MALMÖ HÖGSKOLA

Fakulteten för teknik och samhälle
Datavetenskap

Examensarbete
15 högskolepoäng, grundnivå

Evaluating privacy and security risks in smart home entertainment appliances, from a communication perspective

Utvärdera integritet och säkerhetsrisker i smarta underhållningsapparater, ur ett kommunikationsperspektiv

Irengård Gullstrand, Simon
Morales Larsson, Ivan

Examen: Kandidatexamen 180 hp
Huvudområde: Datavetenskap
Program: Datavetenskap och applikations utveckling
Datum för slutseminarium: 2016-05-30

Handledare: Joseph Bugeja
Bihandledare: Andreas Jacobsson

Andrabedömare:
Dimitris Paraschakis

Abstract

The concept of smart home technology becomes more and more a part of our everyday life. Because of the hasty evolution and considering that wireless communication has become the norm, the security and privacy problems have become more of a concern. The purpose of this work is to examine what kind of information can be extracted from an entertainment-based smart home involving an off-the-shelf game-console, Playstation, connected to the Internet. This scenario has been investigated with experiments focusing on the interception of networking traffic occurring when using such a device under everyday operations. The results of the study shows that sensitive data such as images is infact possible to extract.

Keywords— sercurity, privacy, internet, smart home, playstation, wireshark, wireless communication, entertainment

Sammanfattning

Konceptet smarta hem blir mer och mer en del av vår vardag. På grund av den hastiga utvecklingen och med tanke på att trådlös kommunikation har blivit normen, har säkerhetsproblem och integritet blivit mer av ett bekymmer. Syftet med detta arbete är att undersöka vilken typ av information som kan utvinnas ur en underhållning-baserade smarta hem innebär en off-the-shelf spel-konsol, Playstation, ansluten till Internet. Detta scenario har undersökts med ett experiment som fokuserar på avlyssning av nätverkstrafik som inträffar vid användning av en sådan enhet i det dagliga livet. Resultaten av studien visar att känsliga data såsom bilder är i själva verket möjligt att utvinna från nätverks kommunikationen.

Acknowledgements

We wish to thank fellow students Andreas Stridh from Computer Engineering and Mobile Sensing Systems and Dina Eid Musalam from Master in Computer Science program, both from Malmö University, Sweden. They have used and commented upon much of the material in this thesis, and helped us refine it. We also want to thank Joseph Bugeja, Doctoral researcher, part of the Internet of Things and People Research Centre, Malmö University, for suggestions, advice and lively discussions about the nature of research in Information Security and computing. Finally we must thank Andreas Jacobsson, Vice Dean at the Faculty of Technology and Society, Head of Intelligent Support for Privacy Management in Smart Homes – iSMASH project, which is a project at Internet of Things and People Research Centre, at Malmö University, for the help and support as well as the opportunity to be part of the research in the smart home security and privacy field at Malmö University.

Glossary

Arch Linux Arch Linux is a Linux distribution predominantly of free and open-source software .

Backdoor A backdoor is a method used to bypass normal authentication of a product, computer system, etc .

Commercial off-the-shelf (COTS) Commercial off-the-shelf "COTS" means that the product is a standard manufactured product rather than a customized version of the product .

Cryptography Cryptography refers to constructing unreadable data to prevent third parties or the public to be able to read private data. Information security aspects such as confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography.

Encryption In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it.

Hacker In computing, hacker is a term which refers to a skilled computer enthusiast. Depending on the field of computing it has slightly different meanings, and in some contexts has controversial moral and ethical connotations .

Hash A hash function is used to map data of arbitrary size to data of fixed size, this means that readable data will be unreadable without knowing the stored hash value. This allows the communication of cryptographic messages.

Home Gateway/Hub The term gateway often means a device on a network that acts as a central point and or a relay to another network and often used to translate between different communications protocols, data formats, etc.

Internet of Things (IoT) The Internet of Things is a term used for a development of a network consisting of objects which are embedded with electronics, software, sensors and network connectivity that enables these objects to collect and exchange data. .

Malware Malware is any software that is developed for the purpose of doing harm to computers or via computers. The main types of malware include worms, viruses, trojans, backdoors, spyware, rootkits and spam .

Man-in-the-middle attack (MitMA) Man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication.

Network address translation (NAT) Network address translation "NAT" is a method used for remapping one IP address space into another by modifying network address information in Internet Protocol datagram packet headers while they are in transit across a traffic routing device .

Ubiquitous Computing (ubicomp) The idea to integrating computers anywhere to be able to use a single user interface throughout the whole environment .

Wireshark Wireshark is a network analysis tool that lets the user analyse each package individually.

Contents

1 Introduction

In recent years, the industrial interest in smart home appliance and enhanced automation features of the home has increased significant [1]. We are at a point where we can almost control anything in our houses remotely with great ease. Forecasts estimate a global increase in units sold at an average annual growth rate of 67%, from around 400 million units in 2014 to 1.8 billion units in 2019 [10]. This increased interest in smart appliances has created an increased need for research in this area [1].

The vision of *Ubiquitous Computing (ubicomp)* in smart home environments aims to integrate all individual devices to the smart home and control them all though one control interface [7, 25]. Fulfilling this vision is where the majority of the research within the field is focused [17]. While the technology to satisfy the customers is developing, problems with the security and maintainability arises [25]. This problem is exacerbated when the wireless medium between the home utilities in the smart homes is used. The view of accepting the smart home concept lays in the complication to create a satisfyingly secure smart home for the end user. Studies with focus on social barriers within smart homes [4, 7], presents problems that has to be addressed before the smart home concept is fully accepted. One of the problems is that users generally appreciates the idea of a remote accessible home, where for example cameras and temperature can easily be adjusted. More than half of the respondents experience that this kind of convenience makes the smart home more vulnerable to outside attacks [7]. According to a study about State of the Smart Home [21] they found that consumers are most eager to connect their entertainment room to their smart home illustrated in Figure. 1, when comparing which of all of the rooms in the house that was most relevant for individuals, regarding the purpose of connecting to a smart home. In this study it was also found that entertainment has emerged as a new and powerful driver to smart home adoption. One of the major reasons to why consumers wanted to purchase a smart home system was that they were able to remotely control and/or monitor the TV and sound systems. This was based on the nearly 45% of the respondents in the study who found this function important. Additionally the results showed that the interest in entertainment had increased since the previous year where only 29% listed this as a top benefit of a smart home [21]. Also the Playstation usage has increased, since it is the perfect device to have as a center entertainment device in the entertainment room. Because it can perform almost any task commonly needed in an entertainment room [22]. With this kind of upturn in interest of entertainment devices the security and privacy has to keep up with the development. Conceptually a smart home consists of technology that is supposed to raise residents' peace of mind and security [4]. But by letting the system know more and more about us, we also open up ourselves to being easier exposed. This might bring major security and privacy concerns to the owner of the smart home. These surfaced problems should not exist and be of no concern to the end user. Where in that case the system should be designed in a way so that it is easily managed and as automated as possible [19].

1.1 Purpose

The purpose of this study is to discover potential data leakages in a typical Smart Home setup occurring through the network communication channels. This work will help us to

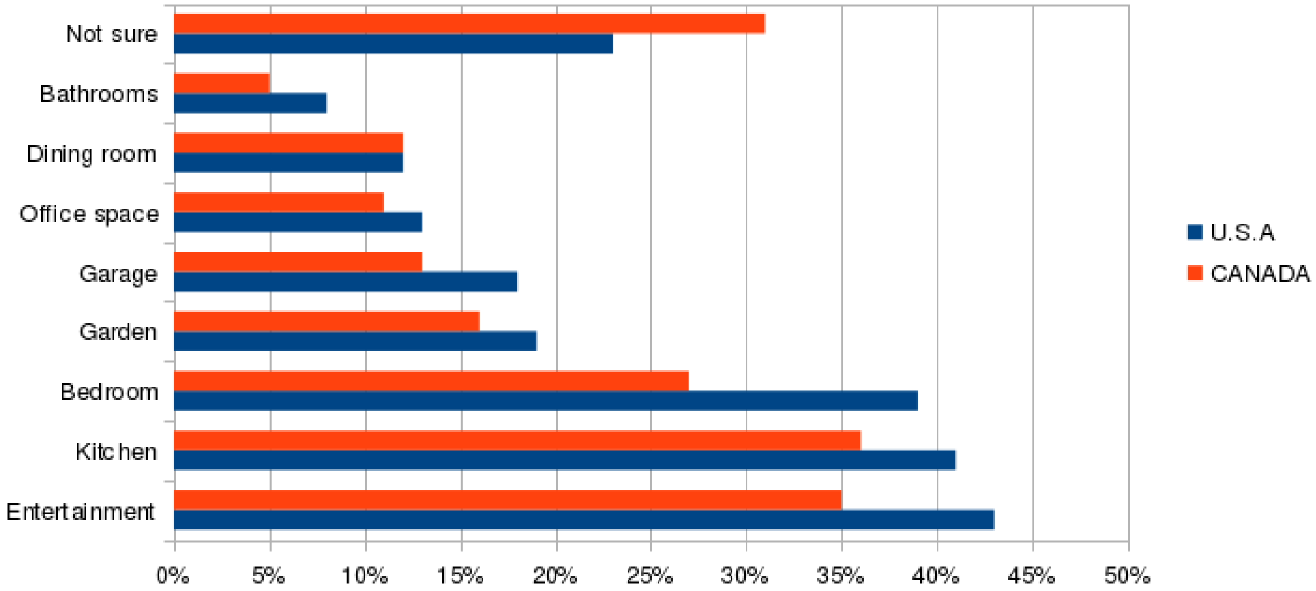


Figure 1: Most desired connected area

understand and answer questions such as, can we really trust a smart home appliance to store and use confidential data about us in a secure and private way?

1.2 Enclosure

To narrow down the study we decided from a security and privacy perspective to focus on the Smart home entertainment category. For the purpose of answering the research questions existing technologies will be investigated. For the practical part of the study to be feasible, experiments will be limited to one of the many smart home devices in the entertainment category available on the market today. The study will also be limited to investigate security flaws in the network communication, specifically between the Smart *Home Gateway/Hub* and the Internet. The entertainment appliances of today are communicating all sorts of confidential data about us, like payment information, purchase history and social media outlet information such as Facebook, Twitter and Youtube. By examining different ways of interacting with the device we were able to conclude if there were any common data sets that are being shared to and from the gateway. Hopefully leading to improvements in the security and privacy fields of Smart homes. This study also serves as a preliminary to a larger research project in the field of smart home called the Internet of Things and People conducted at Malmö University.

1.3 Problem discussion

Based on the discussion above and the statistics as shown in Figure. 1 it can be argued that the Playstation 4 is a good candidate to investigate further. Considering that the Smart home entertainment area of the house is such a central point in the home and therefore a very important candidate for security and privacy. Deficiencies in the security, specifically regarding entertainment devices generate risks both in terms of credit card theft and also privacy. It is reasonable to assume that the user will expect the highest level of security in the most relaxed section of the house [4]. The lack of trust in the security of smart home technology, described in the thesis introduction, manifests itself in the form of the slow transition that has been taken place during the last decade. Also a 2015 research results in that more than half of the respondents experience that convenience like remote access to the smart home devices makes the smart home more vulnerable to outside attacks [7]. The lack of trust indicates a potential for further research in the field to evaluate the safety of smart home entertainment devices and whether the concerns over these are justified.

1.4 Research questions

Based on the problem discussion the following research questions were raised:

1. *Are there data leakages that are of a security or privacy concern in a Commercial off-the-shelf (COTS) smart home entertainment appliance?*
2. *Can such data be intercepted and used to identify users and their environment?*

1.5 Hypothesis

Recent research oriented in the smart home field [17, 20, 42] involve similar scenarios as this paper. They are demonstrating for example how it is possible to infiltrate and take control over a smart home device as well as intercept and extract data in clear text. Based on the problems raised in the problem discussion we believe this kind of studies are of high interest and therefore want to study this topic further. A directed hypothesis was chosen based on our first prediction, concerning research question 1, which is that we think based on similar studies [17, 20] that we will find data leakages within the communication between the chosen smart home entertainment device and the Internet. To suggest that data is secure we expect that the transmission of all and especially confidential data such as passwords or credit card numbers are hashed and/or encrypted. What we expect to find within the data is that there are actually some confidential data that we are able to exploit.

This thesis is organized as follows. Chapter two provides background information and key concepts, chapter three will describe our methodology where we describe in detail how our experiment were conducted, chapter four and five will present, discuss and analyze the gathered data from the experiment. Finally, chapter six will be the conclusions of the study.

2 Background

This chapter provides background information and key concepts that are used in this thesis such as smart home, Internet of things, recent exploits, privacy and security. It presents and discusses theories and ideas that we have found relevant to understanding the problem domain.

2.1 Smart Homes

A Smart home is a home that takes advantage of automation technologies, to provide an increasing comfort for the residents. The home automation technologies are electrical devices that are able to process and exchange data. You can control the devices or let them perform tasks on their own. To understand what home automation is, we have to break down the concept as shown in Figure. 2. First up is “House Infrastructure”, this is a centralized control of a building’s for example heating, lighting, water, ventilation and air conditioning. The goal of this kind of system is to improve comfort, reduce energy consumption and operating costs. Also, by automatically turning off utilities improve their life span.

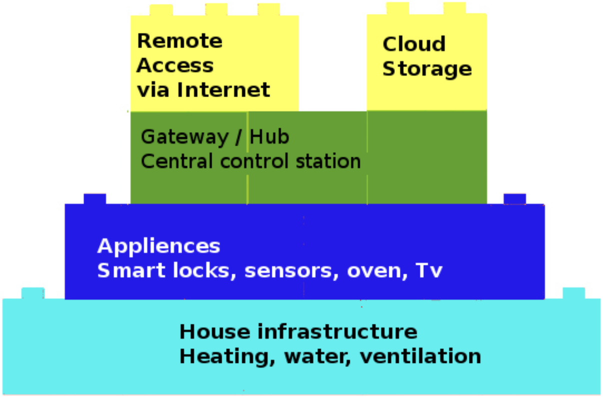


Figure 2: Smart home centralized architecture

Second part is “Appliances”, security locks of doors and gates etc. These kind of systems are what we call *Internet of Things (IoT)* devices, more details in Section 2.2. For example there are specially adapted systems to provide the specific help elderly and disabled people need that otherwise would require caregiver or institutional care [24, 40]. You can automate tasks like yard watering, pet feeding and control of domestic robots. The systems are integrated for easy living, convenience, increased comfort, security and safety, energy efficiency and as well as automation of simple tasks that are performed multiple times [24]. The home automation devices may be connected to a *Home Gateway/Hub* which may be connected to a Local Area Network. This would allow you to control and program the systems from a personal computer, tablet and smartphone, and may allow remote access from the Internet.

You can integrate sensors, biomedical monitors and cameras to the system in your home that will collect data about your behaviors and patterns [24]. This data can be stored locally and/or in a Cloud storage. Systems can use the data to ensure the greatest comfort and advantages possible for you. Example of benefit, if the system recognizes that you are not home it can turn off the water, all the lights and also perform checks on different other utilities in your home like a stove or an oven and turn them off automatically as well. While you’re at home, it is able to perform different kind of tasks; one example is if you leave or enter a room the light goes off/on automatically. If you choose to install speakers in every room, the music you are currently listening to is also able to follow you throughout the house. If you start cooking the potentially dimmed light goes to 100%

[8, 24].

2.1.1 Types of smart homes

The list of differents types of smart homes is open-ended and is only being limited by the human imagination. But as it stands today there are four major categories of which a smart home can be identified as [5], they are as follows:

- Home care/Elderly care
- Energy Efficiency
- Entertainment
- Security and Safety

The listed categories are not always necessarily disjoint, an example of this is that Security and Safety can be related with Home care/Elderly care. Additionally, functions belonging to one or more different application types can be found within the same category. Finally, these applications can share approaches. For example, applications related to eldercare and safety very often use the same methods for video surveillance [6].

2.1.1.1 Home care/Elderly care The main purpose of the technology created for this category is to help people in need, people that are disabled and can not help them self. Also elderly people who are in a constant need for help and attention. This type of smart home is part of a more general interest for developing new smart home technologies for addressing the problems of the elders related to health, loneliness, disability, cognitive limitation, etc. Two main subcategories were identified within the category of Home care and Elderly [37]:

1. Assistance at any given time that focuses on assisting elders during their daily activities, as well as addressing their disabilities and cognitive limitations.
2. Ubiquitous care that addresses elders' social limitations by providing them with services and facilities for social inclusion with purpose of reducing their sense of loneliness.

2.1.1.2 Energy Efficiency Reduction of energy consumption is a very important development within technology for the modern society with a major impact on future development of the mankind [5]. On the one hand the technology progress requires the use of more energy, while on the other hand energy is on the verge of becoming a limited resource. Therefore there are smart devices and appliances, that can control energy savings. For example switching off or to low-power mode on the appliances currently not in use or according to the user preference settings, that can be implemented to a home in order to reduce the inevitable energy consumption, and through that save both energy and money.

2.1.1.3 Entertainment A category that address users comfort and entertainment. Typical examples are ambience control (for example lighting and background music), advanced user interfaces used to control devices (for example based on voice or gestures), automation of routine activities, etc. And it is within this category our work will focus on.

2.1.1.4 Security and safety Safety refers to the detection of unusual situations inside the smart home [5], like for example fires, floods, accidents even possible falls of disabled or the elderly. Security refers to the detection of malicious behaviors that might harm the home or the residents, like for example burglars, unauthorized access, and others. For the detection, signalling and response to such safety or security violation situations, the smart home are equipped with sub-systems for video surveillance, remote monitoring, alarming, and emergency response.

2.1.2 Architecture

A traditional smart home is often implemented using a centralized architecture by reason of that it is the most popular architecture, also easier to manage and has better security [27]. A general build for centralized architecture is shown in Figure. 3. The home appliances are connected to the homes local network and controlled by the home gateway, which is the platform for service providers to provide services to residents [42]. The way it works is that the different smart devices, such as smart thermostats and smart refrigerators or in our case entertainment devices like a smart tv or gaming consoles to be communicating with the home gateway. In turn the gateway directs all traffic to and from the Internet as shown in Figure. 3. The person shown in Figure. 3, represents a smart home user and is able to through the Internet and then through the home gateway, control and communicate with the devices in the smart home. This can all be done with the designated android or IOS application.

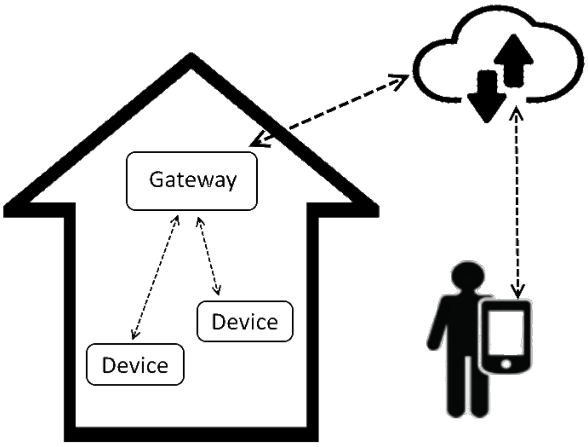


Figure 3: Centralized architecture

Another solution for a smart home architecture is the Distributed Architecture. It is a topology where all peers communicate symmetrically, have equal roles and collaborates together on a certain task. Each device in the network has the ability to communicate with or through any other device as seen in Figure. 4.

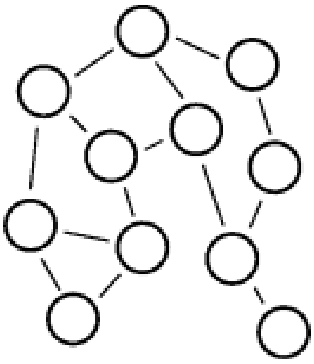


Figure 4: Decentralized architecture

2.2 Internet of Things

The Internet of things or "IoT" for short is a term for a development of a network with physical objects that consist of but is not limited to, devices, vehicles, buildings, appliances, clothes and even creatures (including humans). Which are embedded with electronics, software, sensors and network connectivity that enables these objects to collect and exchange data. These can observe their environment, communicate with it, and thus create a specific behaviour and help create smart, helpful environments, products and services. There are many big fields where The Internet of Things can be applied to such as the field of media. The media industry appears to be moving away from the traditional approach such as newspapers, magazines, or television shows and instead distribute their content through personalized technology. That way the person who is using the device will decide what content (articles) and advertisements that appeals to him. Another field is environmental monitoring where Internet of Things applications can use sensors to monitor air or water quality, atmospheric or soil conditions, and can even include areas like monitoring the movements of wildlife and their habitats. Medical and healthcare is also a field that can greatly benefit from Internet of Things applications, such applications could be remote health monitoring and emergency notification systems [24, 40].

2.3 Security and Privacy

Cyber criminals are identified as a raising hostile threat category. With increasing number of smart devices and homes connected to the Internet, there is a high potential abuse of smart homes. Therefore the priority of security should be considered more important. Furthermore, several economic factors generate security vulnerabilities, based on that design choices are competing against cost and convenience. Not all smart homes are created equally due to multiple design strategies which result in their own security and privacy solutions. Just as in many other areas of Internet connected things, applying basic information security can significantly increase overall security in the smart home [15].

Computer security in a communication network depends not only on the security investment made by individual users, but also on the correlation between them. If a user puts in little effort in protecting its computer system, then it is easy for viruses to infect this computer and through it continue to infect others'. On the contrary, if another user invests more effort to protect itself and its computer system, then other users will also gain a benefit because the chance of *Malware* spreading is reduced [23]. Besides user preferences, the network topology, which describes the relationship among different users, is also important. For example, assume that in a local network, user A is directly connected to the Internet. All other users are connected to A and exchange a large amount of traffic with A. The security level of A is important for the local network since A has the largest influence on other users. That means if A has low security then whole network might suffer.

There have been many definitions of privacy over the years. One of the early definitions of privacy was forwarded by Louis Brandeis and Samuel Warren in a Harvard Law Review article [32]. They tried to explain how the right to privacy was different from legal rights. They believed in the "... right to be let alone" [32]. In a more recent journal [16], the author defines privacy as "the limitation of other people's access to individuals". Her definition has three points: secrecy, anonymity, and solitude. Spinello states that "Anonymity is protection from undesired attention; solitude is the lack of physical proximity to others; and secrecy (or confidentiality) involves limiting the dissemination of knowledge about oneself" [33, 35]. When security becomes an increasing concern privacy and ethical aspects is not to forget. We live in a society with access to all types of information. Leading to privacy growing more important, how much personal information should we really teach the system at hand about us, to be able to grant the promised benefits? It is a hard question and still we're forced to answer this question everyday.

But what information is regarded confidential? Any information that someone can use to identify an individual constitutes personal data. For example, a list of usernames and email addresses will count as personal data [38]. Geographical location is one of the most sensitive data types currently able to be collected. A recent MIT study [12, 31] by de Montjoye et al. showed that four spatio-temporal points, approximate locations and times, are enough to identify 95% of 1.5M people uniquely in a mobility database. Further the study presents that these constraints hold even when the resolution of the dataset is low. This results in that, even coarse or blurred datasets provide poor anonymity [13].

Time and date are another data type that is of a sensitive nature from a privacy and security perspective. When a file is timestamped, a unique identifier, for the file (a SHA Hash) is created by the computer. This identifier is a unique number calculated from the file's contents [14]. By altering this information interesting things can happen. One example of this is a recently found bug in the iOS 5 operating system where by changing the date to some point in the past, the *Hacker* were able to view previously taken images without unlocking the Iphone [26]. Additionally images are also a privacy concern out of initially a user identification perspective. Pictures about us is not very pleasant to be shared around the Internet without our acknowledgement or even worse, being used for blackmail. Still there are countless hacks where this type of behavior has happened [36]. Also a image contains privacy and security related data about for example date, device and geographical location it was taken or created on and sometimes even information about the device it is located on. One way of ensuring that the data is more secure is to use an *Encryption* protocol when communicating sensitive data. A problem is that it is still hackable if an older version of the protocol is used [9]. Since the release of SSL (secure socket layer) v3.0, several vulnerabilities have been discovered. One example is the “POODLE” issue where cleartext data were extracted by conducting a padding-oracle attack on the communication [11]. The solution for this issue is to restrict the usage of secure protocols to only the latest version, which at the time of publication is TLS v1.2 [9].

2.4 Examples of recent exploits

This section describes a few recent smart home exploits. A hacker, if successful, can study smart device wireless communication to identify residents locations in a home, unlock doors, disable sensors and alarms for further infiltration [44]. In brief, the security of Smart appliances is very important to withhold the privacy of the residents.

Two practical attacks has been conducting in a laboratory environment against ZigBee Smart home security [41]. The first attack is based on sabotaging the ZigBee EndDevice by sending a special signal that makes it wake-up constantly until the battery runs out. The second attack is based on exploiting the key exchange process in ZigBee when using the Standard Security level defined by the ZigBee specification [3, 41]. Which would possibly mean that the hacker could take control of the smart home devices.

The Nest Thermostat is a smart home automation device that aims to learn a user’s heating and cooling habits to help optimize scheduling and power usage. This system was exploited through a connected USB device, which bypassed where the firmware verification is done by the Nest software stack, providing the means to completely alter the behavior of the unit. The compromised Nest Thermostat will then act as a *Backdoor* to attack other nodes within the local network. Also, any information stored within the unit is now available to the attacker wirelessly [18].

Security firm Proofpoint report 2014, that hackers are attacking "smart" appliances in your household. The firm looked into attacks that occurred between Dec. 23 and Jan. 6, and found that more than 25 percent of spam email was sent by home-networking routers, connected multimedia centers, televisions and at least one refrigerator [30].

Vulnerabilities were found in a mobile app developed by Samsung to wirelessly control the refrigerator. Where hackers figured out that they were able to conduct man-in-the-middle attack to gain access to the Gmail login credentials, if they had an access to the same Wifi network as the Samsung refrigerator where connected to. This leads to access to for example shopping habits and other stored confidential data in the refrigerator [20].

2.5 Related work

The authors of [43] performed a study about traffic analysis of SmartThings devices to demonstrate that a hacker might perhaps identify obvious traffic pattern of smart home products [43] [22]. In their study, the authors had built a SmartThings system consisting of a SmartSense Open/Closed sensor - a door sensor, a SmartSense Motion sensor, and a GE

Link - a SmartThings-compatible LED bulb, all of which are connected to the SmartThings cloud server through a SmartThings Hub and a router. In order to capture all of the packets between the SmartThings Hub and the cloud server, the authors connected a computer running Ubuntu as a bridge between the router and the home gateway. This allowed the gateway to obtain an IP address and connect to the Internet while we could monitor the network traffic before it was forwarded to the router. This is also called to conduct a *Man-in-the-middle attack (MitMA)*. The tool *Wireshark* was used to capture all of the Ethernet network traffic to observe communications taking place on the network between the gateway and the SmartThings server. In their study the authors discovered privacy vulnerabilities in the smart home environment [43] and that the use of a Virtual Private Network (VPN) is desired to prevent packet captures. This can prevent a hacker from directly monitoring the traffic between the home gateway and associated smart home server.

Another study was about network behavior within the smart home on selected smart devices were performed in a study by Notra [28] to examine if the implementation of encryption, authentication and privacy solutions are acceptable and secure or may contain vulnerabilities. The smart devices for the experiment consists of a lightbulb, a light-switch and a smoke detector detector that are directly connected to the Internet and a mobile application that can control these devices, according to the authors these devices are the most frequently bought and distributed devices that are considered to be IoT devices. The investigation of the devices individual communication was performed in a controlled lab environment where the network activity was intercepted by using Wireshark software tool. The results varied between devices and for example the testing of the smoke detectors smart features include motion, light and heat sensors did not show any direct weaknesses, but all communication was encrypted. The authors [28] found that some packets are of a larger size and the risk of sensitive data to be logged and collected do exists. The lightbulb, lacks encryption and communicates in cleartext over the network. Only the username is hidden, but in the form of a *Cryptography Hash*. This means that a person who observes the network communication can extract data containing for example the location of the residents. According to the authors [28] vulnerabilities of this specific type of light-bulb was already demonstrated by the manufacturers in the past, and they have taken measures for how to communicate the username safer. The text however, at the time of the study (2014) was still shown in cleartext. Testing of the light-switch demonstrates several security flaws when it comes to communication, for example content is communicated in cleartext and lack of authentication between devices. This means that an interceptor can access sensitive data related to the status of the home and also could take control of connected devices.

One study performed by a couple of students from Malmö högskola evaluated security of a smart door lock from a communication perspective [17]. Their study were consisted of practical experiments on a smart home lock that existed on the market at the time their study were conducted. The lock was examinated by intercepting and collecting quantitative data of the radio based communication that transpire between the smart home lock and the centralized home gateway. After the interception the collected data was analysed with the help of a pattern recognition algorithm and finally analyzed manually with Wireshark in order to find common features in the data that formed some sort of system information [17]. Their study showed that it is possible for outsiders to extract information from the smart locks' communication. Approximately 70% of the door communication is encrypted with what seems to be the AES-128 and these messages are real payload and they may not be recover within a reasonable time. The information that can be extracted is metadata containing the communication in the form of message length (number of packets per message), package types and the length of the data in packets. This information can be used to categorize the interaction with the door in six different categories: interaction from a distance, closing the door, unlocking with a cipher code or key card, opening the door, locking via physical button and input of incorrect cipher code.

3 Methodology

This chapter is aimed to describe the research approach undertaken for this thesis. According to Carolyn B [34], "Qualitative data are data represented as words and pictures, not numbers". Qualitative study was chosen to investigate the security in a smart home and to answer the research questions which is about finding out if there are any data leakages, what kind of information and how to extract it. The choice to perform experiments on an entertainment device through intercepting the communication is based on methodologies in similar studies [17, 28]. These methodologies is about intercepting communication in a controlled environment, followed by analysing packets with filters (only displaying relevant packets for our study) and/or scripts to recognize important data. We conducted our experiments based on the way these similar experiments were conducted.

3.1 Metod of choice

The chosen method for this study is a practical experiment due to the need for setting up a research environment as close to a real life scenario as possible and because the study is focused on how the Playstation 4 behave in reality and not in simulation. To be able to answer the research questions and to evaluate the security and privacy concerns the study have to be conducted as a practical experiment with real devices. We also believe this approach could deliver unpredictable and interesting outcomes on top of the expected results described in the hypothesis section.

3.2 Experimental setup environment

In order for the experiment to be conducted a setup environment was constructed. The construction as seen in Figure. 5 is a replica and a miniature version of the setup as shown in Figure. 3. Also both hardware and software components are needed. The hardware includes a laptop, a Playstation and a WiFi USB Adapter. The laptop functions as a home gateway (or hub), the Playstation is the entertainment device being analyzed, and the WiFi USB Adapter -is responsible for channeling the communication between the laptop and the Playstation The software include Wireshark and a scrip. Wireshark is used to intercept communication and a script, Create_AP see Appendix A - to create a *Network address translation (NAT)* software access point.

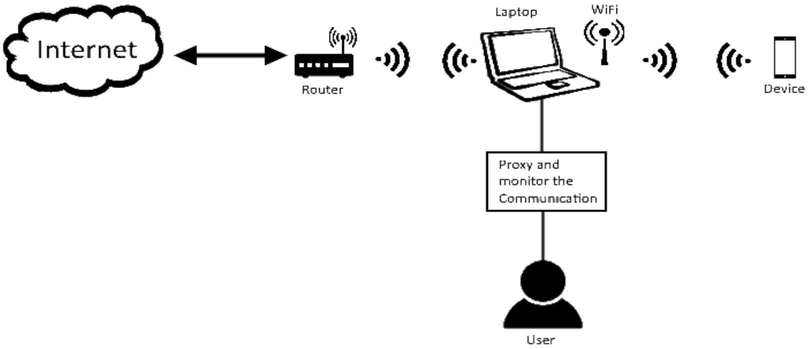


Figure 5: Illustration of our setup.

3.2.1 Hardware

3.2.1.1 Laptop The laptop that was used during the experiment was Lenovo Yoga 2 Pro running Arch Linux 4.4.1-2 as the operating system. The purpose for the laptop during the experiment was for it to work as the home gateway and for the laptop to also monitor and log the network communication with Wireshark.

3.2.1.2 WiFi USB adapter The WiFi USB Adapter that was used in the experiment is called TP-LINK TL-WN722N. It was chosen since it is highly recommended and used within the linux and network administration community. This means there is a lot of documentation.

3.2.1.3 The Smart home entertainment device As for the smart device we wanted an existing smart entertainment device which currently exist on the market today during execution of this study, in our case that would be a Playstation 4. The main purpose for the Playstaion 4 is for it to work as the smart device for the experiment. The Playstation in question is a regular stock product that has not gone through any modifications but it has been in use for approximately thirteen months. The reason for why a used Playstation 4 were used in the experiment was on account of that we wanted the experiment to be as close to a real scenario as possible to simulate what is communicated in a real smart home.

3.2.2 Software

3.2.2.1 Create_Ap To make the laptop act like a home gateway we used the script Create_Ap [29]. The script was recommended on the Arch networking forum. It consists of the commands used to create a access point on linux. More about Create_Ap consult Appendix A.

3.2.2.2 Wireshark Wireshark version 2.0.1 with libpcap version 1.7.4. Built using gcc 5.3.0 was used to intercept, log and analyse the network communication.

A similar tool considered for the experiment was TCPdump which is a Linux based terminal software. Wireshark was chosen based on what previously used in previous studies [17, 28]. Wireshark is a free and open-source packet analyzer, it is widely used and recommended for network troubleshooting, analysis, software and communications protocol development, and education.

3.3 Experimental task

Before the experiment was conducted we started with identifying the most common activities to be performed while interacting with the Playstation 4. This information was gathered by conducting a survey on twenty random “gamers” on the Playstation 4 forum and the Playstation 4 chat network. Most common tasks on the device involved logging on to the Playstation network, downloading applications from the Playstation store, Chatting with people on the Playstation chat and Playing online games. We added two extra tasks that we believe might relieve interesting packages, which are: Letting the device stand in standby mode for one minute and using the Playstation built in web browser to visit a common website. The chosen website is Facebook.com by reason of that it is the third most visited website on the web [2]. With this information in consideration we also want to do further research based on previous experiments conducted in the same field. With Trapps [39] paper in mind, where he suggests investigating: “Attach a console like a Wii or PS3 and see what kind of information it sends at startup and logon.”

1. Log on the device.

   Description: This task contains startup and a normal login process, conducted by starting the Playstation 4 and letting everything that is loading finish.

2. Let the device stay on standby for one minute.

   Description: Located on the Dashboard without any interaction with the device during the one minute.

3. Log in and out of Facebook, using the web browser on the device.

   Description: Opening the preinstalled web browser, searched “facebook.com” and logged in. Next we scrolled for a 5 seconds and then logged out.

4. Download a free application on the Playstation store.

   Description: Opened the preinstalled Playstation store application and searched “media player” and downloaded the first in the list named “MediaPlayer”.

5. Exchange a few messages with another user using the Playstation chat function.

   Description: Started a chat with a current friend in the friend list on the Playstation chat. Exchanged a few messages with each other then exit chat.

6. Play an online game for five minutes.

   Description: Started the game “Tom Clancy’s The Division” and entered an online match. Played for five minutes and then quit the game.

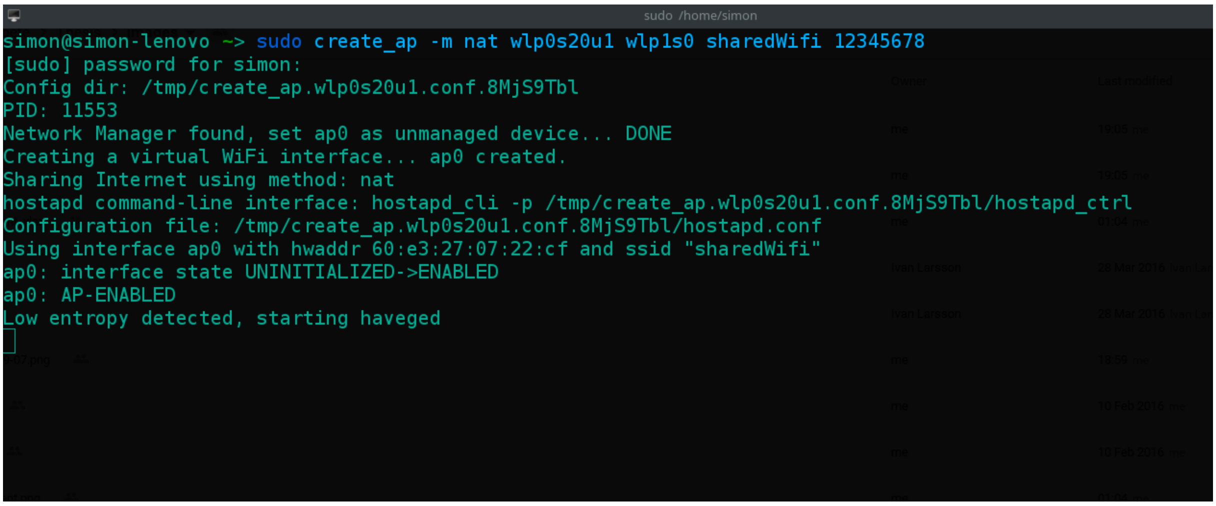
3.4 Procedure

The study consisted of practical experiments by intercepting the network communication between the Playstation 4 and the Internet. This was done by initially setting up the environment so that the interception could be performed.

Firstly we connected the laptop running *Arch Linux* to the Internet, then the Internet connection was NATed to the Playstation 4. This was done by inserting the WiFi USB Adapter into the laptop. To be sure that the WiFi USB Adapter could perform the task at hand we decided to configure it to be set in Monitor mode. This was done by firstly acquiring the "interface name" Arch gave the WiFi USB Adapter. In the terminal we ran the command: *Ifconfig* . This command lists all active interfaces. Next we had to put the interface in idle mode to be able to change the mode. In the terminal we ran the command: *sudo ifconfig wlp0s20u1 down.* Then we change the mode by running the command: *sudo ifconfig wlp0s20u1 monitor.* At last we put the interface in active state by running the command: *sudo ifconfig wlp0s20u1 up.*

Subsequently a shell script named Create_ap [29] was used, which created a NATed Software Access Point by after installing it running the command shown in Figure. 6.

The Create_Ap command works by this syntax: create_ap [options] wifi-interface [interface-with-Internet] [access-point-name [passphrase]], where [options] defines what method to be used to transfer Internet over to the other interface.



```
simon@simon-lenovo ~> sudo create_ap -m nat wlp0s20u1 wlp1s0 sharedWifi 12345678
[sudo] password for simon:
Config dir: /tmp/create_ap.wlp0s20u1.conf.8MjS9Tbl
PID: 11553
Network Manager found, set ap0 as unmanaged device... DONE
Creating a virtual WiFi interface... ap0 created.
Sharing Internet using method: nat
hostapd command-line interface: hostapd_cli -p /tmp/create_ap.wlp0s20u1.conf.8MjS9Tbl/hostapd_ctrl
Configuration file: /tmp/create_ap.wlp0s20u1.conf.8MjS9Tbl/hostapd.conf
Using interface ap0 with hwaddr 60:e3:27:07:22:cf and ssid "sharedWifi"
ap0: interface state UNINITIALIZED->ENABLED
ap0: AP-ENABLED
Low entropy detected, starting haveged
```

Figure 6: Terminal window while the Create_Ap script is running.

When the access point was up and running we connected the Playstation 4, and simultaneously started Wireshark on the laptop to intercept all the network communication done by the tasks described in the Experimental task section.

3.4.1 Data analysis

Every package received and sent by the device was saved and categorized in a separate log file for each task performed. These log files were then processed by Wireshark filters and string search queries to extract data of interest.

To be able to simplify and perform the analysis as effective as possible multiple filters were developed for each of the tasks with the device. These filters allowed us to quickly separate non relevant data from data that is actually interesting for our study. Non relevant data is for example keep alive packages communicated from the laptop to the device. Each filter used is listed below with description, followed by the filter code marked in bold text.

Strings	**Descriptions**
date, time	Looking for data containing package timestamps
location	Looking for data containing geographical location
username, user	Looking for username related data
password, pass	Looking for password related data
other username	Username of the user who messages were exchanged in task 5
username	Real users username, currently logged in on the device
password	Real users password, currently logged in on the device
SWF	Shockwave Flash
PNG, JNG, MNG	Portable/JPEG/Multiple-image Network Graphics
MP3	Audio file format
AAC	Advanced Audio Coding
ZIP	ZIP archive
GPX	Geotag for images from a GPS, the GPX file format contains a track log
NMEA	Global Positioning file (GPS)
KLM	Keyhole Markup Language, an XML notation for expressing geographic annotation.
CSR, CER	Stores certificates
SSH, PUB	OpenSSH private key, Secure Shell private key; format generated by ssh-keygen.
PPK	PuTTY private key ,Secure Shell private key, in the file format generated by PuTTYgen instead of the format used by OpenSSH.
KDB, KDBX	Encrypted password file created by KeePass password manager
BPW	Encrypted password file created by Bitser password manager
INI	Configuration text file
HTML	HyperText Markup Language
JSON	Data file format used by many programming languages
XML	An open data file format

Table 1: contains all the strings with description used for the string searches.

Filter 1 A filter was developed to hide packages to and from the host laptop as well as arp, icmp, dns, which are protocols that may produce background noise. Allowing us to focus on the traffic of interest from the Playstation 4 and the Internet. **!(ip.src==192.168.1.1)&&!(ip.dst==192.168.1.1)&&!(arp or icmp or dns)**.

Filter 2 To filter out only HTTP GET requests the following filter was written: **http.request**. This filter allowed us to filter out so that all remaining was the images.

Filter 3 The following filter was used to bring forth as much clear text communication as possible since the majority is sent over these protocols: **http or dns**.

Filter 4 This filter was built to be able to show only SSL encrypted packages to conclude if there were any communication conducted over old versions of this protocol: **ssl**.

3.4.2 Manual analysis

Finally manual analysis on the gathered data was conducted. The purpose of finding out what kind of information we were able to extract. For example clear text (unencrypted) messages or images from the collected packages and if there was any data to put together about the system or the systems users. To be able to search for a specific String in the gathered data packages the Wireshark Find Packet Tool was used. Accessed by clicking Edit -> Find Packet. This tool is similar to the filter: **tcp contains traffic** which displays all TCP packets that contain in this example the word 'traffic'.

Table 1 contains all the strings used for searching inside the collected packages. The strings consists of file types (written in capital letters), common privacy and security related keywords (written in lowercase letters) and finally (written in blue color) username and password for the currently logged in user as well as the username of the other user, where messages were exchanged in task 5. Each string are also followed by a short description [58]. The decision on which strings to use for the string searches is based out of the privacy section in the background.

4 Results

This chapter is conducted to present the results gathered during the experiment to answer if there are any data leakages in the communication between the Playstation 4 and the Internet. In that case what kind of information we are able to extract and how that is done. The results are broken down into sections based on the tasks in same order as mentioned in methodology chapter. Each section presents initially if any encrypted communication was conducted with outdated protocols, followed the result of those string queries previously described in Table. 1 where something was found.

4.1 Results from each tasks

4.1.1 Task 1: Log on the device

After the filter for ssl was applied we could conclude that one tenth of the packages displayed was sent over an old version of TLS more specifically version 1.0.

The results gathered from task 1 are as shown in table 2. First of which is the string "png", which resulted in that we got some cleartext urls to images and a couple of json tables containing URLs to images of different games and applications. One of the images found and its url is shown in figure 7. While searching for "user" we were able to find certificates with hashed values. The same jsons containing the URLs to images that was

Strings	Returned result
png	Cleartext url to images and Json containing URLs to images of different games
user	A couple of certificates containing hashed values
pass	Json containing URLs to images of different games
csr	Certificates found with encryption
cer	Certificates found with encryption
json	Containing URLs to images

Table 2: This table presents the strings that returned a result in task 1.

found while searching for “png” were also found when the search for “pass” and “json” was conducted. Searching for “csr” and “cer” resulted in certificates with a ssl encryption.

4.1.2 Task 2: Let the device stay on standby for one minute

After the filter for ssl was applied we could conclude that a couple of the packages displayed was sent over an old version of TLS more specifically version 1.0.

Strings	Returned result
user	Some certificates found containing encrypted values
cer	certificates found
pub	a couple encrypted pubkeys with key length in cleartext

Table 3: This table presents the strings that returned a result in task 2.

The results gathered from task 2 are as shown in table 3. While searching for “user” and “cer” a couple of certificates with encrypted content were found, one of which can be seen in figure 8. Searching for the string “pub” resulted in that a few pubkeys were found, but they were all encrypted. The length of the pubkeys was also found.

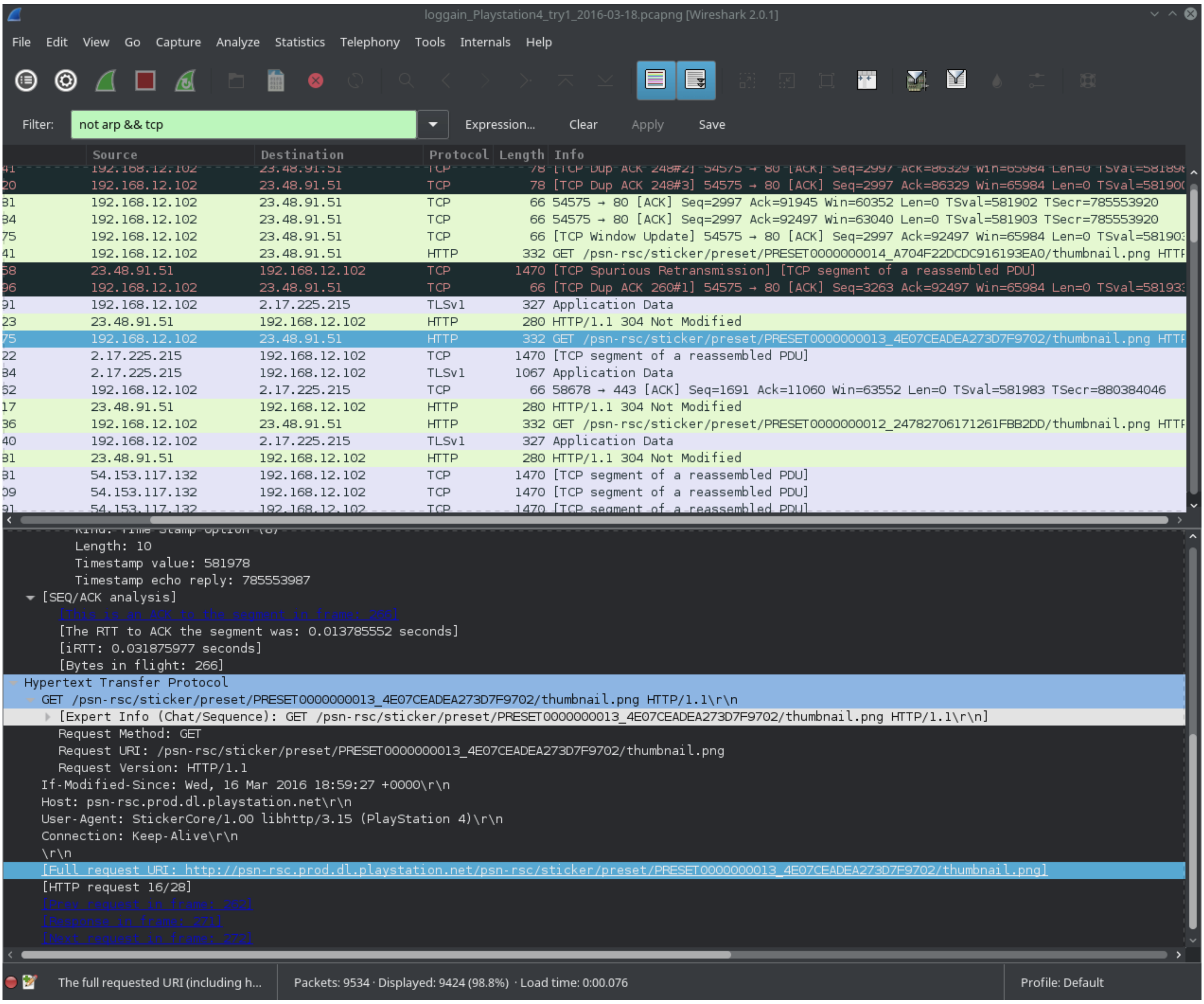
4.1.3 Task 3: Log in and out of Facebook, using the web browser on the device

After the filter for ssl was applied we found out that all the communication was exchanged with the latest version of TLS.

Strings	Returned result
cer	certificates found
pub	a few pubkeys, encrypted and with key length
ini	Facebook’s ip address, both ipv4 and ipv6

Table 4: This table presents the strings that returned a result in task 3.

The results gathered from task 3 are as shown in table 4. While searching for “cer” a couple of certificate containing encrypted data were found. Searching for “pub” returned a few pubkeys, but they were also encrypted. The length of the pubkey was also found.


loggain_Playstation4_try1_2016-03-18.pcapng [Wireshark 2.0.1]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression...
Clear
Apply
Save

Filter: not arp && tcp

```
    Source           Destination      Protocol Length Info
41  192.168.12.102   23.48.91.51      TCP        78 [TCP Dup ACK 248#2] 54575 → 80 [ACK] Seq=2997 Ack=86329 Win=65984 Len=0 TSval=58189
20  192.168.12.102   23.48.91.51      TCP        78 [TCP Dup ACK 248#3] 54575 → 80 [ACK] Seq=2997 Ack=86329 Win=65984 Len=0 TSval=58190
31  192.168.12.102   23.48.91.51      TCP        66 54575 → 80 [ACK] Seq=2997 Ack=91945 Win=60352 Len=0 TSval=581902 TSecr=785553920
34  192.168.12.102   23.48.91.51      TCP        66 54575 → 80 [ACK] Seq=2997 Ack=92497 Win=63040 Len=0 TSval=581903 TSecr=785553920
75  192.168.12.102   23.48.91.51      TCP        66 [TCP Window Update] 54575 → 80 [ACK] Seq=2997 Ack=92497 Win=65984 Len=0 TSval=58190
41  192.168.12.102   23.48.91.51      HTTP      332 GET /psn-rsc/sticker/preset/PRESET0000000014_A704F22DCDC916193EA0/thumbnail.png HTT
58  23.48.91.51      192.168.12.102   TCP      1470 [TCP Spurious Retransmission] [TCP segment of a reassembled PDU]
96  192.168.12.102   23.48.91.51      TCP        66 [TCP Dup ACK 260#1] 54575 → 80 [ACK] Seq=3263 Ack=92497 Win=65984 Len=0 TSval=58193
91  192.168.12.102   2.17.225.215     TLSv1     327 Application Data
23  23.48.91.51      192.168.12.102   HTTP      280 HTTP/1.1 304 Not Modified
75  192.168.12.102   23.48.91.51      HTTP      332 GET /psn-rsc/sticker/preset/PRESET0000000013_4E07CEADEA273D7F9702/thumbnail.png HTT
22  2.17.225.215     192.168.12.102   TCP      1470 [TCP segment of a reassembled PDU]
34  2.17.225.215     192.168.12.102   TLSv1    1067 Application Data
62  192.168.12.102   2.17.225.215     TCP        66 58678 → 443 [ACK] Seq=1691 Ack=11060 Win=63552 Len=0 TSval=581983 TSecr=880384046
17  23.48.91.51      192.168.12.102   HTTP      280 HTTP/1.1 304 Not Modified
36  192.168.12.102   23.48.91.51      HTTP      332 GET /psn-rsc/sticker/preset/PRESET0000000012_24782706171261FBB2DD/thumbnail.png HTT
40  192.168.12.102   2.17.225.215     TLSv1     327 Application Data
31  23.48.91.51      192.168.12.102   HTTP      280 HTTP/1.1 304 Not Modified
31  54.153.117.132   192.168.12.102   TCP      1470 [TCP segment of a reassembled PDU]
09  54.153.117.132   192.168.12.102   TCP      1470 [TCP segment of a reassembled PDU]
91  54.153.117.132   192.168.12.102   TCP      1470 [TCP segment of a reassembled PDU]
```

```
        Kind: Time Stamp Option (8)
        Length: 10
        Timestamp value: 581978
        Timestamp echo reply: 785553987
  ▾ [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 266]
      [The RTT to ACK the segment was: 0.013785552 seconds]
      [iRTT: 0.031875977 seconds]
      [Bytes in flight: 266]
▾ Hypertext Transfer Protocol
  ▾ GET /psn-rsc/sticker/preset/PRESET0000000013_4E07CEADEA273D7F9702/thumbnail.png HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /psn-rsc/sticker/preset/PRESET0000000013_4E07CEADEA273D7F9702/thumbnail.png HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /psn-rsc/sticker/preset/PRESET0000000013_4E07CEADEA273D7F9702/thumbnail.png
      Request Version: HTTP/1.1
    If-Modified-Since: Wed, 16 Mar 2016 18:59:27 +0000\r\n
    Host: psn-rsc.prod.dl.playstation.net\r\n
    User-Agent: StickerCore/1.00 libhttp/3.15 (PlayStation 4)\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://psn-rsc.prod.dl.playstation.net/psn-rsc/sticker/preset/PRESET0000000013_4E07CEADEA273D7F9702/thumbnail.png]
    [HTTP request 16/28]
    [Prev request in frame: 262]
    [Response in frame: 271]
    [Next request in frame: 272]
```

The full requested URI (including h... | Packets: 9534 · Displayed: 9424 (98.8%) · Load time: 0:00.076 | Profile: Default

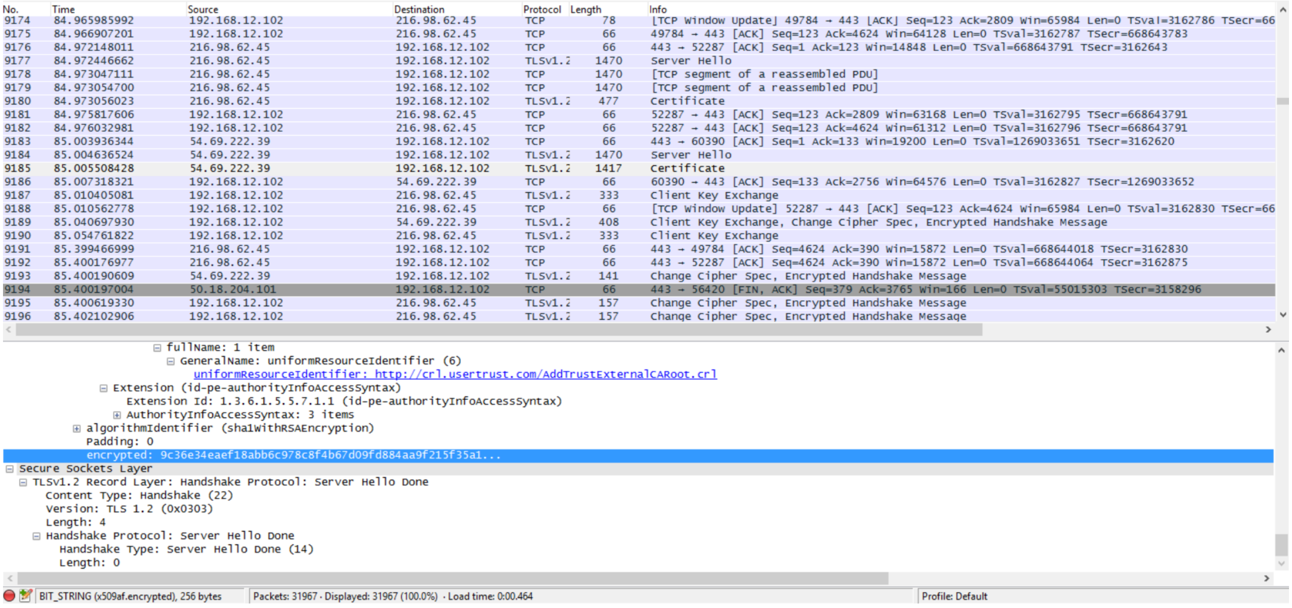
Figure 7: Get request for a png files url in cleartext acquired during task 1.

When "ini" was used as the search string, we were able to locate IP addresses both IPv4 and IPv6 for Facebook's european server.

4.1.4 Task 4: Download a free application on the Playstation store

After the filter for ssl was applied we could conclude that almost one third of the packages displayed was sent over an old version of TLS more specifically version 1.0.

The results gathered from task 4 are as shown in table 5. Searching for "user" resulted in a json file containing the downloaded applications name in different languages and



```
No.   Time         Source          Destination     Protocol Length Info
9174  84.965985992 192.168.12.102  216.98.62.45    TCP        78   [TCP Window Update] 49784 → 443 [ACK] Seq=123 Ack=2809 Win=65984 Len=0 TSval=3162786 TSecr=66
9175  84.966907201 192.168.12.102  216.98.62.45    TCP        66   49784 → 443 [ACK] Seq=123 Ack=4624 Win=64128 Len=0 TSval=3162787 TSecr=668643783
9176  84.972148011 216.98.62.45    192.168.12.102  TCP        66   443 → 52287 [ACK] Seq=1 Ack=123 Win=14848 Len=0 TSval=668643791 TSecr=3162643
9177  84.972446662 216.98.62.45    192.168.12.102  TLSv1.2  1470   Server Hello
9178  84.973047111 216.98.62.45    192.168.12.102  TCP      1470   [TCP segment of a reassembled PDU]
9179  84.973054700 216.98.62.45    192.168.12.102  TCP      1470   [TCP segment of a reassembled PDU]
9180  84.973056023 216.98.62.45    192.168.12.102  TLSv1.2   477   Certificate
9181  84.975817606 192.168.12.102  216.98.62.45    TCP        66   52287 → 443 [ACK] Seq=123 Ack=2809 Win=63168 Len=0 TSval=3162795 TSecr=668643791
9182  84.976032981 192.168.12.102  216.98.62.45    TCP        66   52287 → 443 [ACK] Seq=123 Ack=4624 Win=61312 Len=0 TSval=3162796 TSecr=668643791
9183  85.003936344 54.69.222.39    192.168.12.102  TCP        66   443 → 60390 [ACK] Seq=1 Ack=133 Win=19200 Len=0 TSval=1269033651 TSecr=3162620
9184  85.004636524 54.69.222.39    192.168.12.102  TLSv1.2  1470   Server Hello
9185  85.005508428 54.69.222.39    192.168.12.102  TLSv1.2  1417   Certificate
9186  85.007318321 192.168.12.102  54.69.222.39    TCP        66   60390 → 443 [ACK] Seq=133 Ack=2756 Win=64576 Len=0 TSval=3162827 TSecr=1269033652
9187  85.010405081 192.168.12.102  216.98.62.45    TLSv1.2   333   Client Key Exchange
9188  85.010562778 192.168.12.102  216.98.62.45    TCP        66   [TCP Window Update] 52287 → 443 [ACK] Seq=123 Ack=4624 Win=65984 Len=0 TSval=3162830 TSecr=66
9189  85.040697930 192.168.12.102  54.69.222.39    TLSv1.2   408   Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
9190  85.054761822 192.168.12.102  216.98.62.45    TLSv1.2   333   Client Key Exchange
9191  85.399466999 216.98.62.45    192.168.12.102  TCP        66   443 → 49784 [ACK] Seq=4624 Ack=390 Win=15872 Len=0 TSval=668644018 TSecr=3162830
9192  85.400176977 216.98.62.45    192.168.12.102  TCP        66   443 → 52287 [ACK] Seq=4624 Ack=390 Win=15872 Len=0 TSval=668644064 TSecr=3162875
9193  85.400190609 54.69.222.39    192.168.12.102  TLSv1.2   141   Change Cipher Spec, Encrypted Handshake Message
9194  85.400197004 50.18.204.101   192.168.12.102  TCP        66   443 → 56420 [FIN, ACK] Seq=379 Ack=3765 Win=166 Len=0 TSval=55015303 TSecr=3158296
9195  85.400619330 192.168.12.102  216.98.62.45    TLSv1.2   157   Change Cipher Spec, Encrypted Handshake Message
9196  85.402102906 192.168.12.102  216.98.62.45    TLSv1.2   157   Change Cipher Spec, Encrypted Handshake Message

                ⊟ fullName: 1 item
                  ⊟ GeneralName: uniformResourceIdentifier (6)
                      uniformResourceIdentifier: http://crl.usertrust.com/AddTrustExternalCARoot.crl
            ⊟ Extension (id-pe-authorityInfoAccessSyntax)
                Extension Id: 1.3.6.1.5.5.7.1.1 (id-pe-authorityInfoAccessSyntax)
              ⊞ AuthorityInfoAccessSyntax: 3 items
        ⊞ algorithmIdentifier (sha1WithRSAEncryption)
          Padding: 0
          encrypted: 9c36e34eaef18abb6c978c8f4b67d09fd884aa9f215f35a1...
⊟ Secure Sockets Layer
  ⊟ TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 4
    ⊟ Handshake Protocol: Server Hello Done
        Handshake Type: Server Hello Done (14)
        Length: 0

BIT_STRING (x509af.encrypted), 256 bytes | Packets: 31967 · Displayed: 31967 (100.0%) · Load time: 0:00.464 | Profile: Default
```

Figure 8: A certificate acquired during task 2.

Strings	Returned result
user	Found a json file with the downloaded applications name in different language the applications icon
cer	multiple certificates found
ppk	json containing pkg files
pub	a couple pubkeys, encrypted and with key length
json	json file with the downloaded applications name in different language and the applications icon. Also another json with pkg files inside.

Table 5: This table presents the strings that returned a result in task 4.

the applications icon. Searching for the string “cer” returned a couple of certificates with encrypted content. While searching for “pub” a few pubkeys were found, but they were also encrypted. The length of the pubkey was also found. “ppk” resulted in a json containing pkg files. Pkg file type contains instructions on how to create SIS files on a Symbian OS device, including the vendor name, software dependencies, and application files to copy; stored in a plain text format [62]. And by searching for “json” we got two jsons, the first one was the same as the one we got while searching for “user” and the second one was the same as the one we got while searching for “ppk”.

4.1.5 Task 5: Exchange messages with another user using the Playstation chat

After the filter for ssl was applied we could conclude that nearly half of the packages displayed was sent over an old version of TLS more specifically version 1.0.

Strings	**Returned result**
png	picture of users avatar
aac	certificate
user	some certificate, image of users avatar
cer	multiple certificates found
ppk	found a json, containing pkg files
pub	a certificate

Table 6: This table presents the strings that returned a result in task 5.

The results gathered from task 5 are as shown in table 6. Searching for “png” resulted in that we were able to obtain the user’s profile picture shown in figure 9. And while searching for “aac”, “cer” and “pub” a couple of certificate containing encrypted data were found. “ppk” resulted in a json containing pkg files. And we searched for “user” we once again got the user’s profile picture and also a few certificate containing encrypted data.

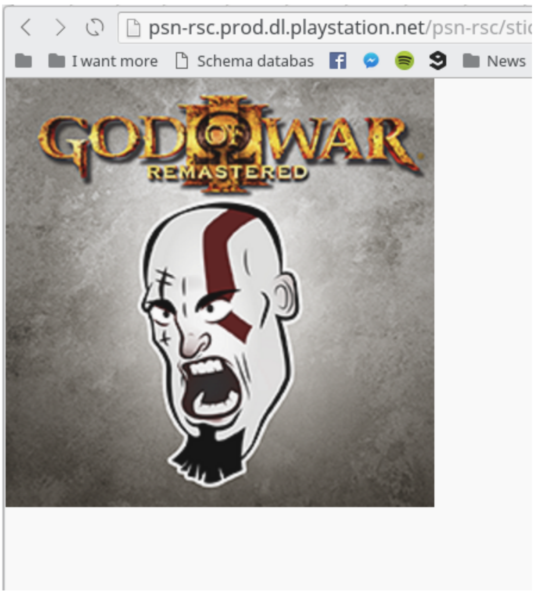


Figure 9: This image is the profile picture of one of the users in the chat session acquired during task 5.

4.1.6 Task 6: Play an online game for five minutes

After the filter for ssl was applied we found out that all the communication was exchanged with the latest version of TLS.

The results gathered from task 6 are as shown in table 7. While searching for “user” and “cer” a couple of certificate containing encrypted data were found. And searching for “pub” resulted in a few pubkeys, but they were also encrypted. The length of the pubkey was also found. Searching for “png” and “pass” resulted in a couple of pictures from the

Strings	Returned result
png	found about 20 images
user	some certificate
pass	found a few images
cer	multiple certificates found
pub	a couple pubkeys, encrypted and with key length
json	found a json file containing the game name also an icon and a background picture

Table 7: This table presents the strings that returned a result in task 6.

game itself. And finally while searching for json we got a json file with the game name and an icon and a background picture.

4.2 Summarization of the results

This section aims to summarize the results.

Tasks	Data leakages	No data leakages
Task 1	x	
Task 2		x
Task 3	x	
Task 4	x	
Task 5	x	
Task 6		x

Table 8: This table shows what tasks contained data leakages and which ones did not.

Table 8 illustrates a summarization of the results gathered during the experiments. It shows that 66% of the tasks analysed had at least one data leakage. All the tasks where there were data leakages, leaked images. As discussed in the security and privacy section in the background chapter, images could contain sensitive data about the user or the user's system. For the Wireshark dump files containing the complete data, see Appendix B.

References

[1] Alam, M. R., Reaz, M. B. I., Ali, M. A. M., Nov 2012. A review of smart homes 2014;past, present, and future. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews).

[2] Alexa, 2016. The top 500 sites on the web. `http://www.alexa.com/topsites`, Accessed: 2016-04-09.

[3] Alliance, Z., 2015. Open standards development. `http://www.zigbee.org/zigbeealliance/developing-standards/`, Accessed: 2016-04-08.

[4] Balta-Ozkan, N., Davidson, R., Bicket, M., Whitmarsh, L., 2013. Social barriers to the adoption of smart homes. Energy Policy.

[5] Brezovan, M., 2013. An overview of smart home environments: Architectures, technologies and applications.

[6] Brezovan, M., Badica, C., May 2013. A review on vision surveillance techniques in smart home environments. In: Control Systems and Computer Science (CSCS), 2013 19th International Conference on.

[7] Brush, A. B., Lee, B., Mahajan, R., Agarwal, S., Saroiu, S., Dixon, C., 2011. Home automation in the wild: Challenges and opportunities. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM.

[8] Brush, A. B., Lee, B., Mahajan, R., Agarwal, S., Saroiu, S., Dixon, C., 2011. Home automation in the wild: Challenges and opportunities. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM.

[9] Council, P. S. S., 2015. Migrating from ssl and early tls.

[10] Danova, T., 2014. The connected-home report: Forecasts and growth trends for the leading 'internet of things' market. `http://uk.businessinsider.com/connected-home-forecasts-and-growth-2014-9`, Accessed: 2016-04-08.

[11] database, N. V., 2014. National cyber awareness system. `https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566`, Accessed: 2016-04-08.

[12] de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., Blondel, V. D., 2013. Unique in the crowd: The privacy bounds of human mobility. Scientific reports.

[13] Deng, J., Han, R., Mishra, S., Sept 2005. Countermeasures against traffic analysis attacks in wireless sensor networks. In: Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on.

[14] e Time Stamp, 2015. How a digital timestamp works. https://www.digistamp.com/technical/how-a-digital-time-stamp-works/, Accessed: 2016-04-08.

[15] ENISA, E., 2015. Are smart homes cyber-security smart? https://www.enisa.europa.eu/media/press-releases/are-smart-homes-cyber-security-smart, Accessed: 2016-04-08.

[16] Gavison, R., 1980. Privacy and the limits of law. The Yale Law Journal.
URL http://www.jstor.org/stable/795891

[17] Gustafsson, R., Janstad, L., 2015. Säkerhetsutvärdering av smarta dörrlås utifrån ett kommunikationsperspektiv.

[18] Hernandez, G., Arias, O., Buentello, D., Jin, Y., 2014. Smart nest thermostat: A smart spy in your home. Black Hat USA.

[19] Hoque, M. E., Rahman, F., Ahamed, S. I., Liu, L., 2009. Trust based security auto-configuration for smart assisted living environments. In: Proceedings of the 2Nd ACM Workshop on Assurable and Usable Security Configuration. ACM.

[20] Hussain, F., 2015. Samsung smart refrigerator hacked, left gmail login credentials vulnerable. https://www.hackread.com/samsung-smart-refrigerator-gmail-login-hack/, Accessed: 2016-04-08.

[21] iControl Networks, 2015. 2015 state of the smart home report Statistics on entertainment area in smart homes.

[22] James, D., Rivington, J., 2016. Playstation 4 is a fantastic console that's improved with age. http://www.techradar.com/reviews/gaming/games-consoles/sony-ps4-1131803/review, Accessed: 2016-04-08.

[23] Jiang, L., Anantharam, V., Walrand, J., 2008. Efficiency of selfish investments in network security. In: Proceedings of the 3rd International Workshop on Economics of Networked Systems.

[24] Kientz, J. A., Patel, S. N., Jones, B., Price, E., Mynatt, E. D., Abowd, G. D., 2008. The georgia tech aware home. In: CHI '08 Extended Abstracts on Human Factors in Computing Systems. ACM.

[25] Mennicken, S., Vermeulen, J., Huang, E. M., 2014. From today's augmented houses to tomorrow's smart homes: New directions for home automation research. In: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing. ACM.

[26] Mills, E., 2012. Time stamp bug exposes photos on locked iphone. http://www.cnet.com/news/time-stamp-bug-exposes-photos-on-locked-iphone/, Accessed: 2016-04-08.

[27] Networking, L., 2008. A guide to network topology. http://learn-networking.com/network-design/a-guide-to-network-topology, Accessed: 2016-04-08.

[28] Notra, S., Siddiqi, M., Gharakheili, H. H., Sivaraman, V., Boreli, R., Oct 2014. An experimental study of security and privacy risks with emerging household appliances. In: Communications and Network Security (CNS), 2014 IEEE Conference on.

[29] oblique, 2014. create_ap. https://github.com/oblique/create_ap, Accessed: 2016-04-09.

[30] Ordoñez, S., 2014. Hackers can get into your refrigerator, too. http://www.cnbc.com/2014/01/17/hackers-attack-home-appliances-including-your-refrigerator.html, Accessed: 2016-04-08.

[31] Palmer, J., 2013. Mobile location data 'present anonymity risk'. http://www.bbc.com/news/science-environment-21923360, Accessed: 2016-04-08.

[32] Rubenfeld, J., 1989. The right of privacy. Harvard Law Review.
URL http://www.jstor.org/stable/1341305

[33] Rutherfoord, R. H., Rutherfoord, J. K., 2010. Privacy and ethical concerns in internet security. In: Proceedings of the 2010 ACM Conference on Information Technology Education.

[34] Seaman, C. B., Jul 1999. Qualitative methods in empirical studies of software engineering. IEEE Transactions on Software Engineering.

[35] Spinello, R., 2010. Cyberethics: Morality and law in cyberspace. Jones & Bartlett Learning.

[36] Storm, D., 2012. Hackers create pixsteal trojan to copy all photos from your pc, then blackmail you. http://www.computerworld.com/article/2473399/cybercrime-hacking/hackers-create-pixsteal-trojan-to-copy-all-photos-from-your-pc-then-blackmail-yo.html, Accessed: 2016-04-08.

[37] Taleb, T., Bottazzi, D., Guizani, M., Nait-Charif, H., May 2009. Angelah: a framework for assisting elders at home. IEEE Journal on Selected Areas in Communications.

[38] Taylor, A., 2011. What is personal data? http://www.seqlegal.com/blog/what-personal-data, Accessed: 2016-04-08.

[39] Trapp, B., 2014. Monitoring android traffic with wireshark. Linux J.

[40] Velentzas, R., Marsh, A., Min, G., 2008. Wireless connected home with integrated secure healthcare services for elderly people. In: Proceedings of the 1st International Conference on PErvasive Technologies Related to Assistive Environments.

[41] Vidgren, N., Haataja, K., Patiño-Andres, J. L., Ramírez-Sanchis, J. J., Toivanen, P., Jan 2013. Security threats in zigbee-enabled systems: Vulnerability evaluation, practical experiments, countermeasures, and lessons learned. In: System Sciences (HICSS), 2013 46th Hawaii International Conference on.

[42] Wu, C. L., Liao, C. F., Fu, L. C., March 2007. Service-oriented smart-home architecture based on osgi and mobile-agent technology. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews).

[43] Yoshigoe, K., Dai, W., Abramson, M., Jacobs, A., Dec 2014. Overcoming invasion of privacy in smart home environment with synthetic packet injection. In: TRON Symposium (TRONSHOW), 2015.

[44] Young, C., 2014. Smart home invasion. https://www.iotvillage.org/slides_DC23/, Accessed: 2016-04-08.

Appendices

(A) Create_Ap script - A shell script to create a NATed/Bridged Software Access Point

https://github.com/oblique/create_ap

(B) Experimental tasks Wireshark dump files for each task performed.

https://drive.google.com/open?id=0BxJ1ec4LM8hfODRqVFp4NDVfRjQ