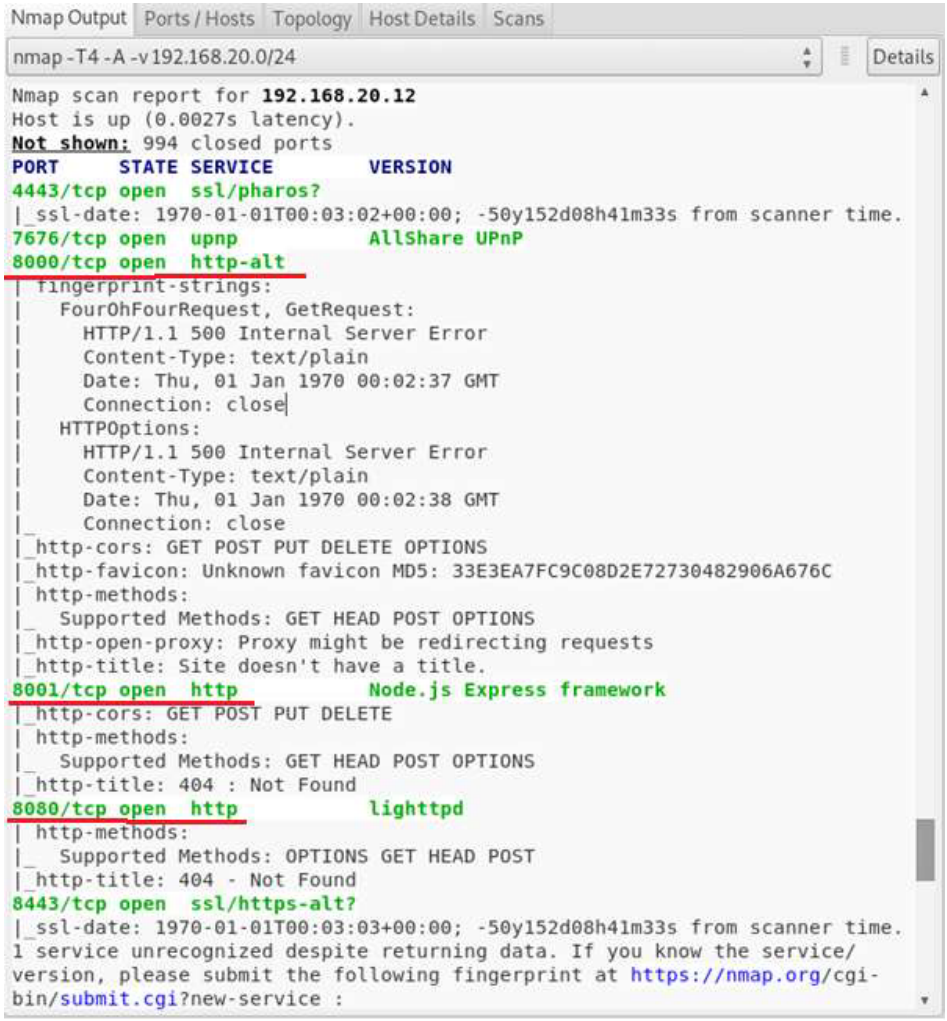


Figure 4.7 Zenmap sniffing report for the targeted STV and the possible targeted ports

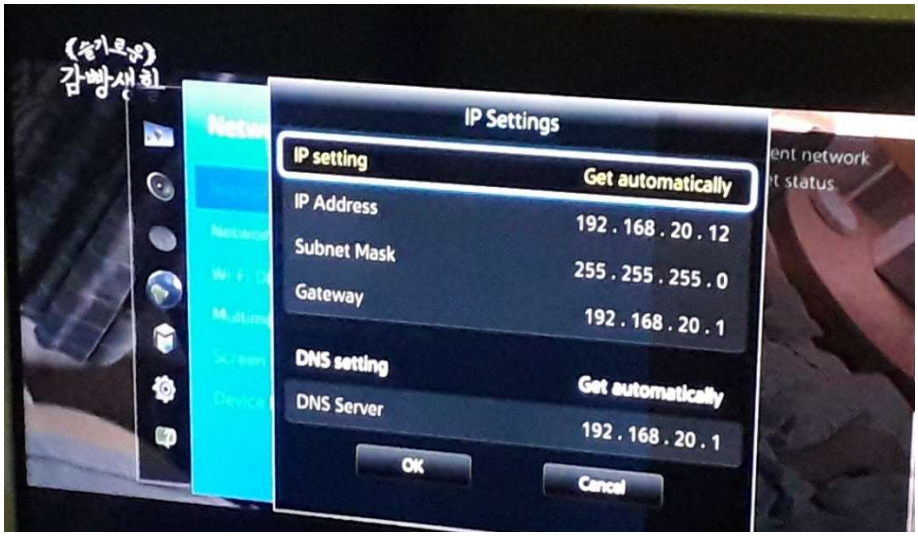


Figure 4.8 STV A IP address 192.168.20.12 for Test Case T001

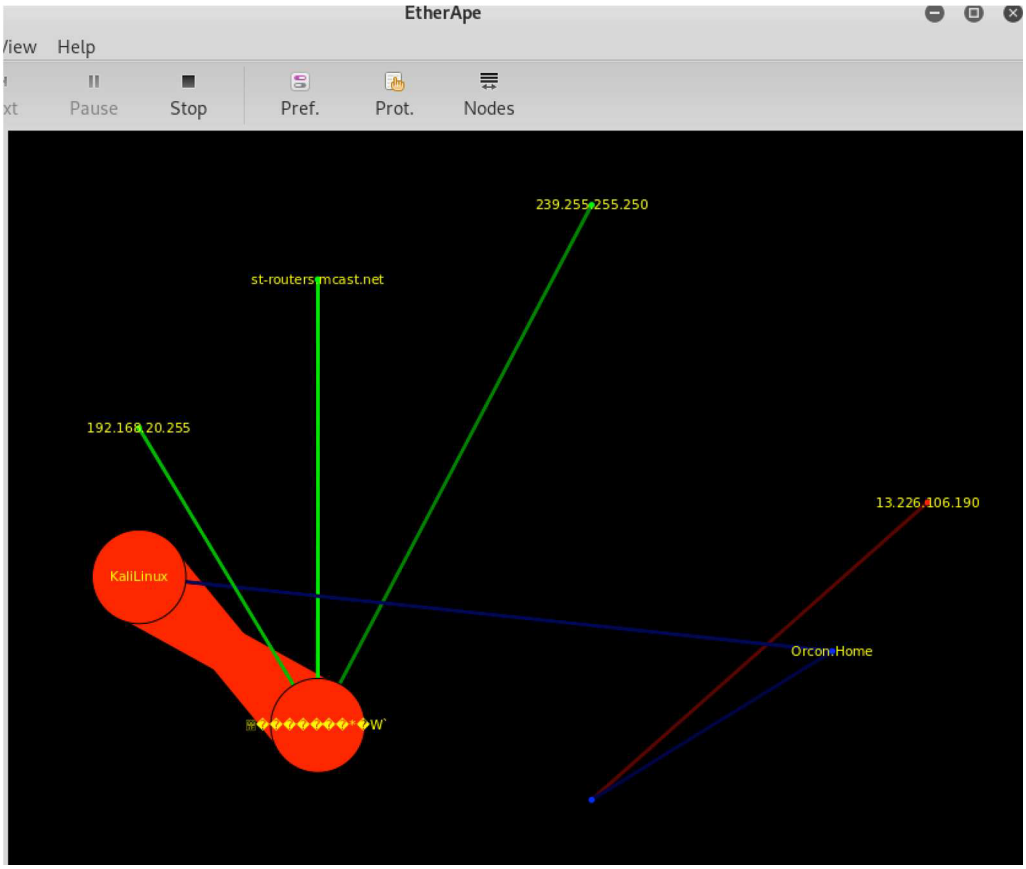


Figure 4.9 EtherApe shows the traffic load while DoS attack on execution against STV A

Same as STV B, the STV A works normal without service interruptions or buffering during the DoS attacks execution.

Table 4.3 T001 Findings for STV A

Test Case	IP Address on STV	Targeted Ports	Service Down
T001-2-1	192.168.20.12	8000,8001, 8080	No
T001-2-2	192.168.20.12	8000,8001, 8080	No
T001-2-3	192.168.20.12	8000,8001, 8080	No

4.4.2 Test Case T002

The Man in the Middle Attack (MITM) is the most famous attacking method that cyber attackers use to seize data from its origin. This test case is designed to check what type of data can be captured from STVs while operating on a home network. The MITM attack means intercepting communication between two end points. Moreover, when an attacker intercepts the data communication, they act like a proxy server between the two nodes. Therefore the attacker can change, insert or delete original data in the communication channel (Man-in-the-middle attack, 2020) . To set up this test case I used Ettercap as the ARP spoof tool and Wireshark to capture and record the intercept data packet.

The same as in test case T001, the Zenmap tool is used to get the IP address details of the STV. Then the Ettercap is used with Wireshark as shown in Figure 4.10. It is used with the same approach for both STVs to keep the consistency of the test cases.

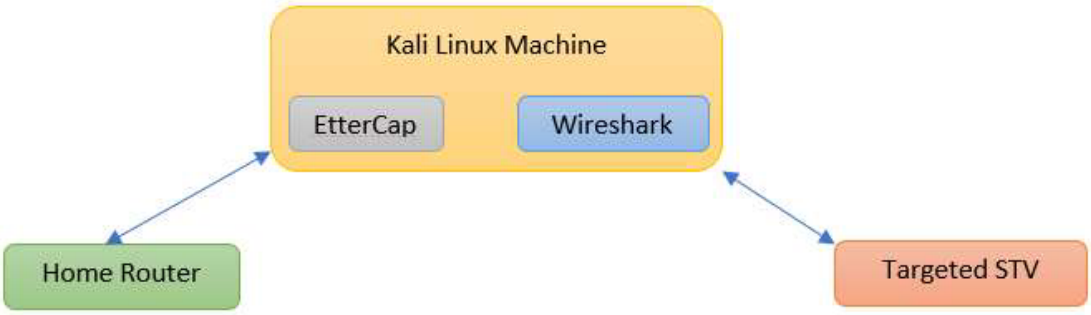


Figure 4.10 MITM attack setup for test case T002

Finally, the Linux system should forward the IPs as it acts as a router in this scenario. Therefore, to forward IPs it needs to execute system control commands as well.

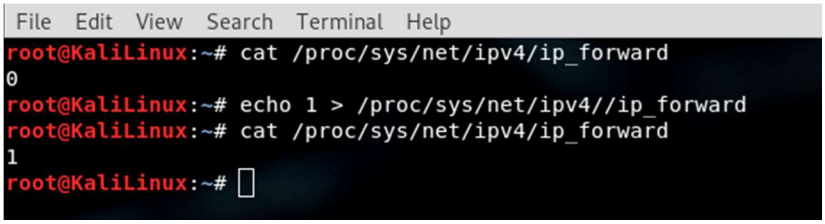


Figure 4.11 IP Forward before and after

Note: this test case was not focused on browser based MITM attacks.

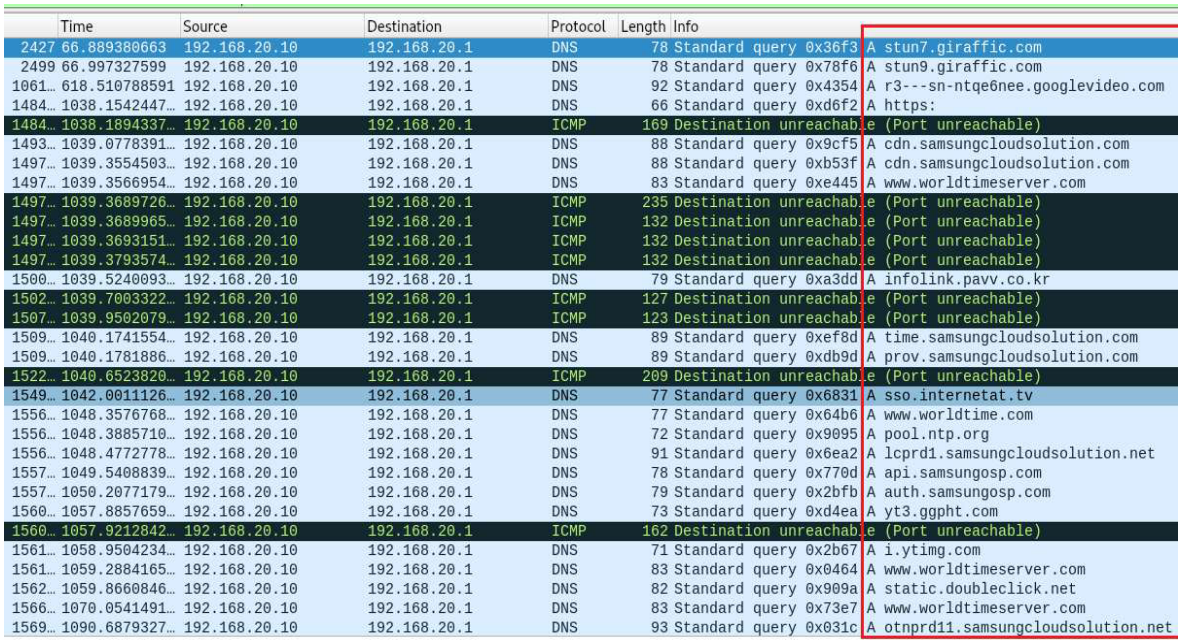
MITM attack against STV A

When the STV was first connected to the test network, it checked for DNS names and tried to resolve them from the default gateway. In this test case the STV A allocated IP 192.168.20.10 from the DHCP and the default gateway IP was 192.168.20.1. The other important factor is that this was the first time that the test STV is connected to the test environment. Figure 4.12 shows captured DNS requests that were generated from IP 192.168.20.10 .

The test result shows that the STV needed to connect with several servers. The user did not setup any relevant account or configure any application. The Table 4.4 shows the facts found in regard to the above captured DNS record and the main purpose of connecting to the STV.

The infolink.pavv.co.kr, internetat.tv are domains that are owned by Samsung Electronics and it is not clear the kind of data that these two domains collect from the STV. Both download TCP and upload traffic are strongly encrypted and hard to crack.

The yt3.ggpht.com url, has most Pi-hole users mentioning as malware though it belongs to Google. (Pi-hole is a product that is used by smart device users to stop unnecessary traffic such as from advertisements and data collection from the users. I will discuss this product in the next chapter). ytimg.com is a support site for YouTube to host thumbnails.



	Time	Source	Destination	Protocol	Length	Info
2427	66.889380663	192.168.20.10	192.168.20.1	DNS	78	Standard query 0x36f3 A stun7.giraffic.com
2499	66.997327599	192.168.20.10	192.168.20.1	DNS	78	Standard query 0x78f6 A stun9.giraffic.com
1061…	618.510788591	192.168.20.10	192.168.20.1	DNS	92	Standard query 0x4354 A r3---sn-ntqe6nee.googlevideo.com
1484…	1038.1542447…	192.168.20.10	192.168.20.1	DNS	66	Standard query 0xd6f2 A https:
1484…	1038.1894337…	192.168.20.10	192.168.20.1	ICMP	169	Destination unreachable (Port unreachable)
1493…	1039.0778391…	192.168.20.10	192.168.20.1	DNS	88	Standard query 0x9cf5 A cdn.samsungcloudsolution.com
1497…	1039.3554503…	192.168.20.10	192.168.20.1	DNS	88	Standard query 0xb53f A cdn.samsungcloudsolution.com
1497…	1039.3566954…	192.168.20.10	192.168.20.1	DNS	83	Standard query 0xe445 A www.worldtimeserver.com
1497…	1039.3689726…	192.168.20.10	192.168.20.1	ICMP	235	Destination unreachable (Port unreachable)
1497…	1039.3689965…	192.168.20.10	192.168.20.1	ICMP	132	Destination unreachable (Port unreachable)
1497…	1039.3693151…	192.168.20.10	192.168.20.1	ICMP	132	Destination unreachable (Port unreachable)
1497…	1039.3793574…	192.168.20.10	192.168.20.1	ICMP	132	Destination unreachable (Port unreachable)
1500…	1039.5240093…	192.168.20.10	192.168.20.1	DNS	79	Standard query 0xa3dd A infolink.pavv.co.kr
1502…	1039.7003322…	192.168.20.10	192.168.20.1	ICMP	127	Destination unreachable (Port unreachable)
1507…	1039.9502079…	192.168.20.10	192.168.20.1	ICMP	123	Destination unreachable (Port unreachable)
1509…	1040.1741554…	192.168.20.10	192.168.20.1	DNS	89	Standard query 0xef8d A time.samsungcloudsolution.com
1509…	1040.1781886…	192.168.20.10	192.168.20.1	DNS	89	Standard query 0xdb9d A prov.samsungcloudsolution.com
1522…	1040.6523820…	192.168.20.10	192.168.20.1	ICMP	209	Destination unreachable (Port unreachable)
1549…	1042.0011126…	192.168.20.10	192.168.20.1	DNS	77	Standard query 0x6831 A sso.internetat.tv
1556…	1048.3576768…	192.168.20.10	192.168.20.1	DNS	77	Standard query 0x64b6 A www.worldtime.com
1556…	1048.3885710…	192.168.20.10	192.168.20.1	DNS	72	Standard query 0x9095 A pool.ntp.org
1556…	1048.4772778…	192.168.20.10	192.168.20.1	DNS	91	Standard query 0x6ea2 A lcprd1.samsungcloudsolution.net
1557…	1049.5408839…	192.168.20.10	192.168.20.1	DNS	78	Standard query 0x770d A api.samsungosp.com
1557…	1050.2077179…	192.168.20.10	192.168.20.1	DNS	79	Standard query 0x2bfb A auth.samsungosp.com
1560…	1057.8857659…	192.168.20.10	192.168.20.1	DNS	73	Standard query 0xd4ea A yt3.ggpht.com
1560…	1057.9212842…	192.168.20.10	192.168.20.1	ICMP	162	Destination unreachable (Port unreachable)
1561…	1058.9504234…	192.168.20.10	192.168.20.1	DNS	71	Standard query 0x2b67 A i.ytimg.com
1561…	1059.2884165…	192.168.20.10	192.168.20.1	DNS	83	Standard query 0x0464 A www.worldtimeserver.com
1562…	1059.8660846…	192.168.20.10	192.168.20.1	DNS	82	Standard query 0x909a A static.doubleclick.net
1566…	1070.0541491…	192.168.20.10	192.168.20.1	DNS	83	Standard query 0x73e7 A www.worldtimeserver.com
1569…	1090.6879327…	192.168.20.10	192.168.20.1	DNS	93	Standard query 0x031c A otnprd11.samsungcloudsolution.net

Figure 4.12 DNS requests generated from STV A when connected to test environment

Table 4.4 Companies that owned DNS names and relation to STVs

DNS	Company	Related to STV	Country of Origin
stun7.giraffic.com	Giraffic	Adaptive Video acceleration	Israel
ntqe6nee.googlevideo.com	Google	Advertising and Video	US
samsungcloudsolution.com	Samsung Electronics	Electronics, Apps and firmware update	S.Korea

www.worldtimeserver.com	World time server	STV time, Apps time	US
infolink.pavv.co.kr	Samsung Electronics	Not clear	S.Korea
internetat.tv	Samsung Electronics	Not clear	S.Korea
pool.ntp.org	NTP Organization	stv Time	
yt3.ggpht.com	Google LLC	Domain management security, Data science	US
i.ytimg.com	Youtube	Image and Video service	US
static.doubleclick.net	Google	Data analytics, marketing	US
fe.api.amazonvideo.com	Amazon	Video streaming	US
device-metrics-us.amazon.com	Amazon	Video streaming, Advertisement	US
yahoo.com	Yahoo	Not sure	US
facebook.com	Facebook	Social media	US

Artifacts that getting advertisements to STV A

The advertisements are one of the major incomes for all STVs. By using the MITM attack it is easy to capture what kind of advertisements that STVs get from nominated servers. Essentially, this may not harm privacy, however it can expose user behaviour to unauthorized people, and can predict what users watch on STVs. Importantly these advertisement request traffic are not encrypted (Figures 4.13, 4.14).

```
GET /d/2$pgAwYzFbBLYqFMSt8EJ3f5N1v98~/ondemand/ww_syd/b5bd/5ede/955a/4e15-
b926-8603c05732b7/837115fa-149c-4f29-bd74-              _en-us_dialog_0.ism/
QualityLevels(10000000)/Fragments(video=2082080000) HTTP/1.1
User-Agent: samsungsmooth-agent/1.1
Host: avodsls3ww-s.akamaihd.net
Accept: */*
Accept-Encoding: deflate, gzip

GET /d/2$pgAwYzFbBLYqFMSt8EJ3f5N1v98~/ondemand/ww_syd/b5bd/5ede/955a/4e15-
b926-8603c05732b7/837115fa-149c-4f29-bd74-              _en-us_dialog_0.ism/
QualityLevels(192000)/Fragments(audio_EC-3_192k=2200000000) HTTP/1.1
User-Agent: samsungsmooth-agent/1.1
Host: avodsls3ww-s.akamaihd.net
Accept: */*
Accept-Encoding: deflate, gzip
```

Figure 4.13 STV A smart agent requesting advertisement from Akamaihd

```
GET /d/2$x9sQEQS9tpPKipxQLyi17rM7NHc~/ww_syd/92f0/14ff/9029/4ae8-804d-0b5dc845ffac/
47af81d9-aadb-4d48-b69a-              _en-us_dialog_0.ism/QualityLevels(10000000)/
Fragments(video=580000000) HTTP/1.1
User-Agent: samsungsmooth-agent/1.1
Host: m-6118s3.ll.smooth.row.aiv-cdn.net
Accept: */*
Accept-Encoding: deflate, gzip

GET /d/2$x9sQEQS9tpPKipxQLyi17rM7NHc~/ww_syd/92f0/14ff/9029/4ae8-804d-0b5dc845ffac/
47af81d9-aadb-4d48-b69a-              _en-us_dialog_0.ism/QualityLevels(192000)/
Fragments(audio_EC-3_192k=580160000) HTTP/1.1
User-Agent: samsungsmooth-agent/1.1
Host: m-6118s3.ll.smooth.row.aiv-cdn.net
Accept: */*
Accept-Encoding: deflate, gzip
```

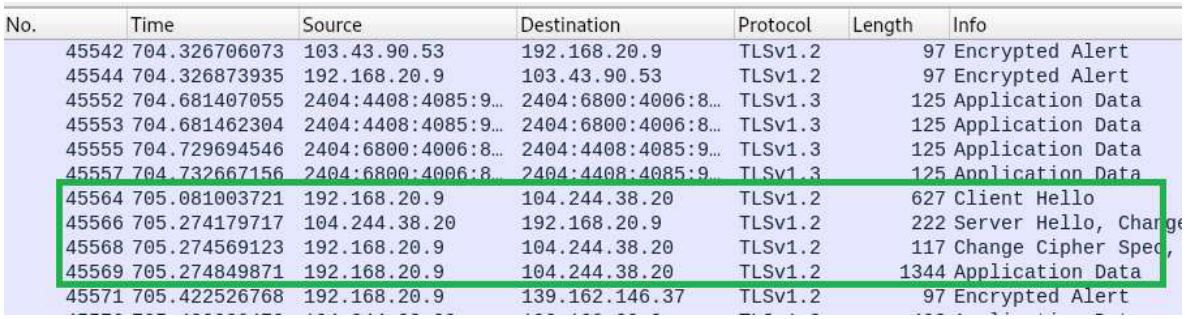
Figure 4.14 STV A agent is requesting advertisement from Amazon (Aiv-cdn.net)

Certificate cypher exchange in STV A

After seeing that all the main communications are encrypted and secure, attackers try to steal the cypher details of the certificate to decrypt encryption details illicitly. This can be done by making a self-signed fake certificate and passing it via a proxy server. However, while doing this attack I realized that cypher details are pre-installed in the STV. The Wireshark traffic confirmed it by not capturing the server handshake packets. This can happen in two possible scenarios where either Wireshark has technical issues or the server handshake does not happen. In this circumstance it cannot be a bug or a technical issue of Wireshark as it had traced other server handshake traffic. Therefore, the only possible explanation is that the STV has pre-installed root certificate(s) for some vendor(s).

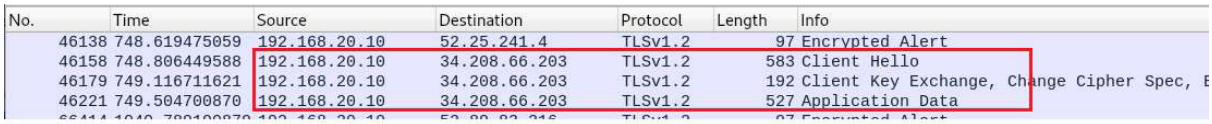
This can be confirmed by the fact that when a client says hello, without the server's response the client gets the encrypted details.

The following figures show how Wireshark normally captures a three-way handshake and the cypher exchange traffic from the STV.



No.	Time	Source	Destination	Protocol	Length	Info
45542	704.326706073	103.43.90.53	192.168.20.9	TLSv1.2	97	Encrypted Alert
45544	704.326873935	192.168.20.9	103.43.90.53	TLSv1.2	97	Encrypted Alert
45552	704.681407055	2404:4408:4085:9…	2404:6800:4006:8…	TLSv1.3	125	Application Data
45553	704.681462304	2404:4408:4085:9…	2404:6800:4006:8…	TLSv1.3	125	Application Data
45555	704.729694546	2404:6800:4006:8…	2404:4408:4085:9…	TLSv1.3	125	Application Data
45557	704.732667156	2404:6800:4006:8…	2404:4408:4085:9…	TLSv1.3	125	Application Data
45564	705.081003721	192.168.20.9	104.244.38.20	TLSv1.2	627	Client Hello
45566	705.274179717	104.244.38.20	192.168.20.9	TLSv1.2	222	Server Hello, Change
45568	705.274569123	192.168.20.9	104.244.38.20	TLSv1.2	117	Change Cipher Spec,
45569	705.274849871	192.168.20.9	104.244.38.20	TLSv1.2	1344	Application Data
45571	705.422526768	192.168.20.9	139.162.146.37	TLSv1.2	97	Encrypted Alert

Figure 4.15 Normal three-way handshake captured packets shown in Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
46138	748.619475059	192.168.20.10	52.25.241.4	TLSv1.2	97	Encrypted Alert
46158	748.806449588	192.168.20.10	34.208.66.203	TLSv1.2	583	Client Hello
46179	749.116711621	192.168.20.10	34.208.66.203	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, E
46221	749.504700870	192.168.20.10	34.208.66.203	TLSv1.2	527	Application Data

Figure 4.16 Cypher exchange on STV captured packets shown in Wireshark

The IP address shown in Figure 4.15 belongs to Amazon according to the WHO IS IP lookup tool. This evidence explains why it generated DNS requests for Amazon servers when the STV is attached to the network.

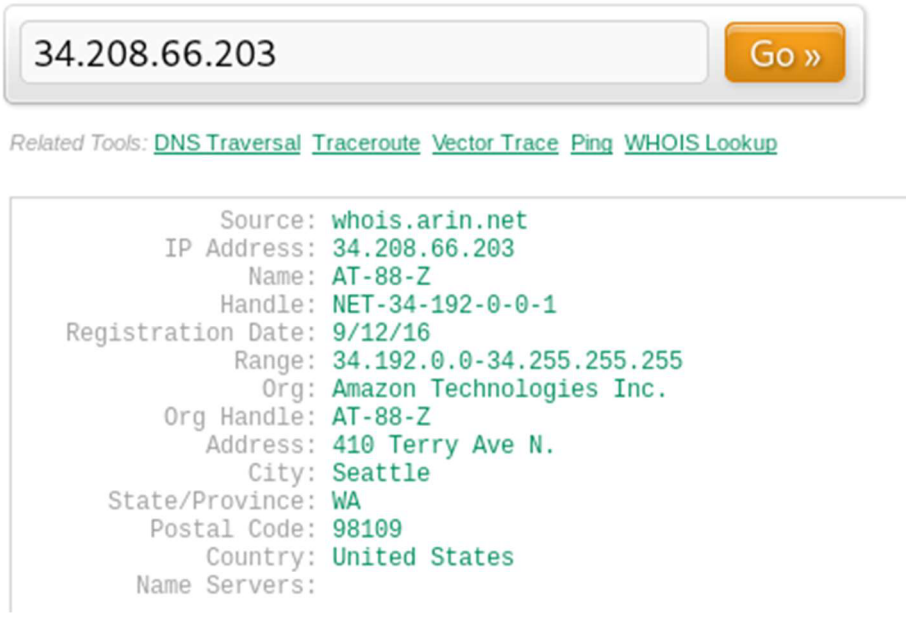


Figure 4.17 34.208.66.203 who is this

In contrast Netflix does not have this mechanism as it is relatively a new application for STVs. From a security point of view this is security hardening to restrict unauthorized data or information access by hackers. However, there are few drawbacks in security hardening and to be discussed in the Chapter 5.

Note: The following graph shows the data packet errors while the MiTM attack is in place against the Samsung TV. This is because the STV A generates a high traffic volume to the destination servers that wireshark cannot captured.

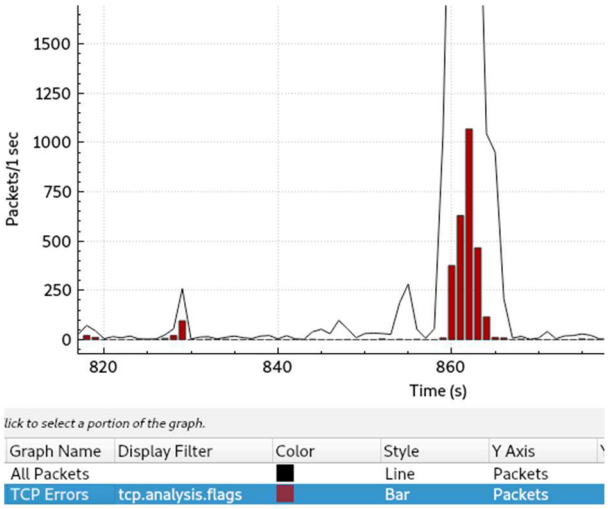


Figure 4.18 shows the error packets on STV A

MITM attack against STV B

The same procedure is followed against the STV B to execute an MITM attack. Initially I reset the factory settings of the STV and connected to the test environment to get the IP (In this test the STV B got IP 192.168.20.8) address from the DHCP. The following table shows the DNS names that Wireshark captured from STV B that are requested from the default gateway as soon as it was switched on.

Table 4.5 Companies that owned DNS names and relationship to STV B

DNS	Company	Related to STV	Country of Origin
lgtvcommon.com	LG Electronics Inc	Not Clear	S.Korea
lgsmartad.com	LG Electronics Inc	Advertisement	S.Korea
mediaservices.cdn-apple.com	Apple Inc	Content Delivery and Certificate authentication	USA
lge.com	LG Electronics Inc	LG App	S.Korea
www.google.com	google LLC	search engine	USA
AU.lgtvsdp.com	LG Electronics Inc	Certificate Authentications	S.Korea
NZ.lgrecommends.lgappstv.com	LG Electronics Inc	STV App	S.Korea
LG-TV-1.prod.partner.netflix.net	Netflix, Inc.	Video streaming	USA
www.ueiwsp.com	PERFECT PRIVACY, LLC	Not Clear	USA

Compared to STV A, STV B initial DNS requests are low and it does not have unclear DNS requests except for ueiwsp.com. This can happen as server keeps an agreed privacy agreement record of details of the LG Company and the end user.

Figure 4.19 Encrypted data communication between STV B and its servers.

Certificate cypher exchange in STV B

Same as the STV A, STV B did not get the Server acknowledgement (Server Hello) message from the certificate server and STV B must also have pre-installed certificate(s). The figure 4.18 shows the SSL traffic that Wireshark captured for the STV B.

When analysing SSL traffic packets I can see some readable data in the encrypted communication. First the STV B generated traffic for the AJ7.lgtvsdp.com site and returned with certificate details and cipher details (Figure 4.18). To decrypt the data packets a MITM attacker needs the master cipher details. However, those details cannot be obtained from the STV without physical contact or installing a remote access agent.

No.	Time	Source	Destination	Protocol	Length	Info
1168	23.723054454	192.168.20.8	52.78.30.154	TLSv1.2	583	Client Hello
1179	24.004508386	192.168.20.8	52.78.30.154	TLSv1.2	192	Client Key Exchange, Change Cipher Spec,
1195	24.278472058	192.168.20.8	52.78.30.154	TLSv1.2	1401	Application Data
1210	24.602251821	192.168.20.8	52.78.30.154	TLSv1.2	97	Encrypted Alert
1305	25.153244709	192.168.20.8	52.78.30.154	TLSv1.2	583	Client Hello
1312	25.431230205	192.168.20.8	52.78.30.154	TLSv1.2	192	Client Key Exchange, Change Cipher Spec,
1317	25.685525098	192.168.20.8	52.78.30.154	TLSv1.2	1079	Application Data
1475	26.261798779	192.168.20.8	52.78.30.154	TLSv1.2	97	Encrypted Alert

Figure 4.20 SSL Traffic in STV B

Note: The following graph shows the data packet errors while the MiTM attack is in place against the LG TV. This can be because the STV B generates high traffic to the destination servers that wireshark cannot capture.

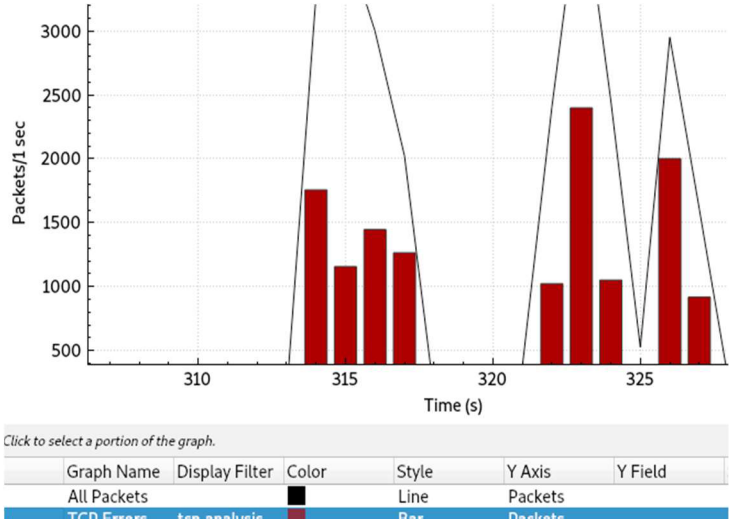


Figure 4.21 The error packets on STV B

4.4.3 Test Case T003

Social engineering via web advertising is a less conditioned area for study. Most of the web advertisements are based on user behaviour on webpages and they will pop up on smart device applications, SMS and more rarely, voice calls.

The goal of this test case is to monitor STV viewer behaviour via adverts on connected devices in the same network. For example, if someone watches Money Heist series on STV Netflix, what other do users see in their advertising pop ups. Ultimately it took 3 weeks to get an idea about what users watch on the STV such as the kind of programs, interests and searches. This test case used a mobile phone and an extra connected laptop device in the test network without further modification.

Social engineering when watching STV B.

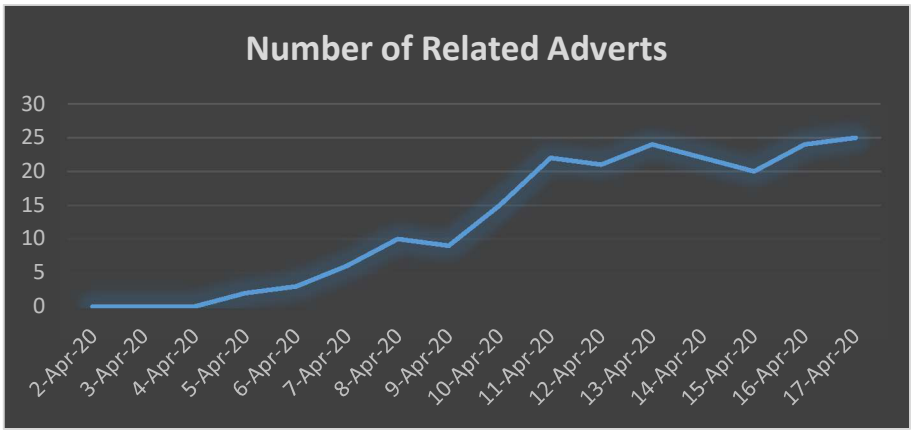
To test the STV B social engineering, I searched higher study programs in New Zealand using the Google search engine and YouTube. The user has searched various programs at different universities

such as Fashion designing programs in AUT, Marketing management at Auckland University and some other tertiary related educational programs through the search engine.

During the first three days did not show any adverts that were related to what the user has searched on the STV B. However, from the beginning of the 4th day it gradually started showing up related adverts on the monitored computer and on the YouTube stream. Initially it was irregular and popped advertisement related to online marketing programs and fashion websites. The monitored computer (Social engineering computer) was not used to search anything rather than to play YouTube with default settings.

Following Table 4.6 shows how advertisements showed up on STV B during the 15 days period.

Table 4.6 Trending of adverts showed on monitored computer that related to what user watched in STV B



As shown on the trending graph when the user searched more about a specific area such as education, more adverts started to show up in the monitored computer. Moreover, some related adverts showed up in the attached mobile phone as well. Figure 4.22 shows the advertisements that showed on an application installed in Samsung J phone.

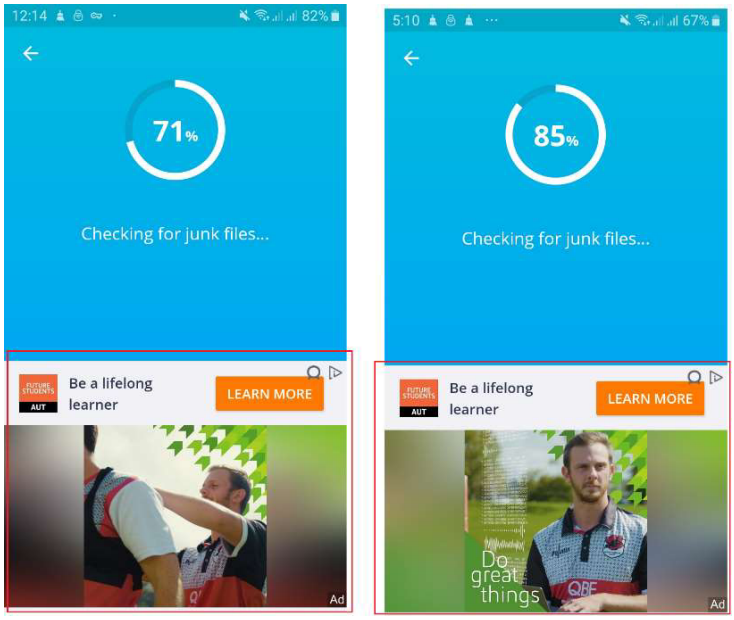


Figure 4.22 AUT adverts shown on a mobile app after user started to search education programs on STV B

Social Engineering when watching STV A.

The user has watched Money Heist, House of Cards and Sense 8 via Netflix on the STV A. In addition, the user watched the TV series Jack Ryan on Prime video. The user continuously watched these TV series almost every day on STV that is attached to the test network.

When compare with STV B, advertisements started to show up fast and aggressively in the Samsung monitored system. During the first 2 days normal advertisements on YouTube appeared. However, soon after it started showing specific adverts that related to what the user watched on the STV. For example, YouTube started showing VPN related products in advertising influencing the user that they can watch US Netflix programs via VPN.

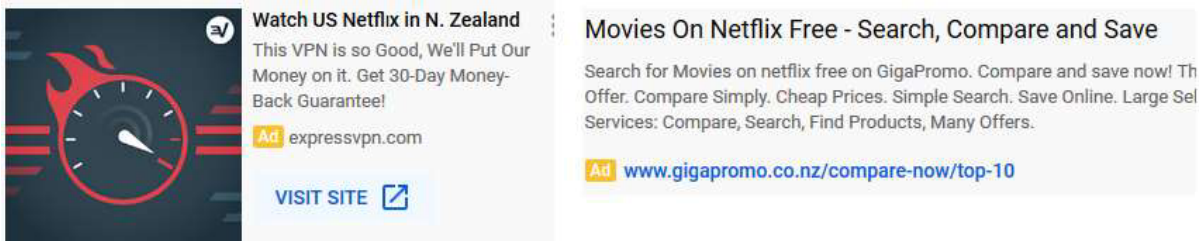
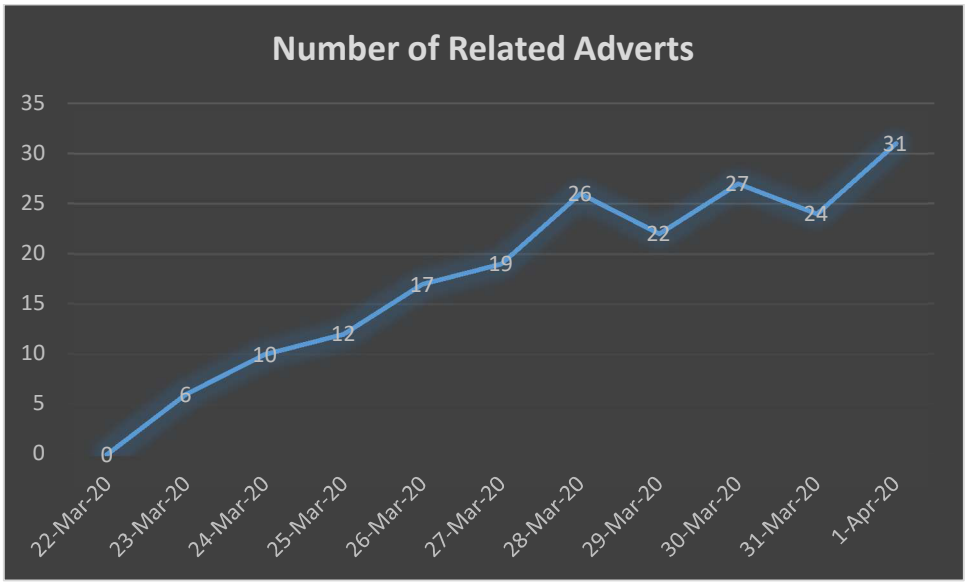


Figure 4.23 The monitoring computer shows adverts that relates to what user watched on STV

The following trending graph shows related advertising on the monitoring computer within the test time frame.

Table 4.7 Number of adverts showed on the monitored computer in relation to what the user watched on the STV A



The user has watched Money Heist TV series on STV A via Netflix. After watching the series, advertising in several categories started showing on the monitored computer. Such as a PlayStation video game that is related to Money Heist and related TV series such as Breaking Bad, Narcos. Apart from these categories, some advertising were related to “Money” (Western Union money transfer). This was supporting evidence that the STV Viewer has watched something that is approximately related to Money.

On analysing this, it is hard to come to a conclusion that user has watched exactly the same movie, yet an attacker can get an idea about what the user is interested in watching, and what he/she watched on the STV in that time period. However, to some extent the test results showed that an external user can monitor what the STV user watches on TV without using any special tools or knowledge.

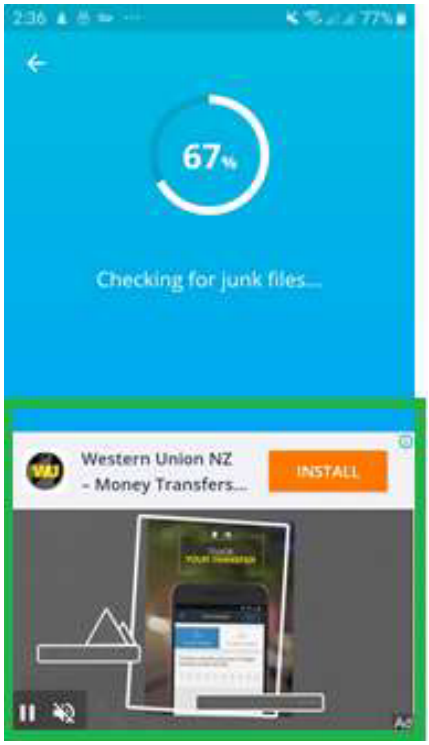


Figure 4.24 Adverts showing on the connected Smartphone and showing Western union money transfer advertisement when the STV user watched Money heist

Overall, the test case results demonstrated that user behaviour on STVs can be reflected on the attached home network and influence other users with similar kinds of products. However, this process can also be used by the attacker for social engineering about what user watches on STV and collect the artifacts to prepare a cyber-attack or breach of security, or in the worst case scenario harm someone who lives in the house. When compared with other monitoring tools used in cyber-attacks, social engineering is relatively easy to carry out as STV collected data also influences other users in the STV attached network.

This can be a serious privacy issue especially for people who use the Internet on STVs to search on privacy sensitive topics, such as mental health issues.

4.4.4 Test Case T004

The test case T004 is concentrated on obtaining the root access to the STV without a physical connection. That is to gain the root access remotely. The root is a super user in Linux systems who

has the access to all the files in Linux based systems. Consequently, if an attacker can gain the root access, they can do any task they want within the system. Normally some IoT devices enable root access by default due to several reasons, such as for user support, for configurations, or it may temporarily enable the root access for firmware update.

This test case has used telnet as some IoT devices still come to the market with enabled telnet (Gamache, 2016) . By getting the grant to access the root, the attacker can get into the local file system such as stored cookies and many more options. Normally telnet has default ports, and 22 and 23 are the main ports.

STV B remote attack to acquire root access.

To enable this attack, it followed the same procedure that is used in the test case T002, as it is convenient to find the open ports and IP address of the targeted device. The following Figure 4.25shows that telnet services are not enabled in the targeted device.

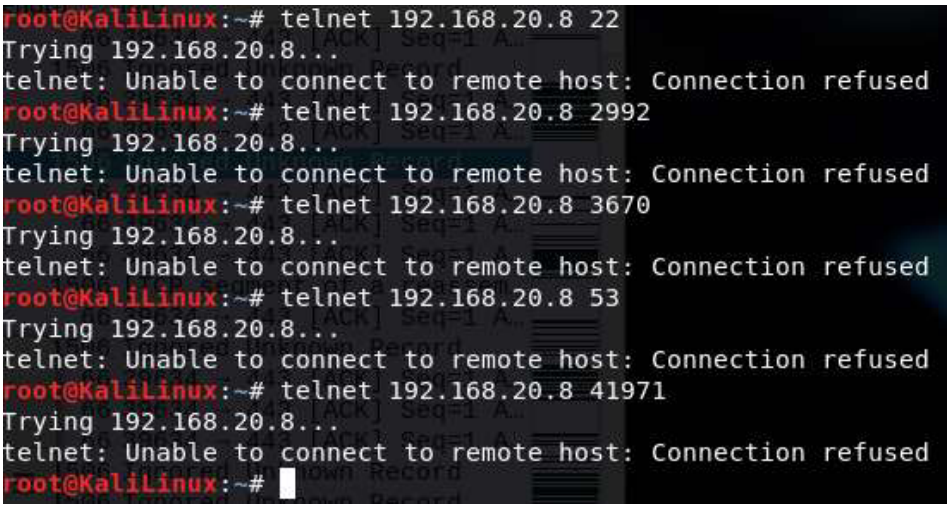


Figure 4.25 Telnet services are disabled in the targeted device (STV B)

However, it is beneficial to check whether the Netcat service is installed or running in the STV B. The following figure shows that the destination target refused to connect.

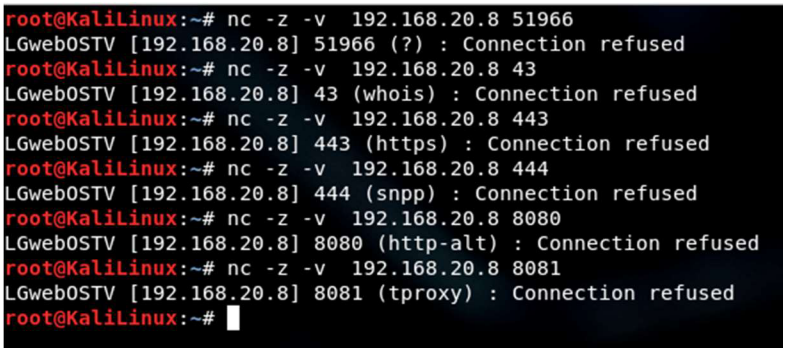


Figure 4.26 Netcat services are not responded

Note: While testing and researching about the root accessing of STV B I found that a jailbreaking program can allow hackers to get access to the root. This is called GetMeIn. However, to get the root access needs physical access to the STV and it needs to run several commands on the STV (Athul, 2019). This research project does not intend to report the outcomes and the findings of these methods. However, future research can include these investigation actions on STVs.

4.5 ANALYSIS

Compared to the literature review, current STV manufacturers strongly show counter measures for the data communication between STVs, and the vulnerabilities in the STV systems. However, the test results illustrate that STVs are disclosing user behaviour to the outer world without any hesitation and this can cause problems with privacy issues via social engineering. In addition, the test case T002 showed that some applications have pre-installed certificate details and this can cause privacy issues or STV functionality issues in the future. However, the MITM attacks failed to acquire the data that is sent out from the STV.

Overall test results showed some improvements of the STV security, specifically about the data communication between STV ports and nominated server. However, users still need to be vigilant about what data that STVs collect and send out for marketing purposes, and take necessary counter measures to prevent the data being sent out.

4.6 CONCLUSION

Chapter 4 reports the results of the experimental test cases for STV privacy issues and the ways that STVs react against the chosen attacks. Furthermore, it described how STVs can be used in social engineering and monitoring of user behaviour. The test cases are built to cover how an attacker can engage with STVs to breach the privacy of home viewers, such as gathering information for social engineering. This identifies the user behaviour and also by performing DoS attacks to get physical access to a STV (this can be either physical, or by giving misleading information to users to do alternatives on STVs to open backdoors for hackers). Chapter 5 will discuss these findings in relation to the literature, and examine the research question and sub questions for answers.

Chapter 5

Discussion of Findings

5.0 INTRODUCTION

Chapter 2 has shown several privacy issues that are caused by a lack of security enforcement, and security practices for STVs. In addition, Section 2.3 analyzed three major STV manufacturers' privacy policies and related law suits that consumers and governments claimed against STV manufacturers and support businesses. In Section 2.4 privacy issues and several attack models that can compromise the privacy of the STV users, were reviewed. In Section 3.1 several studies conducted by other researchers on STV privacy issues and vulnerabilities were analyzed. These similar studies helped in building the research methodology in order to find answers to the research questions. Furthermore, by reviewing previous studies of STV privacy issues the right tools to use to do the practical research were identified. Chapter 4 presented the findings of each test case that was conducted according to the research methodology described in Chapter 3. The purpose of Chapter 4 is to implement the test cases and present the research findings and screen shot evidence. Section 4.1 also described the variations required to make the testing work in practice.

The objective of chapter 5 is to discuss the findings of Chapter 4 according to the expected results found in the Chapter 2 literature review. Chapter 5 contains 3 sections. The section 5.1 will focus on evaluating the sub questions. The sub questions are SQ1 "*What data and information that STVs send out and to where*?", SQ2 "*What are the security mechanisms that is used in STVs to protect data*?" and SQ3 "*How does the upcoming NZ privacy bill will help protect STV consumers?*". The following Section 5.2 will address the following hypotheses H1 "*Every penetration testing tool that used to attack STVs will succeed every time. However, these commonly used and well-established penetration testing tools will be expected to work without any errors in all recommended environments*", H2 "*When executing attacks against STVs it is expected that attackers might already*

be in the network or have neutralized the network security enforcement in the particular network." and H3 "*When it comes to network packet capture tools it is expected those tools will perform well under a high level of network stress without any errors*.". The main research question is answered in the Section 5.3 and the Section 5.4 discusses the findings and the privacy issues of STVs which were outlined in the Chapter 2 literature review. Finally, Section 5.5 will conclude the chapter.

5.1 SUB QUESTIONS

This section evaluates and answers three sub questions that were developed in Section 3.2.2. These sub questions are generated to help answer the main research question. Subsequently these questions were identified and generated by evaluating various literatures in Chapter 2. Section 2.4 discussed the privacy issues with STVs.

5.1.1 Sub Question 1

SQ1: What data and information do STVs send out and to where?

Evidence and Discussion:

This sub question is designed to get an idea about to where do STVs send out the data about users' viewing habits and in what format, plus whether they are encrypted. The Figure 4.11 shows DNS requests to various servers to establish the connection with the STV. When connected to the network with default factory settings, many irrelevant DNS requests were generated in both the tested STVs (There are no previous user activity records on STVs after resetting the factory settings, according to the manufacturers). Some of the DNS requests are fundamentally needed such as manufacturer servers to install any system patches or upgrade STVs operating system patches. However, it is not clear why STVs need to connect to some companies that are directly involved in collecting user data for marketing purposes. The table 4.4 shows several DNS requests that the STV A generates and are directly involved in user data collection for marketing purposes (eg. Amazon, and Google). The Table 4.5 shows STV B requested DNS records from the default gateway in the test network.

However, the MITM attacks could not capture what data were sent out from both the test STVs, as all outward data packets are heavily encrypted and cannot be decrypt. In contrast I can read data packet headings as shown in Figure 4.19. There is no clear evidence that both STVs have sent out user behaviour data to anyone. However, Test case T003 findings suggest the advertisers have specific information for advertising targeting. The reason is only the test STVs were used to search a topic and they have sent out details of what the user had searched in the Internet. Therefore, this is likely the reason for related adverts popping up on the smart phone applications and the monitored computer in the test network.

To conclude, the answer to this sub question, there are no specific evidence that STVs send out user behaviour as the data cannot be decrypted. However, the supporting evidence from the social engineering test case and initial DNS request evidence, that STVs send out details about what user do on STVs and attached network devices detail.

5.1.2 Sub Question 2

SQ2: What are the security mechanisms that is used in STVs to protect data?

Evidence and Discussion:

Sub question number 2 is designed to address the kind of security mechanisms that are implemented in tested STVs to protect the privacy of STV consumers. Hypothetically when comparing STVs in the market a few years back, current STVs have improved their security mechanisms. Chapter 2 discussed several research reports that easily compromised the STVs communication data and data stored inside by getting the root access. However, it has changed today. The test case T0001 showed both STVs worked perfectly while a DoS attack took place against the STVs. The Figure 4.6 and Figure 4.7 demonstrate how DoS attacks are taking place and Tables 4.2 and 4.3 show the test result of the attack. Equally this might not seriously affect user privacy however it can open a door to other attacks with social engineering, such as stopping STV functionality by DoS attacks and opening physical access to install malware in the STV by covering up as a STV technician to fix a problem.

Secondly both tested STVs have encrypted their apps and data communications between the STV and servers. The Figure 4.19 shows how data are encrypted in the STV B while it communicates its servers. Moreover, cypher details of some applications are pre-installed and a STV never asks certificate details from the servers. This was proved by capturing the three-way handshake communication data via Wireshark (see the Figure 4.15, and Figure 4.16).

Thirdly in any system if someone can get the root access then, basically he/she can do anything in the system. Therefore, test case T004 is designed to get the access to the root directly and remotely. As showing in Figure 4.22 telnet services are disabled in both the tested STVs which prevented gaining root access. In the literature review, researchers claimed some STVs have pre-installed Netcat services for remote assistance which opens a backdoor to hackers to get in to the STV remotely. However, in this case both STVs showed that there are no Netcat services installed.

To conclude the answer for this sub question both Samsung and STV B have now applied a considerable amount of security enforcements to protect the data communication between the STV and the servers. Moreover, by disabling the default root access gates tested STV manufacturers succeeded in preventing the attackers gaining root access remotely. The pre-installed cypher details is a good practice as it prevents the compromising of cypher details to third-parties. However, this can lead to other problems of STV functionality or may cause data breaches similar to the Sony game station.

5.1.3 Sub Question 3

SQ3: How does the upcoming NZ privacy bill help protect STV consumers?

Evidence and Discussion:

Section 2.2.4 discussed the upcoming New Zealand Privacy bill and the reasons to include it as a sub question. This is the right time for the New Zealand government to consider changing the law to enforcement against data collection companies that are located off shore. The Section 4.3.3 clearly shows how aggressively the advertising started to show up on the attached mobile phone and the

monitored computer of the test network when STV A is switched on. In the test environment only the search function is operated on a STV and there is no way that specific advertising popup on the mobile phone and the monitored computer without targeting. Therefore, this is evidence that STVs collect data from the devices that are on the paired network and collect details about user viewing habits as well. The concern is what happens if there is a privacy breach in offshore data collection servers or if a harmful thing happens to the STV users as exemplified in chapter 2. The New Zealand government has addressed that issue under the new privacy bill by introducing a new Information Privacy Principle to control off shore agencies who collect consumer information (Privacy Bill update – April 2020, 2020).

In contrast it is a tedious task (practically impossible to be done remotely) to breach data communications between the STVs and the servers. Therefore, if the government needs to interfere in the communication for a criminal investigation, the law enforcement agencies could not do it. To cover these kinds of scenarios the government has two options, either manufacturers need to give cypher details to NZ government that are especially deployed to New Zealand STVs or order STV manufacturers to provide the necessary details that government agencies need when they require access. However, in the new privacy Bill the New Zealand government selected the second option, making the impact quite low compared to privacy bills of other countries. The justice.govt.nz website states the maximum penalty is $10,000 which is small fine for big companies and little disincentive to collect data for marketing purposes (Key initiatives Privacy, 2020).

To conclude the answer for this sub question, the upcoming New Zealand privacy Bill covers offshore agencies who collect personal information to some extent. However, the maximum penalty should be more than $10,000, like the GDPR or the Australian privacy Act.

5.2 HYPOTHESIS TESTING

Research hypotheses were generated through the assessment of the research sub questions that are stated in Section 3.2.2. These hypotheses are derived by reviewing the various literature in Chapter

2. In Section 2.4 discussed the privacy issues of STVs and gave rise to the hypothesis. The following three sections evaluate the hypotheses based on the results of Chapter 4.

5.2.1 Hypothesis H1

H1: *Every penetration testing tool that is used to attack STVs will not succeed every time. However, these commonly used and well-established penetration testing tools will be expected to work without any errors in all recommended environments.*

Argument For	Argument Against
Wireshark was able to capture network traffic from the STV in the default gateway in the tested network. It shows the basic details about where the data packets are sent to. Ettercap successfully re-routed the data packet to the attacking computer for sniffing.	
Conclusion justification	
This hypothesis is true as all tools worked correctly as per the research expectation of each test case. See two figures (Figure 4.14 and Figure 4.15) and comparison in Section 4.4.2	

5.2.2 Hypothesis H2

H2: *When executing attacks against STVs it is expected that attackers might already be in the network or else neutralize the network security enforcement of the STV*

Argument For	Argument Against

Data Security depends on how hard it is to breach it with various types of methods and tools. Therefore, one system cannot depend on another when it comes to data security matters. The reason is when a main system breach or exposure of security holes happens then the rest of the systems are automatically expose to attackers. Therefore, considerable and meaningful security reinforcements to individual systems are required. In this case STVs should have their own security mechanisms for data communication and stored data protection.	Various security measurements and reinforcement hardware and software are available in today's market. Therefore, attackers should get into the home network first and then breach the security barriers in STVs.
Conclusion and Justification	
This hypothesis is true as both tested STVs have their own security mechanisms for data communications and to protect stored data inside STVs. Section 4.3.1 and 4.3.4 showed that when an attacker gets access to the network that a STV is connected, they cannot get into the STV storage or grab important data from its data communications. However, it is possible to get access if the attacker can get physical access to the STV and install jailbreak software which is not covered in this research. Moreover Section 4.3.2 shows that an attacker cannot interfere to get cipher details even when they get access to the STV attached network.	

5.2.3 Hypothesis H3

H3: *When it comes to network packet capture tools it is expected they will perform well under a high level of network stress without any errors.*

Argument For	Argument Against
Ettercap redirected the traffic to the research computer and without any disturbance both STVs functions well without buffering.	Both STVs generated high traffic to the router in a short period of time. Therefore, Wireshark may lose some data packets while a MITM attack takes place.
Conclusion and Justification	
This hypothesis is false. The reason is both the pcap files captured from A and B STVs during the MITM attack show a considerable amount of TCP packet errors in that time (see Figure 4.18 and Figure 4.21 both show TCP data packet errors). This is the only explanation that can be given for this scenario as both the STVs generated huge traffic to the destination servers that Wireshark cannot capture in that time period. Therefore, as a network data capturing tool Wireshark did not performed well against the STV data traffic.	

5.3 THE RESEARCH QUESTION

This goal of this section is to address the main research question: *what are the active and passive privacy issues in current STVs*. The primary aim of this research is to examine how actual privacy issues can occur, either by on premises by cyber-attacks or by collecting data about what users watch on STVs. A few years back STVs did not have security enforcements compared to present, and so the findings of this research are an update of the previous knowledge.

Section 5.1 answers the sub questions according to the findings of Chapter 4 that are evaluated to support the research main question in Section 3.2.2. From that section it was clear that captured data communications are well encrypted, and the manufacturers consider various attack types that cyber attackers can use against STVs. Moreover, their current products are not vulnerable for the previous reported attack methods and security holes. By closing the root access for STVs, manufacturers completely shut the main gate for attackers. This is a positive improvement when compared with the old STVs.

Since STVs collect data about its user behaviour and try to influence other users in the same network, this can cause passive privacy issues for consumers. As demonstrated in Section 4.3.3, using social engineering, attackers can gain knowledge about what a user watches on the STV and can get an idea of what they search for on the STV. This may not be as harmful as compromising credit card details and yet it can cause a moderate level of privacy issues for users.

Compared to previous generations of STVs in the market, modern generation STVs have a considerable amount of security enforcement to harden against different attacking models. In contrast due to data collection these security enforcements are not adequate for protecting user privacy.

5.4 DISCUSSION

Day by day STVs acquire computer power and hence have enough power to compute complex cypher algorithms the same as smart phones or computers do. Furthermore, the open source community is actively engaged in developing related applications for growing the market and STV use. On the other hand currently government agencies try to keep an eye on the latest STV products that collect their citizens' personal information for marketing purposes. Therefore, pressure on STV manufacturers to improve the security of STVs is effective.

This research has demonstrated that interfering with the data communication and decrypting the data packets remotely are nearly impossible. However, the STV A can be rooted and can get access to the root directories by using SamyGo firmware which was developed by an open source

group (Welcome to SamyGO Wiki, 2018). Essentially to use SamyGo attacker needs to have physical access to the STV and to downgrade the firmware according to the TV series that Samygo supports. This method is not demonstrated in this research as a test case as it needs physical access. However, this is an effective method for digital forensic investigators to fetch the data from STVs. Equivalently STV B's have a similar kind of product called GetMeIn (Athul, 2019). To gain the root access it needs physical access to the STV and has to run commands on the STV. This method is jailbreaking the system.

Regarding the data collection process of the STV it is quite obvious as they influence the search and user watching behaviours, and influence other devices in the same network. This is strong evidence that STVs collect data from the devices in the same network. However, to justify a general claim requires dedicated research only to that topic. To improve the security of New Zealanders privacy the government has introduced a new privacy Act from the new privacy Bill which will come into effect from November 1st 2020.

5.5 CONCLUSION

Chapter 5 has discussed the findings presented in the chapter 4. In this chapter the sub questions have been answered. Further conclusions for all the hypotheses based on the findings in chapter 4 have been made. The main research question is also answered and has discussion. Chapter 6 will conclude this research report by expressing the limitations of the research and give counter measures to prevent social engineering on STVs. Finally, recommendations for further research will be made.

Chapter 6

Conclusion

6.0 INTRODUCTION

The main purpose of this research is to evaluate the active and passive privacy issues that exists in current STVs. Chapter 2 reviewed literature to form the research question and Section 2.5 identified privacy issues in STVs and the vulnerabilities that researchers have found in STVs. By reviewing similar studies, in Section 3.1 research method and relevant tools were identified. The methodology was designed to obtain answers for the research questions and hypothesis. The findings presented in Chapter 4 were used to evaluate the answers for sub questions, hypothesis and main research question. Section 5.3 gave the answer for the main research question.

This chapter presents the final conclusion of this research project. Section 6.1 describes the limitations of this research. Section 6.2 suggests the areas for future research based on STV privacy issues and security vulnerabilities. Section 6.3 gives the final conclusion.

6.1 LIMITATIONS

Every research project has its own limitations and, in this section, the limitations of this project are addressed. This research was focused on finding active and passive privacy issues of current STVs. Even after setting up the correct test environment particular limitations were recognised, and they are described in the following paragraphs.

WebOS from LG and Tizan OS from Samsung are the two operating systems tested for STVs in this research. However, there are many more other platforms that are available in the STV market such as Android TV, Roku, Xbox 360, and tvOS. This research did not test other vendors' operating systems, platforms and middleware. Furthermore, the other vendors may have different strategies to monitor user behaviour on STVs plus there are different versions and updates available for different platforms. That is different security vulnerabilities and privacy issues can occur depending on the

operating system and the attacking method that the attacker uses against the targeted STV. It is quite challenging to cover all the available STV platforms and the middleware due to the barriers of funding and time in this project.

At present manufacturers have introduced several modes into STVs such as game mode, hotel mode, default mode, intelligent modes, and so on. These modes have their own settings and limitations. Therefore, in this research I used only the default mode. However, some researchers have investigated security vulnerabilities in different modes such as hotel mode which allows the execution of certain Linux commands of input text on STV A's. Nowadays STV manufacturers update operating systems, patches and change upgrade versions frequently. For example, if you upgrade to a version then you cannot downgrade. Even though you downgrade, you cannot open previous vulnerabilities or security holes. While doing the research I have managed to crash the Prime video application on the STV A using a hulk python script for DoS attack. However, after the attack, the STV restarted and upgraded the version (Please see Appendix 1 for crash screen error message). After the version upgrade, the above script failed when it executed on any application on the STV A. These are all limitations imposed by the chosen scope of the research and available for further research topics.

Modern STVs have several communication ports to establish connectivity. For example, Bluetooth, infrared port, RJ45 for network, Wi-Fi and RCA connectivity. This research only focused on network connectivity based communications. To conduct security testing on other connectivity media requires a greater resource allocation and an extended time frame. This is another limitation to this research as it was not able to cover all the connectivity and vulnerabilities that could breach user privacy on STVs.

There are hundreds of tools and different kinds of penetration scripts available to test security vulnerabilities in computers and smart phones. However, selecting the proper tools and methods for STV penetration is a tedious task as the STV security area is still not popular like smart phones or computers. This is a great limitation that I came across during the research. The reason is though there are several tools available for tasks, there is little information regarding whether those tools are

capable of executing security testing in a STV related environment. Therefore, I had to test recommended tools before selecting them for the actual test. Plus, there is little trusted information about the tools' popularity, reputation and the technical help that can be expected from forums (Q&A in technical forums). Therefore, due to the limitation of the tools, testing all of the tools for specific STV security checks is not feasible in a limited time frame.

6.2 FUTURE RESEARCH

STV is new to the research topics and it has many areas for research especially when it comes to privacy issues. Therefore, in this section I would like to list areas that researchers can focus on when it comes to STV privacy issues.

The modern day STVs are not single units, they are a combination of several units and collection of several technologies, such as smart remotes (touch pad for mouse or track for mouse cursor, voice recognition remote), smart cams, keyboards, and so on. Therefore, each unit might have several privacy issues that could compromise the STV data for unauthorized access. The reason is these units are often connected to STVs via Bluetooth or infrared, consequently these connections can lead to security breaches for the STVs. For future research, these topics are unique and can help to improve the security of STVs. Modern STVs can connect to other devices via direct Wi-Fi and the STVs maintain incoming device MAC addresses in the registry for future connections. It is a known fact that MAC address can easily be spoofed and can connect a STV as a spoofed device. In addition, I used wire connectivity to the router and STV for the testing phase, hence in the future a researcher can measure how hard or easy it is to interfere the Wi-Fi data communication on STVs.

The data collection of STVs is not a new thing. In this research I have proved that collected data can influence other device users in the same network. This research is done using a home network and therefore another researcher can find the advertising behaviour and influence in other types of network. The research area is beneficial to improve and implement counter measures for STVs to stop uploading data for marketing purposes and blocking advertising as well.

Third and lastly, I would recommend further research can be undertaken on STVs forensic capabilities due to the reason that STVs are getting more common nowadays and many times people use STVs as a second screen. Therefore, if someone uses a STV as a monitor they might keep a digital footprint inside of the STV like smart phones (smart phones keep thumbnail of every picture that is downloaded or taken on your phone). Moreover, to access internal storage STVs need to jailbreak (like SamyGo, Getmein) or need to do physical extraction. If jailbreaking works, then how the evidence can be sent from the STV, and what evidences will show in EnCase will be a good research area for digital forensic researchers.

6.3 CONCLUSION

In the last five years STVs have become popular in a way similar to mobile phones and attracted manufacturers and investors of several industries. These business opportunities have driven application development for STVs, user behaviour data collection for marketing purposes, and so on. Compared to the early stages of STV use, the current generation gains enormous improvement regarding the security enhancements to protect the data communication and internal systems. These improvements are enforced due to the rules establish by governments, security research, the competitive market, and consumer awareness regarding the security of STVs. Still data collection and their influence on the same network can lead to social engineering about the user behaviour and hence create user privacy issues on STVs. Finally, the New Zealand government has improved the privacy law regarding data collection companies that are based in offshore, but needs to rethink the maximum level of penalty for breaching the privacy law.

REFERENCES

Amazon's Echo Dot Kids puts kids at risk, complaint alleges. (2019, May 9). Retrieved from CBS News: https://www.cbsnews.com/news/amazon-echo-dot-kids-privacy-violations-puts-kids-at-risk-complaint-alleges/

Amended order granting motion for preliminary approval of class action settlement [Netflix Privacy Litigation], 5:11-CV-00379EJD (United States District CourtFor the Northern District of California December 5, 2012).

Athul. (2019, Jan 15). *How To Root LG Smart TV Running WebOS.* Retrieved from www.techofweb.com: https://www.techofweb.com/google/root-lg-smart-tv.html

Automated Content Recognition creating content aware ecosystems. (2012, September). Retrieved from www.csimagazine.com: https://www.csimagazine.com/csi/whitepapers/ACR%20Creating%20%20content-aware%20ecosystems%20-Civolution%20White%20Paper%20-%20Sept%202012.pdf

Brewster, T. (2017, Mar 7). *Here's How The CIA Allegedly Hacked Samsung Smart TVs -- And How To Protect Yourself*. Retrieved from Forbes: https://www.forbes.com/sites/thomasbrewster/2017/03/07/cia-wikileaks-samsung-smart-tv-hack-security/#63f0c72c4bcd

Brookman, J. (2013, November 27). *Eroding Trust: How New Smart TV Lacks Privacy by Design and Transparency*. Retrieved from International Association of Privacy Professional: https://iapp.org/news/a/eroding-trust-how-new-smart-tv-lacks-privacy-by-design-and-transparency/

Chapple, M., Michel, J., & Gibson, D. (2018). *(ISC)² CISSP Certified Information Systems Security Professional.* Indianapolis, indiana: John Wiley & Sons.

Children's Online Privacy Protection. (2012, August 6). Retrieved from Federal Trade Commission: https://www.govinfo.gov/content/pkg/FR-2012-08-06/pdf/2012-19115.pdf

Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business. (2017, June). Retrieved from Federal Trade Commission: https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance

CIO upfront: Privacy Bill update. (2019, April 8). Retrieved from CIO New Zealand: https://www.cio.co.nz/article/659748/cio-upfront-privacy-bill-update/

Collin, M., & Michéle, B. (2012). Read it twice! a mass-storage-based TOCTTOU attack. *Proceedings of the 6th USENIX conference on Offensive Technologies*, (pp. 1-8). {Bellevue, WA, USA.

Cushing, T. (2013, November 20). *LG Smart TV Caught Collecting Data On Files Stored On Connected USB Drives*. Retrieved from techdirt:

https://www.techdirt.com/articles/20131119/06503625288/lg-smart-tv-caught-collecting-data-files-stored-connected-usb-drives.shtml

Cushing, T. (2014, May 20). *LG Will Take The 'Smart' Out Of Your Smart TV If You Don't Agree To Share Your Viewing And Search Data With Third Parties*. Retrieved from techdirect: https://www.techdirt.com/articles/20140511/17430627199/lg-will-take-smart-out-your-smart-tv-if-you-dont-agree-to-share-your-viewing-search-data-with-third-parties.shtml

David A. , H., & W E, K. (2019). Implementing Privacy Policy: Who Should Do What? *Media Entertainment Law Journal*, 1117-1150.

Device Security and Security Console. (2019, September 01). Retrieved from Open Connectivity Foundation: https://openconnectivity.org/search/SecurityConsole

Dickson, B. (2017, May 21). *These smart firewalls will keep hackers out of your home*. Retrieved from The Daily Dot: https://www.dailydot.com/layer8/best-smart-firewalls-internet-of-things-security/

Efthimios , A., Constantinos , P., & Nikas., A. (2018). I know what you streamed last night: On the security and privacyof streaming. *Digital Investigation*, 78-89.

Foulsham, M., Hitchen, B., & Denley, A. (2019). *GDPR - How to Achieve and Maintain Compliance.* Abingdon: Routledge.

Franceschi-Bicchierai, L. (2017, Mar 8). *The CIA Spied on People Through Their Smart TVs, Leaked Documents Reveal*. Retrieved from Vice: https://www.vice.com/en_us/article/8qbq5x/the-cia-spied-on-people-through-their-smart-tvs-leaked-documents-reveal

Gadbaw, T. (2016). Children's Online Privacy Protection Act of 1998. *Children's Legal Rights Journal*, 228-234.

Gamache, P. (2016, May 7). *Samsung SmartCam: root telnet, no password needed.* Retrieved from www.peerlyst.com: https://www.peerlyst.com/posts/samsung-smartcam-root-telnet-no-password-needed-peter-gamache-cissp

Ghiglieri, M., & Waidner, M. (2016, June). HbbTV Security and Privacy :Issues and Challenges. *IEEE Security & Privacy IEEE Secur. Privacy Security & Privacy*, pp. 61-67.

Ghiglieri, M., & Waidner, M. (2016). HbbTV Security and Privacy: Issues and Challenges. *IEEE Security & Privacy* , 61 - 67.

Gilbert, B. (2019, Jan 14). *www.businessinsider.com.au.* Retrieved from There's a simple reason your new smart TV was so affordable: It's collecting and selling your data, and serving you ads: https://www.businessinsider.com.au/smart-tv-data-collection-advertising-2019-1?r=US&IR=T

Goode, L. (2019, May 29). *Amazon Debuts a New Echo Show Amid Alexa Privacy Concerns*. Retrieved from wired: https://www.wired.com/story/amazon-echo-show-5-and-alexa-privacy-hub/

Google's revitalization of its Android-based TV effort via Marvell SoC and reference design. (2012, January 5). Retrieved from Experiencing the cloud: https://lazure2.wordpress.com/2012/01/05/googles-revitalization-of-its-android-based-tv-effort-via-marvell-soc-and-reference-design/

Gunes , A., Ben , B., Arunesh , M., Danny Yuxing , H., Nick , F., Edward W., F., . . . Moghaddam, M. (2019). Watching You Watch: The Tracking Ecosystem of Over-the-TopTV Streaming Devices. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security}* (p. 17). London, UK: ACM.

Hacked in Translation – from Subtitles to Complete Takeover. (2017, May 23). Retrieved from Check Point: https://blog.checkpoint.com/2017/05/23/hacked-in-translation/

Hasib, A., & Mottalib, M. (2010). Vulnerability analysis and protection schemes of Universal Plug and Play protocol. *IEEE 13th International Conference on Computational Science and Engineering (CSE)* (pp. 222-228). Hong Kong: IEEE Conference.

Intention to fine British Airways £183.39m under GDPR for data breach. (2019, July 08). Retrieved from Information Commissioner's Office: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/

James. (2018, June 11). *Privacy Policy on Smart TV's*. Retrieved from Samsung: https://eu.community.samsung.com/t5/TV/Privacy-Policy-on-Smart-TV-s/td-p/555555

Jordan, B. (2018). Privacy and Outrage. *Case Western Reserve Journal of Law*, 1-17.

Kab, S. (2019, April 19). *What is EPG Guide?* Retrieved from IPTV Guide: https://iptvapks.com/epg-guide/

Katsaounis, D. (2019, November 05). *The Best Vizio TVs of 2019 Reviews and Smart Features*. Retrieved from www.rtings.com: https://www.rtings.com/tv/reviews/vizio

Kelion, L. (2015, February 18). *Samsung's smart TVs fail to encrypt voice commands*. Retrieved from BBC News: https://www.bbc.com/news/technology-31523497

Key Initiatives , Privacy. (2019, March 20). Retrieved from Ministry Of Justice , New Zealand: https://www.justice.govt.nz/justice-sector-policy/key-initiatives/privacy/

Key initiatives Privacy. (2020, June 19). Retrieved from https://www.justice.govt.nz: https://www.justice.govt.nz/justice-sector-policy/key-initiatives/privacy/

Kho, N. D. (2018). What you need to know about GDPR. *EContent*, 4-8.

Kinsella, B. (2018, Jul 19). *Smart TV Market Share to Rise to 70% in 2018 Driven by Streaming Services, Alexa and Google Assistant*. Retrieved from voicebot.ai: https://voicebot.ai/2018/07/19/smart-tv-market-share-to-rise-to-70-in-2018-driven-by-streaming-services-alexa-and-google-assistant/

Kumar , K., & Vembu, D. (2017, May). *Anatomy of Smart TVs.* Retrieved from www.sasken.com: https://www.sasken.com/sites/default/files/files/white_paper/Sasken_Whitepaper_Anatomy%20of%20Smart%20TV.PDF

Lambe, J. (2017, May). *Applying VPPA to Online Video Privacy.* Retrieved from https://iapp.org: https://iapp.org/media/pdf/resource_center/Lambe-VPPA_2017-05.pdf

Little, A. (2019, April 26). *Privacy Bill*. Retrieved from New Zealand Parliment: https://www.parliament.nz/en/pb/bills-and-laws/bills-digests/document/52PLLaw25881/privacy-bill-2018-bills-digest-2588

Lowery, C. (2003, August). *A Tour of TOCTTOUs.* Retrieved from Sans.org: https://www.sans.org/reading-room/whitepapers/securecode/tour-tocttous-1049

Man-in-the-middle attack. (2020, May 13). Retrieved from owasp.org: https://owasp.org/www-community/attacks/Man-in-the-middle_attack

Mattoussi, F., Crussiere, M., Helard, J.-F., & Zaharia, G. (2019, February 12). Analysis of Coding Strategies Within File Delivery Protocol Framework for HbbTV Based Push-VoD Services Over DVB Networks. *EEE Access Access*, pp. 15489-15508.

Mauro Junior, D., Luis , M., Hao, L., Marcelo d', A., & Atul , P. (2019). A Study of Vulnerability Analysis of Popular Smart Devices Through Their Companion Apps. *2019 IEEE Security and Privacy Workshops* (pp. 181 -186). San Francisco, CA, USA,: Institute of Electrical and Electronics Engineers.

Mesellem, M. (2013, July 7). *https://github.com*. Retrieved from Samsung-TV-Denial-of-Service-DoS-Attack: https://github.com/r00t-3xp10it/Samsung-TV-Denial-of-Service-DoS-Attack

Michéle, B. (2015). *Smart TV Security Media Playback and Digital Video Broadcast.* Berlin: SpringerBriefs in Computer Science.

Michéle, B., & Karpow, A. (2014). Watch and be Watched: Compromising All Smart TV Generations. *The 11th Annual IEEE CCNC - Security, Privacy and Content Protection* (pp. 351 -356). Las Vegas: IEEE.

Musil, S. (2015, Feb 25). *Samsung may face FTC probe over voice-recognition TVs*. Retrieved from www.cnet.com: https://www.cnet.com/news/ftc-asked-to-probe-samsung-over-voice-recognition-tvs/

Nearly 50 Countries Switch Off Analog TV. (2015, July 7). Retrieved from www.atsc.org: https://www.atsc.org/news/nearly-50-countries-switch-off-analog-tv/

Newman, J. (2019, January 17). *In defense of smart TV snooping*. Retrieved from TechHive : https://www.techhive.com/article/3334138/in-defense-of-smart-tv-snooping.html

Newman, N. (2009, December 28). *Netflix Sued for "Largest Voluntary Privacy Breach To Date"*. Retrieved from privacylaw.proskauer.com: https://privacylaw.proskauer.com/uploads/file/doe-v-netflix.pdf

Niemietz, M., Somorovsky, J., Mainka, C., & Schwenk, J. (2015). Not so Smart: On Smart TV Apps. *International Workshop on Secure Internet of Things (SIoT)* (pp. 72- 81). Vienna, Austria: IEEE.

Nitin, N. (2012, June 4th). *What is Digital Fingerprinting*. Retrieved from www.mediaentertainmentinfo.com: https://www.mediaentertainmentinfo.com/2013/06/3-concept-series-what-is-digital-fingerprinting.html/

Pascale, G. (2014). *HbbTV Overview.* Retrieved from w3.org: https://www.w3.org/2014/10/tv-ig-meeting/TPAC%20-%20HbbTV%20Overview%20-%20Giuseppe%20Pascale.pdf

Phillips, A. (2020, May 28). *How to Decrypt SSL with Wireshark – HTTPS Decryption Guide.* Retrieved from comparitech.com: https://www.comparitech.com/net-admin/decrypt-ssl-with-wireshark/

Posses, S. (2017, August 4). *Disney Slapped With Suit Over Games That Swipe Kids' Info*. Retrieved from Law360: https://www.law360.com/articles/951354

Privacy Bill update – April 2020. (2020, April 22). Retrieved from https://duncancotterill.com: https://duncancotterill.com/publications/privacy-bill-update-%E2%80%93-april-2020

Samsung "SmartTV" Complaint. (n.d.). Retrieved from Electronic Privacy Information Center: https://epic.org/privacy/internet/ftc/samsung/

Samsung,Privacy. (n.d.). Retrieved from samsung.com/: https://www.samsung.com/nz/info/privacy/

Schubert, C. (n.d). *What is a smart TV and the privacy risks of a smart TV*. Retrieved from Symantec Corporation: https://us.norton.com/internetsecurity-iot-smart-tvs-and-risk.html

Smith, C. (2014, May 21). *Agree to share stuff with LG or it'll make your Smart TV 'stupid'*. Retrieved from BGR: https://bgr.com/2014/05/21/lg-smart-tv-privacy-policy/

Solovet, D. (2002). Conceptualizing privacy. *California Law Review*, 1087-1156.

Sortor, E. (2019, May 28). *Disney, Viacom Must Face Kids Data Scrape Class Action*. Retrieved from Top Class Actions: https://topclassactions.com/lawsuit-settlements/privacy/898913-disney-viacom-must-face-kids-data-scrape-class-action/

Stojancic, M. (2011, June 28). *http://site.ieee.org.* Retrieved from Audio-Vedio content fingerprinting for Smart TV & synchronous mobile content identification: http://site.ieee.org/scv-ces/files/2015/06/Zeitera_IEEE_CE_SantaClara-5.pdf

Sweney, M. (2019, July 10). *GDPR fines: where will BA and Marriott's £300m go?* Retrieved from The Guardian: https://www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog

The Video Privacy Protection Act as a Model Intellectual Privacy Statute. (2018, Apr 10). Retrieved from harvardlawreview.org: https://harvardlawreview.org/2018/04/the-video-privacy-protection-act-as-a-model-intellectual-privacy-statute/

Tidy, J. (2019, January 3). *PewDiePie hackers take over Google smart TV systems*. Retrieved from BBC News: https://www.bbc.com/news/technology-46746592

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' Consen. (2017, February 6). Retrieved from Federal Trade Commission: https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it

Vulnerability Statistics. (2019). Retrieved from www.cvedetails.com: https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224

Wagenseil , P. (2018, June 20). *Millions of Roku and Sonos Devices Easily Hacked: What to Do*. Retrieved from toms guide: https://www.tomsguide.com/us/roku-sonos-dns-rebinding-attack,news-27485.html

Wagstaff, K. (2012, March 02). *You'd Need 76 Work Days to Read All Your Privacy Policies Each Year*. Retrieved from techland.time.com: http://techland.time.com/2012/03/06/youd-need-76-work-days-to-read-all-your-privacy-policies-each-year/

Wei , J., & Pu , C. (2010, November). Modeling and preventing TOCTTOU vulnerabilities in Unix-style file systems. *Computers & Security*, 155-167.

Wei, J., & Pu, C. (2006). *File-based Race Condition Attacks on Multiprocessors Are Practical Threat.* Atlanta, USA: Georgia Institute of Technology.

Welcome to SamyGO Wiki. (2018, Feb 18). Retrieved from http://wiki.samygo.tv: http://wiki.samygo.tv/index.php?title=Main_Page#Welcome_to_SamyGO_Wiki

What is a denial of service attack (DoS) ? (2020, Jan 2). Retrieved from https://www.paloaltonetworks.com/: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

Whittaker, Z. (2019, December 19). *Many smart home device makers still won't say if they give your data to the government.* Retrieved from https://techcrunch.com: https://techcrunch.com/2019/12/11/smart-home-tech-user-data-government/

Wollerton, M. (2019, June 12). *Amazon launches new Alexa device for kids but privacy issues will still scare some parents*. Retrieved from cnet: https://www.cnet.com/news/amazon-launches-new-alexa-device-for-kids-but-privacy-issues-will-still-scare-some-parents/

www.cn.vizio.com. (n.d.). Retrieved from Privacy Policy: https://cn.vizio.com/privacy.html

yt3.ggpht.com malware. (2019, Dec 21). Retrieved from www.reddit.com: https://www.reddit.com/r/cybersecurity/comments/edkc5p/yt3ggphtcom_malware/

APPENDIX

Appendix 1 – In the STV A, a Prime video app was crashed when the hulk DoS script executed but after the crash the STV A restarted itself. The Prime video app did not crashed for the DoS attack.