

IoT Smart Home Device's Security, Privacy, and Firmware Labeling System

A Dissertation

Presented in Partial Fulfillment of the Requirements for the

Degree of Doctor of Philosophy

with a

Major in Computer Science

in the

College of Graduate Studies

University of Idaho

By

Naif Rajkhan

Approved by:

Major Professor: Jia Song, Ph.D.

Committee Members: Terence Soule, Ph.D.; Xiaogang (Marshall) Ma, Ph.D.;

Dilshani Sarathchandra, Ph.D.

Department Administrator: Terence Soule, Ph.D.

August 2022

Abstract

A smart home is one of the most popular Internet of Things (IoT) implementations. It is widely used because of the autonomous functions it provides to homeowners. It is equipped with smart IoT devices designed to automatically perform unique and specific functions. The IoT smart home network has different types of connections based on the application's requirements. Any attacks or unauthorized access to IoT smart home systems or connected devices could harm the system and lead to unauthorized access to the homeowner's information. Therefore, IoT smart home devices' security, privacy, and firmware vulnerabilities are getting more attention from researchers because of the danger that comes from attacking such devices that collect personal information about an individual's lifestyle and behavior.

This research aims to provide an IoT labeling system that covers the IoT smart home devices' security, privacy, and firmware factors. This label will target the Saudi Arabian market. The label will help IoT smart home device consumers make better decisions on which device to purchase and increase their awareness of the attacks and, therefore, use the devices more safely. Based on a review of the literature on IoT smart home devices' security, privacy, and firmware aspects, a data collection and analysis process is used to demonstrate the importance of the factors on the label. A scoring system is designed to provide a weight for all chosen factors. An online survey is conducted and distributed among computer science and security experts, regular IoT consumers, risk management and communication experts, and label designers across Saudi Arabia and the United States to develop a better labeling system for the devices. This survey produces the best quality of the IoT smart home device's security, privacy, and firmware label. The proposed label is expected to help the IoT smart home device's consumers be educated and aware of the potential issues associated with the smart home devices, hence protecting them from being a victim of many problems and attacks when using the devices.

Acknowledgments

First and foremost, I must thank Allah the almighty for giving me the ability and success to accomplish this dissertation. Without Allah's blessings and favor, this dissertation would not be achieved.

I would like to thank my advisor, Dr. Jia Song, for her support, encouragement, patience and guidance throughout my graduate studies. Her supervision and support drove me to conduct the research, gain comprehensive knowledge, write, and complete this dissertation. Without her guidance throughout the days and years, I would not imagine finishing or conducting the research. She has the talent that any researcher dreams of in their research advisor. I am proud of being one of Dr. Song's students.

I would also like to thank my other committee members, Dr. Soule and Dr. Marshall, for their support and valuable comments on my dissertation. I appreciate your time and effort in all my classes with you; you are my ideal professor. Also, I want to thank Dr. Dilshani for her support and cooperation in the survey work. Thank you for being a very useful and quick responder.

I would Like Mr. Mohammad Khayat for his significant label design development.

I want to thank the Saudi Culture Mission and King Abdulaziz University for their support and funding of my studies at UI and finish this dissertation.

Finally, I would like to thank the Department of Computer Science staff for their help during my study. I want to thank all the College of Graduate Studies team for their help and support throughout my research at UI.

Dedication

I dedicated this work to my dearest parents, my father, Waheb Rajkhan, and my mother, Sahar Rajkhan. I do not have the words to express my gratitude and appreciation for their enormous sacrifice, patience, support, encouragement, care, interest, trust, and raising me.

Also, this work is dedicated to the love of my life, my soulmate Samaher Othman. Thank you for being with me, through the good and bad. Thank you for being my pillar when everything was shaking. I appreciate your support, patience, and taking care of our son Awss during my studies and taking care of our coming babies Sahar and Mariam. Also, I dedicated this work to my brothers Asem and Bandar, and my sisters Fatimah and nouf, my aunts Jihan, Afaf, and Amerah, my father-in-law Ahmed and mother-in-law Samerah, my dear uncles Talal and Mahmoud Saati for their understanding, support, encouragement, and love which have helped me through this gurney.

Table of Content

Abstract	ii
Acknowledgments	iii
Dedication	iv
List of Tables	viii
List of Figures	ix
Chapter 1: Introduction	1
1.1 IoT Smart Home challenges and concerns	2
1.2 Security issues related to IoT smart homes	3
1.2.1 Weak or bypass-able node authentication and identification	4
1.2.2 Weak security and privacy protection to the end users	5
1.2.3 Lack of security, privacy, and firmware information for users	5
1.3 The research problem statements and objectives	6
1.3.1 Problem statements	6
1.3.2 Dissertation objectives	8
1.3.3 Dissertation Contributions and Timeline	10
1.3.4 Dissertation Overview	11
Chapter 2: Background and Related Work	12
2.1 Background	12
2.1.1 IoT smart home architecture	12
2.1.2 Communications in IoT smart home systems	13
2.1.3 Node authentication mechanisms in smart homes	14
2.1.4 IoT smart home devices	15
2.2 Related work	15

2.2.1	IoT smart home devices analysis procedures	15
2.2.2	IoT smart home devices label	17
Chapter 3: Methodology		21
3.1	Phase 1: Information collection	22
3.1.1	Collecting information from different Sources	22
3.1.2	Firmware Security and Privacy Analysis	24
3.1.3	Experimental Environment Setup	24
3.1.4	Current IoT smart home devices labeling system's content	26
3.2	Phase 2: Scoring system	30
3.2.1	Scoring Rubric	30
3.2.2	Security, privacy, and firmware factors scoring description	34
3.2.3	Scoring grades range	34
3.2.4	Example: Device "XY"	35
3.3	Phase 3: Survey	35
Chapter 4: The survey implementation		39
4.1	Survey for experts and Scientists with computer science backgrounds	40
4.2	Survey for regular consumers	51
4.3	Social data analysis, risk management researchers, and label's design experts	65
4.4	The final versions for the IoT smart home devices security, privacy, and firmware labels	67
Chapter 5: The Implementation of the IoT smart home devices security, privacy, and firmware label		69
Chapter 6: Conclusion and Future Work		81
6.1	Conclusion	81
6.2	Future Work	81

References	83
Appendices	86

List of Tables

Table 1: IoT Smart Home applications challenges	2
Table 2: Classification of Authentication threats and attacks	5
Table 3: IoT smart home devices examples	15
Table 4: Summarized label overview	27
Table 5: Second label overview	29
Table 6: Internet pairing technology	31
Table 7: Configuration and authentication	31
Table 8: Update modes	32
Table 9: Exposed services	32
Table 10: Vulnerabilities	33
Table 11: Protocols	33
Table 12: Network encryption	33
Table 13: Security, privacy, and firmware factors scoring	34
Table 14: Scoring grades range	35
Table 15: Factors Range levels	47
Table 16: Internet Pairing Technology ranges	47
Table 17: Configuration and Authentication ranges	47
Table 18: Update modes ranges	48
Table 19: Exposed services ranges	48
Table 20: Firmware Vulnerabilities ranges	48
Table 21: Protocol ranges	48
Table 22: Network encryption ranges	48
Table 23: Final scores calculations	77

List of Figures

Figure 1: The water efficiency label and the energy efficiency labels	7
Figure 2: IoT Smart Home Architecture	13
Figure 3: Linux kernel versions 2.6.21 vulnerabilities	25
Figure 4: Linux kernel versions 3.10.1 vulnerabilities	26
Figure 5: Highest completed level of education	41
Figure 6: Experience in the Computer Science or Data Security field (in years)	41
Figure 7: Security and privacy factor's score representation	42
Figure 8: General information section content	43
Figure 9: Technical specifications section content	44
Figure 10: Security and privacy factors	45
Figure 11: Final security and privacy score	45
Figure 12: The IoT smart home security, privacy, and firmware summarized label (experts version)	49
Figure 13: The IoT smart home security, privacy, and firmware detailed label (experts version)	50
Figure 14: Age	52
Figure 15: Highest completed level of education	52
Figure 16: Familiarity with computer security and privacy issues	52
Figure 17: Passwords changing period	53
Figure 18: Changing default username and password	53
Figure 19: Software updates check	54
Figure 20: Summarized label most important section	55
Figure 21: Summarized label is enough	55
Figure 22: Detailed label preferred section	56

Figure 23: Reading the detailed label	57
Figure 24: Labeling sponsor	58
Figure 25: Data sensing procedures	59
Figure 26: Trusting the label's information	59
Figure 27: IoT smart home devices preferences	60
Figure 28: Security and privacy fears	61
Figure 29: Get information about the device	62
Figure 30: Purchase factors	63
Figure 31: Purchase non-secure IoT devices	63
Figure 32: The IoT smart home security, privacy, and firmware summarized label (final version)	67
Figure 33: The IoT smart home security, privacy, and firmware detailed label (final version)	68
Figure 34: Local Wi-Fi network credentials	69
Figure 35: Choose the smart home Wi-Fi network	69
Figure 36: Install the combined application	70
Figure 37: Add the device using the QR code inside the box	70
Figure 38: Create a new account	71
Figure 39: Activate the new account	71
Figure 40: Access permission request	72
Figure 41: Auto-update mode availability	72
Figure 42: All device's functions	72
Figure 43: CVSS for default network credentials vulnerability	73
Figure 44: CVSS for UPnP cannot be disabled vulnerability	74
Figure 45: MAC ID sticker	74
Figure 46: CVSS for MAC address access vulnerability	75

Figure 47: Local device's network access	75
Figure 48: HTTPS protocol availability	76
Figure 49: The IoT smart home security, privacy, and firmware summarized label (smart plug)	78
Figure 50: The IoT smart home security, privacy, and firmware detailed label (smart plug)	79
Figure 51: The IoT smart home security, privacy, and firmware summarized label on the package	80

Chapter 1: Introduction

Nowadays, most of the human industries' developments and innovations that have been used to simplify and facilitate any simple or complex tasks are supported by technology procedures, especially the tasks performed daily. Internet of Things (IoT) deals with connecting devices and physical objects, also known as "things." The IoT devices are usually embedded with sensors, software/firmware, or other technologies to automatically connect and communicate with other devices or the control system in the network to exchange information. IoT is one of the most valuable and exciting technologies in recent years because of the great makings of the connected automated systems and its ability to be adopted and combined with other technologies [1]. This technology opens a new field to create solutions for many obstacles that lack affordable solutions that regular people can adopt and purchase.

IoT smart home is a home automation system that utilizes IoT devices. It collects data from smart home devices for monitoring and controlling the devices via the internet. Under certain situations, it can automatically activate or deactivate a smart home device. For example, smart lights can be turned on or off based on the room occupancy and the location of the individuals inside the room. IoT smart homes present a spectacular improvement in quality of living and intelligent benefits from using its customized applications to save time, money, and human interactions. If a smart thermostat is installed at home, homeowners can turn the heating and cooling system on and off to adjust room temperature via phone or voice, even if the user is not at home. Some smart thermostats can even learn the owner's habits and automatically set unique environment customization before they arrive.

Moreover, IoT smart homes are supported by other advanced technologies to provide a better user experience for homeowners. For instance, the intelligent personal assistant "Alexa," developed by Amazon, has been installed in many IoT smart home devices. It provides a service center that connects and controls IoT smart home devices in the same network [4]. "The smart floor" aims to identify the individual's identity and exact location inside the IoT smart home environment based on their footsteps [5].

IoT smart home research has been adopted internationally since the early 2000s. The enhancement of smart technologies makes our lives easier and more comfortable, and people are interested in spending money to keep up with modern and intelligent technologies. Therefore, IoT smart home market is growing enormously. A report estimates that by 2024 more than 53% of North Americans will live in IoT smart homes [2]. Famous global companies such as Samsung Electronics, Amazon, and Google provide different types of IoT smart home services and products to take advantage

of this rapidly growing market. The Compound Annual Growth Rate (CAGR) of this market in Saudi Arabia from 2017 to 2022 is 28.69% which was 25.76% from 2012 to 2017 [26].

1.1 IoT Smart Home challenges and concerns

Most IoT smart home devices are the “stand alone” kind, such as a smart bulb or smart plug, which ought to be safe, secure, and do not have any limitations. Unfortunately, this is not true. IoT smart home devices have certain restrictions, and there are some challenges associated with using them. Table 1 summarizes the IoT smart home challenges and concerns [1].

Table 1: IoT Smart Home applications challenges [1]

IoT smart home applications challenges	
Hardware limitation	<ul style="list-style-type: none"> • Motion sensors. • No RAMs. • Remote controlling. • Handling expiration of DHCP IP address.
Device connectivity	<ul style="list-style-type: none"> • A huge number of new devices from manufacturers. • No standards. • No standard communication protocols.
Data management	<ul style="list-style-type: none"> • Interpretable by machines. • Collect personal information about human life and behavior.
Machine learning	<ul style="list-style-type: none"> • Decision-making capabilities. • Status of the device. • Data prediction.
Habit and lifestyle	<ul style="list-style-type: none"> • Record user behavior. • Classify patterns based on position and energy information.

Unfaithful manufacturers: Seeking a secure and safe home is challenging these days because of the amount of information collected from individuals. Most social media and search engines contain user preferences to support their business. The situation worsens when the user is not aware of the sensitive data collected from unsecured devices. Security and privacy are the individuals' responsibilities in the first place. Allowing permission for any untrusted application or device to access personal information should be denied. The IoT smart home device vendors are accelerating their business by developing new products that support human beings' quality of life. However, not all of them follow the high security and privacy standards that meet the end users' expectations.

Sensitive information in the IoT smart home systems: Many things could happen by attacking IoT smart home devices. The amount of information that could be accessed is enormous. The data often includes sensitive personal information about homeowners such as email addresses, phone

numbers or contact lists, private pictures and videos, valued documents, messages, etc. The situation might worsen if the hacker uses this accessed data to blackmail the owner for any reason.

Controlling the IoT smart home devices: IoT smart home systems connect the devices to the central control center. By collecting data from different smart home devices, the central control center can analyze the collected information, make decisions, and control devices in this environment. For example, if the device collected room occupancy information and learned that nobody is at home then the central control center may alert the homeowner and shut down the air conditioner to save energy. Because the central control center is powerful and can control many smart home devices, if someone hacks into the system, the intruder can do many things, such as control certain smart home devices to mess up the home environment or even cause problems and harms to the system. For example, a hacker hacked into a stuffed cat which was equipped with Alexa with a Bluetooth device and speaker to order cat food [18].

Lack of international standards in IoT smart home devices manufacturing: The IoT smart home devices market is growing rapidly and internationally. There are large scale manufacturers such as Samsung Electronics, Amazon, and google who follow the ISO/IEC 30141 standards in their designs. ISO/IEC 30141 provides a standardized IoT reference architecture using a common IoT vocabulary and reusable development designs along with industry best practices [51]. Their products are highly adopted among IoT smart homeowners because of the enormous numbers of IoT devices using the same system as their embedded features such as Samsung speakers that could be accessed by Alexa, a product from another manufacturer. However, there are no international standards available for IoT smart home devices. No international organization monitors the launched products for any security and privacy aspects. So, vendors can sell their products without showing that they meet specific standards or proving they have implemented a security mechanism to protect sensitive data collected by the device. In addition, vendors are selling their products locally and internationally through a low-cost market and leaving the consumers at their own risk without any protection.

1.2 Security issues related to IoT smart homes

Individuals and organizations around the world recognize Cyber attacks. These attacks happen every minute and may not be noticed from the hacked systems [20]. These attacks could be identified and counted using special software in influential organizations. According to the United States FBI, on the 1st of January 2015, there were 42 committed random attacks in just an hour, 1000 in a day, 3000 in a month, and 0.36 million in a year. The surprising fact is that these numbers increased by 300% in

January 2016. Additionally, annual Cyber crime reports that 1.1 million web attacks were committed in just one day [20]. This significant number of attacks estimates today's massive numbers of cyberattacks; as IoT smart homes are widely used, many cyberattacks also target the IoT smart homes systems.

This section summarizes the major security issues related to IoT smart homes, such as weak node authentication and identification, weak security and privacy protection.

1.2.1 Weak or bypass-able node authentication and identification

Node authentication and identification are essential in the IoT smart home environment because it is considered the first stage of network protection and an essential security requirement for IoT smart home network connection. Weak authentication techniques may lead to easy and harmful attacks. IoT smart homes should adopt the highest standards of security to prevent such attacks because of the sensitive information that could be exposed, such as owners' names, addresses, and financial accounts. IoT smart homes connect heterogeneous smart devices that support different automated functions such as smart lights and smart security cameras. Any successful attack on a single smart home device might harm the whole system because IoT smart home devices are all connected to the same network. The authentication process during this heterogeneity is a dilemma in the IoT smart homes industry that requires attention from IoT security researchers and manufacturers [17].

The IoT smart home devices suffer from weak authentication and identification techniques. Many IoT devices do not require any authentication or identification to establish a connection to the combined application or to join the home network [28]. The heterogeneity of the IoT smart home devices and the resource constraints are two significant shortcomings of the IoT smart home system that prevent a fixed or general authentication approach from being adopted in all IoT smart home devices. Besides, the environment has a significant impact on adopting authentication and identification techniques and methods. The smart home is considered crucial because of the sensitive information that these devices would observe and collect [28].

There are different threats against authentication in smart devices such as DoS, eavesdropping, physical attacks, tracking, and cloning attacks. Smart devices have some crucial vulnerabilities which can happen by using weak user credentials, un-encrypted or un-scanned data transmissions or downloading un-encrypted updates. Here is a classification of the IoT authentication threads and attacks on smart homes. Table 2 lists the common threats at the device, network, and application levels.

Table 2: Classification of Authentication threats and attacks [12]

Layer	Threats	Attacks	
		In Transit	At Rest
Device Level	<ul style="list-style-type: none"> Limited Resources Architecture Interfaces Software 	<ul style="list-style-type: none"> Firmware Brute force Defraud DoS 	<ul style="list-style-type: none"> Firmware Physical Credentials
Network Level	<ul style="list-style-type: none"> Architecture Openness Protocols 	<ul style="list-style-type: none"> Eavesdropping Device scan Spoofing MITM Reply Unknown key Sharing 	<ul style="list-style-type: none"> Device scan Brute force
Application Level	<ul style="list-style-type: none"> Interactions Constrains Environment Human 	<ul style="list-style-type: none"> Impersonation Malware Insider 	

1.2.2 Weak security and privacy protection to the end users

Consumer behavior is different from one to another; some decisions or actions might differ based on the individual's knowledge and evaluation of the current situation of the problem. Some IoT smart home devices come with weak default credentials that are easy to guess or find online. This issue gets worse when the end users leave these default credentials unchanged. Malware exploitation could result from such security issues. Most IoT smart home device configuration processes require end users to enter information about the home network, create a new account, set up some customizations, and allow access permissions. Naive users may click "next," "continue," or "allow" for any screen prompt without understanding the consequences of doing so. Such unresponsive actions due to high trust in such technologies could harm the users because not all IoT devices are equipped with security and privacy specifications that protect the end user's information [25].

1.2.3 Lack of security, privacy, and firmware information for users

The IoT smart home devices need some attention by monitoring the market to protect consumers from weak security and privacy products. Therefore, the number of cyberattacks would decrease, and the consumers would trust this technology and buy more devices for a better quality of living in their homes [41]. In the IoT smart home devices market, there is no information provided to

consumers about security, privacy, and firmware update lifetime information. This missing information makes naive consumers suffer from bad purchases. Blink, Amazon's smart security camera, is an example of an IoT smart home device. As presented on the website, there is no information about any security, privacy, and firmware update lifetime information and it is rated by 85,889 with 4.5 stars [27]. Companies design and implement their product with careful considerations about security and privacy throughout the whole process. On the other hand, some companies develop their products without thinking about security. However, consumers cannot tell this before they make the purchase.

1.3 The research problem statements and objectives

This section discusses the problems on which the research will focus. The research objectives are later introduced to show what is planned to solve the issues.

1.3.1 Problem statements

Problem 1: No international standard on security and privacy requirement in IoT smart home devices

The issue of weak security and privacy aspects in IoT smart home devices might need a lot of time until the government assigns this problem to a particular organization that focuses on fixing this kind of problem to overcome the massive loss in money and resources by suffering the consequences. There is no international organization that provides security and privacy standards that could be adopted by IoT smart home device manufacturers to guide them in providing secure products. On the other hand, Saudi Arabia has a special organization called the Saudi Arabian Standards Organization (SASO), responsible for all product standards in their market. This organization adopts the highest international standards and forces all the manufacturers targeting the Saudi market to sell their products to follow these standards and receive a certificate of proof about this specific product. SASO follows the international regulations international Accreditation Forum IAF, ISO, and IALC [19].

Problem 2: Lack of security and privacy awareness among consumers

Today, there is a lack of security and privacy awareness among many internet users, especially IoT smart home device consumers. Devices and applications access permissions required more attention to avoid privacy and security breaches. This issue is getting worse if the adopted IoT smart home device is purchased and provided with more access permissions to personal and behavior information. It is essential to know the provided functions and their vulnerabilities or attacking scenarios of all devices. It is considered the first line of self-defense against such attacks.

Problem 3: No security and privacy information on the device's packaging

So far, this organization has two labels specially designed for water efficiency and electric efficiency product labeling systems. The idea of a labeling system helps the consumer for a better and trusted purchase decision because of the government enforcement over the products manufacturers companies. All water and electricity products must present this label on the product's packaging for proof of passing the SASO standards and to show all the user expected information about the desired product. Here are the available labels in the Saudi market, which are the water efficiency label and the energy efficiency label:

Figure 1: The water efficiency label and the energy efficiency labels [19]



However, there are no IoT smart home devices security or privacy labels in the Saudi market. The Saudi market is highly adopting the technology of IoT smart home devices, but there is a lack of information labeling on them. This high adoption encouraged different researchers to create such useful labels.

The security and privacy information is usually not listed on the product packaging. Hence there is no way that consumers could use or read about IoT smart home devices' security and privacy aspects before purchasing. Therefore, consumers are not aware of buying products' security and privacy issues. Moreover, most companies will present their devices in the best way to avoid any exposure to weak aspects of any kind. Most IoT smart home devices come with usage, connectivity, electricity information, troubleshooting, etc. They never tell the purchaser anything about security, privacy, and firmware characterizations. There is a need to analyze such devices and explore their functions to understand their functionality better and test all possible vulnerabilities used to hack such machines to gain unauthorized access to the owner's personal information. This testing could be done by creating a

new technical committee or organization funded and trusted to do all possible security and privacy testing and provide a “security and privacy standards certificate” for all IoT smart home devices in the market [24]. Unfortunately, creating this type of responsive organization could take so much time. On the other hand, IoT smart home device manufacturers are rapidly developing new devices and launching them in the international market.

1.3.2 Dissertation objectives

To solve the previous problem statements, new IoT smart home devices’ security, privacy, and firmware labels were developed. These labels have major security and privacy information about the IoT smart home device such as firmware analysis, device’s technical specifications, different security or privacy factors, sensor practices, IoT smart home devices security and privacy general score or grade, along with general information about the model, brand, and privacy policy. By developing such labels, the problem of lack of security and privacy awareness among consumers should be solved. Moreover, this research is presenting a new IoT smart home device security privacy and firmware labels that were never used in the Saudi Arabian market. The adoption of these labels would help the Saudi Arabian standards organization to have powerful standards that they can create and force the IoT smart home devices manufacturers to follow to sell their products in the Saudi Arabian market. This will control the rapid selling of IoT smart home devices in the market. General IoT smart home devices consumers’ education and outreach plans would help in widely recognition and usage of the labels.

This dissertation introduces two complementary versions of the IoT smart home devices’ security, privacy, and firmware labels. The first version is the summarized label. It provides bullet points about the IoT smart home devices’ security and privacy aspects that any consumer should be aware of before purchasing. It represents each security and privacy factor and its score to provide adequate information about each analyzed factor and its importance in analyzing and testing procedures of the IoT smart home device. Also, it includes a graph that represents the final grade that the IoT smart home device achieved after analyzing its security and privacy factors.

The second version is the detailed label. It provides a bigger picture about all security and privacy features that any consumers may look for about the IoT smart home device. It represents information about the available sensors and their practices in collecting the data from the surrounding environment, technical specifications, privacy policies, and a detailed description of the analyzed security and privacy factors’ that were represented on the summarized label.

The IoT smart home security, privacy, and firmware summarized, and detailed labels should be put together by a government agency or organization such as SASO or any cyber security or IoT

organization. Usually, these organizations follow high security and privacy standards to protect different types of consumers from bad devices. This would help in solving the problem of there being no international standard on security and privacy requirement in IoT smart home devices. Therefore, the Saudi Arabian organizations would state their standards for all IoT smart home devices in their market. This adoption would encourage different vendors to make sure that they pass any test or certificate requirements to sell their products in the Saudi Arabian market. Moreover, it will gain the trust of the IoT smart home devices' consumers because they usually trust the government organizations. These labels will be presented on the product's packaging to inform the consumers about the security, privacy, and firmware features and to understand more about the devices they are purchasing. By doing so, the problem of no security and privacy information on the device's packaging will be solved because these labels would present major security and privacy features about the device along with scores for seven security and privacy factors that derive a final score or grade for the IoT smart home devices.

There are several benefits of using these labels; the main goal is to provide helpful information about the product that covers privacy, security, and firmware update lifetime information. Also, the labels will give some general information that supports the purchaser's needs and expectations for a knowledgeable and wise purchasing decision [24]. Moreover, the labels will encourage the market's manufacturers to provide better devices because of the high awareness level consumers developed by reading and understanding such labels. Also, these labels could provide an additional link for more information about the product features or some extra explanation about its features that not every consumer looks for [41]. Finally, this would lead to a knowledgeable community that knows how to deal with such powerful technologies [24].

The development of the IoT smart home devices' security, privacy, and firmware labels has three phases. It starts by presenting basic information about major security and privacy aspects that any consumers might look for before purchasing. The security and privacy features in the IoT smart home devices are different from one type to another. Therefore, it is important to choose the important ones to describe the device properly. There is a need to find resources to collect information about the security and privacy aspects to create the prototype of the labels. The available resources are the IoT smart home device's manufacturer or third-party websites, user manual, firmware analysis, and network analysis. Moreover, there is a need to analyze the device's security and privacy features along with its firmware vulnerabilities to better evaluation of the IoT smart home devices and to provide a final security and privacy grade or score. Therefore, in phase two a scoring system is designed to solve this part. There are seven security and privacy factors that are evaluated, and each factor is assigned with an individual calculated score. This scoring system helps in better presentation of the IoT smart home

devices' security and privacy aspects. After the second phase, the initial designs of the IoT smart home devices' security, privacy and firmware labels are ready to be used in the final phase of the development process. Finally, phase three is about conducting surveys. This phase is designed to collect comments from IoT smart home experts, consumers, label designers, and risk management professionals. These comments help in creating the content and finalizing the design of the labels. A detailed explanation can be found in Chapter Three (Research Methodology).

1.3.3 Dissertation Contributions and Timeline

First contribution: Enhance IoT smart home devices consumers' security and privacy awareness. Reading such labels will educate the community of the IoT smart homeowners and make them understand the device's functionality, security, and privacy features along with different attacks that they could easily avoid. Increasing security and privacy awareness will protect the IoT smart home community from different types of attacks that could be easily avoided.

Second contribution: Developed new security, privacy, and firmware labeling system that supports the consumer's knowledge for better purchase decisions. The proposed IoT smart home device labels would help the consumers in better and more confident purchasing decisions because they will read all security and privacy information about the target IoT smart home device. Along with the evaluation score that will help in comparing different devices based on different security and privacy factors.

Third Contribution: Encourage IoT smart home device manufacturers to produce better and safer products. Because they know that there will be a label that presents all the security and privacy features after a detailed evaluation. This would require them to produce better products. This will protect the IoT smart home consumers from bad devices.

Fourth Contribution: The IoT smart home device label will help the government agencies to adopt higher standards of IoT smart home devices in their market. This IoT smart home devices label could be adopted by any standards organizations or government agencies and help them derive the standards for all the IoT smart home devices that will be sold in their markets. This will help them come up with standards based on all the evaluated factors that these labels present. This will force the manufacturers who target their market to ensure that all presented factors that this label evaluates should be in the best shape in order to sell their products in that market.

Fifth Contribution: Enhance the security of IoT smart home system by not introducing insecure devices into it. Such IoT smart home labels would be used to determine the minimum score

for any devices that could be added to IoT smart home systems. This will ensure that all used devices in a specific IoT smart home are in the very good range to be added to that IoT smart home system.

1.3.4 Dissertation Overview

The remainder of this dissertation is organized as follows. Chapter one provides a comprehensive introduction to IoT technology and its implementation of smart home devices. Also, it discusses the IoT smart home device challenges, environment architecture, and its security and privacy concerns. Moreover, presenting the problem statements that this dissertation is trying to solve along with its objectives and contributions. Chapter two presents a detailed background and related work about the IoT smart home devices' security and privacy labels. It discusses the evaluation of the IoT smart home devices along with the creation of such labels to be used in the IoT smart home devices market. Chapter three presents the methodology for this dissertation. It describes the three phases of the IoT smart home devices security and privacy creation along with the technical work results. Chapter four presents the survey implementation and all the stages processed to conclude the final IoT smart home devices security, privacy, and firmware labels. Chapter five discusses the implementation of the created labels and the procedures to fill the labels with the information about the testes IoT smart home device. That includes a full evaluation of the seven security and privacy factors. Chapter six concludes the IoT smart home devices security, privacy, and firmware labels work that has been done. It is followed by the future work section, which proposes the possible future work. Finally, the Appendix section has four appendices that present the firmware technical work on two different IoT smart security cameras along with the surveys that target the IoT smart home devices experts and regular consumers.

In summary, this dissertation proposes IoT smart home devices' security and privacy labels. These labels would help the consumers to better understand the technology and have confident purchase decisions. These labels target the IoT smart home devices market in Saudi Arabia. The dissertation describes the process of creating the security and privacy factors that should be evaluated to understand the device's features. In addition to the development of a scoring system to better describe the results of the factors' evaluation procedures and to derive a final grade for the IoT smart home devices' security and privacy aspects. Also, the conducted surveys that support the creation of the labels' design and contents. This label can be adopted by any standards organization in the country to gain the trust of the IoT smart home device's consumers.

Chapter 2: Background and Related Work

The Internet of Things (IoT) is a special network that connects heterogeneous smart and digital devices, such as sensors and actuators, to the internet and allows the devices to communicate and share information through wired or wireless connections [8]. One of the most popular and globally used implementations of IoT is smart homes. It is a combination of heterogeneous automation systems or regulations that can be managed or customized through a remote user with the help of the internet to ease communications [9].

Different smart devices are widely used in smart homes; each smart home device is responsible for a particular task that it was manufactured to do, such as Security-Smart Door Locks (e.g. August Smart Lock Pro 3rd), Entertainment-Smart TVs (e.g. Apple TV), Electricity-Smart Plugs (e.g. Amazon Smart plugs.). IoT smart home automation environments have a high risk for cyber threats because of the heterogeneous smart devices that power the smart home, which are automatically based on the available information from the communications in the surrounding environment [1]. It's a double-edged sword. Although, the wireless remote access and control via smartphones and web applications, which raises the risk of unauthorized access to IoT devices in smart homes.

This chapter presents the background of IoT technology and smart home systems. A related work section is summarized at the end of this chapter.

2.1 Background

This section discusses the IoT smart home system background and its devices.

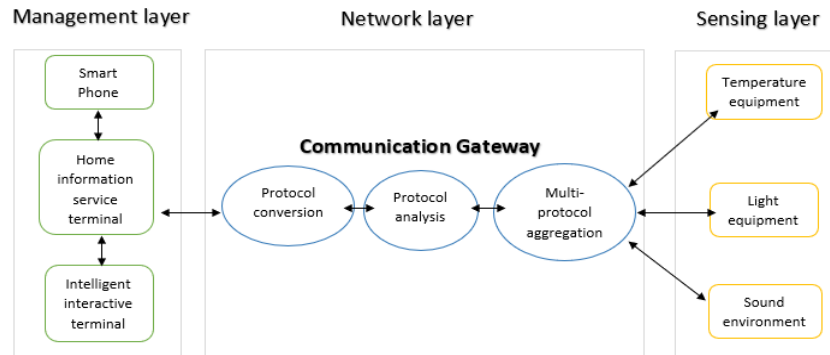
2.1.1 IoT smart home architecture

Smart homes are one of the best examples of the specific and crucial application of the IoT. They implement network communication, automation, control technologies, and artificial intelligence in one integrated platform [35]. As shown in Figure 2, IoT smart homes system architecture can be divided into three layers [36]:

1. **The sensing layer:** usually called the perception layer, it consists of adaptors that collect information from the surrounding home environment.
2. **The network layer:** is responsible for data communications and transmission using different media types within the environment. It also works as a multi-protocol aggregator and convertor.

3. **The management layer:** all data is managed and processed by this layer using the home information service terminal. The end-user presents the results using the IoT devices' companion applications through mobile applications or web services.

Figure 2: IoT Smart Home Architecture [36]



IoT device authentication is the first security aspect considered when designing an IoT device that uses communication methodology (e.g. user authentication) [12]. It is an essential part of the perception layer of IoT smart home architecture because these devices must be authenticated to use and share accurate data. IoT network connects a large scale of heterogeneous devices that cooperate for different goals, and any unauthorized device would harm the network at different levels. There are two authentication types: 1) Source authentication guarantees that the source object is the one that it claims to be and is well known to everybody in the domain of the IoT network, and 2) Data authentication guarantees that this message is original, and not a replay of the original one [37].

An intelligent interactive IoT device can control and affect the adaptors/sensors in smart homes for any changes in the environment parameters [36]. An IoT-based smart home has five components to achieve the best intelligent automation environment:

1. **IoT devices:** sensors that collect information and actuators to execute actions.
2. **Coordinators:** control all processes and report everything to the IoT service provider.
3. **IoT services:** a cloud-based service accessed by users at any time.
4. **Controllers:** control the IoT system.
5. **Sensor bridge:** the connection between the local IoT network and the IoT cloud services [14].

2.1.2 Communications in IoT smart home systems

Smart homes use different wireless technologies to manage communications using different standards that vary based on the implemented applications [17]. The standard technologies include Wi-Fi, ZigBee, Z-Wave, Bluetooth LE (Low Energy), etc.

The communication between the IoT-based smart home devices is a critical issue because of the personal and sensitive information that these devices pass to each other to make crucial decisions in the IoT environment.

Four Communication Models are used by IoT-based smart home devices in general [38]:

1. **Device to device communications:** The communication is established when two or more IoT devices are directly connected, without any intermediary object (e.g. server).
2. **Device to cloud communication:** Communication is established when a connection between the device and the IP network using Wi-Fi or an ethernet cable such as the Samsung Smart Kit.
3. **Device to gateway communication:** Application Layer Gateway service establishes a connection between the IoT device and the cloud service. It is an intermediary between them and acts as a local gateway for data translation and security, such as a fitness tracker watch.
4. **Back-end data sharing model:** This model uses an architecture that helps users export data and smart object data analyzing from different sources (service clouds). All data are collected from IoT sensors and utility systems then uploaded to multiple application service providers.

2.1.3 Node authentication mechanisms in smart homes

The authentication of IoT smart devices is essential. The current IoT device authentication schemes that are used in smart homes could be categorized as the following [14]:

- **One-time password:** create a new passcode used once for each time there is a communication or transaction. This scheme is widely used in international banking systems and e-Commerce.
- **Zero-knowledge proof:** This technique verifies information between the communicator parts without revealing any sensitive information.
- **Mutual authentication:** two-way authentication, both entities authenticate each other.
- **Public-key cryptography:** It's asymmetric encryption by generating public and private key pairs used between the IoT devices.
- **Digital signature:** use the private source key, widely used in authentication technology.

The IoT device should be authenticated before any data transmission or communication. This authentication should be done from the IoT device source. Any cryptographic keys generated in this transmission should not make any overhead for the IoT devices in the IoT system. IoT authorization and access control are two different things [39].

2.1.4 IoT smart home devices

The definition of a “smart home device” is any single-purpose Internet-connected device designed for a home or a hub, like a device designed to connect and control more than one single-purpose device [10]. The smart IoT devices are in almost half of the houses in each continent, with at least one smart IoT device per home [11]. These devices increase the owner's time efficiency and save money. However, safety and security may be reduced when using low-quality standard devices because of the high breach affection probability. There are different types of this kind of device, all based on the provided functions and services, such as smart cameras, smart bulbs, smart air conditioners, smart thermostats, etc.

Table 3: IoT smart home devices examples

#	Types	Description	Product Example
1	Security Cameras	A standalone system with vision sensors to monitor the surrounding environment.	Blink Mini
2	Smart Thermostat	Monitor and adjust the surrounding environment temperature. Some are equipped with smoke sensors.	Google Nest Thermostat
3	Smart Plugs	Wi-Fi outlet that works with smart home assistants such as “Alexa.” It provides run-time and usage tracking features.	Kasa smart Plugs
4	Smart TV	Traditional TV with integrated internet to stream pictures or videos and browse the web.	Samsung Smart TV
5	Smart Lights	A personal wireless lighting system that provides light control and ambiance adjustments.	Philips Hue
6	Smart Doorbell	Answer the doorbell from any authorized smartphone. Most of them are equipped with security cameras.	Ring Doorbell
7	Smart Lock	Manage doors (lock or un-lock) from any location using authorized smartphones.	August Smart Lock
8	Smart Virtual assistance and speaker	It is a stand-alone system equipped with microphone and speaker to analyze user’s commands and make decisions or actions over any connected devices on the network.	Amazon Echo

2.2 Related work

This section has two subsections. The first subsection discusses the different evaluation techniques to analyze the IoT smart home device’s security and privacy aspects. It presents different test beds and cyber security forensics tools to help in the firmware analysis procedures. The second subsection is about the current IoT smart home devices’ security or privacy labels. It discusses different approaches of developing the labels along with different designs and standards used in the developments.

2.2.1 IoT smart home devices analysis procedures

There are different testing methodologies to evaluate IoT smart home devices. Each methodology has its own procedures to ensure the best results. In the following studies, one of the

researchers attacks the IoT smart home device after recognizing its vulnerabilities. Another researcher designed a testbed to analyze the device and to find any available vulnerabilities.

Bjørneset et al. [21] developed a testing methodology that has been used for testing five different IP cameras through various methods, including ethical hacking. This author's approach started by gathering some information about the target device. Then, the authors scan the target for vulnerability. Finally, attack the target and report results. For analysis, they exposed some of how hackers use to find IoT smart home devices. One of the common vulnerabilities that they found among the tested IP cameras is the default user credentials (username and password). This issue would affect the IoT smart home system if the user did not fix it before the hacker reached him. Their testing methodology starts by performing an attack based on previously done ones, using some of the ethical attacking tools embedded in the Kali Linux penetration testing platform. This paper demonstrates different tools such as Nmap, Ncrack, Patator, Medusa, and Wireshark.

Abdalla et al. [22] targeted another IP camera called “Intelligent Onvif YY HD” to be a case study of their testing methodology to explore the security and privacy vulnerabilities. This device records the surrounding environment continuously, knowingly and unknowingly. They found that several problems might be exposed in almost all IP smart cameras. These are the default login username and password, guessable and straightforward keys, and low encryption techniques in data collection and transmission. They followed an approach that started with data collection traffic analysis and finally checked flaws in the application that works with this IP camera. The pen testing of the IP camera methodology starts from defining the area describing the experiment scope. Then, the implementation of the process summarizes all gaps and vulnerabilities that may put the entire system to risk. Finally, the researchers conclude the whole procedure in a report that contains the following: 1) all device vulnerabilities, 2) classify all possible threats and assign their levels (low, medium, high), 3) Present all vulnerabilities, threats, and weaknesses on the target, 4) provide information about the weaknesses and strengths of the target’s security system. This paper uses several tools such as Wireshark, Netdiscover, Bettercap, Nmap, and Kali Linux platform. After using the designed bed test, the authors found several issues with this IP camera. There is a weak Identifier Default number that is easily guessable, a lack of encryption in all transmissions, and the combined Android application is storing the user-sensitive information in plain text, which is a crucial issue.

A testbed was designed to combine hardware and software with exploring the IoT devices in basic and advanced approaches [23]. This testbed is fully functioning to test IoT devices for security requirements. This testbed supports multiple penetration tests such as scanning (data traffic, IP, and port scanning), fingerprint, data leakage, data protection, and breaking encrypted traffic. This testbed found that it is hard to test all IoT devices because of the heterogamy of this field. The IoT devices are

different in hardware and software. Daily updates and developments are another challenges to state that this presented method will work on all IoT devices in the market. This testbed applies several approaches for better testing mechanisms. This testbed can simulate the real environment of the IoT device to identify possible context-based attacks after the comptonization of the target. Also, a machine learning approach is applied to better IoT device identification after analyzing the device's network traffic. This testbed could be used on many IoT devices with a bit of modification to follow the target features for the best results.

2.2.2 IoT smart home devices label

The IoT smart home devices are growing internationally. The market is expected to grow at a compound annual growth rate of 28.30%, in value terms, during 2017 – 2022, on account of higher gross domestic product per capita of the countries like Qatar, the United Arab Emirates, and Kuwait [26]. This growth is never monitored for any security and privacy aspects by many countries worldwide, especially in the middle east region. Some countries like the U.K. adopt the Labeling System, and some regulations are applied in this approach for better security and privacy implementations that satisfy the need of consumers.

Emami-Naeini et. al. [24] have designed an IoT smart devices labeling system that presents information about security and privacy effortlessly and clearly that consumers would easily define and understand. This design is developed after surveying 22 security experts and 15 IoT consumers. It uses the three-round Delphi method to understand the consumer needs better and engages some expert knowledge from people with a solid technical background. This paper proposes two types of labeling systems, summarized and complete information. The summarized label contains the most important information that all IoT consumers usually look for when purchasing IoT smart home devices. This label has a website link or QR code that presents all other information that is not presented on the summarized one. Using this approach, the size of the label would fit on most IoT smart home device boxes [24]. The survey audience is not enough and needs to expand and include more regular consumers and people with a limited technical background.

Emami-Naeini et al. [41] followed the previous research with a survey conducted with 1371 Mechanical Turk (MTurk) participants to test the effectiveness of each of the privacy and security attribute-value pairs proposed in that prior work along two key dimensions: the ability to convey risk to consumers and impact on their willingness to purchase an IoT device. They proposed some recommendations for effective presentation of privacy and security aspects on the IoT smart home devices labels to better communicate risk to consumers. For example, they recommend that

manufacturers should provide additional information about the following: 1) specify the use of the security and privacy practice in the device, 2) determine what could harm or protect the user by using these security and privacy practices, 3) specify the controls related to the security and privacy practices, 4) provide customization steps for any security and privacy options if applicable. The researchers decided to add a plus sign next to any information on the detailed label in case the consumer wants to know more details about the factor. This label does not provide any rating for the security and privacy aspects at all; rather it provides the information that a consumer should know about the device before purchasing.

From Germany; Morgner et al. [25] state that most IoT smart home devices are suffering from the firmware update lifetime information. IoT smart home device manufacturers are doing their best to launch new products in the early stages without mentioning the lifetime of that product, leaving the consumer bared without any help after discontinuing that model. This issue makes this consumer unprotected because they will no longer have any updated patches for their IoT smart home device. Thus, higher risk of vulnerabilities, and he would be considered an easy target of attack. Therefore, this paper proposes a firmware update lifetime label that should be presented on the IoT smart home box to inform the user about the security patches period that he will be receiving manually or automatically. This result came after 1400 participants agreed about the need for such a labeling system. Also, provisioning time information is included on the same label to prove the time frame that this product is going to be patched in case of any bugs or vulnerabilities exposure found. This proposed label has three design goals that are 1) It can be easily understood by IoT smart home devices consumers. 2) It can be easily used for products comparison 3) It does not require third parties testing or analyzing.

Hosein F. Badran [48] supports the IoT smart devices labeling system. The Internet Society (ISOC) in the Asia Pacific Region conducted a survey in which they found that 81% of participants are concerned about personal information being leaked, 73% are concerned about hackers who can take control over their devices to commit crimes and 71% are concerned about being recorded without their consent. These outcomes indicate the need for an educational label that could be used for a better understanding of the security and privacy aspects of IoT smart devices. IoT consumers' trust is highly desired for the adoption of such technologies.

Moreover, the certification of IoT smart devices is required for products and services. Thus, the certification would encourage consumers to purchase more devices. The Netherlands adopts the Cybersecurity Act (CSA) and the active development of a European Cybersecurity Certification Framework for IoT smart devices. This adoption is supported by the Dutch government, and it's a mandatory certification for products that have high risk and insecure practices. Also, the certification of IoT smart devices in the United Kingdom is supported by the government. This certificate is awarded

after a set of tests and measures to ensure the safety of the IoT devices. There are different types of BSI Kitemark (product and service quality certification) for IoT devices, which will be awarded according to the device's usage: residential, commercial, and enhanced. In addition, IoT product certification in Australia encourages manufacturers of IoT products to submit their new products for testing by an accredited test laboratory-like the National Association of Testing Authority (NATA) or Australasian Information Security Evaluation Program (AISEP). If the device passed the test, it is awarded a security certificate. Lastly, The Canadian Standards Association (CSA) Group Cyber Verification Program is designing a standard to address the IoT smart devices' security aspects. It aims to test the organization to ensure that a security organization would develop a secure product. These standards consider 6 domains and 18 practices areas within these domains. Once the test is completed, the organization will be provided with a maturity rating.

Hosein F. Badran proposed an IoT smart devices label that covered the main security aspects after testing. The proposed label includes 1) identification of the organization overseeing the certification and formal testing, 2) QR code or URL (web site) link that provides updated information about the product that includes, A) Product model and version, B) firmware version number, C) recent vulnerability information, D) testing framework, E) security configuration guide, F) declare what data is collected and how it will be shared.

Yun Shen et al. [49] adopted a new approach to secure IoT smart home devices, which is "security by design." The main idea is to ensure that security and privacy are built-in IoT devices so that they are secured at all system levels. The proposed security and privacy label was designed based on the idea of the "food nutrition facts" label created by the Food and Drug Administration (FDA). They used similar sectioning and grouping for major security and privacy aspects to present the information in an informative way that regular IoT smart devices consumers could understand. This label has five categories, each category of the label provides a set of guidelines to consumers to consider from their perspective in terms of security and privacy, which are called factors. The categories and their factors are as follows: 1) system (security) category, which has the following factors: certificate, secure boot, firmware, password, remote access, and authentication, 2) communication (security), it has the following factors: encryption, internet access and talk to other devices. 3) data (privacy), it has the following factors: Personal information, telemetry data, and data storage, 4) sensory (privacy), it has the following factors: audio, video, motion, location, environment, 5) connectivity (information), it has the following factors: Ethernet/LAN, Wi-Fi, Bluetooth, Zigbee, Z-Wave. They used three techniques to extract information from the device that are passive discovery, active probing (fuzzing), and hardware and software analysis. However, there is a shortcoming in this design: the proposed IoT smart home devices label is only one label that presents all information, and there is no additional label

that contains extra information about the technical characteristics of the device. Also, this label design does not provide any testing results for the tested security and privacy factors that have been tested to generate the content of this label. Such results would provide a better vision for consumers so they can make confident purchase decisions.

Chapter 3: Methodology

This chapter presents the development of the IoT smart home devices' security, privacy, and firmware labeling system in detail. It discusses all phases and their stages to achieve the best outcomes for the labels. Overall, there are three phases in this development. The first phase is the IoT smart home device security, privacy, and firmware information collection. There is a need to find the best resources to create the content of some of the label sections such as general information and technical specifications sections. Moreover, firmware analysis tools are required to test the IoT smart home device's firmware for any vulnerabilities and to monitor its network performance. This phase has two stages: (1) the information resources such as the manufacturer or third-party websites, user manual, firmware analysis, and network analysis and (2) the types of useful information such as internal storage availability and connectivity methodology. All outcomes of this phase are used in the next phase. The second phase is about choosing security and privacy factors to be evaluated along with designing a scoring system to better represent the evaluation results. This phase uses the CVSS calculator to ease the evaluation and factors score calculation. Finally, the survey phase (third phase) is about conducting surveys that target different groups of IoT smart home device's experts and consumers. This phase helps in creating of the labels' content and final designs. It has four stages that complement each other. These stages start with the IoT smart home devices expert's survey. Then, the IoT smart home devices consumers survey. After that, the data analysis, and label designers short survey. Finally, the final versions of the IoT smart home devices' security, privacy, and firmware labels are created. The following is a presentation of the general architecture of the proposed design and development of the IoT smart home devices labeling system:

- Phase one: Information collection.
 1. Stage one: information resources.
 2. Stage two: types of useful information.
- Phase two: The scoring system.
 1. Internet pairing.
 2. Configuration & authentication.
 3. Update modes.
 4. Exposed services.
 5. Vulnerabilities.
 6. Protocols.
 7. Network encryption.

- Phase three: The survey.
 1. Stage one: A survey that targets the IoT smart home devices experts.
 2. Stage two: A survey that targets the IoT smart home devices consumers.
 3. Stage three: A short survey that targets social data analysis, risk management researchers, and label's design experts.
 4. Stage four: final version for the IoT smart home device labeling system

3.1 Phase 1: Information collection

This is the first phase of the development procedures of the IoT smart home devices security, privacy, and firmware labels. It is designed to collect data about the IoT smart home device to be used as contents of the labels. There is a need to determine the useful information resources that provide the useful information about the targeted IoT smart home devices, along with the best cyber security forensics tools to analyze the firmware of the IoT smart home devices.

3.1.1 Collecting information from different sources

After choosing the IoT smart home device target, information collection is needed to explore the device features and to understand all provided functions to check all possible security, privacy, and firmware vulnerabilities in it. This phase contains two stages that are described in detail in the following:

1. Information resources

Most of the IoT smart home devices share the same information resources that are manufacturers, the third-party website, user manuals, firmware analysis, network analysis, consumer experience, and feedback. However, firmware and network analysis require more technical work to extract the important details that are not presented in other resources and are hidden usually from consumers because it might change their purchase decisions if weak firmware is used.

2. Useful information

The amount of information that could be collected and analyzed is big, depending on how weak or open is the IoT smart home device designed and manufactured. Here is a list of all possible information that could be collected from each resource of the targeted IoT smart home device:

IoT smart home device website (manufacturer) & third-party seller website:

1. Last revision date and time.
2. Notification methodology (push or pull).
3. Cloud services and storage.
4. A Combined application or/and web access availability.
5. OS support options (iOS, Android, Microsoft).
6. Connectivity methodology (wi-fi, Bluetooth, wired).
7. Compatibility with other IoT smart home devices assistants (Alexa or Google).
8. Warranty specifications and lifetime (software, hardware, updates, vulnerability fix).
9. Wi-Fi Ethernet Technology: Fast Ethernet Protocols (DDNS Protocols: DHCP Protocols)
10. Network ports (RJ-45)
11. Internal storage (MicroSD).

IoT smart home device user manual:

1. Firmware version without any updates.
2. Networking platforms supportive (TCP/IP, HTTP, Intranet/internet)
3. Web configuration option.
4. Is there any human interaction needed to install the device or just plug and play?
5. Default username and password.
6. Default IP addresses.
7. Wireless security mode “encryption” (None, 802.11b/g/n Wireless with WEP/WPA/WPA2/WPS security).
8. Built-In Protocol (10/100BASE-TX Fast Ethernet, 802.11b/g/n WLAN).
9. Emission (EMI), Safety & Other Certifications (FCC Class B, IC, C-Tick, CE).

Firmware analysis:

1. Passwords
2. API endpoints (URLs)
3. Vulnerable services
4. Backdoor accounts
5. Configuration files
6. Source code
7. Private keys
8. How data is stored
9. Hidden emails.

Network analysis:

1. Authentication process issues.
2. Network data flow issues.
3. Data encryption.

3.1.2 Firmware Security and Privacy Analysis

There are different types of vulnerabilities in the IoT smart home devices. It is important to understand the shortcomings of such devices to better evaluate the security and privacy features. Some of the technical information cannot be found online or from the device package such as the information about the firmware and its vulnerabilities. Therefore, to understand the firmware and its related information, firmware analysis needs to be conducted with the help of cyber security tools. There are different types of vulnerabilities to look for in this analysis such as hidden username and passwords, IP addresses and default configurations. This section provides two examples of the firmware analysis work.

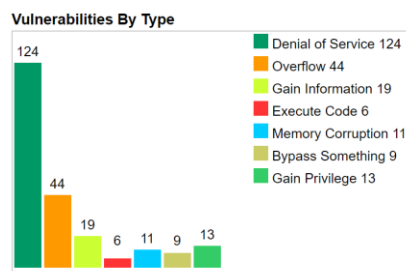
3.1.3 Experimental Environment Setup

This section presents the Firmware security and privacy analysis process for two popular IoT smart home device cameras. This type of IoT smart home device is one of the most popular devices that consumers purchase. However, this type of camera is connected to the Internet all the time to provide the best live surveillance for the surrounding environment. Lack of security and privacy in such devices might cause serious problems, especially if the devices are not presenting any privacy or security information, such devices must be avoided. This problem influenced many security researchers to explore and analyze such technology for a safer future. This study is adopting two of the powerful tools that support this kind of security and privacy analysis, which are Binwalk and Firmwalker tools. These tools are working on Kali Linux OS v2021.1 on VMware workstation player 16. This section presents all the steps and methods that result in finding vulnerable security, privacy aspects in the tested firmware. The detailed analysis can be found in Appendix A and Appendix B. Meanwhile, the preparation of the analysis of the results will be carried out on a machine with Intel(R) Core(TM) i7-1065G7 CPU @ 1.30GHz 1.50 GHz and 16GB RAM [33] [34].

A. First firmware security and privacy analysis results (Details in Appendix A)

- The image uses U-Boot as the bootloader by tracing the uImage file which is a Linux Kernel type (image header at address 327680 0x50000 and compressed bootloader image at address 327744 0x50040). Based on the uImage header at address 327680 0x50000, we know the CPU architecture is MIPS. This firmware is using a compression type of “lzma” archive.
- This firmware uses an old version (Linux kernel versions 2.6.21). however, the product itself is younger than the version used in it. Here are some statistics about it from [32]:

Figure 3: Linux kernel versions 2.6.21 vulnerabilities [32]



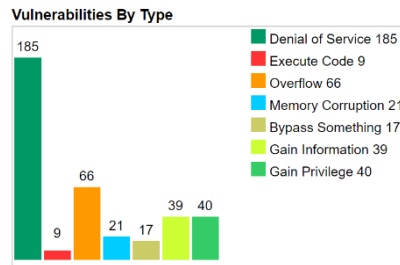
- (account.htm) shows how to create a new account. The user password max length is “8” and the username max length is “12”. All user credentials are encrypted.
- (Upgrade.htm) shows that this device is following push mode updates in which a manufacturer's server sends a notification to the devices and requires users to accept the new update installation.
- Network usernames and passwords default credentials and DHCP IP addresses.
- Default configuration information.
- The FTP setup file.
- The firmware image has some encryption.
- Firmwalker tool shows that there are some emails, IP addresses, Keys, password locations, configuration files, etc. All these files and directories are vulnerable and could cause serious damage if explored.

B. Second firmware security and privacy analysis results (Details in Appendix B)

- The image uses U-Boot as the bootloader by tracing the uImage file which is a Linux Kernel type (image header at address 64 0x40 and compressed bootloader image at address 128 0x80). Based on the uImage header at address 64 0x40, we know the CPU architecture is MIPS. This firmware uses a compression type of “lzma” archive. This

firmware is using “kernel Linux3.10.1” which has a high rate of DoS vulnerabilities [32].

Figure 4: Linux kernel versions 3.10.1 vulnerabilities [32]



- Some of the cryptography information and configurations.
- Network port 80 configuration information, Server name, and address are available.
- Information about wireless Pre-shared Key (PSK).
- UDHCPC configuration file with IP addresses.
- The firmware image has some encryption.

3.1.4 Current IoT smart home devices labeling system's content

This IoT smart home devices labeling system has two versions for each IoT smart home device which are summarized and detailed labels. There is a need for two versions because the summarized label will be presented on the IoT smart home device's box or packaging. Usually, these boxes are small and might not fit all details about all security and privacy features. A scan of the QR code on this summarized label will direct the purchaser to the second version of the IoT smart home devices label for extra details. The detailed label has information that is not presented on the summarized label. These two labels should cover the most important security and privacy aspects that any consumer would like to know about before purchasing. These labels should provide enough information for safer and more confident purchasing decisions.

The first one should be a summarized label that covers the most important security and privacy of the IoT smart home device. The information is described in scored factors. Each factor represents the main security, privacy, or firmware feature that any consumer should be aware of when purchasing. It has five main sections: 1) general information that presents basic information about the IoT smart home device such as name and version number, 2) security privacy factors scores that represent all security and privacy factors that are evaluated to calculate the final score of the IoT smart home device, 3) label barcode that is created specifically for this summarized label to provide a unique ID for the IoT smart home device's security and privacy evaluation details, 4) detailed label QR code is presented to access the second version of the IoT smart home devices label to read extra information about the

security and privacy features, 5) final device score is a graph or chart that represents the final security and privacy score after the evaluation of the seven security and privacy factors. Overall, each section would represent some information that should help the IoT smart home devices consumers, to make confident and knowledgeable purchase decisions. This label will be presented on the IoT smart home device's packaging (box) to help consumers to know more about it and to make better purchase decisions. This label should contain the basic information about the IoT smart home device and gives clear information about the security and privacy in an easy way to understand by different types of consumers. Table 4 refers to the recommended information for the initial design of the summarized label.

Table 4: Summarized label overview

Section Number	First label	
1	General information	<ul style="list-style-type: none"> • Type • Brand/model ID/name • Version • Operating system options (iOS, Android, Microsoft) • Warranty lifetime • Firmware version • Storage type (internal, cloud)
2	Security factors (scored)	<ul style="list-style-type: none"> • Internet pairing • Configuration and authentication • Update mode • Exposed service • Firmware Vulnerabilities • Protocols • Network encryption
3	Final Device score	<ul style="list-style-type: none"> • Grade, graph, or emojis based on the calculated factors
4	Label barcode number/ID	<ul style="list-style-type: none"> • Specifically, for this device
5	Link to more detailed label	<ul style="list-style-type: none"> • QR code, URL link

Secondly, the detailed label presents in detail all security, privacy, and firmware features information that consumers might need when looking for certain details. This could be bigger and have more written details rather than numbering or graphical information. It has five main sections that represent some accurate information about the smart home devices' security and privacy concerns that consumers might need to know about for purchase decisions. These sections are the 1) general information, security, privacy, and firmware factors scoring description table (describe all scored

security and privacy factors represented on the summarized label), 2) data sensor practices (provide information about all device's sensors and their work methods), 3) technical specifications (provide information about major technical characteristics and usage of the device beside network and storage details), 4) label barcode (is created specifically for this detailed label) and 5) privacy policy (documented from the device's manufacturer). This label would be accessed by scanning the QR code on the summarized label.

This label is designed to provide better picture than the previous label about security and privacy information that any consumers should be aware of before purchasing. It provides a detail description about the evaluated security and privacy factors that derive the final score of the device that is presented on the summarized label. Moreover, this label has additional sections that are not presented on the summarized label such as the data sensor practices section. This section describes the sensor behaviors and the data collection scenarios along with the storing location of the collected data. Also, a technical specification section that represents information about hardware or software features such as the connectivity information, power consumption, and any smart assistance (e.g. Alexa). Table 5 refers to the recommended information for the initial design of the detailed label.

Table 5: Second label overview

Section number	Second label		
1	General information	Type Brand/model ID/name Version Operating system options (iOS, Android, Microsoft) Warranty specifications (software, hardware, updates, vulnerability fix). Firmware version Storage type (internal, cloud)	
2	Security factors (summarize factor's details)	Internet pairing Configuration and authentication Update mode Exposed service Firmware Vulnerabilities Protocols Network encryption	
3	Technical specifications	Sensor data practices: Power and Max power consumption Any certifications awarded such as (CE,IC,FCC class B) SDRAM and Flash Memory Data Codecs (JPEG, MUPEG) operation environment temperature limitation and humidity. Combined application Compatibility with other IoT smart home devices assistants (Alexa nor google) Network Port (RG-45)	<ul style="list-style-type: none"> • Sensor data collection (camera, audio, presence, temperature, carbon monoxide) • Data storage location and reiteration time. • Shared with the third party or sold to the third party or for children's practices
4	Privacy policy	URL link or documentation	
5	Label barcode number/ID	Specifically, for this device	

3.2 Phase 2: Scoring system

There is a need to present the result of the security and privacy factors evaluation along with the final device score that is represented in the summarized label. It is important to choose the best common security and privacy factors to be evaluated and ensure they will help the IoT smart home consumers in their purchasing decisions. Therefore, a scoring system is designed based on the Common Vulnerability Scoring System (CVSS) version 3 [30]. This scoring system provides a universal way to help evaluate different security and privacy factors of the IoT smart home devices such as internet pairing that represent the method that the IoT smart home device is using to connect to the internet, configuration and authentication that discusses if there is any manual or automatic configuration required to launch the IoT smart home device, update modes that describe the updates scenarios to update the IoT smart home device's firmware, exposed services that discuss the services that this IoT smart home device accessing or controlling using the smart home network, vulnerabilities that analyze all IoT smart home device limitations in the hardware and software, protocols that present all the network protocols and standards used in communications by the IoT smart home device, network encryption that discusses the availability of the encryption in any data transmission inside and outside the home environment. It also helps in evaluating vulnerability severity in software, hardware, and firmware by setting metrics and formulas to calculate the score that helps in determining the urgency and priority of responses. Moreover, it provides a standard for reporting vulnerabilities and threats that could be used by anyone. This scoring system has a calculator that could be used to evaluate the vulnerability and provide a score for it based on three metric groups (base, temporal, environmental). Also, it uses a score range from 0/no-risk to 10/critical-risk [31].

3.2.1 Scoring Rubric

Seven factors will be examined, and values will be assigned for them to calculate the score for each factor and for the device to represent security, privacy, and firmware grade/score. This scoring rubric presents the weight for each scored factor in the IoT smart home labeling system. The calculated points are configured to emphasize the importance of the factor's attributes across the environment of the IoT ecosystem besides the CVSS support.

Device (total 57 Points): is for all scored factors. The higher the total the better grade it deserves. Here is a description of each factor in detail.

1. **Internet Pairing Technology (max of 3 points):** it describes the establishment of the network connection between the IoT smart home device and the local smart home network to provide internet connection and configuration to the IoT smart home device. The detailed points are shown in Table 7. Based on the connection technology, devices get different points.

Table 6: Internet pairing technology

Technology	Description	Points
Wi-Fi	The device is using a Wi-Fi connection to connect directly to the local network without any user interaction or network customization.	0
Low Energy	The device is connected to a combined mobile application for configuration and internet access (e.g Bluetooth).	1
Wired/cable	The device is connected to a local network router using a wired medium.	2
Manual network setup	The user is required to fill up the network credentials into the device to enable internet connection and configuration.	3

2. **Configuration and Authentication (max of 7 points):** This category refers to the configuration and authentication procedures that are required to set up the IoT smart home device for operation. As shown in Table 8, if the device is using a build-in default username and password, it gets 0 points. If no default configuration is involved, it gets 7 points.

Table 7: Configuration and authentication

Setup type	Description	Points
Default Configuration	The device is using the build-in default configuration such as the default username/password.	0
Manual configuration	The device required user interaction to set up the configuration such as creating a new user account with active email.	7

3. **Update Modes (max of 3 points):** A newly purchased device comes with firmware running on it. However, people usually reveal vulnerabilities and bugs in the firmware later. Good manufacturers can keep track of this and launch security updates regularly to fix the bugs. This requires the user to update the device's firmware when an update is available. The update modes refer to the procedure that is used to install the latest updates for the IoT smart home device's firmware. The scores are shown in Table 9. Devices that require a manual check and update to the firmware get 0 points. If a device can automatically install updates, it gets 3 points, which is the best update mode.

Table 8: Update modes

Technology	Description	Points
Manual	Updates are using the pull mode (the user is required to check for update and install it).	0
Permission required	Updates are using the push mode (the user will receive a notification for update downloading and installation).	2
Automatic	Updates are installed without user interactions.	3

4. **Exposed Services (max of 3 points):** Exposed services refer to the total number of services that a user of the smart home device could access using a local network connection to this device. Table 10 shows the number of exposed services of a smart home device and their corresponding points.

Table 9: Exposed services

Total services	Description	Points
More than 5	Such as video, audio, temp, presence, carbon monoxide.	0
3 to 4 services	Such as video, audio, temp, presence.	1
1 to 2 services	Such as video, audio.	2
No services	No services could be accessed or controlled using any local network access.	3

5. **Firmware vulnerabilities (max of 24 points):** A firmware is a mini system running on the IoT smart home device. Some of them may be very simple, and some of them are much more complex than others. Multiple vulnerabilities are often found in the firmware. Based on the CVSS list, each vulnerability is assigned to a risk level from critical to low. From a list of vulnerabilities for a smart home device, the numbers of critical risk vulnerabilities, high-risk vulnerabilities, medium risk vulnerabilities, and low-risk vulnerabilities can be found. One score is assigned based on the number of vulnerabilities of each risk level (see Table 11). Therefore, 4 scores are given to the device. The sum of the 4 scores is calculated to be the final score for vulnerabilities. For instance, if there are 4 vulnerabilities of critical risk level, 1 at high-risk level, 3 medium risk level vulnerabilities, and 5 low-risk vulnerabilities. Then the score will be 3, 6, 6, and 3 separately, and the total score is 18 (out of 24) points.

Table 10: Vulnerabilities

Risk Level	Description	Points		
		7 or more	4 to 6	1 to 3
Critical	Refer to the CVSS vulnerabilities list to check the risk level of the targeted vulnerability.	0	3	6
High				
Medium				
Low				

6. **Protocols (max of 8 points):** Table 13 shows that the smart home devices get scores based on the protocols it uses. The protocols in this category include non-standard custom protocol, 3rd party DNS, UPnP, HTTPS, NTPv3.

Table 11: Protocols

Protocol	Description	Points
Standard custom protocol	Such as IEEE wireless standards.	1
3rd party DNS	Using the DNS of the vendor or smart home assistance.	1
UPnP	universal plug and play protocol.	2
HTTPS	Hypertext transfer protocol + SSL	2
WPA/WPA2/WPA3	security standards that protect wireless networks	2

7. **Network Encryption (max of 9 Points):** The category refers to the encryption techniques or procedures that are used in the data transmission in the IoT smart home ecosystem network. As shown in Table X, it is divided into three categories to cover all communication types. Full data encryption means the data is encrypted when stored in the device and at transmission. Half data encryption indicates the data is only encrypted during transmission. And none means the data is not encrypted to protect its confidentiality at rest and in transmission.








Table 12: Network encryption

Communication parties	Description	Data encryption		
		Full	Half	None
Device-to-Cloud	The data between the IoT smart home device and the cloud service is encrypted when transmitted.	2	1	0
Mobile Application-to-Cloud	The data between the IoT smart home device's combined mobile application and the cloud service is encrypted when transmitted.	3	2	
Mobile Application-to-Device	The data between the IoT smart home device's combined mobile application and the IoT device itself is encrypted when transmitted.	4	3	

3.2.2 Security, privacy, and firmware factors scoring description

The table below represents all the detailed descriptions of the security, privacy, and firmware factors that are represented on the summarized label. Thus, provide factors information for the IoT smart home devices consumers for a better understanding of the evaluated factors.

Table 13: Security, privacy, and firmware factors scoring

#	Factor	Symbol	Description	Used method
1	Internet pairing		Establish of the network connection between the IoT device and the local network to provide an internet connection.	Wi-Fi, Bluetooth, Zigbee.
2	Configuration and Authentication		Configuration and authentication procedures that are required to set up the IoT smart home device for operation	Use default, customized or Manual.
3	Update mode		The procedure that is used to install the latest updates for the IoT smart home device firmware.	Permission required (Push mode), Manual (Pull Mode), Automatic.
4	Exposed service		The total number of services that a user of the smart home device could access using a local network connection to this device.	video, audio, temp, presence, carbon monoxide (fire).
5	Firmware Vulnerabilities		The shortcomings in the mini system running on the IoT smart home device.	Password Exploitation, Rogue Recordings, Outdated Software.
6	Protocols		The set of rules that format the data transmission over the local network and Internet.	non-standard custom protocol, 3rd party DNS, UPnP, HTTPS, NTPv3.
7	Network Encryption		Encryption techniques or procedures that are used in the data transmission in the IoT smart home ecosystem network.	Device to Cloud, Mobile Application to Cloud, Mobile Application to Device.

3.2.3 Scoring grades range

The scoring range has five levels. Each level has its own range. To find the right grade, it is required to calculate the total points that the IoT smart home device got after the evaluation of all security and privacy factors. Table 14 shows the scoring grades range in detail.

Table 14: Scoring grades range

Range	Grade
90-100	A
80-89	B
70-79	C
60-69	D
0-59	F

3.2.4 Example: Device “XY”

To illustrate the points calculation process, an example is presented here. In the device category, it got a total of 49 points based on the following factors: (1) Internet pairing ”3”, (2) Configuration and authentication “7”, (3) Update mode “3”, (4) Exposed service “3”, (5) Firmware vulnerabilities ”21”, (6) Protocols “5” and (7) Network encryption “7”. Then, the scores are the following: Device score: $49/57 = 0.86$. Finally, the grade assignments are the following: $0.86 \Rightarrow 86\%$ gets a “B” based on the following scoring grades range: A is for 90% to 100%, B is for 80% to 89%, C is for 70% to 79%, D is for 60% to 69% and F is for all lower than 60%.

3.3 Phase 3: Survey

The main goal of conducting the survey is to collect comments and feedback from IoT smart home devices experts, consumers data analysts and label designers to create a useful, powerful design and content for IoT smart home devices labeling system. Different factors should be considered and covered when designing the label to provide a high-quality labeling system that could be easily adopted and implemented by vendors or standards organizations. This phase is totally online [29]. This survey will be using Qualtrics [40] because of its powerful survey mailer to track, remind, online data collection, and thank respondents.

The survey should help in answering many questions that lead to the best decision in creating the high informative labeling system for IoT smart home devices. Some questions that could be answered are consumer awareness checks such as, what are IoT smart home consumers looking for when purchasing and are they afraid of such new technologies that are collecting sensitive and personal information about their lifestyle or environment [29].

There is a need to survey IoT smart home consumers, experts, and researchers to create a high-quality labeling system that could be adopted by IoT regulation organizations, specifically SASO. One of the survey methods that present a high-quality result and helps to create wise purchasing decisions is the probability sample survey. This type of survey is conducted if a researcher wants to generalize a result with statistical confidence from a few individuals who represent a larger number of people. This

survey must overcome or minimize four errors (coverage, sampling, nonresponse, and measurement) to improve the survey estimates for the best outcomes. A mixed-mode framework is applied if needed.

The surveys are web-based questionnaires because of the many benefits that internet service provides for both the surveyor and the researcher. Currently, internet access through computers and smartphones or tablets allows the questionnaire to be answered by a larger audience than before. Therefore, the survey design should meet all screen types and resolutions to avoid any issues when the user views the survey to answer. Mobile optimization is required for this survey. The survey will be distributed in Arabic and English languages to facilitate understanding and to reach a larger segment of participants.

This phase has four stages that are working in sequence to provide or output the desired results for the next stage inputs. Here are the stages with descriptions to show the expected output information:

1. **Survey for experts and scientists with a computer science background:** This stage targets Ph.D. degree holders who have a solid background in computer science or security. This stage helps in designing the prototype of both labels and provides a full picture about what is the content of the IoT smart home labeling system. The expert's feedback would help in choosing the best content to cover the main security and privacy factors. Also, it would help in choosing the best presentation of the information on the labels. This stage should cover:
 - What factors/features should be on the label, and which should not (provide a range of factors to choose from or add if the surveyor wants).
 - Specify a weight or value for each factor (a range from high, medium, or low).
 - The provided information from this factor is for (consumers with technical backgrounds, experts in IoT devices, manufacturers, etc.).
 - The place for each factor in the appropriate section.
 - What is the right order for the sequence of the section on the label (general information, security, privacy, technical specifications)?
 - The factors should be on the first label and the second label.

2. **Survey for regular consumers:** This survey narrowed the results of the outcomes from the consumers and provided a solid base to create a better version of the first prototype version of the IoT smart home device label. This stage should cover:
 - Consumer's security and privacy awareness check.

- When purchasing; do they look for the IoT product details document or do they trust the store's salesman representative or website?
- What do they look for when purchasing (security and privacy, price, functions provided, etc.)?
- Do they compare between the IoT devices when purchasing, what do they compare (price, brand name, etc.), or what piece of information helped in purchasing?
- Is security, privacy, and firmware label going to help you with better purchasing decisions?
- What will make you trust this label? Is it trusted if it is enforced or managed by (device manufacturer, government committees such as SASO, third party store or distributor)?
- Which are the most IoT devices that they are up to buying (security cameras, bulbs, sockets, etc.)?
- What privacy, security, or firmware issues that they are most afraid of when purchasing (selling their information, hacked, no privacy, etc.).
- What is the best information presentation (grades "A, B, C, D", Numbers, Emojis, Graphs)?
- What is the preferred layout and format for the IoT label (for both labels)?
- Do they recommend one label or two labels (summarized, detailed)?

The layout and content for IoT smart home devices labeling system prototype's is created.

This uses the data collected from the previous two stages to create an updated prototype of the IoT smart home label system. It should match the previous surveys' results and expectations.

3. **Short survey for social data analysis, risk management researchers, and label design experts:** This phase targets expert individuals in risk management and communication. This is the final stage that results in the final version of the IoT smart home security, privacy, and firmware labeling system.
 - Test the final version of the designed IoT smart home labeling system and examine all the sections and factors for general understanding, usability, and adaptability.
 - Are there any arguments that they need to address or change in any section/factors?
 - Is there any preference for grouping all the factors under one section or separating them into different sections would be better?

4. The final version for the IoT smart home device labeling system after the previous stage researchers and scientist examination and recommendations comments.

All the survey details are in chapter four (the survey implementation). Also, the distributed surveys could be found in appendix section (C,D).

Chapter 4: The survey implementation

This chapter is discussing the third phase of the development of the IoT smart home devices security, privacy, and firmware labeling system. It presents the four stages in detail and reflects their conclusions on the content and the design of the labels. There is a need to ask different groups of people who are familiar with the IoT smart home devices to have a good understanding of their needs and expectations from such new labels that discuss security and privacy features of IoT smart home devices. Therefore, the first survey is designed to ask IoT smart home devices experts about the major concerns about any security and privacy features that they believe should be covered in the new labels. Also, the best presentation of the information to make sure that all IoT smart home devices consumers will easily understand the labels and use them for better purchasing decisions. The result of this experts' survey helped in creating the first draft of the initial versions of the IoT smart home devices labels. These drafts are used in the second survey. After that, the second survey is targeting the IoT smart home devices consumers in Saudi Arabia and the United States. This helps in evaluating the consumers' security and privacy awareness and determining the need for such labels in the Saudi Arabian IoT smart home devices market. This survey collects data about the content and the purchasing scenarios to better group the information to fit them in the best section that describes them properly. This survey should update the first initial labels and provide better versions that will be discussed by IoT smart home devices data analysts, risk management professionals, and labels designers in the third stage. The third stage helps in adding the final comments on the design and the contents of both labels to output the best IoT smart home devices security, privacy, firmware summarized, and detailed labels. The conclusion of this phase is two versions of IoT smart home devices security, privacy, and firmware labels that complement each other. The first label is the summarized one and will be presented on the IoT smart home devices boxes with a QR code to be scanned to direct the consumer to the second version of the IoT smart home devices detailed label for extra information about different security and privacy features about the target device.

All surveys were conducted electronically and distributed in Saudi Arabia and the United States using shared direct links Through Whatsapp application and emails. Qualtrics application help in providing a smooth multiple access to the surveys in the same time by different participants.

4.1 Survey for experts and scientists with computer science backgrounds:

This survey is targeting IoT and computer security experts to provide their feedback on IoT smart home devices' privacy and security aspects. This survey is designed to support some major concerns about the content and design of the IoT smart home devices' security, privacy, and firmware label, which should describe the IoT smart home device from different points of view to help consumers with brief security and privacy characteristics about it. Also, the technical aspects covered about the IoT smart home device, in the detail labels technical specification section, are created to provide information about IoT smart home devices like power consumption, network connectivity, and any supportive combined applications. Moreover, for the security and privacy factor's development and usage, these factors are considered the main purpose for calculating the device's final security and privacy score. This score would help in providing a confident purchase decision by the IoT smart home devices consumers. In addition, the best representation for the security and privacy factor's score and the IoT smart home devices' security and privacy final score. Experts are familiar with the security and privacy issues that IoT smart home devices are suffering from. Therefore, their feedback on the score's representation would have a great impact on the label's design.

Moreover, one of the IoT smart home devices' label design concerns was the best presentation of the device's final security and privacy score and the individual score for each security and privacy factors. However, different representations are widely used internationally on electricity and water efficiency labels. For example, Australia uses the star shape to represent the energy rating result. Brazil uses face emojis to represent the energy rating; a smiley face for good devices or black straight face for below-average rated devices. Canada uses a bar graph numbered with the final score that ranged from 0 to 100. The Kingdom of Saudi Arabia uses a bar graph with letters that ranged from A to F where A is the best and F is the worst [42] [19]. After reviewing the different representations around the world, it is important to ask the IoT smart home devices experts about IoT smart home devices' preferred final security and privacy score representation and the individual security and privacy Factor's score representation.

The IoT smart home devices security, privacy, and firmware survey for experts is in the appendix section C.

A. Survey for experts with a computer science background results and analysis:

This survey was distributed through emails and shared links on the Whatsapp application. The total number of participants in this survey is 71 IoT smart home devices experts. 90% of participated experts are from King Abdul-Aziz university from the faculty of computer science and information technology in Saudi Arabia and 10% are from different Saudi Arabian universities. Here are two Figures 5 and Figure 6 for their highest completed level of education and their experience in the Computer Science or Data Security field (in years):

Figure 5: Highest completed level of education

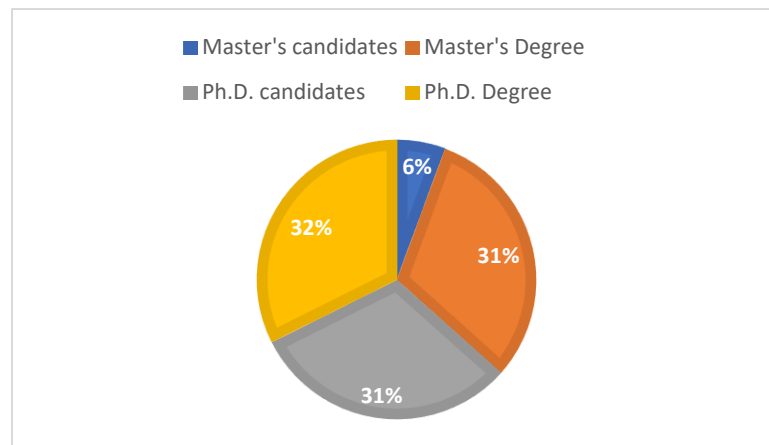
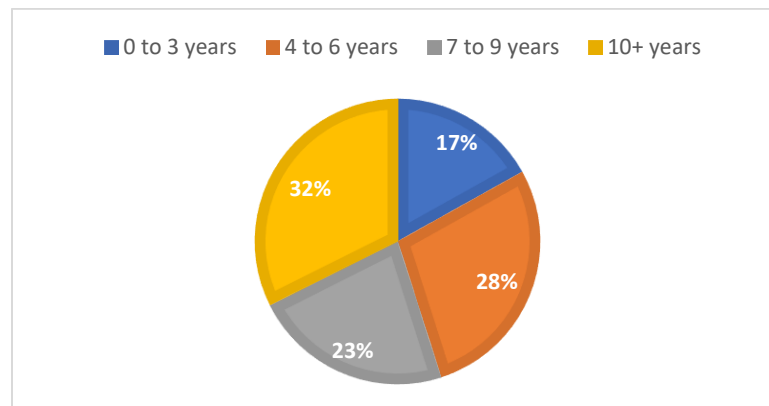


Figure 6: Experience in the Computer Science or Data Security field (in years)



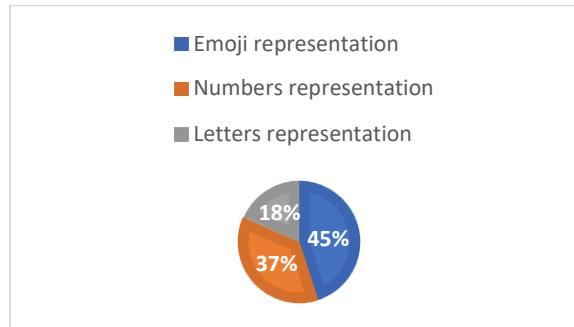
- **Data analysis for Q1:**

Which representation do you prefer for describing the factor's score?

The three provided options (Emoji, numbers, and letters representations) are very common in different label information representations. The choice should provide clear and quick information for the reader to understand the label's information in seconds. Based on the chart below, 32 experts believe the Emoji representation is the best representation of the security and

privacy factor's score, making up 45% of the vote. Figure 7 below shows experts' answers about the three options:

Figure 7: Security and privacy factor's score representation

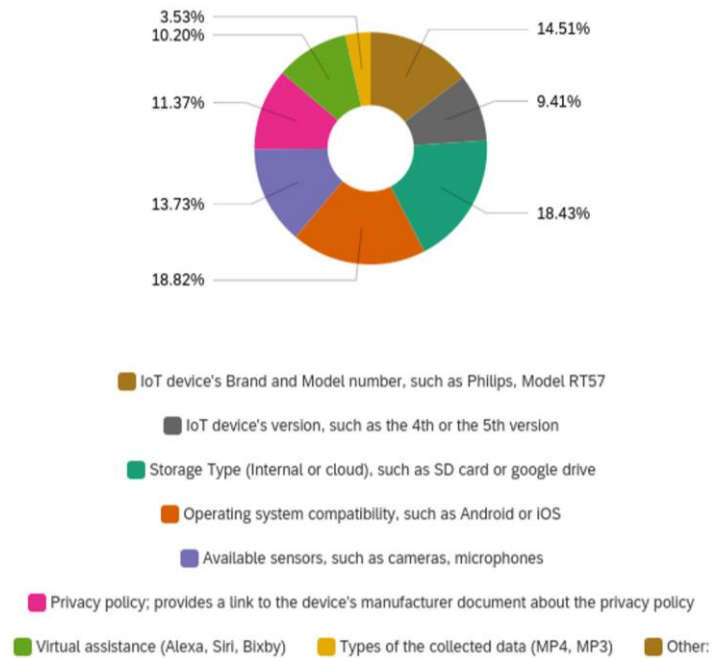


- **Data analysis for Q2:**

In the general information section of all label designs, I have included 4 default categories: Name, Warranty Lifetime, Firmware version, and Firmware update lifetime. Please choose 4 additional categories to include based on your expertise?

This question provided options for the label's content that will be presented in the general section of the summarized and detailed labels. Experts are allowed to choose more than one answer to facilitate the need for each label's content and to prioritize the top-rated ones to be added to the label's content. Four default types of information are already added to the labels which are the device's Name, Warranty Lifetime, Firmware version, and Firmware update lifetime. The four highest-rated choices by the experts will be added to the default ones to conclude the general information section by having 8 different information types related to the security and privacy aspects. This Figure 8 represents the experts' answers and their preferences.

Figure 8: General information section content

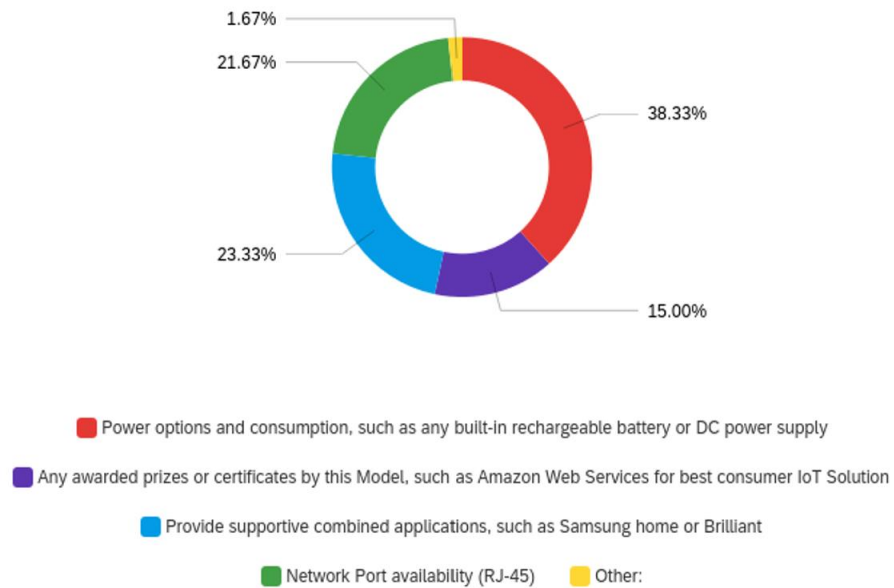


- **Data analysis for Q3:**

For the detailed label's technical specification section, do you prefer to know about any of the followings?

This question provided 5 options to select the best content that will be presented in the technical specifications of the detailed label. Experts are allowed to choose more than one answer to facilitate the need for each label's content and to prioritize the top-rated ones to be added to the label's content. There are three default types of information that are already added to the labels which are the device's SDRAM or Flash Memory, Smart assistance, and Network ports availability (connectivity information). The two highest-rated choices by the experts will be added to the label's default ones to conclude the technical specifications section by having 5 different information types related to the device's technical security and privacy aspects. Figure 9 represents the experts' answers and their preferences:

Figure 9: Technical specifications section content

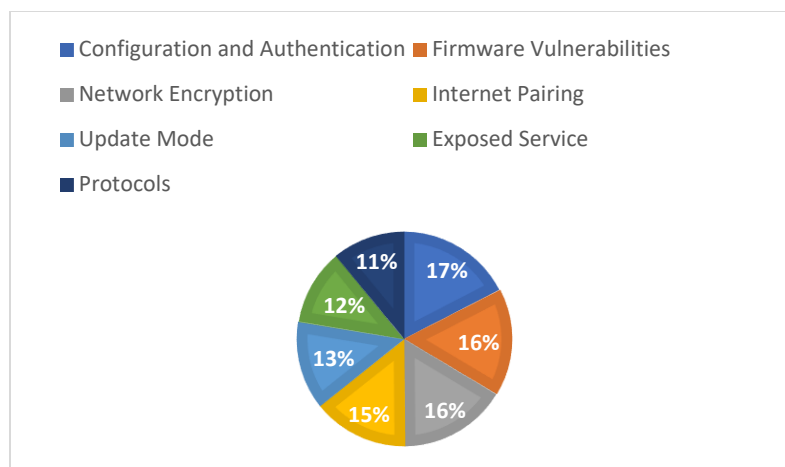


- **Data analysis for Q4:**

Which security and privacy factors do you prefer to see on the IoT smart home device's label, to assist consumers to make better purchase decisions? Pick the best 5 useful and understandable factors based on your expertise?

This question has a major impact on the development of the IoT smart home devices' security, privacy, and firmware labeling because it reflects the understanding of each factor's purpose in examining the final security and privacy score. Each factor is designed to assess specific security or privacy aspect that should make a big change in a consumer's purchase decision. Experts are allowed to pick more than one answer to reflect their preferred security and privacy factors that they believe would help IoT smart home devices consumers choose the best available device. Figure (10) represents all factors that experts choose, and higher percentage means more remarkable security and privacy factors

Figure 10: Security and privacy factors

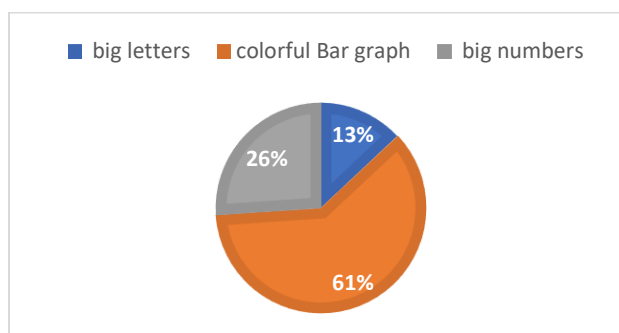


- **Data analysis for Q5:**

Which representation do you prefer for the final security and privacy score?

One of the important features of this label design is to provide a clear and quick understanding of the IoT smart home device from reading the IoT security and privacy label. The design of the summarized label should reflect the security and privacy aspects of the IoT smart home devices in seconds. This would help the consumer in comparing different IoT smart home devices quickly and save some time in finalizing their purchasing decision after reading the detailed label if that is required for an extra confident purchase. Therefore, three different representation of the final security and privacy score are represented for the experts to choose from. Their choice should reflect the intention of the IoT smart home devices consumers. More than half of the experts preferred the bar graph representation and after calculating the mean (1.87) and the trend direction, it is the majority choice. The bar graph is widely used in different countries such as the Kingdom of Saudi Arabia [19]. It provides a clear vision of different levels of scores besides the colors that reflect the final score of the device. Figure 11 that represents the experts' choices about the final security and privacy score:

Figure 11: Final security and privacy score



B. Survey for experts with a computer science background conclusions and decisions:

After analyzing the IoT smart home devices security and privacy survey for experts, there is a need to update the design and content of the proposed summarized and detailed labels. After calculating the mean (1.73) and the trend direction of the collected data for Q1, we found that IoT smart home experts preferred the Emoji representation for the security and privacy factors score representations. This choice will provide a quick and clear appearance for the labels to be recognized and understood by different types of consumers.

Based on the collected data from Q2, the highest four choices that experts preferred to see on the general sections of both labels are the IoT device's Brand and Model numbers, such as Philips, Model RT57, IoT device's version, such as the 4th or the 5th version, Storage Type (Internal or cloud), such as SD card or google drive, and Operating system compatibilities, such as Android or iOS. This information would provide a powerful insight that should be known by IoT smart home devices consumers before any purchase because they are considered important components for any safe purchase. These choices will be added to the label in addition to the default information of this section on the summarized and detailed labels.






The technical specifications section is located only on the detailed label. It is designed to provide answers for major technical concerns that a regular IoT smart home device consumer would like to know about for a safer and more confident purchase decision. Therefore, based on Q3, IoT smart home devices experts' preferred choices that they believe would provide the IoT smart home consumers with the best answers. This section has three default information types that are SDRAM or Flash Memory, Smart assistance, and Network ports availability (connectivity information). In addition, the experts' added Power options and consumption, such as any built-in rechargeable battery or DC power supply, and provide supportive combined applications, such as Samsung home or Brilliant to the default information.

Based on data collected from Q4 about the IoT smart home devices' security and privacy factors, the importance of the factor's differs for each expert. Their preference helps in understanding which factors they believe will have a great impact on the IoT smart home consumers' purchase decisions. The data collected shows that all factors are preferred by different experts because all choices have been selected by them.

The main section that the summarized label is designed to present is the final security and privacy score. This score should provide a great impact on the IoT consumer's preference when purchasing. Therefore, it should be presented in a clear and understood way to save more time for the purchaser to compare different devices or continue reading through the summarized label and look for the detailed label for extra information. The collected data shows that IoT smart home experts believe that the Bar graph is the best presentation of this important information. Therefore, this choice will be added to the summarized label along with the Emoji representation for security and privacy factors that are calculated and presented in the following.





In the beginning, the range of security and privacy factors representation has five levels. Each level has an assigned emoji for it as shown in the following table (15), where level 1 is the best condition or score and 5 is the lowest and worst level.

Table 15: Factors Range levels

Level	Emoji score
1	
2	
3	
4	
5	



1. Internet Pairing Technology (max of 3 points):

Table 16: Internet Pairing Technology ranges

Technology	Points	Score
Wi-Fi	0	
Low Energy	1	
Wired/cable	2	
Manual network setup	3	




2. Configuration and Authentication (max of 7 points):

Table 17: Configuration and Authentication ranges

Setup type	points	Score
Default Configuration	0	
Manual Configuration	7	





3. Update Modes (max of 3 points):

Table 18: Update modes ranges

Technology	points	Score
Manual	0	
Permission required	2	
Automatic	3	






4. Exposed Services (max of 3 points):

Table 19: Exposed services ranges

Total Services	points	Score
More than 5	0	
3 to 4 services	1	
1 to 2 services	2	
No services	3	






5. Firmware Vulnerabilities (max of 24 points):

Table 20: Firmware Vulnerabilities ranges

Risk Level	Points	Score
	21 to 24	
	19 to 20	
	17 to 18	
	14 to 16	
	13 or lower	






6. Protocol (max of 8 points):

Table 21: Protocol ranges

Protocol	Points	Score
standard custom protocol	7 to 8	
3 rd party DNS	5 to 6	
UPnP	3 to 4	
HTTPS	2	
WPA/WPA2/WPA3	1	

7. Network Encryption (max of 9 points):

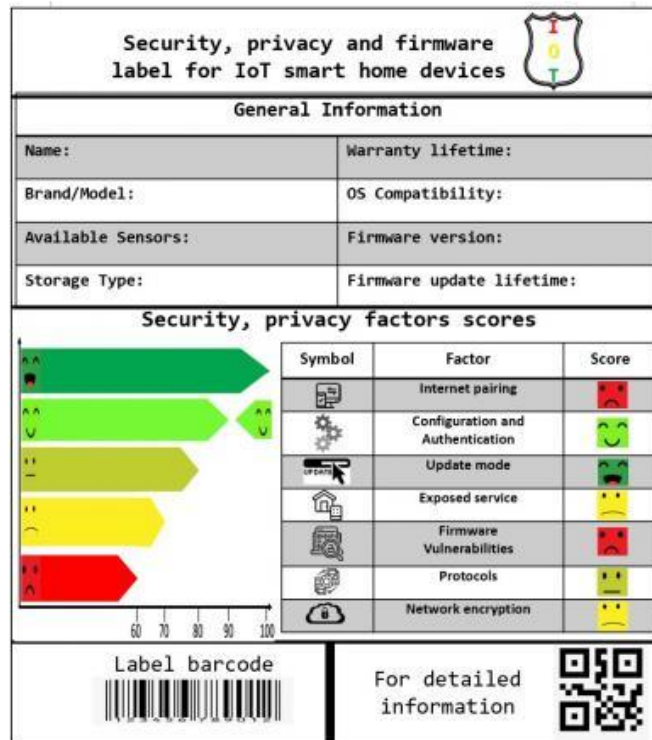
Table 22: Network encryption ranges

Communication parties	points	Score
	8 to 9	
	6 to 7	
	4 to 5	
	2 to 3	
	0 to 1	

It is important to mention that If any of the security and privacy are in poor level (red color) it is not encouraged to purchase this IoT smart home device because it is very easy to gain access to the information that this factor presents. After discussing the survey’s data collected from IoT smart home devices experts, this is the updated version of the IoT smart home security, privacy, and firmware labels. These labels will be presented and discussed with regular consumers of IoT smart home devices for different goals and better development procedures for the labels. Both labels are translated into Arabic languages for non-English speakers.















- ***The smart home security, privacy, and firmware summarized label:***

Figure 12: The IoT smart home security, privacy, and firmware summarized label (experts version)



- *The IoT smart home security, privacy, and firmware detailed label:*

Figure 13: The IoT smart home security, privacy, and firmware detailed label (experts version)

Security, privacy and firmware label for IoT smart home devices 					
General Information					
Name:		Warranty lifetime:			
Brand/Model:		OS Compatibility:			
Available Sensors:		Firmware version:			
Storage Type:		Firmware update lifetime:			
Security, privacy and firmware factors scoring					
#	Factor	Symbol	Description	Used method	
1	Internet pairing		Establishment of network connection between the IoT device and the local network to provide internet connection.	Wi-Fi, Bluetooth, Zigbee.	
2	Configuration and Authentication		Configuration and authentication procedures that are required to set up the IoT smart home device for operation	Use default, customized or Manual.	
3	Update mode		The procedure that is used to install the latest updates for the IoT smart home device firmware.	Permission required (Push mode), Manual (Pull Mode), Automatic.	
4	Exposed service		Total number of services that a user of the smart home device could access using a local network connection to this device.	video, audio, temp, presence, carbon monoxide (fire).	
5	Firmware Vulnerabilities		The shortcomings in the mini system running on the IoT smart home device.	Password Exploitation, Rogue Recordings, Outdated Software.	
6	Protocols		The set of rules that format the data transmission over the local network an Internet.	non-standard custom protocol, 3rd party DNS, UPnP, HTTPS, NTPv3.	
7	Network encryption		Encryption techniques or procedures that are used in the data transmission in the IoT smart home ecosystem network.	Device to Cloud, Mobile Application to Cloud, Mobile Application to Device.	
Data sensor practices					
Type	Symbol	Data storage location	Data retention time	Shared or sold	Collection recurrence
Camera					
Microphone					
fire					
Temperature					
Movement/Location					
Technical specifications					
Specifications			Description		
Power and max power consumption					
SDRAM or Flash Memory					
Combined Applications					
Smart Assistance					
Connectivity Information					
Label Barcode 			Privacy Policy www.Privacy.sa		

4.2 Survey for regular consumers:

This survey targets the IoT smart home devices, regular consumers because they are the main subject that this label is designed for. Therefore, this step requires engaging them in the development of it and to request their feedback about the content, design, and adaptability of such a new label that focuses on enhancing their security and privacy knowledge to create an educated society that knows how to use this technology. The survey is designed based on the outcomes of the previous survey to ensure the best development procedures for the labels.

There are several goals that this survey aims to support. Firstly, a consumer's security and privacy awareness check to assess the IoT smart home consumers' security and privacy understanding and practices. Secondly, the purchasing scenarios that regular consumers follow to purchase IoT smart home devices. Thirdly, the comparison factors that are considered by regular IoT smart home devices' consumers without the availability of labeling ideas. This should support the selection of the presented security and privacy factors on the label. Finally, measuring the level of acceptance for this label, and understanding the real need for such a one.

The IoT smart home devices' security, privacy, and firmware survey for regular consumers are in appendix D.

A. Survey for regular consumers results and analysis:

This survey was distributed through direct shared links on the Whatsapp application with two language options (Arabic and English) in the United States and Saudi Arabia. Both versions are identical but with different languages. This survey targets all IoT smart home devices in different universities, technology companies, friends, and families who are using this technology. The total number of participants in this survey is 382 IoT smart home devices consumers. 86% of them are from Saudi Arabia. Figure 14 shows that 55% of the participants are between the ages of 30 and 49 years. It proves that this technology is widely adopted among this segment and their participation in this study will increase their confidence in the IoT smart home products because they are supporting the creation of the IoT smart home security, privacy, and firmware labels. In addition, Figure 15 shows the highest completed level of education for this survey participants. It shows that 42% of them completed a bachelor's degree.

Figure 14: Age

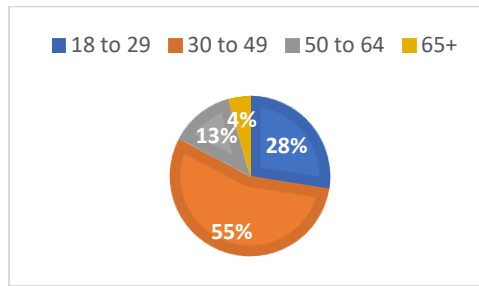
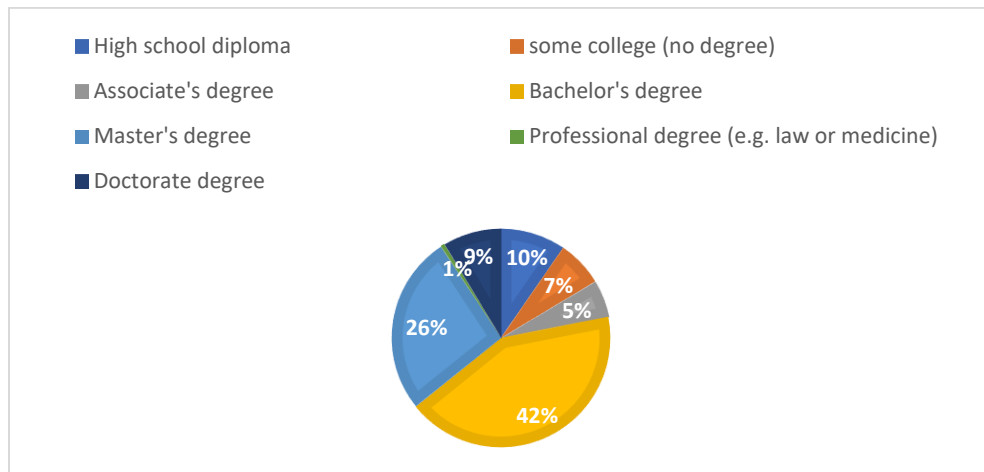


Figure 15: Highest completed level of education

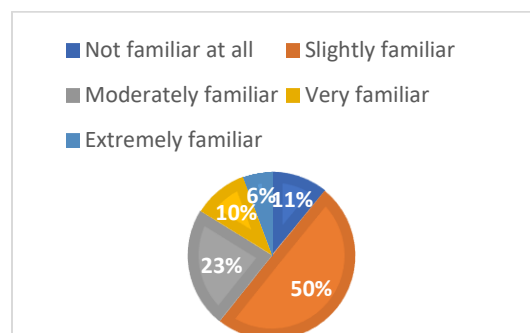


- **Data analysis for S1/Q1:**

How familiar are you with computer security and privacy issues?

By calculating the average and the segment direction, the participants are slightly familiar with computer and security issues. This shows that they have some background in IoT technology and its privacy and security issues that this label mentions for consumers. Figure 16 shows the analysis statistics for this question.

Figure 16: Familiarity with computer security and privacy issues

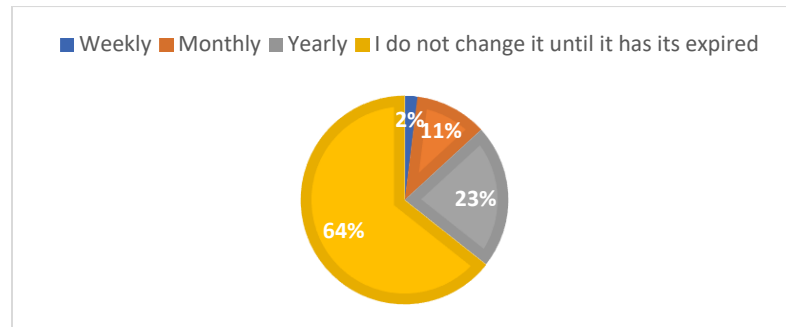


- **Data analysis for S1/Q2:**

How often do you change your passwords?

Figure 17 shows that 64% of the participants do not change their passwords until it expires. This is a security issue because the participants' familiarity with their passwords would eventually lead them to being compromised if they did not change their passwords regularly.

Figure 17: Passwords changing period

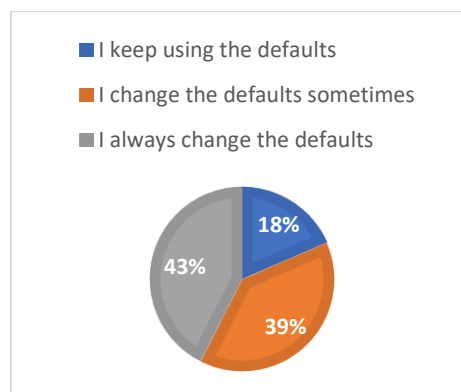


- **Data analysis for S1/Q3:**

Do you change your default username and password that come with the device?

The participants believe that changing the default username and passwords for any new accounts is important. The segment direction of this question is always changing the default user credentials. Figure 18 shows that 43% of the participants care about their information privacy and security, and they will appreciate any service that could provide support to this area.

Figure 18: Changing default username and password

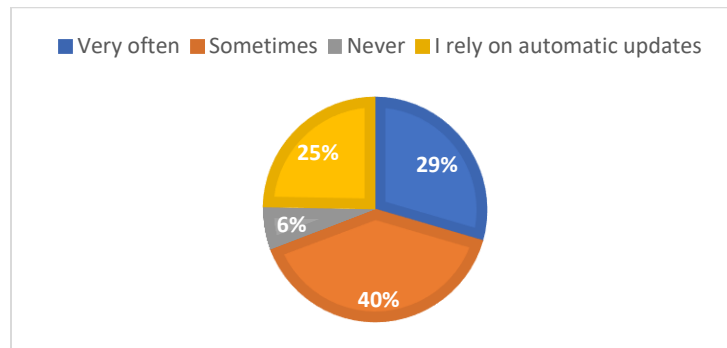


- **Data analysis for S1/Q4:**

How often do you check for the device's software updates?

Figure 19 shows that only 25% of the participants rely on automatic updates to ensure that their devices are up to date. Thus, a need for automatic updates to be the default mode is required by IoT smart home devices manufacturers, because almost 40% of the participants are sometimes checking for new updates. It is very important to ensure that IoT smart home devices are up to date to ensure the highest security and privacy levels for homeowners.

Figure 19: Software updates check

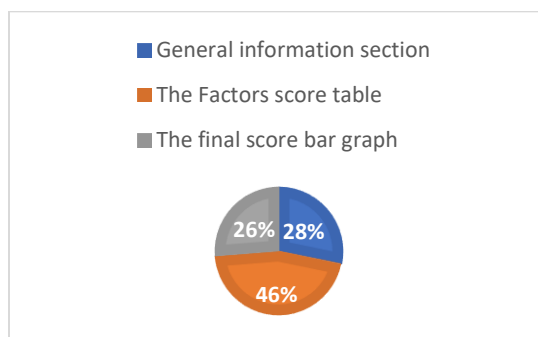


- **Data analysis for S2/Q1:**

In the summarized label, which section do you think would help you the most in purchasing decisions?

This question focuses on the most important section that IoT consumers would look for on the label to have quick and adequate information about the IoT smart home devices' security and privacy aspects. Figure 20 shows that 46% of the participants think that a factors' score table would help them the most in having the required amount of information for a purchase decision. They believe that the representation of a score for each factor would show the strength and weaknesses of each factor. Therefore, they might prefer some factors to be higher than others to create a purchase decision.

Figure 20: Summarized label most important section

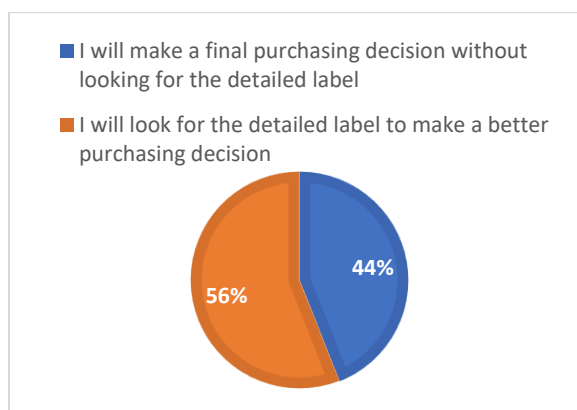


- **Data analysis for S2/Q2:**

Based on the information provided by the summarized label, if all security, privacy and firmware features about an IoT smart home device matches what you need, would you still look for the detailed label or would you directly make a purchasing decision instead?

Figure 21 shows that 56% of the participants would look for the detailed label for extra confident purchase decisions. This shows the need for extra details about the IoT smart home devices that should describe additional characteristics of IoT devices. The detailed label presents important information that most IoT smart home consumers would like to know about before purchasing such as the available sensor types and how they record and store the collected data.

Figure 21: Summarized label is enough

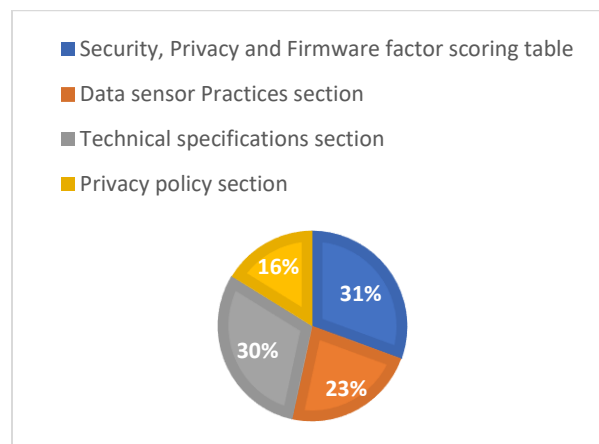


- **Data analysis for S2/Q3:**

There are four sections in the detailed label. Which section are you going to look for the most in this label?

The detailed label is considered the last source of information that provides security and privacy aspects for the IoT consumer. It has sections that are designed to explain any conflicts or missing information that were not presented on the summarized label. Figure 22 shows that there is no specific section that is preferred by IoT smart home devices' consumers because there is no adoption that they agreed on the most or even more than 40%. Therefore, all sections look important to the participants, and they feel that all should be provided in this label. However, the privacy policy section has the minimum preference of 16%, because it provides information that is provided by the manufacturer and could not provide a direct impact on the IoT devices consumer's purchase decision.

Figure 22: Detailed label preferred section

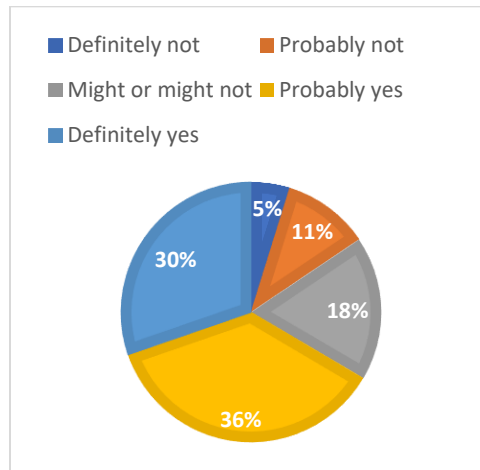


- **Data analysis for S2/Q4:**

When purchasing an IoT smart home device, will you look for the product's detailed label?

Figure 23 and the statistical analysis for this question show that the segment direction answer is willing to read the detailed label. Their desired need is based on the IoT device that they are willing to purchase. However, if the device has no sensor to collect data, the need to read this label will decrease and vice versa. Therefore, all IoT smart home devices should have this label even if they have basic functions to perform such as smart bulbs.

Figure 23: Reading the detailed label

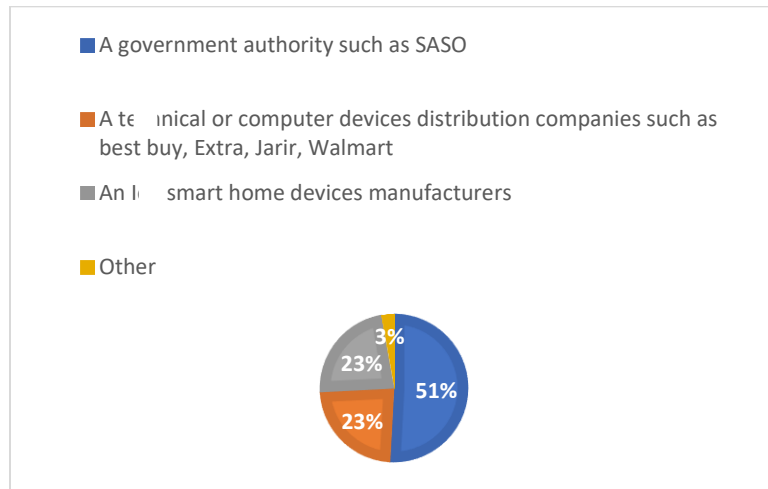


- **Data analysis for S2/Q5:**

Will you trust a IoT smart home devices label if it was created by: (Select all that apply)

Consumer trust is hard to achieve, especially when it deals with sensitive information about them. There are different ways that IoT smart home devices' manufacturers use to influence consumers to purchase their products, such as YouTube videos that show the product's functionality or by presenting their products in use by celebrities around the world. However, different kinds of consumers would appreciate any government support for any product because they assume that governments would not support any weak devices of any kind. Therefore, Figure 24 shows that 51% of the participants (most of them are participants from Saudi Arabia) agreed to have a government sponsor for the label to trust it. Besides, the idea of this label is not implemented yet in Saudi Arabia. It is important to be presented and sponsored by a trusted authority to be adopted and used by IoT consumers.

Figure 24: Labeling sponsor

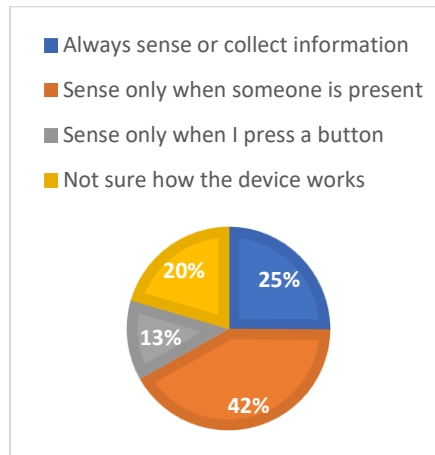


- **Data analysis for S2/Q6:**

If you own a smart doorbell that is equipped with a camera and microphone sensors, how often do you think these sensors would sense or collect information?

IoT smart home devices consumers are adopting these devices and installing them in their environment such as homes or offices which ought to be safe and secure places, to perform a specific function that these devices were designed to do so. However, different stories or videos on the internet show some bad or tragic experience that prevents some people from adopting such technology. Understanding the way that these devices work would help in feeling comfortable. This question aims to measure the understandability of the IoT consumers on the way that these devices work and collect data from their surrounding environment. This understanding would help simplify the need for the label to present all available sensors that each device has and how they are functioning. Figure 25 shows that 42% guessed the right answer that doorbells will sense data when someone is presenting in front of the door, this shows that the participants are familiar with the IoT smart home devices functionality. However, 20% of this question's participants state that they are not sure how these devices work. Therefore, one of the major goals of this label is to educate this type of IoT smart home device's consumers and help them understand the functionality of the targeted devices before purchasing to be safe, secure and to protect their home environment.

Figure 25: Data sensing procedures

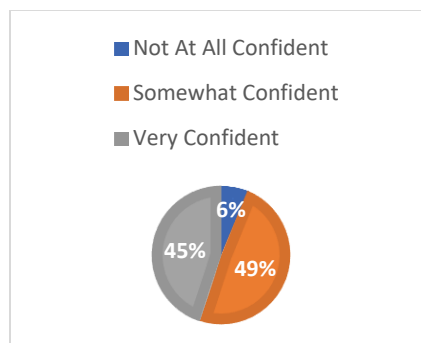


- **Data analysis for S2/Q7:**

If you see that an IoT smart home device has a full score on its security, privacy and firmware attributes, how confident would you be in your purchasing decision?

The IoT smart home security, privacy, and firmware label is new and has never been implemented in many countries around the world. Adopting such new ideas to the huge electronic market in the kingdom of Saudi Arabia and influencing regular IoT smart home consumers to accept it and trust it is a big challenge. However, when they read this label and use it to support their purchase decisions and see that the label is providing scores for different security and privacy factors, they will trust it and look for it whenever they purchase such devices. Figure 26 shows that segment direction with a 49% of this question participants feel some confidence to see this label when purchasing. Their feeling proves the need for such ideas to help IoT smart home devices' consumers to be safe and protect themselves from non-secure IoT devices.

Figure 26: Trusting the label's information

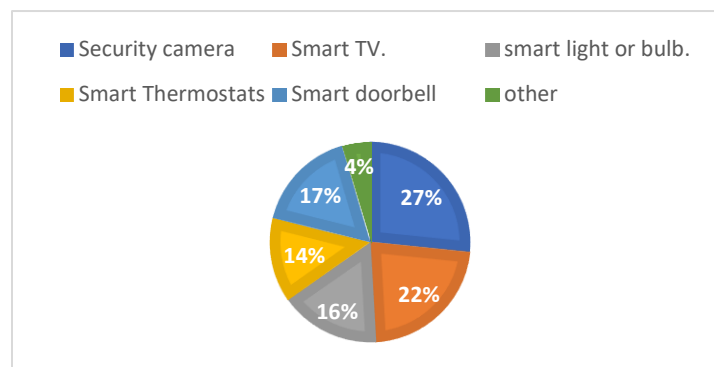


- **Data analysis for S3/Q8:**

What IoT smart home devices are you willing to buy? (Select all that apply)

Figure 27 shows that the smart security camera is the first device that participants are willing to purchase, by having 27% of the answers among other options. This is because the wide adoption of security cameras provides the same functions but with limitations such as no motion detection and cloud storage on the regular smart security cameras. However, this type of smart home device is crucial because of the personal data that could be collected about the homeowner and his environment if this device is hacked. It is very important to use the best security and privacy aspects in such devices because of the sensitivity of the data that could be breached.

Figure 27: IoT smart home devices preferences

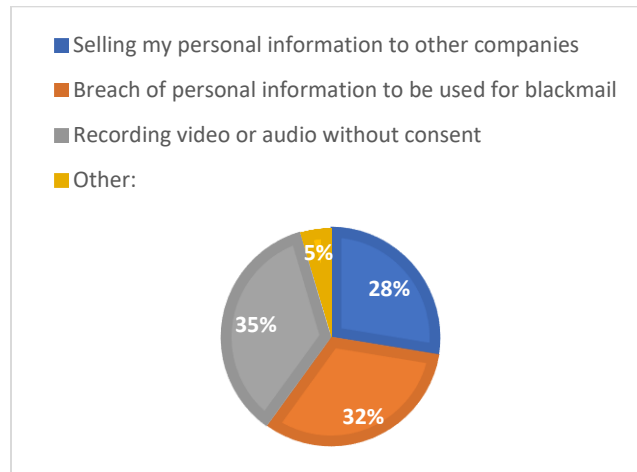


- **Data analysis for S3/Q9:**

What privacy, security, or firmware issues are you most afraid of when purchasing an IoT smart home device?

Figure 28 shows that IoT smart home devices' consumers are afraid of different types of personal data breaching and usage. The results show that 35% of the participants are afraid of being recorded without their consent, which is the worst-case scenario that any homeowner is afraid of. The main reason for this fear is that they know that these devices are connected 24/7 with internet service to function, this would make them easy targets if weak security and privacy network protocols are used. Shodan.io [43] is a library that presents a lot of weak IoT smart devices around the world that could be accessed without any authorized access. Thus, it is very important to choose the best smart home security camera that is equipped with the best security and privacy aspects.

Figure 28: Security and privacy fears

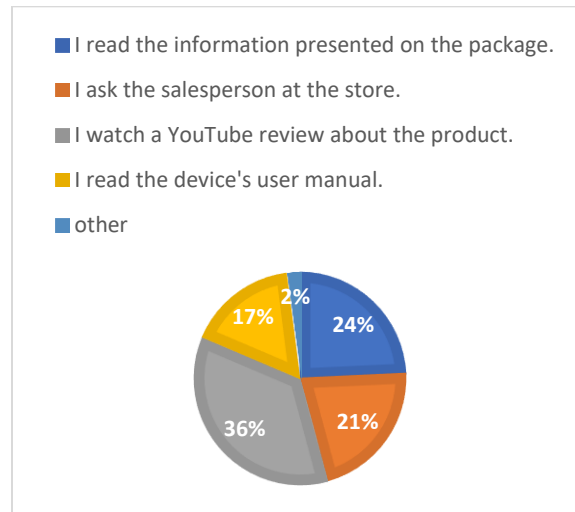


- **Data analysis for S3/Q10:**

How do you typically research for IoT smart home devices that you purchase?

Today, there are different resources to find information about any topic. The internet eases this by providing different data presentations such as articles, audio, or video that could be freely accessed. One of the most popular channels that provide video content about different topics is YouTube. Figure 29 shows that 36% of the participants are watching YouTube videos about any IoT smart home devices that they are about to purchase. These videos normally show how to install the device, provided functions, configuration, or troubleshooting, they don't discuss any security or privacy issues that homeowners suffer. Moreover, 24% of the participants prefer to read the information that is displayed on the device's package. This information may not mention anything about security or privacy aspects too. In addition, 21% of the participant ask the salesperson in the stores, this could be misleading for different reasons. Only 2% of them mentioned that they look for devices rating on third party websites such as Amazon or BestBuy, others mentioned that they ask their friends about their experience. Therefore, it's important to educate regular IoT smart home devices' consumers and provide them with some important information that they can rely on to have a confident purchase decision.

Figure 29: Get information about the device

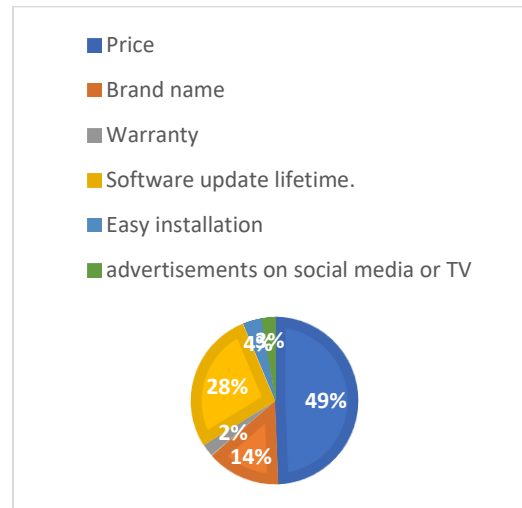


- **Data analysis for S3/Q11:**

Please order the factors that you usually consider when purchasing IoT smart home devices? (1st factor is the highest priority in the list)

Different factors influence IoT devices' consumers to purchase them. However, Figure 30 shows that the price factor is playing a major role in their purchase decision with 49% among other factors. Budget imitation is always important, but it is important to make sure that saving money on such technology should not be at the expense of the bad consequences that might cost more than the saved amount such as personal bank account breaching. Furthermore, 28% of the participants believe that the software update lifetime availability is considered in their purchase decisions. It is good to know that participants are not trusting the advertisement on social media or TV. This factor is the lowest with only 3%.

Figure 30: Purchase factors

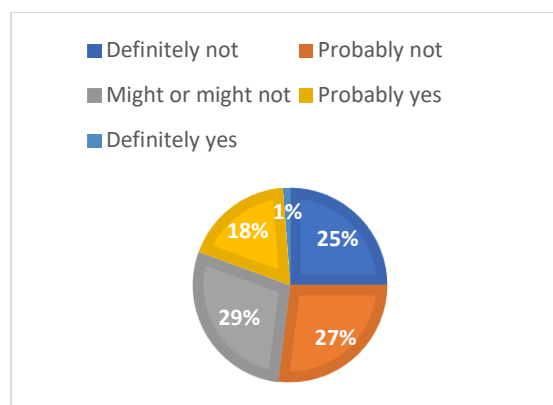


- **Data analysis for S3/Q12:**

If the device that you are about to purchase is in the right budget range and comes from a well-known manufacturer, but it does not have trustworthy security and privacy characteristics, will you still purchase this IoT smart device?

Figure 31 shows that the segment direction for the answers is going towards not buying the IoT smart home devices if they are in the budget range, but the label presents weak security and privacy scores. This proves that they care about the security and privacy aspects of their devices and the protection of their data too.

Figure 31: Purchase non-secure IoT devices



B. Survey for regular consumers conclusion and decisions:

The answers provided in this survey are providing a good example of the concerns and interests of regular consumers of the IoT smart home devices. However, there are some important points that this survey concludes that help in understanding the need for the IoT smart home devices' security, privacy, and firmware labels, and the adoption of such ideas by regular consumers. Here are the points that this survey concludes:

The IoT smart home devices' consumers understand the need for their data protection, and they believe that it's important to ensure the highest standards in any IoT smart home devices they adopt. Additionally, they have some basic technical background about the IoT smart home technology that helps them in choosing the proper way to update and control their devices.

The factor score table in the summarized label is providing the most important information that helps the IoT smart home consumers to make purchase decisions about any IoT smart home devices they target. This section should be easy to read and have some symbols that provide a hint about the security and privacy factors in case the reader does not understand the meaning of the factor. However, they appreciate the need for extra details that are provided on the detailed label. Therefore, more than half of the participants will look for the QR code in the summarized label to read more about the device that they are about to purchase.

The detailed label has more information that would help the IoT smart home devices', consumers to better understand the target device and have a confident purchase decision. However, all label sections are important to be read because every section is providing special information about the device that is not available in the summarized label. Besides, the participants do not have a preference for one section over another, because of the importance of the presented information in each section.

The idea of the IoT smart home devices' security, privacy and firmware labels is new. It needs time to be used and recognized by the IoT smart home devices consumers. However, a sponsor with a powerful reputation would help the adoption and the distribution of this idea to reach the Saudi Arabia market soon. This is clear because more than half of the participants recommend that this label is managed and created by government authority. This procedure will gain the trust of the consumers and make them accept all the presented information on the labels.

The adoption of IoT smart home technology is increasing around the world. However, this adoption will increase if the consumer's fear about this technology is explained and reduced. This could be done using the IoT smart home devices' security, privacy, and firmware labels. This will also provide honest feedback on any IoT smart home devices for others (consumers or manufacturers) to help in protecting the community and to force the manufacturers to develop better IoT smart home devices with the most updated security and privacy standards without expensive prices to help more people to try this great and powerful technology.

The distributor stores such as BestBuy should educate their salespersons about the security and privacy aspects that IoT smart home devices should be equipped with. This would also assist in consumers understanding the way that these devices work and the used procedures that these devices follow to collect data from their surrounding environment, to warn the purchasers if they are not comfortable with these procedures.

The survey's results affected the design and the content of the IoT smart home security, privacy and firmware labels (summarized and detailed) will be presented for the social data analysis, risk management researchers, and label's design experts for any comments and feedback.

4.3 Social data analysts, risk management researchers, and label design experts:

This stage of the survey section is created to ensure that the final versions of the IoT smart home devices' security, privacy, and firmware labels are complete and ready to be published and used. Therefore, Social data analysis, risk management researchers, and label design experts were requested to review them to ensure the best outcomes for both labels. Overall, the participants of this survey are two label designers, one Risk management, and two data analysts. That concludes the sample size of five participants.

A short online survey was distributed among social data analysts and risk management experts through emails and Zoom meetings to get feedback about the content of the final versions of the labels. Also, they were requested to evaluate the amount of the information in both labels' different sections to ensure their understandability of them. They found that the information provided was enough and grouped them in the right section. Also, they evaluate the importance of each section of the labels and the average time to read them, especially the summarized label's security and privacy factor section and final scores section. Moreover, they provided a list of all popular types of sensors that are used by IoT smart home devices that are temperature, humidity,

pressure, proximity, level, accelerometers, gyroscope, gas, infrared, and optical sensors. The data sensor practices section in the detailed label will be edited based on the available sensors that are used by the IoT smart home device in the evaluation process.

Moreover, label designers were requested to evaluate the coloring of the label to ensure that consumers' eyes will target the important section (e.g bar graph in the summarized label) first. Also, they have changed the shape of the emojis used on the summarized label to be brighter and easily recognized. Also, they have added a 3D shape (Pyramid) that presents the IoT smart home device's final score in a clear and informative way by describing the different levels and ranges of each score.

4.4 The final versions for the IoT smart home devices security, privacy, and firmware labels:

- **Final IoT smart home devices security, privacy, and firmware Summarized label:**

Figure 32: The IoT smart home security, privacy, and firmware summarized label (final version)

Security, privacy and firmware label for IoT smart home devices

Name.....

Warranty lifetime.....

Brand/Model.....

OS Compatibility.....

Available Sensors.....

Firmware version.....

Storage Type.....

Firmware update lifetime.....

Security and Privacy Factors Scores

Symbols	Factors	Scores	Symbols	Factors	Scores
	Internet pairing			Firmware Vulnerabilities	
	Configuration & Authentication			Protocols	
	Update mode			Network encryption	
	Exposed service				

100%	
90%	
80%	
70%	
60%	

Scan this QR code to
access the detailed label

1 2 3 4 5 6 7 8 9 0 1 2

Label Barcode

- **Final IoT smart home devices security, privacy, and firmware detailed label:**

Figure 33: The IoT smart home security, privacy, and firmware detailed label (final version)

Security, privacy and firmware label for IoT smart home devices

Name..... Warranty lifetime.....

Brand/Model..... OS Compatibility.....

Available Sensors..... Firmware version.....

Storage Type..... Firmware update lifetime.....

Security, privacy and firmware factors scoring

Factors	Symbols	Description	Used Method
Internet Pairing		Establishment of network connection between the IoT device and the local network to provide Internet connection	Wi-Fi, Bluetooth, and Zigbee
Configuration & Authentication		Configuration and authentication procedures that are required to set up the IoT smart home device for operation	Use default, customized or Manual
Update Mode		The procedure that is used to install the latest updates for the IoT smart home device firmware	Permission required (Push mode), Manual (Pull mode), Automatic
Exposed Services		Total number of services that a user of the smart home device could access using a local network connection to this device	video, audio, temp, resence, carbon monoxide (fire)
Firmware Vulnerabilities		The shortcomings in the mini system running on the IoT smart home device	Password Exploitation, Rogue Recordings, Outdated Software
Protocols		The set of rules that format the data transmission over the local network and Internet	non-standard custom protocol, 3rd party DNS, UPnP, HTTPS, NTPv3
Network Encryption		Encryption techniques or procedures that are used in the data transmission in the IoT smart home ecosystem network	Device to Cloud, Mobile Application to Cloud, Mobile Application to Device

Data sensor practices

Type	Symbols	Data storage location	Data retention time	Shared or sold	Collection Recurrence
Camera					
Microphone					
fire					
Temperature					
Movement / Location					

Technical specifications

Specifications	Description
Power and max power consumption	
SDRAM or Flash Memory	
Combined Applications	
Smart Assistance	
Connectivity Information	

Privacy Policy
www.Privacy.sa

Label Barcode

Chapter 5: The Implementation of the IoT smart home devices security, privacy, and firmware label

Here are detailed procedures to create the IoT smart home devices security, privacy, and firmware label for a Mini Wi-Fi Smart Plug (DSP-W118) from the D-LINK brand. The content of the general information section, technical specification section, and privacy policy is collected from the device's user manual [44], firmware documentation [45], D-LINK privacy policy [46], and manufacturer website and customer service [47]. All security and privacy factors scores are calculated in the following:

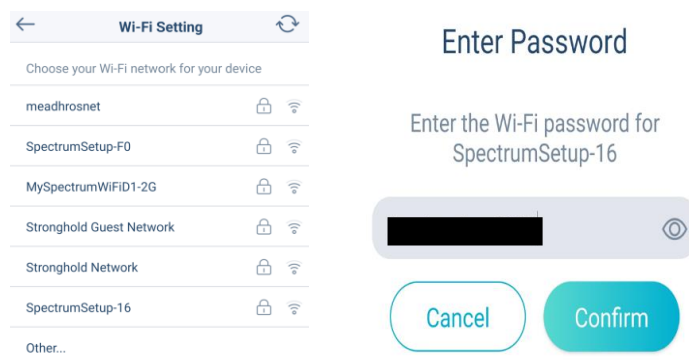
1. *Internet pairing:*

This device requires some network information to be added to provide an internet connection to the IoT smart plug. This mini smart plug is providing a local network that is designed to give access and control to the device without the internet service, by accessing the network with the information provided in a small sticker provided inside the device's package (Figure 34). However, controlling the device if the owner is out of home requires configuring the local network information using the combined application and setting the network credentials to provide an internet connection to the IoT smart plug. Therefore, this device deserves 3 points because of the manual network setup and emoji (🏠).

Figure 34: Local Wi-Fi network credentials



Figure 35: Choose the smart home Wi-Fi network and enter the password

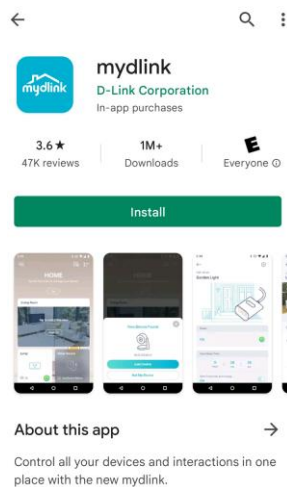


2. Configuration and Authentication:

This factor is important to ensure the highest security mechanisms for a secure installation and customization of the IoT smart home device. It requires some authentication and configuration steps that must be accomplished by the owner to use the device. This stage requires some account creation, account authentication through email, setting up passwords, and downloading a combined application that provides full control on the device. Therefore, this device deserves 7 points, and this emoji representation (👉) because of the manual authentication and configuration required to use the device.

- Download mydlink application:

Figure 36: Install the combined application



- Add the device by scanning a QR code that is printed on the IoT smart home devices itself and provided on a special label inside the IoT device's package.

Figure 37: Add the device using the QR code inside the box



- Create a new account that links to all your D-link IoT smart home devices.

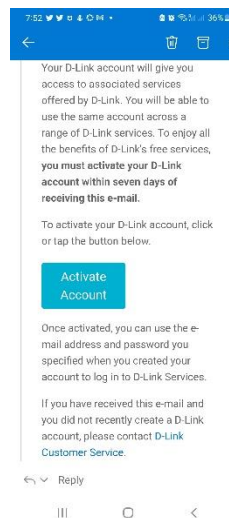
Figure 38: Create a new account



The screenshot shows the 'mydlink' account creation interface. At the top left is a back arrow. The 'mydlink' logo is centered at the top. Below the logo, there are four input fields: 'Name (Optional)' with the text 'naif', 'Email' with the text 'ra', 'Password' with masked characters '*****', and 'Confirm Password' with masked characters '*****'. Below the password fields are two terms and conditions checkboxes, both of which are checked. The first checkbox text is 'I agree to the Terms of Use and Privacy Policy, and certify that I am 18 years of age or older.' The second checkbox text is 'I agree to receive emails on D-Link services and product information.' At the bottom center is a blue 'Sign Up' button.

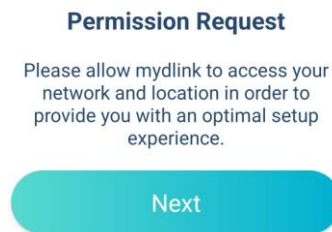
- Authenticate the email address through an authentication link sent to the owner's email address:

Figure 39: Activate the new account



- Grant permission to access network and location:

Figure 40: Access permission request



3. Update mode:

This device is using the Automatic update mode and provides time options that could be customized by the owner to download and install it. Therefore, it deserves 3 points, and this emoji representation (🇩🇪)

Figure 41: Auto-update mode availability



4. Exposed service:

This IoT smart plug connects to the internet through the local home network. It could be accessed and controlled locally using the application or from any place around the world using the internet. This device provides one service to be accessed which is switching on or off the devices to provide the connected device with electricity. Therefore, the device deserves 2 points, and this emoji representation (😊).

Figure 42: All device's functions



5. Firmware Vulnerabilities

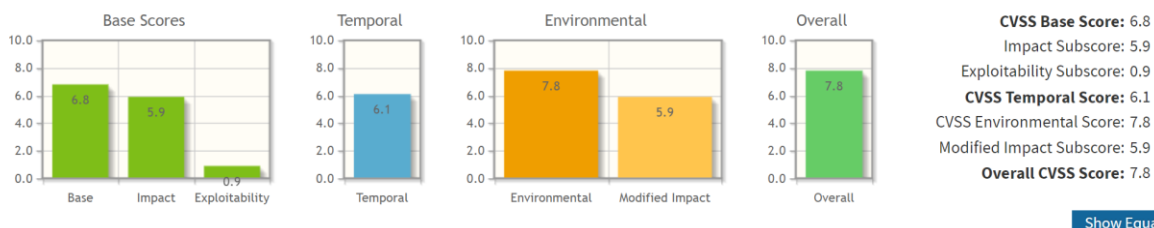
This factor requires the use of CVSS V3.1 calculator to analyze the available vulnerabilities in this device. The calculator will provide a risk level that will be used to derive the factor's score. In the following is the description of the available vulnerabilities and their calculations:

A. Default network credentials:

This device is providing default network credentials that should be used to have access to the network to control the IoT smart home device. This information is provided in a sticker inside the device's package as you can see on figure 34.

This vulnerability should be addressed and examined. Here is the calculated risk score for it and its CVSS v3.1 vector which details each metric:

Figure 43: CVSS for default network credentials vulnerability



CVSS v3.1 Vector:

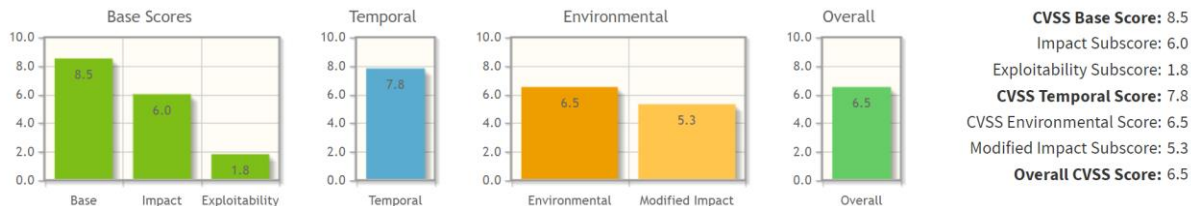
AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:W/RC:X/CR:X/IR:X/AR:X/MAV:A/MAC:L/
MPR:X/MUI:X/MS:X/MC:H/MI:H/MA:H

As presented in the picture above, the final score for this vulnerability is 7.8, which is in (high) risk level.

B. UPnP can not be disabled:

This feature is important to protect the device's local network from accepting any device that tries to have connection to the same network. The temporary local network does not provide this option and it will be always enabled. it provides no configuration to establish a connection. Ports will automatically be forwarded to establish a connection when they receive any UPnP request. This vulnerability should be addressed and examined. Here is the calculated risk score for it and its CVSS v3.1 vector which detail each metric:

Figure 44: CVSS for UPnP cannot be disabled vulnerability



CVSS v3.1 Vector:

AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:U/RC:X/CR:X/IR:X/AR:X/MAV:A/MAC:H/MP
R:L/MUI:N/MS:C/MC:H/MI:L/MA:L

As presented in the picture above, the final score for this vulnerability is 6.5 which is in (medium) risk level.

C. *MAC address access:*

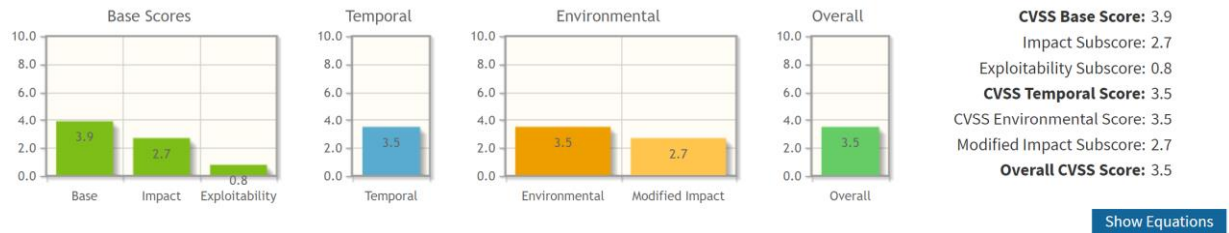
This device labels the serial number and the MAC address on the device's package. This type of information is vulnerable and should be hidden. As represented in the picture below, it is very clear that anybody can see the MAC address (MAC ID ECADE0525C89) and perform a death attack or intercept your traffic by posing as the network router.

Figure 45: MAC ID sticker



This vulnerability should be addressed and examined. Here is the calculated risk score for it and its CVSS v3.1 vector which detail each metric:

Figure 46: CVSS for MAC address access vulnerability



CVSS v3.1 Vector:

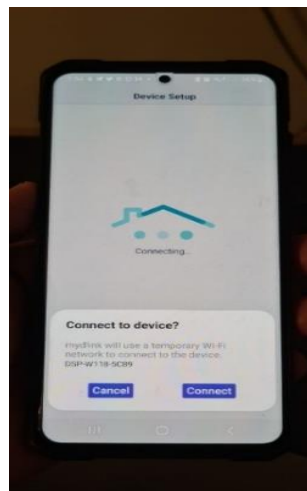
AV:L/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:N/E:X/RL:W/RC:U/CR:X/IR:X/AR:X/MAV:L/MAC:H/MP
R:H/MUI:N/MS:C/MC:L/MI:L/MA:N

Therefore, the device has 1 high-level vulnerability which deserves 6 points, 1 medium vulnerability which deserves 6 points, and 1 low vulnerability which deserves 6 points. The total score for this factor is 18 points and the emoji representation is (🟡)

6. Protocols:

The device is providing a local Wi-Fi network that could be accessed using the network credentials on the sticker found inside the device's package as presented in Figure 34. After connecting with the device using this local network, the device uses UPnP (Universal Plug and Play) to allow the user to find the IoT device and add it to his smart home devices list on mydlink application. However, there is no way to disable the UPnP feature. In addition, this device is using a 3rd party DNS that is provided by the vendor to be identified and controlled by the combined application or smart home assistance such as Alexa.

Figure 47: Local device's network access



Moreover, this device is using Wi-Fi Protected Access WPA/WPA2 security standards that protect wireless networks. This is found in the user manual document. This technology supports powerful encryption and authentication. The WPA2 is using AES encryption, dynamic session keys, automatic distribution availability, and using 802.1x & EAP (advanced encryption standards) for authentication procedures [50]. Furthermore, the device is using “IEEE 802.11n/g” standards, it's usually called Wi-Fi 4. It was developed in 2009 to improve the speed, reliability and extend the range of the wireless transmission. This standard is using MIMO (Multiple-Input Multiple-Output) technology for the first time. This technology helps in receiving more data for faster data transmission. This standard uses 2.4 GHz and 5GHz radio frequencies to be compatible with 802.11/g devices such as this one. It supports a bandwidth speed of up to 600Mbps with a theoretical range of 230 ft indoors. Besides, this device is using HTTPS (Hypertext transfer protocol) protocol as presented in the installation procedures Figure 48 below.

Figure 48: HTTPS protocol availability

☆ 🔒 mp-us-openapi.auto.mydlink.com 🔄

D-Link[®]

By analyzing this factor, this device is using the following protocols: IEEE 802.11n/g, UPnP, WPA/WPA2, and HTTPS, 3rd party DNS. This protocol factor has a total point of 8 and deserves this emoji representation (🇩🇪).

7. Network encryption:

This device does not transmit data directly to the cloud. It uses its combined application to send it. On the other hand, this device is accessed and controlled by the application that is accessed by username and password that are linked with the device. This application is using secure sockets layer (SSL), Transport layer security (TLS), Hypertext Transfer Protocol Secure (HTTPS), File transfer protocol (FTP), Wi-Fi Protected Access WPA/WPA2, and UDP to transfer and encrypt the data transmission between the device and the application and between the device and the cloud directly or through the smart home network router. Therefore, this device's data transmissions are fully encrypted and get 9 points and deserve this emoji representation (🇩🇪).

After analyzing the security and privacy factors of this IoT smart home device, here are the final scores:

Table 23: Final scores calculations

Factor	Score
Internet pairing	3
Configuration and Authentication	7
Update mode	3
Exposed service	2
Firmware Vulnerabilities	18
Protocols	8
Network encryption	9

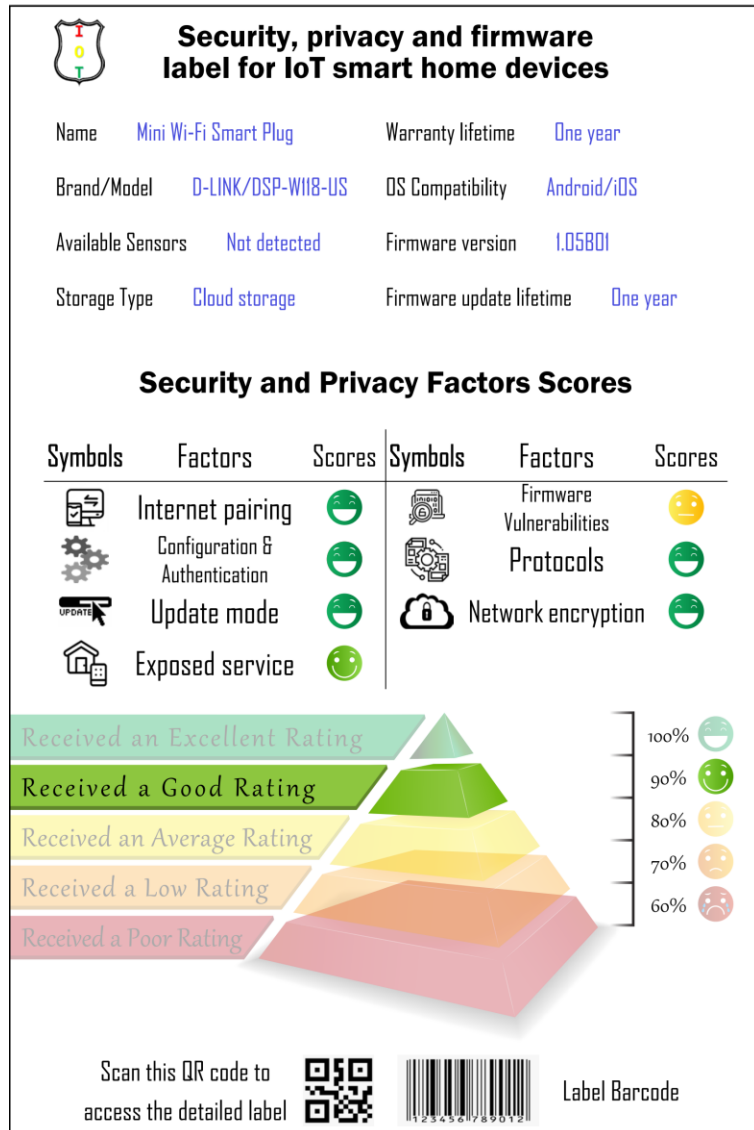
The final IoT smart home device's score is calculated as following:

Total security and privacy factors score: $50/57 = 0.87$. Finally, the grade assignments are the following:
 $0.87 \Rightarrow 87\%$ gets a "B"

The final IoT smart home devices' security, privacy, and firmware labels are as follows:















A. The IoT security, privacy, and firmware summarized label:

Figure 49: The IoT smart home security, privacy, and firmware summarized label (smart plug).



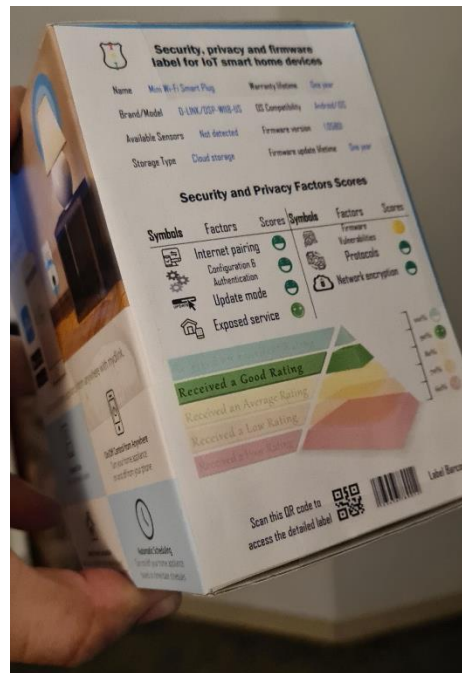
B. The IoT security, privacy, and firmware detailed label:

Figure 50: The IoT smart home security, privacy, and firmware detailed label (smart plug)

 Security, privacy and firmware label for IoT smart home devices					
Name	Mini Wi-Fi Smart Plug	Warranty lifetime	One Year		
Brand/Model	D-LINK/DSP-WIIB-US	OS Compatibility	Android/iOS		
Available Sensors	Not Detected	Firmware version	1.05801		
Storage Type	Cloud Storage	Firmware update lifetime	One Year		
Security, privacy and firmware factors scoring					
Factors	Symbols	Description	Used Method		
Internet Pairing		Establishment of network connection between the IoT device and the local network to provide Internet connection	Wi-Fi, Bluetooth, and Zigbee		
Configuration & Authentication		Configuration and authentication procedures that are required to set up the IoT smart home device for operation	Use default, customized or Manual		
Update Mode		The procedure that is used to install the latest updates for the IoT smart home device firmware	Permission required (Push mode), Manual (Pull mode), Automatic		
Exposed Services		Total number of services that a user of the smart home device could access using a local network connection to this device	video, audio, temp, resence, carbon monoxide (fire)		
Firmware Vulnerabilities		The shortcomings in the mini system running on the IoT smart home device	Password Exploitation, Rogue Recordings, Outdated Software		
Protocols		The set of rules that format the data transmission over the local network and Internet	non-standard custom protocol, 3rd party DNS, UPnP, HTTPS, NTPv3		
Network Encryption		Encryption techniques or procedures that are used in the data transmission in the IoT smart home ecosystem network	Device to Cloud, Mobile Application to Cloud, Mobile Application to Device		
Data sensor practices					
Type	Symbols	Data storage location	Data retention time	Shared or sold	Collection Recurrence
Camera			Not Detected		
Microphone			Not Detected		
fire			Not Detected		
Temperature			Not Detected		
Movement / Location			Not Detected		
Technical specifications					
Specifications	Description				
Power and max power consumption	120V~/60Hz Max is 1800W				
SDRAM or Flash Memory	Not Detected				
Combined Applications	mydlink Smart and IFTTT				
Smart Assistance	Alexa, Google				
Connectivity Information	Wi-Fi Network				
Privacy Policy https://us.dlink.com/en/privacy-policy			Label Barcode 		

C. The summarized label represented on the Mini Wi-Fi Smart Plug (DSP-W118):

Figure 51: The IoT smart home security, privacy, and firmware summarized label on the package.



Chapter 6: Conclusion and Future Work

6.1 Conclusion

IoT smart home devices' security and privacy characteristics are different and hard to be determined, especially when the consumers are not familiar with this powerful technology that collects personal information about the owners. In this study, an IoT smart home device's security, privacy, and firmware labeling system is designed to provide detailed security, privacy, and firmware information about any IoT smart home device in the Saudi Arabian market. Also, it helps compare different factors between the target options to conclude better and more knowledgeable purchase decisions. Moreover, this labeling system would increase the regular IoT smart home device's consumer's security and privacy awareness and encouraged them to educate themselves about such new and sensitive technologies.

The proposed label consists of three phases in sequence, which are information collection, the scoring system, and the survey. The information collection phase presents the security, privacy, and firmware factor's information along with the procedures to collect them manually or technically (Firmware analysis). The second phase is the scoring system which represents the scoring value or weight for each factor that is going to be represented in the final version of the label. The third phase is the survey which is about collecting field information that would help in creating the content, design, and layout of the final version of the labeling system. This would provide confident decisions to increase the quality of the label outcomes.

6.2 Future Work

Creating security and privacy labels for IoT smart home devices is still challenging, and there is much work to be done. In this dissertation, the tools that were used to analyze the IoT smart home device's firmware were useful and powerful on two devices out of three, there is a need for a new testing bed to access the firmware and explore it for any vulnerabilities. This could be done by adopting the Fuzzing technology. In addition, government adoption of the IoT smart home device's security, privacy, and firmware labeling system would encourage the IoT smart home device manufacturers to post it on their product's packaging. This would make it used by different types of IoT smart home devices consumers in the Saudi Arabian Market. Moreover, there is a need for security and privacy standards that all IoT smart home devices manufacturers should implement in their products. Researching this area would maintain the highest level of security and privacy for homeowners along with higher adoption of such technology. Additionally, identical versions of the IoT smart home device's security, privacy, and firmware labels could be designed for people with visual impairment, and this version could be an audio version or use the Braille language. Moreover, a YouTube channel

could be created to go through the evaluation of the IoT smart home devices and the procedures of creating the labels would be useful because a large number of second survey participants (IoT smart home devices regular consumers) declared that they watch YouTube videos to know more about their target IoT smart home devices. Reviewing the security and privacy features of the IoT smart home devices will help the consumers in their safer purchases.

References

1. Zaidan, A.A., Zaidan, B.B. "A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations". *Artif Intell Rev* 53, 141–165 (2020).
2. M. Bäckman, J. Fagerberg, B. Insight, "Smart Homes and Home Automation", BERG Insight, IoT research series.
3. S. Mahmud, S. Ahmed and K. Shikder, "A Smart Home Automation and Metering System using Internet of Things (IoT)," 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), Dhaka, Bangladesh, 2019, pp. 451-454. DOI: 10.1109/ICREST.2019.8644232
4. Heetae Yang, Wonji Lee, Hwansoo Lee, "IoT Smart Home Adoption: The Importance of Proper Level Automation", *Journal of Sensors*, vol. 2018, Article ID 6464036, 11 pages, 2018.
5. Kidd, Cory & Orr, Robert & Abowd, Gregory & Atkeson, Christopher & Essa, Irfan & Macintyre, Blair & Mynatt, Elizabeth & Starner, Thad & Newstetter, Wendy. (1999). "The Aware Home: A Living Laboratory for Ubiquitous Computing Research". Pages 191-198.
6. S. Mahmud, S. Ahmed and K. Shikder, "A Smart Home Automation and Metering System using Internet of Things (IoT)," 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), Dhaka, Bangladesh, 2019, pp. 451-454, doi: 10.1109/ICREST.2019.8644232.
7. W. Zhou, Y. Jia, Y. Yao, L. Zhu, L. Guan, Y. Mao, P. Liu, Y. Zhang, "Discovering and Understanding the Security Hazards in the Interactions between IoT Devices, Mobile Apps, and Clouds on Smart Home Platforms", 28th USENIX Security Symposium.
8. Li, Q. Yan, and V. Chang," Internet of Things: Security and privacy in a connected world", ELSEVIER, vol. 78, 3, pp. 931-932, 2018.
9. A. K. Sahu, S. Sharma, D. Puthal, A. Pandey and R. Shit, "Secure Authentication Protocol for IoT Architecture," 2017 International Conference on Information Technology (ICIT), Bhubaneswar, 2017, pp. 220-224.
10. N. Apthorpe, D. Reisman, and N. Feamster, "A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic", Computer Science Dept. Princeton University, pp. 1-6, 2017.
11. D. Kumar, K. Shen, B. Case, D. Garg, G. Alperovich, D. Kuznetsov, R. Gupta, Z. Durumeric, "All Things Considered: An Analysis of IoT Devices on Home Networks", 28th USENIX Security Symposium.
12. Gamundani, Attlee & Phillips, Amelia & Muyingi, Hippolyte. (2018). "An Overview of Potential Authentication Threats and Attacks on Internet of Things (IoT): A Focus on Smart Home Applications", 10.1109/Cybermatics_2018.2018.00043.
13. M. Fagen, M. Yang, A. Tan, L. Randolph, K. Scarfone, "Security Review of Consumer Home Internet of Things (IoT) Products", Draft NISTIR 8267.
14. A. Albalawi, A. Almrshed, A. Badhib, and S. Alshehri, "A Survey on Authentication Techniques for the Internet of Things," 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 2019, pp. 1-5. DOI: 10.1109/ICCISci.2019.8716401

15. Hussain, S., Kamal, A., Ahmad, S., Rasool, G., & Iqbal, S. (2014). "Threat modeling methodologies: a survey", *Sci. Int. (Lahore)*, 26(4), 1607-1609.
16. ISO - ISO/IEC 30141:2018 - Internet of Things (IoT) — Reference Architecture
17. S. S. I. Samuel, "A review of connectivity challenges in IoT-smart home," 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, 2016, pp. 1-4. DOI: 10.1109/ICBDSC.2016.7460395
18. Andrew Loughlin. "Watch as the voice of this child's toy cat is taken over by hackers – Which?" accessed on 03/15/2021
19. Saudi Arabian Standards Organization (SASO).
20. W. Ali, G. Dustgeer, M. Awais and M. A. Shah, "IoT-based smart home: Security challenges, security requirements and solutions," 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, 2017, pp. 1-6. DOI: 10.23919/ICAC.2017.8082057,
21. K. Bjørneset, "Testing Security for Internet of Things" University of Oslo, Department of informatics, 2017
22. P. A. Abdalla and C. Varol, "Testing IoT Security: The Case Study of an IP Camera," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 2020, pp. 1-5, doi: 10.1109/ISDFS49300.2020.9116392.
23. S. Siboni et al., "Security Testbed for Internet-of-Things Devices," in *IEEE Transactions on Reliability*, vol. 68, no. 1, pp. 23-44, March 2019, doi: 10.1109/TR.2018.2864536.
24. P. Emami-Naeini, Y. Agarwal, L. Faith Cranor and H. Hibshi, "Ask the Experts: What Should Be on an IoT Privacy and Security Label?," 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2020, pp. 447-464, doi: 10.1109/SP40000.2020.00043.
25. P. Morgner, C. Mai, N. Koschate-Fischer, F. Freiling and Z. Benenson, "Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products," 2020 IEEE Symposium on Security and Privacy (SP), 2020, pp. 429-446, doi: 10.1109/SP40000.2020.00021.
26. Amna Puri-Mirza, "Market size of smart homes in the Middle East 2012-2022", Statista publications on 08/2020.
27. Blink security camera by amazon
28. N. Rajkhan, J. Song, "A Study On Node Authentication and Identification In IOT Based Smart Homes", Vol 14, Issue 5.
29. Dillman, D. A., Smyth, Jolene D., & Christian, Leah Melani. (2014). *Internet, phone, mail, and mixed-mode surveys: the tailored design method (Fourth edition.)*
30. Common Vulnerability Scoring System v3.1: User Guide
31. O. Alrawi, C. Lever, M. Antonakakis and F. Monroe, "SoK: Security Evaluation of Home-Based IoT Deployments," 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2019, pp. 1362-1380. doi: 10.1109/SP.2019.00013
32. Linux Kernel 2.6.21 : Related security vulnerabilities (cvedetails.com)
33. Binwalk tool, GitHub - ReFirmLabs/binwalk: Firmware Analysis Tool.
34. Firmwalker tool, GitHub - craigz28/firmwalker: Script for searching the extracted firmware file system for goodies!

35. Y. Han and B. Liu, "Interactive smart home design based on Internet of Things," 2017 12th International Conference on Computer Science and Education (ICCSE), Houston, TX, 2017, pp. 449-453. DOI: 10.1109/ICCSE.2017.8085534,
36. R. Liu and Y. Ge, "Smart home system design based on Internet of Things," 2017 12th International Conference on Computer Science and Education (ICCSE), Houston, TX, 2017, pp. 444-448. DOI: 10.1109/ICCSE.2017.8085533.
37. Hasan and K. Qureshi, "Internet of Things Device Authentication Scheme Using Hardware Serialization," 2018 International Conference on Applied and Engineering Mathematics (ICAEM), Taxila, 2018, pp. 109-114. DOI: 10.1109/ICAEM.2018.8536286.
38. M. Husamuddin and M. Qayyum, "Internet of Things: A study on security and privacy threats," 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, 2017, pp. 93-97. DOI: 10.1109/Anti-Cybercrime.2017.7905270.
39. M. Conti, A. Dehghantaha, K. Franke and S. Watson, "Internet of Things security and forensics: Challenges and opportunities", ELSEVIER, vol. 78, 2, pp. 544-546, 2018.
40. Qualtrics XM // The Leading Experience Management Software, accessed 04/22/2021
41. P. Emami-Naeini, J. Dheenadhayalan, Y. Agarwal and L. Cranor, " Which Privacy and Security Attributes Most Impact Consumers' Risk Perception and Willingness to Purchase IoT Devices?," 2021 IEEE Symposium on Security and Privacy (SP), Oakland, CA, USA, 2021
42. Lloyd Harrington, Jack Brown, "Energy standards and labelling programs throughout the world in 2013", Super-efficient application deployment (SEAD), Australia, 2013.
43. shodan.io
44. Mini Wi-Fi smart plug user's manual, accessed on December 2021,
45. Mini Wi-Fi smart plug firmware documentation, accessed on December 2021
46. D-LINK privacy policy, accessed on December2021
47. D-LINK manufacturer website and customer service, accessed on December2021.
48. Hosein Badran. IoT Security and Consumer Trust. In Proceedings of the 20th Annual International Conference on Digital Government Research (2019). Association for Computing Machinery, New York, NY, USA, 133–140.
49. Y. Shen,P. Vervier, "IoT Security and Privacy Labels", Symantec Research Labs. URL: IoT Security and Privacy Labels - Norton LifeLock. 2020
50. Khasawneh, Mahmoud & Kajman, Izadeen & Alkhudaiby, Rashed & Althubyani, Anwar. (2014). A Survey on Wi-Fi Protocols: WPA and WPA2. 420. 496-511. 10.1007/978-3-642-54525-2_44.
51. ISO/IEC 30141:2018, Internet of Things (IoT) Reference Architecture. Accessed on 04/14/2022.

Appendices

Appendix A



Here are all the tools, steps, and commands that have been used to discover and analyze the Firmware.

1. Download the last firmware version of the DCS-932L IoT smart camera from ([legacyfiles.us.dlink.com - /DCS-932L/REVA/FIRMWARE/](http://legacyfiles.us.dlink.com/-/DCS-932L/REVA/FIRMWARE/)) on the Kali Linux.
2. The firmware folder name is (DCS-932L_REVA_FIRMWARE_1.14.04.ZIP) needs to be “unzipped” to work on the firmware file only. The “File” command shows that there is data in the extracted file.

```
(root@kali) ~ | /home/nraj Khan/Downloads |
# ls
2.1.1_20171024151200home      2.1.1_20171024151200home-3.extracted  2.1.1_20171024151200home.extracted  _demo.bin-0.extracted  _demo.bin.extracted  u-boot.bin
2.1.1_20171024151200home-0.extracted  2.1.1_20171024151200home-4.extracted  binwalk                               _demo.bin-1.extracted  firmwalker            uImage
2.1.1_20171024151200home-1.extracted  2.1.1_20171024151200home-5.extracted  DCS-932L_REVA_FIRMWARE_1.14.04.ZIP  _demo.bin-2.extracted  Image.lzma
2.1.1_20171024151200home-2.extracted  2.1.1_20171024151200home-6.extracted  demo.bin                               _demo.bin-3.extracted  kernel

(root@kali) ~ | /home/nraj Khan/Downloads |
# unzip DCS-932L_REVA_FIRMWARE_1.14.04.ZIP
Archive: DCS-932L_REVA_FIRMWARE_1.14.04.ZIP
  inflating: DCS-932L_REVA_RELEASENOTES_1.14.04_EN.PDF
  inflating: dcs932l_v1.14.04.bin

(root@kali) ~ | /home/nraj Khan/Downloads |
# file dcs932l_v1.14.04.bin
dcs932l_v1.14.04.bin: data
```

3. The “strings” command shows some of the important information about the extracted firmware such as u-boot 1.1.3. (universal bootloader)

```
(root@kali) ~ | /home/nraj Khan/Downloads |
# strings -10 dcs932l_v1.14.04.bin | head
U-Boot 1.1.3
NetInitTcp
NetTcpSend
NetReceive
send_syn_ack
send_reset
ArpTimeoutCheck
HttpHandler
mpfd_decode
do_httpsrv
```

4. Now, let us Binwalk the firmware to explore more information. This tool finds the location of the files to provide some access to them.

```
(root@kali) ~ - [~/home/nrajkhan/Downloads]
# binwalk dcs932l_v1.14.04.bin
```

DECIMAL	HEXADECIMAL	DESCRIPTION
106352	0x19F70	U-Boot version string, "U-Boot 1.1.3"
106816	0x1A140	CRC32 polynomial table, little endian
124544	0x1E680	HTML document header
124890	0x1E7DA	HTML document footer
124900	0x1E7E4	HTML document header
125092	0x1E8A4	HTML document footer
125200	0x1E94C	HTML document header
125953	0x1EC01	HTML document footer
327680	0x50000	uImage header, header size: 64 bytes, header CRC: 0x88345E96, created: 2016-09-09 13:52:27, image size: 3804958 bytes, Data Address: 0x80000000, Entry Point: 0x80988000, data CRC: 0x531E94DE, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "Linux Kernel Image"
327744	0x50040	LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size: 6558763 bytes

The image uses U-Boot as the bootloader by tracing the uImage file which is a Linux Kernel type (image header at address 327680 0x50000 and compressed bootloader image at address 327744 0x50040). Based on the uImage header at address 327680 0x50000, we know the CPU architecture is MIPS. This firmware is using a compression type of "lzma" archive.

- Crave it for more exploring directories and files using "dd" command. Then use "file" command to check the results.

```
(root@kali) ~ - [~/home/nrajkhan/Downloads]
# dd if=dcs932l_v1.14.04.bin skip=327744 bs=1 of=932Lkernel.lzma
3866560+0 records in
3866560+0 records out
3866560 bytes (3.9 MB, 3.7 MiB) copied, 4.65896 s, 830 kB/s

(root@kali) ~ - [~/home/nrajkhan/Downloads]
# file 932Lkernel.lzma
932Lkernel.lzma: LZMA compressed data, non-streamed, size 6558763

(root@kali) ~ - [~/home/nrajkhan/Downloads]
# unlzma 932Lkernel.lzma

(root@kali) ~ - [~/home/nrajkhan/Downloads]
# file 932Lkernel
932Lkernel: data
```

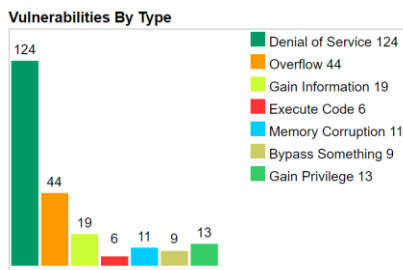
```
(root@kali) ~ - [~/home/nrajkhan/Downloads]
# strings -i0 932Lkernel | head
~C6t~H6~-I6IH1
~h6t~i6~-j6:
%$ version %$ (andy@ipcam-linux.alphanetworks.com) (gcc version 3.4.2) %$
Linux version 2.6.21 (andy@ipcam-linux.alphanetworks.com) (gcc version 3.4.2) #3121 Fri Sep 9 21:52:18 CST 2016
context_switch
__put_task_struct
__local_bh_enable
local_bh_enable
local_bh_enable
__devm_release_region
```

- Use Binwalk again on the craved kernel.

```
(root@kali) ~ - [~/home/nrajkhan/Downloads]
# binwalk 932Lkernel
```

DECIMAL	HEXADECIMAL	DESCRIPTION
3145804	0x30004C	Linux kernel version 2.6.21
3175792	0x307570	SHA256 hash constants, little endian
3389960	0x33BA08	Unix path: /usr/gnenuML/irix/
3392244	0x33C2F4	Unix path: /usr/lib/libc.so.1
3393940	0x33C994	Unix path: /dev/vc/0
3408260	0x340184	Copyright string: "Copyright (c) 2010 Alpha Networks Inc."
3491536	0x3546D0	Unix path: /etc/Wireless/RT2860STA/RT2860STA.dat
3573187	0x3685C3	Neighborly text, "neighbor %.2x%.2x%.2x%.2x%.2x%.2x%.2x%.2x lost on port %d(%s)(%s)"
3807776	0x3A1A20	CRC32 polynomial table, little endian
4038656	0x3DA000	LZMA compressed data, properties: 0x5D, dictionary size: 1048576 bytes, uncompressed size: 8072704 bytes

This firmware is using an old version (Linux kernel versions 2.6.21). however, the product itself is younger than the version used in it! Here are some statistics about it from [32]:



- We can look for (CPIO) files that contain important information about the file system. Most manufacturers store this data here. So, using “dd” and “lzma” commands would help in finding the CPIO. It is going to be a big filesystem. Therefore, creating a directory to store everything in is highly encouraged. Using the “—no-absolute-filenames” command would avoid any overwriting on the workstation.

```
(root@kali)~/Downloads
# dd if=932Lkernel skip=4038656 bs=1 of=deepin932Lkernel.lzma
2520107+0 records in
2520107+0 records out
2520107 bytes (2.5 MB, 2.4 MiB) copied, 2.94921 s, 855 kB/s

(root@kali)~/Downloads
# unlzma deepin932Lkernel.lzma

(root@kali)~/Downloads
# file deepin932Lkernel
deepin932Lkernel: ASCII cpio archive (SVR4 with no CRC)
```

```
(root@kali)~/Downloads
# mkdir cpio; cd cpio

(root@kali)~/Downloads/cpio
# cpio -Hm --no-absolute-filenames <../deepin932Lkernel
cpio: Removing leading '/' from member names
15767 blocks

(root@kali)~/Downloads/cpio
# ls
bin dev etc etc_ro home init lib media mnt mylink proc sbin sys tmp usr var
```

- Now, we have access to all directories in the firmware filesystem. This would help in exploring all the directories and looking for vulnerabilities. Here are the vulnerability findings:

- Let us take a look at web application vulnerabilities:

```
(root@kali)~/Downloads/cpio/etc_ro/web
# ls
account.htm cgi edit.jpg errrdns.htm errrwlan.htm helphome.htm iphone.htm network.htm replyd.htm setvdo.htm time.htm version.htm wps.htm
advanced.htm crossdomain.xml email.htm errrenl.htm factory.htm helpstat.htm jview.htm night.htm replyf.htm sharp.htm title.gif video.htm
api dds.htm errmsg.htm errrftp.htm favicon.ico helpool.htm logout.htm pack replyk.htm showmsg.js top.htm vjview.htm
aplist.htm deployjava.js errradv.htm errring.htm file.htm home.htm lphone.htm radiooff.gif replym.htm stsdev.htm trash.jpg waitscan.htm
audio.htm devmodel.jpg errraud.htm errrnet.htm frmsize.htm html.htm mobile.htm radioon.gif replyu.htm stssys.htm upgrade.htm wireless.htm
aview.htm dlink.css errrcan.htm errrnght.htm function.js image.htm motion.htm reboot.htm restore.htm stsuser.htm upload.htm wizard.htm
bootver.htm dloadbar.gif errrdate.htm errrvdo.htm helpadva.htm imode.htm mvideo.htm region.htm security.gif support.htm vaview.htm wizsetup.htm
```


- Upgrade.htm file shows that this device is following a push mode update in which a manufacturer's server sends a notification to the devices and require users to accept the new update installation.

```
(root@kali) ~ - [~/home/.../Downloads/cpio/etc_ro/web]
# cat upgrade.htm
<html>
<head>
<link rel="stylesheet" rev="stylesheet" href="dlink.css?cidx=%ReleaseTime();%" type="text/css">
<title>D-Link Corporation. | WIRELESS INTERNET CAMERA | MAINTENANCE | FIRMWARE UPGRADE</title>
<meta http-equiv="X-UA-Compatible" content="requiresActiveX=true">
<meta content="text/html; charset=windows-1252" http-equiv=Content-Type>
<meta HTTP-EQUIV="Pragma" CONTENT="no-cache">
<meta HTTP-EQUIV="Expires" CONTENT="-1">
<script language="Javascript" SRC="function.js?cidx=%ReleaseTime();%"></script>
<script language="Javascript">
//if (top != self) {
//    top.location = self.location;
//}
</script>
</head>
<body topmargin="1" leftmargin="0" rightmargin="0" bgcolor="#757575">
<table id="header_container" border="0" cellpadding="5" cellspacing="0" width="838" align="center">
<tr>
<td width="100%">Product: <a href="http://www.dlink.com/" target="_blank">%CameraName();%</a></td>
<td align="right" nowrap></td>
<td align="right" nowrap>Firmware version: %FirmwareVersion();% &nbsp;&nbsp;&nbsp;</td>
</tr>
</table>
<div id="title_container">
<table id="topnav_container" border="0" cellpadding="0" cellspacing="0" width="838" align="center">
<tr><td align="center" valign="middle"></td></tr>
</table>
</div>
<table id="index_container" border="0" cellpadding="2" cellspacing="1" width="838" align="center" bgcolor="#FFFFFF">
<tr id="topnav_container">
<td></td>
<td id="topnavoff"><a href="home.htm">Live Video</a></td>
```

```
<td id="sidonav_container"><td id="sidonavoff"><a href="file:///system/...></td></tr>
<tr id="sidonav_container"><td id="sidonavoff"><a href="upgrade.htm">Firmware Upgrade</a></td></tr>
<tr id="sidonav_container"><td id="sidonavoff"><a href="logout.htm">Logout</a></td></tr>
<tr id="sidonav_container" height="100"><td id="sidonavoff" align="center" valign="top">&nbsp;&nbsp;&nbsp;</td></tr>
</table>
<!-- END SIDENAV -->
</td>
<td valign="top" id="maincontent_container" height="420">
<table height="420" width="100%" border="0" cellpadding="0" cellspacing="0" bgcolor="white">
<tr><td>
<div id="maincontent">
<!-- BEGIN MAINCONTENT -->
<div id="box_header">
<h1>Firmware Upgrade</h1>
A new firmware upgrade may be available for your camera. It is recommended that you keep your camera firmware up to date to maintain and improve its functionality and performance. Click here <a href="http://www.dlink.com">D-Link Support Page</a> to check for the latest available firmware version.<br><br>
To upgrade the firmware on your IP camera, please download and save the latest firmware version from the D-Link Support Page to your local hard drive. Locate the file on your local hard drive by clicking the Browse button. Once you have found and opened the file using the browse button, click the <b>Upload</b> button to start the firmware upgrade.
</div>
<div class="box">
<h2>Firmware Information</h2>
<table cellpadding="2" cellspacing="1" border="0" bgcolor="white" bordercolor="#FFFFFF">
<FORM ACTION="/setFirmwareUpgrade" METHOD="POST" autocomplete="off" enctype="multipart/form-data">
<input type="hidden" name="ReplySuccessPage" value="replyd.htm">
<input type="hidden" name="ReplyErrorPage" value="replyk.htm">
<input type="hidden" name="ForceBootCodeUpgrade" value="%ForceBootCodeUpgrade();%">
<TR>
<TD width="150">Current Firmware Version :</TD>
<TD>%FirmwareVersion();%</TD>
</TR>
<TR>
<TD width="150">Current Firmware Date :</TD>
<TD nowrap>%ReleaseDate();%</TD>
</TR>
<TR>
<TD width="150">Current Agent Version :</TD>
<TD>%MyDLinkAgentVersion();%</TD>
</TR>
</table>
</div>
```

- Here are some network Username and Passwords default credentials and DHCP IP addresses:

```
(root@kali)~/home/./cpio/etc_ro/Wireless/RT2860AP
└─ cat RT2860_default_vlan
Default
#The word of "Default" must not be removed
WebInit=1
#WiFiTest=0
#HostName=ralink
#Login=admin
#Password=admin
OperationMode=0
Platform=RT3052
Telnet=0
#CountryRegion=5
#CountryRegionABand=7
#CountryCode=
#wanConnectionMode=DHCP
#wan_ipaddr=192.168.1.1
#wan_netmask=255.255.255.0
#wan_gateway=192.168.1.254
#wan_primary_dns=192.168.1.5
#wan_secondary_dns=168.95.1.1
#wan_pppoe_user=pppoe_user
#wan_pppoe_pass=pppoe_passwd
#wan_l2tp_server=l2tp_server
#wan_l2tp_user=l2tp_user
#wan_l2tp_pass=l2tp_passwd
#wan_l2tp_mode=0
#wan_l2tp_ip=192.168.1.1
#wan_l2tp_netmask=255.255.255.0
#wan_l2tp_gateway=192.168.1.254
#wan_ppptp_server=ppptp_server
#wan_ppptp_user=ppptp_user
#wan_ppptp_pass=ppptp_passwd
#wan_ppptp_mode=0
#wan_ppptp_ip=192.168.1.1
#wan_ppptp_netmask=255.255.255.0
#wan_ppptp_gateway=192.168.1.254
#lan_ipaddr=2.65.87.200
#lan_netmask=255.0.0.0
#dhcpEnabled=0
```

```
#dhcpStart=10.10.10.100
#dhcpEnd=10.10.10.200
#dhcpMask=255.255.255.0
#dhcpPriDns=10.10.10.251
#dhcpSecDns=168.95.1.1
#dhcpGateway=10.10.10.254
#dhcpLease=86400
#stpEnabled=0
#lldEnabled=0
#igmpEnabled=0
#natEnabled=0
#IPPortFilterEnable=0
#IPPortFilterRules=
#PortForwardEnable=0
#PortForwardRules=
#MacFilterEnable=0
#MacFilterRules=
#DefaultFirewallPolicy=1
#DMZEnable=0
#DMZIPAddress=
#TZ=
#NTPServerIP=
#NTPSync=
#DDNSProvider=
#DDNS=
#DDNSAccount=
#DDNSPassword=
#BssidNum=1
#SSID1=RT305x_AP_andy
#WirelessMode=9
#TxRate=0
#Channel=6
#BasicRate=15
#BeaconPeriod=100
#DtimPeriod=1
#TxPower=100
#DisableOLBC=0
#BGProtection=0
#TxAntenna=
```

- Here is some default configuration information, all “.sh” files are human-readable:

```
(root@kali)~/home/nrajkan/Downloads/cpio/sbin
└─ ls
automount.sh  config-dns.sh      config-udhcpd.sh  dhcp.sh  halt  insmod  lan.sh  mdev  poweroff  rmod  syslogd  udhcpc  video.sh  web.sh  zcip
cameraname.sh config-igmpproxy.sh config-vlan.sh    fdisk   ifconfig internet.sh logread nat.sh  pppoe.sh route  ucp    udhcpc.sh  vpn-passthru.sh  wifi_unload.sh  zcip.sh
chpasswd.sh   config.sh          ddns.sh          global.sh  init   klogd   lsmod   ntp.sh  reboot  storage.sh  udev    vconfig  wan.sh    wlan.sh
```

```
#####
### IPCam Default Configuration ###
### Company: D-Link ###
### Model : DCS-930 ###
#####
# System #
CameraName=DCS-930
Location=
AdminID=admin
AdminPassword=
LEDControl=0
SnapshotURLAuthentication=0
PrivacyButton=1
# Date and Time #
DateTimeMode=1
TimeServerIPAddress=
TimeServerProtocol=0
TimeZone=0
TimeZoneIndex=0
Date=2012-01-01
Time=00:00:00
# User Access Control # ### UserValue=UserName/Password/Privilege ###
AccessControlEnable=0
```

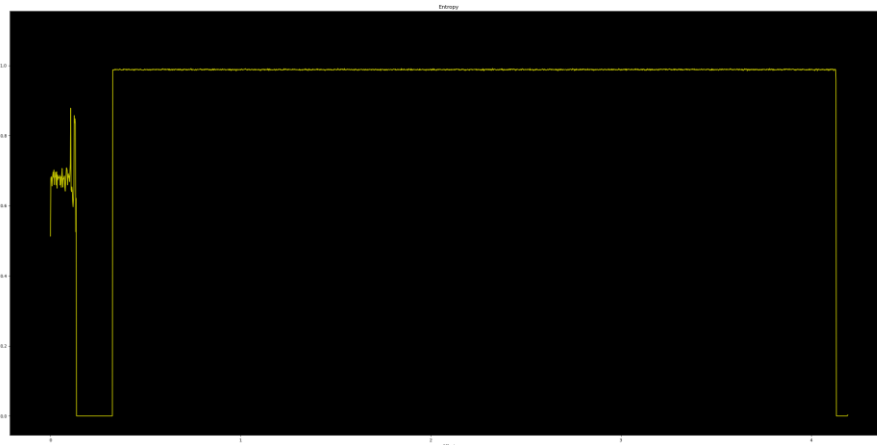
- Here is the FTP setup file:

```

setFtp()
{
    ftpport=$(nvram_get 2860 FtpPort)
    maxuser=$(nvram_get 2860 FtpMaxUsers)
    login=$(nvram_get 2860 FtpLoginTimeout)
    stayt=$(nvram_get 2860 FtpStayTimeout)
    echo "stupid-ftpd-common.sh $ftpport" "$maxuser" "$login" "$stayt"
    stupid-ftpd-common.sh $ftpport "$maxuser" "$login" "$stayt"
    admID=$(nvram_get 2860 Login)
    admPW=$(nvram_get 2860 Password)
    echo "stupid-ftp-user.sh $admID" "$admPW" / 3 A"
    stupid-ftp-user.sh $admID "$admPW" / 3 A
    anonymous=$(nvram_get 2860 FtpAnonymous)
    if [ "$anonymous" = "1" ]; then
        echo "stupid-ftp-user.sh anonymous "*" /tmp 3 0"
        stupid-ftp-user.sh anonymous "*" /tmp 3 0
    fi
    if [ -e "$SPART1" ]; then
        for index in 1 2 3 4 5 6 7 8
        do
            user=$(nvram_get 2860 "User$index")
            ftpuser=$(nvram_get 2860 "FtpUser$index")
            if [ "$user" -a "$ftpuser" = "1" ]; then
                pw=$(nvram_get 2860 "UserPasswd$index")
                max=$(nvram_get 2860 "FtpMaxLogins$index")
                mode=$(nvram_get 2860 "FtpMode$index")
                echo "stupid-ftp-user.sh $user" "$pw" "$SPART1/home/$user" "$max" "$mode"
                stupid-ftp-user.sh $user $pw $SPART1/home/$user $max $mode
            fi
        done
    fi
}

```

- Detecting the entropy of a given firmware image. This can help you identify whether a firmware image is compressed or encrypted. To perform entropy analysis, run Binwalk with the -E flag followed by the firmware name as shown in the following screenshot:



The large variations prove that this firmware image is having some encryption.

➤ **Using Firmwalker on the filesystem that is curved already using Binwalk tool:**

This tool shows that there are some emails, IP addresses, password locations, configuration files, etc. all these files and directories are vulnerable and could cause serious damage if explored.

```
(root@kali) - [~/Downloads/firmwalker]
# ./firmwalker.sh /home/nraj Khan/Downloads/cpio/sbin
***Firmware Directory***
/home/nraj Khan/Downloads/cpio/sbin
***Search for password files***
```

```
***Search for shell scripts***
##### shell scripts
n/zcip.sh
n/cameraname.sh
n/wifi_unload.sh
n/storage.sh
n/chpasswd.sh
n/web.sh
n/dhcp.sh
n/vpn-passthru.sh
n/config-udhcpd.sh
n/global.sh
n/video.sh
n/wan.sh
n/udhcpc.sh
n/config.sh
n/config-dns.sh
n/lan.sh
n/config-vlan.sh
n/internet.sh
n/config-igmp proxy.sh
n/pppoe.sh
n/wlan.sh
n/nat.sh
n/ddns.sh
n/automount.sh
n/ntp.sh

***Search for other .bin files***
##### bin files

***Search for patterns in files***
_____ upgrade _____
_____ admin _____
n/storage.sh
_____ root _____
n/config.sh
n/udev
_____ password _____
n/storage.sh
n/internet.sh
```


Appendix B



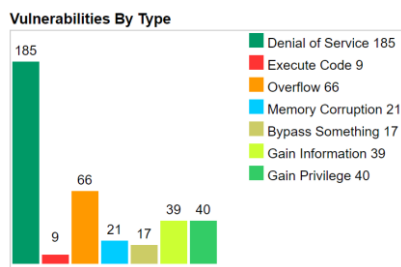
Here are all the tools, steps, and commands that have been used to discover and analyze the Firmware.

1. Download the last firmware version of the Wyze cam v3 IoT smart camera (Webcam Firmware Instructions – Wyze (zendesk.com)) on the Kali Linux.
2. After Binwalk the firmware (demo.bin). Here are the findings:

```

root@kali:~/Downloads# binwalk -t -vv -e demo.bin
Scan Time:      2021-03-10 23:27:03
Target File:    /home/nrajkan/Downloads/demo.bin
MD5 Checksum:  7cccf3f1b2702f15ec6810b90c5f5e5b
Signatures:    391
  
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	uImage header, header size: 64 bytes, header CRC: 0x413EFAFE, created: 2020-03-21 10:10:07, image size: 11075584 bytes, Data Address: 0x0, Entry Point: 0x0, data CRC: 0xC181F3AB, OS: Linux, CPU: MIPS, image type: Firmware Image, compression type: none, image name: "jz_fw"
64	0x40	uImage header, header size: 64 bytes, header CRC: 0x7771D66A, created: 2020-03-20 15:44:39, image size: 1816781 bytes, Data Address: 0x80010000, Entry Point: 0x803E9230, data CRC: 0xBDC20C2D, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "linux-3.10.14"
128	0x80	LZMA compressed data, properties: 0x5D, dictionary size: 67108864 bytes, uncompressed size: -1 bytes
2097216	0x200040	Squashfs filesystem, little endian, version 4.0, compression:xz, size: 3353204 bytes, 407 inodes, blocksize: 131072 bytes, created: 2019-05-21 17:22:45
5570624	0x550040	Squashfs filesystem, little endian, version 4.0, compression:xz, size: 583802 bytes, 13 inodes, blocksize: 131072 bytes, created: 2020-02-23 16:07:18



The image uses U-Boot as the bootloader by tracing the uImage file which is a Linux Kernel type (image header at address 64 0x40 and compressed bootloader image at address 128 0x80). Based on the uImage header at address 64 0x40, we know the CPU architecture is MIPS. This firmware is using a compression type of “lzma” archive. This firmware is using “kernel Linux3.10.1” which has a high rate of DoS vulnerabilities. By executing the Binwalk (-t -vv -e) command, we can locate the file system (Squashfs) extracted in the main directory as shown below:

```
(root@kali)~# cd /home/nraj Khan/Downloads
(root@kali)~/Downloads# cd _demo.bin-2.extracted
(root@kali)~/Downloads/_demo.bin-2.extracted# ls -ls
total 246000
 8 -rw-r--r-- 1 root root 6548 Mar 10 23:27 A8E6AC.zlib
 8 -rw-r--r-- 1 root root 4996 Mar 10 23:27 A8ECBC.jffs2
 4 -rw-r--r-- 1 root root 4035 Mar 10 23:27 A8F530
 4 -rw-r--r-- 1 root root 2832 Mar 10 23:27 A8F530.zlib
 4 drwxrwxr-x 25 501 dialout 4096 May 4 2019 squashfs-root
 4 drwxr-xr-x 2 501 dialout 4096 Feb 23 2020 squashfs-root-0
(root@kali)~/Downloads/_demo.bin-2.extracted# cd squashfs-root
```

3. Here are all the findings in the “squashfs-root” file system:

```
(root@kali)~/Downloads/_demo.bin-2.extracted# cd squashfs-root
(root@kali)~/Downloads/_demo.bin-2.extracted/squashfs-root# ls -ls
total 92
 4 drwx----- 2 501 dialout 4096 Jan 11 2018 backupa
 4 drwx----- 2 501 dialout 4096 Jan 11 2018 backupd
 4 drwx----- 2 501 dialout 4096 Jan 11 2018 backupp
 4 drwx----- 2 501 dialout 4096 Jan 11 2018 bio
 4 drwx----- 2 501 dialout 4096 Jan 11 2018 conFigs
 4 drwx----- 2 501 dialout 4096 Jan 11 2018 dev
 4 drwx----- 2 501 dialout 4096 Jan 11 2018 driver
 4 drwx----- 3 501 dialout 4096 Jan 11 2018 etc
 4 drwx----- 2 501 dialout 4096 Jan 11 2018 lib
 0 lrwxrwxrwx 1 501 dialout 11 May 4 2019 linsarc -> bin/busybox
 4 drwx----- 2 501 dialout 4096 Jan 11 2018 media
 4 drwx----- 2 501 dialout 4096 Jan 11 2018 mt
 4 drwx----- 2 501 dialout 4096 Jan 11 2018 opt
 4 drwx----- 2 501 dialout 4096 Jan 11 2018 params
 4 drwx----- 2 501 dialout 4096 Jan 11 2018 proc
 4 drwx----- 3 501 dialout 4096 Jan 11 2018 root
 4 drwx----- 2 501 dialout 4096 Jan 11 2018 run
 4 drwx----- 2 501 dialout 4096 Jan 11 2018/sbin
 4 drwx----- 2 501 dialout 4096 Jan 11 2018/system
 4 drwx----- 2 501 dialout 4096 May 4 2019/thirdlib
 4 drwx----- 2 501 dialout 4096 Jan 11 2018/tmp
 4 drwx----- 8 501 dialout 4096 Jan 11 2018/usr
 4 drwx----- 4 501 dialout 4096 Jan 11 2018/var
```

- Here is some information about cryptography:

```
(root@kali)~/Downloads/_demo.bin-2.extracted/squashfs-root/thirdlib# cat libmbedcrypto.so.0
```

shows some cipher information!

```
The selected feature is not availableCIPHER - Bad input parameters to functionCIPHER - Failed to
allocate memoryCIPHER - Input data contains invalid padding and is rejectedCIPHER - Decryption o
f block requires a full blockCIPHER - Authentication failed (for AEAD modes)CIPHER - The context
is invalid, eg because it was free(dedDhM - Bad input parameters to functionDhM - Reading of the
DhM parameters failedDhM - Making of the DhM parameters failedDhM - Reading of the public values
failedDhM - Making of the public value failedDhM - Calculation of the DhM secret failedDhM - The
ASN.1 data is not formatted correctlyDhM - Allocation of memory failedDhM - Read/write of file fa
iledECP - Bad input parameters to functionECP - The buffer is too small to write toECP - Requeste
d curve not availableECP - The signature is not validECP - Memory allocation failedECP - Generati
on of random value, such as (ephemeral) key, failedECP - Invalid private or public keyECP - Signa
ture is valid but shorter than the user-supplied lengthMD - The selected feature is not available
MD - Bad input parameters to functionMD - Failed to allocate memoryMD - Opening or reading of fil
e failedPEM - No PEM header or footer foundPEM - PEM string is not as expectedPEM - Failed to all
ocate memoryPEM - RSA IV is not in hex-formatPEM - Unsupported key encryption algorithmPEM - Priv
ate key password can't be emptyPEM - Given private key password does not allow for correct decryp
tionPEM - Unavailable feature, e.g. hashing/encryption combinationPEM - Bad input parameters to f
unctionPK - Memory allocation failedPK - Type mismatch, eg attempt to encrypt with an ECDSA keyPK
- Bad input parameters to functionPK - Read/write of file failedPK - Unsupported key versionPK -
Invalid key tag or valuePK - Key algorithm is unsupported (only RSA and EC are supported)PK - Priv
ate key password can't be emptyPK - Given private key password does not allow for correct decry
ptionPK - The pubkey tag or value is invalid (only RSA and EC are supported)PK - The algorithm ta
g or value is invalidPK - Elliptic curve is unsupported (only NIST curves are supported)PK - Unav
ailable feature, e.g. RSA disabled for RSA keyPK - The signature is valid but its length is less
than expectedPKCS12 - Bad input parameters to functionPKCS12 - Feature not available, e.g. unsupp
orted encryption schemePKCS12 - PBE ASN.1 data not as expectedPKCS12 - Given private key password
does not allow for correct decryptionPKCS5 - Bad input parameters to functionPKCS5 - Unexpected
ASN.1 dataPKCS5 - Requested encryption or digest alg not availablePKCS5 - Given private key passw
ord does not allow for correct decryptionRSA - Bad input parameters to functionRSA - Input data c
ontains invalid padding and is rejectedRSA - Something failed during generation of a keyRSA - Key
failed to pass the library's validity checkRSA - The public key operation failedRSA - The privat
e key operation failedRSA - The PKCS#1 verification failedRSA - The output buffer for decryption
is not large enoughRSA - The random generator failed to generate non-zerosSSL - The requested fea
ture is not availableSSL - Bad input parameters to functionSSL - Verification of the message MAC
failedSSL - An invalid SSL record was receivedSSL - The connection indicated an EOFSSL - An unkno
wn cipher was receivedSSL - The server has no ciphersuites in common with the clientSSL - No RNG
was provided to the SSL moduleSSL - No client certification received from the client, but require
d by the authentication modeSSL - Our own certificate(s) is/are too large to send in an SSL messa
geSSL - The own certificate is not set, but needed by the serverSSL - The own private key or pre-sh
ared key is not set, but neededSSL - No CA chain is set, but required to operateSSL - An unexpe
cted message was received from our peerSSL - A fatal alert message was received from our peerSSL
- Verification of our peer failedSSL - The peer notified us that the connection is going to be cl
osedSSL - Processing of the ClientHello handshake message failedSSL - Processing of the ServerHel
lo handshake message failedSSL - Processing of the Certificate handshake message failedSSL - Proc
essing of the CertificateRequest handshake message failedSSL - Processing of the ServerKeyExchang
e handshake message failedSSL - Processing of the ServerHelloDone handshake message failedSSL - P
rocessing of the ClientKeyExchange handshake message failedSSL - Processing of the ClientKeyExcha
nge handshake message failed in DhM / ECDH Read PublicSSL - Processing of the ClientKeyExchange h
andshake message failed in DhM / ECDH Calculate SecretSSL - Processing of the CertificateVerify h
```


- Here is a network port 80 configuration, Server name and address are available.

```
(root@kali) - [~/home/nrajkhani/Downloads/_demo.bin-2.extracted/squashfs-root]
# cat ./usr/boa/boa.conf
Port 80

#Listen 192.68.0.5

User 0

Group 0

#ServerAdmin root@localhost

ErrorLog /tmp/error_log

#AccessLog /var/log/boa/access_log

#UseLocaltime

#VerboseCGILogs

ServerName www.your.org.here

#VirtualHost

DocumentRoot /tmp/www

UserDir public_html

DirectoryIndex index.html

DirectoryMaker /usr/lib/boa/boa_indexer

# DirectoryCache /var/spool/boa/dircache

KeepAliveMax 1000

KeepAliveTimeout 10

MimeTypes /usr/boa/mime.types

DefaultType text/plain

CGIPath /bin:/usr/bin

#AddType application/x-httpd-cgi cgi

Alias /doc /usr/doc

ScriptAlias /cgi-bin/ /tmp/www/cgi-bin/
```

- Here is some information about wireless Pre-shared Key (PSK).

```
(root@kali) - [~/home/nrajkhani/Downloads/_demo.bin-2.extracted/squashfs-root]
# cat ./usr/share/hostapd/wpa2.conf
interface=wlan0
ctrl_interface=/var/run/hostapd
channel=6
driver=nl80211
beacon_int=100
hw_mode=g
wme_enabled=1
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
max_num_sta=8
wpa_group_rekey=86400
#ssid=rtwap
#wpa=2
#wpa_passphrase=87654321
```

- Here is the UDHCPC configuration file with IP addresses.

```
(root@kali) ~ [~/home/nraj Khan/Downloads/_demo.bin-2.extracted/squashfs-root]
# cat ./usr/share/udhcpd_wpa2.conf
# Sample udhcpd configuration file (/etc/udhcpd.conf)
# Values shown are defaults

# The start and end of the IP lease block
start      10.42.0.100
end        10.42.0.251

# The interface that udhcpd will use
interface  wlan0

# The maximum number of leases (includes addresses reserved
# by OFFER's, DECLINE's, and ARP conflicts). Will be corrected
# if it's bigger than IP lease block, but it's ok to make it
# smaller than lease block.
#max_leases 254

# The time period at which udhcpd will write out a dhcpd.leases
# file. If this is 0, udhcpd will never automatically write a
# lease file. Specified in seconds.
#auto_time 7200

# The amount of time that an IP will be reserved (leased to nobody)
# if a DHCP decline message is received (seconds)
#decline_time 3600

# The amount of time that an IP will be reserved
# if an ARP conflict occurs (seconds)
#conflict_time 3600

# How long an offered address is reserved (seconds)
#offer_time 60

# If client asks for lease below this value, it will be rounded up
# to this value (seconds)
#min_lease 60

# The location of the leases file
#lease_file /var/lib/misc/udhcpd.leases

# The location of the pid file
#pidfile /var/run/udhcpd.pid

# Every time udhcpd writes a leases file, the below script will be called
#notify_file # default: no script
#notify_file dupleases # useful for debugging

# The following are bootp specific options
#next_server to use in bootstrap
#siaddr 192.168.0.22 # default: 0.0.0.0 (none)
#tftp server name
#sname zorak # default: none
#tftp file to download (e.g. kernel image)
#boot_file /var/nfs_root # default: none
```



```

# Static leases map
#static_lease 00:60:08:11:CE:4E 192.168.0.54
#static_lease 00:60:08:11:CE:3E 192.168.0.44

# The remainder of options are DHCP options and can be specified with the
# keyword 'opt' or 'option'. If an option can take multiple items, such
# as the dns option, they can be listed on the same line, or multiple
# lines.
# Examples:
opt dns 10.42.0.1
option subnet 255.255.255.0
opt router 10.42.0.1
opt wins 10.42.0.1
option dns 129.219.13.81 # appended to above DNS servers for a total of 3
option domain local
option lease 864000 # default: 10 days
# Arbitrary option in hex form:
option 0x08 01020304 # option 8: "cookie server IP addr: 1.2.3.4"
opt hostname guozhixin # client's hostname

# Currently supported options (for more info, see options.c):
#opt lease NUM
#opt subnet IP
#opt broadcast IP
#opt router IP_LIST
#opt ipttl NUM
#opt mtu NUM
#opt hostname STRING # client's hostname
#opt domain STRING # client's domain suffix
#opt search STRING_LIST # search domains
#opt nisdomain STRING
#opt timezone NUM # (localtime - UTC_time) in seconds, signed
#opt tftp STRING # tftp server name
#opt bootfile STRING # tftp file to download (e.g. kernel image)
#opt bootsize NUM # size of that file
#opt rootpath STRING # (NFS) path to mount as root fs
#opt wpad STRING
#opt serverid IP # default: server's IP
#opt message STRING # error message (udhcpd sends it on success too)
# Options specifying server(s)
#opt dns IP_LIST
#opt wins IP_LIST
#opt nissrv IP_LIST
#opt ntpsrv IP_LIST
#opt lprsrv IP_LIST
#opt swpsrv IP
# Obsolete options, no longer supported
#opt logsrv IP_LIST # 704/UDP log server (not syslog!)
#opt namesrv IP_LIST # IEN 116 name server, obsolete (August 1979!!!)
#opt cookiesrv IP_LIST # RFC 865 "quote of the day" server, rarely (never?) used
#opt timesrv IP_LIST # RFC 868 time server, rarely (never?) used

```

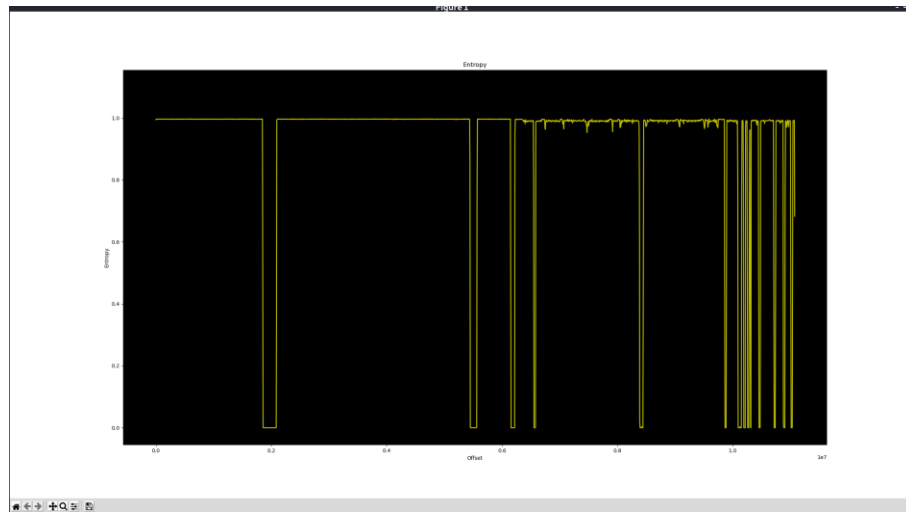
- Here is the entropy result that shows that there this firmware image is having some encryption.

```

(root@kali) ~/home/nra/jkhan/Downloads
└─$ binwalk -E demo.bin

```

DECIMAL	HEXADECIMAL	ENTROPY
0	0x0	Rising entropy edge (0.994544)
1853440	0x1C4800	Falling entropy edge (0.471651)
2097152	0x200000	Rising entropy edge (0.991917)
5451776	0x533000	Falling entropy edge (0.000000)
5574656	0x551000	Rising entropy edge (0.996314)
6152192	0x5DE000	Falling entropy edge (0.456919)
6225920	0x5F0000	Rising entropy edge (0.950929)
6549504	0x63F000	Falling entropy edge (0.781254)
6586368	0x648000	Rising entropy edge (0.987080)
8384512	0x7FF000	Falling entropy edge (0.721105)
8456192	0x810800	Rising entropy edge (0.992783)
9861120	0x967800	Falling entropy edge (0.453895)
9897984	0x970800	Rising entropy edge (0.987870)
10088448	0x99F000	Falling entropy edge (0.769161)
10162176	0x9B1000	Rising entropy edge (0.991231)
10186752	0x9B7000	Falling entropy edge (0.765101)
10223616	0x9C0000	Rising entropy edge (0.971957)
10254336	0x9C7800	Falling entropy edge (0.454122)
10297344	0x9D2000	Rising entropy edge (0.961377)
10303488	0x9D3800	Falling entropy edge (0.427326)
10321920	0x9D8000	Rising entropy edge (0.990403)
10450944	0x9F7800	Falling entropy edge (0.440366)
10485760	0xA00000	Rising entropy edge (0.989939)
10713088	0xA37800	Falling entropy edge (0.453481)
10749952	0xA40800	Rising entropy edge (0.990590)
10878976	0xA60000	Falling entropy edge (0.019284)
10915840	0xA69000	Rising entropy edge (0.990834)
11008000	0xA7F800	Falling entropy edge (0.451583)
11044864	0xA88800	Rising entropy edge (0.990570)
11075584	0xA90000	Falling entropy edge (0.682882)



➤ **Using Firmwalker on the filesystem that already curved using Binwalk tool:**

This tool shows that there are some emails, IP addresses, Keys, password locations, configuration files, etc. all these files and directories are vulnerable and could cause serious damage if explored.

```
(root@kali) - [~/home/nrajkhan/Downloads/firmwalker]
# ./firmwalker.sh /home/nrajkhan/Downloads/_demo.bin-2.extracted/squashfs-root 1 x 1
**Firmware Directory**
/home/nrajkhan/Downloads/_demo.bin-2.extracted/squashfs-root
**Search for password files**
##### passwd
t/usr/bin/passwd
t/etc/passwd

##### shadow
t/etc/shadow

##### *.psk

**Search for Unix-MD5 hashes**

**Search for SSL related files**
##### *.crt
##### *.pem
##### *.cer
##### *.p7b
##### *.p12
##### *.key
```

```
**Search for SSH related files**
##### authorized_keys
##### *authorized_keys*
##### host_key
##### *host_key*
##### id_rsa
##### *id_rsa*
##### id_dsa
##### *id_dsa*
##### *.pub

**Search for files**
##### *.conf
t/root/etc/default/wpa_supplicant.conf
t/usr/boa/boa.conf
t/usr/share/udhcpd_wpa2.conf
t/usr/share/hostapd_wpa2.conf
t/etc/resolv.conf

##### *.cfg
##### *.ini
t/etc/webrtc_profile.ini

**Search for database related files**
##### *.db
##### *.sqlite
##### *.sqlite3

**Search for shell scripts**
##### shell scripts
```



```

**Search for other .bin files**
##### bin files

```

```

**Search for patterns in files**

```

```

_____ upgrade _____
_____ admin _____
_____ root _____

```

```

t/bin/busybox
t/usr/boa/boa.conf
t/usr/boa/mime.types
t/usr/boa/boa
t/usr/share/udhcpd_wpa2.conf
t/etc/shadow
t/etc/group
t/etc/passwd
t/thirdlib/libmp4v2.so.2.0.0
t/thirdlib/libnl-3.so.200.21.0
t/thirdlib/libcrypto.so.1.0.0

```

```

_____ password _____
t/bin/busybox
t/lib/libuClibc-0.9.33.2.so
t/thirdlib/libcurl.so.4.3.0
t/thirdlib/libmbedcrypto.so.0
t/thirdlib/libcrypto.so.1.0.0

```

```

_____ passwd _____
t/bin/busybox
t/lib/libuClibc-0.9.33.2.so

```

```

_____ pwd _____
t/bin/busybox
t/lib/libuClibc-0.9.33.2.so
t/thirdlib/libcurl.so.4.3.0

```

```

_____ dropbear _____

```

```

_____ ssl _____
t/thirdlib/libssl.so.1.0.0
t/thirdlib/libmbedtls.so.10
t/thirdlib/libcurl.so.4.3.0
t/thirdlib/libmbedcrypto.so.0
t/thirdlib/libcrypto.so.1.0.0

```

```

_____ private key _____
t/thirdlib/libssl.so.1.0.0
t/thirdlib/libmbedtls.so.10
t/thirdlib/libcurl.so.4.3.0
t/thirdlib/libmbedcrypto.so.0
t/thirdlib/libmbedx509.so.0
t/thirdlib/libcrypto.so.1.0.0

```

```

_____ telnet _____
t/etc/init.d/rcS
t/thirdlib/libcurl.so.4.3.0
t/thirdlib/libcrypto.so.1.0.0

```

```

_____ secret _____
t/thirdlib/libssl.so.1.0.0
t/thirdlib/libmbedtls.so.10
t/thirdlib/libmbedcrypto.so.0

```

```

_____ pgp _____
t/usr/boa/mime.types

```

```

_____ gpg _____

```

```

_____ token _____
t/bin/busybox
t/thirdlib/libcrypto.so.1.0.0

```

```

_____ api key _____

```

```

_____ oauth _____

```

```

**Search for web servers**
##### search for web servers
##### apache

```

```

##### lighttpd

```

```

##### alphasd

```

```

##### httpd
t/usr/sbin/httpd

```

```

***Search for important binaries***
##### important binaries
##### ssh

##### sshd

##### scp

##### sftp

##### tftp
t/usr/bin/tftp

##### dropbear

##### busybox
t/bin/busybox

##### telnet
t/usr/bin/telnet

##### telnetd
t/sbin/telnetd
t/usr/sbin/telnetd

##### openssl

***Search for ip addresses***
##### ip addresses
0.0.0.0
10.42.0.1
10.42.0.100
10.42.0.251
1.2.3.4
127.0.0.1
129.219.13.81
192.168.0.22
192.168.0.44
192.168.0.54
192.168.1.80
192.68.0.5
255.255.255.0

***Search for urls***
##### urls
http://www.iana.org

```

```

***Search for urls***
##### urls
http://www.iana.org

***Search for emails***
##### emails
andersen@codepoet.org
Tim@Rikers.org

```

Appendix C

This survey has three main sections that focus on supporting the main goals that are described in advance. Here are the sections and questions about IoT smart home devices security, privacy, and firmware label survey for experts:

Please go through below definition of smart home devices and the labels I have created so far carefully, before answering the rest of the questions. The definition of an "IoT smart home device" is any single-purpose internet-connected device that is designed for a home or a hub, like a device that is designed to connect and control more than one single-purpose device. There are different types of it, along with different functions that it provides such as security cameras, smart thermostats, Google and Amazon assistants, smart lights, and so on.



References:


























Text: [14] N. Apthorpe, D. Reisman, and N. Feamster, "A smart home is no castle: privacy vulnerabilities of encrypted IoT traffic", Computer Science Dept. Princeton University, pp. 1-6, 2017.

Picture: <https://www.mhealthtalk.com/smart-home-technologies-mature-homeowners/>

I am designing two IoT smart home device labels that cover the most critical security and privacy aspects.








Firstly, the summarized label will be presented on the device's packaging (box) to help consumers to know more about it and to make better purchase decisions. Here are my two designs for the summarized label so far.



Summarized Label design A:

Security, privacy and firmware label for IoT smart home devices 																									
General Information																									
Name:	Warranty lifetime:																								
Brand:	OS Compatibility:																								
Version:	Firmware version:																								
Storage Type:	Firmware update lifetime:																								
Security, privacy factors scores																									
	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 15%;">Symbol</th> <th style="width: 60%;">Factor</th> <th style="width: 25%;">Score</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"></td> <td>Internet pairing</td> <td></td> </tr> <tr> <td style="text-align: center;"></td> <td>Configuration and Authentication</td> <td></td> </tr> <tr> <td style="text-align: center;"></td> <td>Update mode</td> <td></td> </tr> <tr> <td style="text-align: center;"></td> <td>Exposed service</td> <td></td> </tr> <tr> <td style="text-align: center;"></td> <td>Firmware Vulnerabilities</td> <td></td> </tr> <tr> <td style="text-align: center;"></td> <td>Protocols</td> <td></td> </tr> <tr> <td style="text-align: center;"></td> <td>Network encryption</td> <td></td> </tr> </tbody> </table>	Symbol	Factor	Score		Internet pairing			Configuration and Authentication			Update mode			Exposed service			Firmware Vulnerabilities			Protocols			Network encryption	
	Symbol	Factor	Score																						
		Internet pairing																							
		Configuration and Authentication																							
		Update mode																							
		Exposed service																							
		Firmware Vulnerabilities																							
		Protocols																							
	Network encryption																								
Label barcode 	For detailed information 																								

Summarized Label design B:















General Information	
Name:	Warranty lifetime:
Brand:	OS Compatibility:
Version:	Firmware version:
Storage Type:	Firmware update lifetime:

Security, privacy factors scores		
Symbol	Factor	Score
	Internet pairing	
	Configuration and Authentication	
	Update mode	
	Exposed service	
	Firmware Vulnerabilities	
	Protocols	
	Network encryption	

<p>Label barcode</p> 	<p>For detailed information</p> 
--	---

Secondly, the detailed label presents in detail all security, privacy, firmware features information that consumers might need when looking for certain details. This could be bigger and has more written details rather than numbering or graphical information. This label would be accessed by scanning the QR code on the summarized label.

Here is my design for the detailed label so far.

Security, privacy and firmware label for IoT smart home devices				
General Information				
Name:		Warranty lifetime:		
Brand:		OS Compatibility:		
Version:		Firmware version:		
Storage Type:		Firmware update lifetime:		
Security, privacy and firmware factors scoring				
#	Factor	Symbol	Description	Used method
1	Internet pairing		Establishment of network connection between the IoT device and the local network to provide Internet connection.	Wi-Fi, Bluetooth, Zigbee.
2	Configuration and Authentication		Configuration and authentication procedures that are required to set up the IoT smart home device for operation	Use default, customized or Manual.
3	Update mode		The procedure that is used to install the latest updates for the IoT smart home device firmware.	Permission required (Push mode), Manual (Pull Mode), Automatic.
4	Exposed service		Total number of services that a user of the smart home device could access using a local network connection to this device.	video, audio, temp, presence, carbon monoxide (fire).
5	Firmware Vulnerabilities		The shortcomings in the mini system running on the IoT smart home device.	Password Exploitation, Rogue Recordings, Outdated Software.
6	Protocols		The set of rules that format the data transmission over the local network and Internet.	non-standard custom protocol, 3rd party DNS, UPnP, HTTPS, NTPv3.
7	Network encryption		Encryption techniques or procedures that are used in the data transmission in the IoT smart home ecosystem network.	Device to Cloud, Mobile Application to Cloud, Mobile Application to Device.
Data sensor Practices				
Type	Data storage location	Data retention time	Shared or sold	Collection recurrence
Camera 				
Microphone 				
Fire 				
Temperature 				
Movement 				
Technical specifications				
Specifications	Description			
Power and max power consumption				
Certificate awarded				
Data Codecs				
SDRAM or Flash Memory				
Combined applications				
Smart Assistance				
Network Ports				
Label Barcode		Privacy Policy www.Privacy.sa		
				

Section 1: Label's content and sections questions

Q1. In the general information section of all label designs, I have included 4 default categories: Name, Warranty Lifetime, Firmware version, and Firmware update lifetime. Please choose 4 additional categories to include based on your expertise:








- IoT device's Brand and Model number, such as Philips, Model RT57
- IoT device's version, such as the 4th or the 5th version
- Storage Type (Internal or cloud), such as SD card or google drive
- Operating system compatibility, such as Android or iOS
- Available sensors, such as cameras, microphones
- Privacy policy; provides a link to the device's manufacturer document about the privacy policy
- Virtual assistance (Alexa, Siri, Bixby)
- Types of the collected data (MP4, MP3)
- Other: _____

Q2. For the detailed label's technical specification section, do you prefer to know about any of the followings?

- Power options and consumption, such as any built-in rechargeable battery or DC power supply
- Any awarded prizes or certificates by this Model, such as Amazon Web Services for best consumer IoT Solution
- Provide supportive combined applications, such as Samsung home or Brilliant
- Network Port availability (RJ-45)
- Other: _____

Section 2: Security and Privacy Factors questions

Here are the security and privacy factors with descriptions in the proposed detailed label design:

#	Factor	Symbol	Description	Used method
1	Internet pairing		Establishment of network connection between the IoT device and the local network to provide Internet connection.	Wi-Fi, Bluetooth, Zigbee.
2	Configuration and Authentication		Configuration and authentication procedures that are required to set up the IoT smart home device for operation	Use default, customized or Manual.
3	Update mode		The procedure that is used to install the latest updates for the IoT smart home device firmware.	Permission required (Push mode), Manual (Pull Mode), Automatic.
4	Exposed service		Total number of services that a user of the smart home device could access using a local network connection to this device.	video, audio, temp, presence, carbon monoxide (fire).
5	Firmware Vulnerabilities		The shortcomings in the mini system running on the IoT smart home device.	Password Exploitation, Rogue Recordings, Outdated Software.
6	Protocols		The set of rules that format the data transmission over the local network an Internet.	non-standard custom protocol, 3rd party DNS, UPnP, HTTPS, NTPv3.
7	Network encryption		Encryption techniques or procedures that are used in the data transmission in the IoT smart home ecosystem network.	Device to Cloud, Mobile Application to Cloud, Mobile Application to Device.

Q3. Which security and privacy factors do you prefer to see on the IoT smart home device's label, to assist consumers to make better purchase decisions? Pick the best 5 useful and understandable factors based on your expertise.















- Internet Pairing
- Configuration and Authentication
- Update Mode
- Exposed Service
- Firmware Vulnerabilities
- Protocols
- Network Encryption

Q3.1 Do you have any security or privacy factor that you want to add to the IoT smart home device's label that I may have missed? _____








Section 3: Labels designing and formatting questions

Here are the security and privacy factor's score representations, using a scale of 5 levels:








A. Emoji representation:

Symbol	Factor	Score
	Internet pairing	
	Configuration and Authentication	
	Update mode	
	Exposed service	
	Firmware Vulnerabilities	
	Protocols	
	Network encryption	

B. Numbers representation:

Symbol	Factor	Score
	Internet pairing	1
	Configuration and Authentication	2
	Update mode	4
	Exposed service	3
	Firmware Vulnerabilities	5
	Protocols	4
	Network encryption	1

C. Letters Representation:

Symbol	Factor	Score
	Internet pairing	F
	Configuration and Authentication	D
	Update mode	B
	Exposed service	C
	Firmware Vulnerabilities	A
	Protocols	B
	Network encryption	F

Q4. Which representation do you prefer for describing the factor's score?

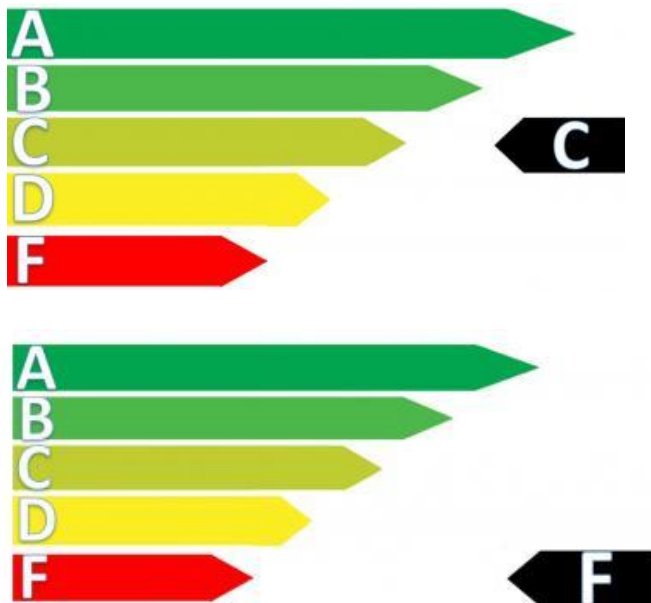
- Emoji representation
- Numbers representation
- Letters representation

Here are different representations for the final score for IoT smart home device's security and privacy factors:

A. The Big numbers (5 is the best score).



B. The colorful Bar graph.



C. The big letters (A is the best score).



Q5 which representation do you prefer for the final security and privacy score?

- Design A, the big numbers
- Design B, the colorful Bar graph
- Design C, the big letters

Appendix D

This survey has three main sections that focus on supporting the main goals that are described in advance. It has two identical version with Arabic and English languages to reach larger segment participants. Here is all sections and questions of IoT smart home devices security, privacy, and firmware label survey for regular consumers:

SECTION 1 Security and Privacy Awareness Check

This section will give me an overview of your computer and technical security and privacy background. Additionally, the collected data will emphasize the content and the design of the IoT smart home devices label.

Q1. How familiar are you with computer security and privacy issues?

- Not familiar at all
- Slightly familiar
- Moderately familiar
- Very familiar
- Extremely familiar

Q2. How often do you change your passwords?

- Weekly
- Monthly
- Yearly
- I do not change it until it has its expired

Q4. How often do you check for device's software updates?

- Very often (1)
- Sometimes (2)
- Never (3)
- I rely on automatic updates (4)

Section 2 IoT smart home devices labels

Please go through below definition of smart home devices and the labels I have created so far carefully, before answering the rest of the questions.

The definition of an "IoT smart home device" is any single-purpose internet-connected device that is designed for a home or a hub, like a device that is designed to connect and control more than one single-purpose device. There are different types of devices, along with different functions that they provide such as security cameras, smart thermostats, Google and Amazon assistants, smart lights, and so on.



References:

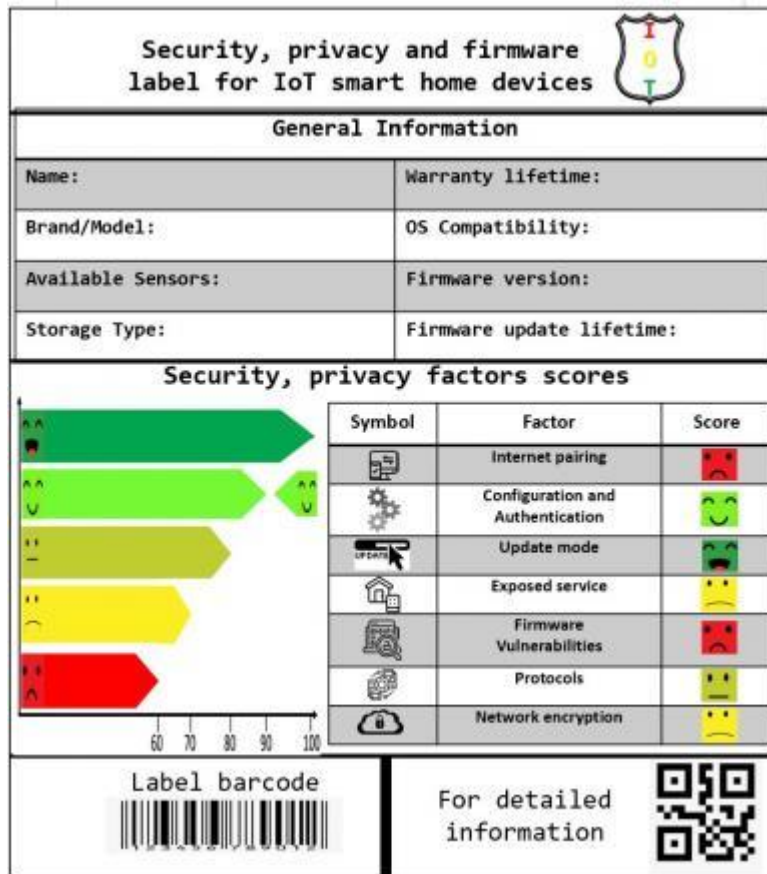
N. Apthorpe, D. Reisman, and N. Feamster, "A smart home is no castle: privacy vulnerabilities of

encrypted iot traffic", Computer Science Dept. Princeton University, pp. 1-6, 2017. Picture: <https://www.mhealthtalk.com/smart-home-technologies-mature-homeowners/>

I am designing two IoT smart home device labels that cover the most critical security and privacy aspects















Firstly, the "summarized label" will be presented on the device's packaging (box) to help consumers learn more about the device quickly and to make better purchasing decisions.

Summarized Label design:



Secondly, the "detailed label" will present detailed information on all security, privacy, firmware features that consumers might need when looking for certain details. This label would be bigger and has more written details rather than numbering or graphical information. This label would be accessed by scanning the QR code on the summarized label.

Detailed Label design:

Security, privacy and firmware label for IoT smart home devices					
General Information					
Name:		Warranty lifetime:			
Brand/Model:		OS Compatibility:			
Available Sensors:		Firmware version:			
Storage Type:		Firmware update lifetime:			
Security, privacy and firmware factors scoring					
#	Factor	Symbol	Description	Used method	
1	Internet pairing		Establishment of network connection between the IoT device and the local network to provide internet connection.	Wi-Fi, Bluetooth, Zigbee.	
2	Configuration and Authentication		Configuration and authentication procedures that are required to set up the IoT smart home device for operation.	Use default, customized or Manual.	
3	Update mode		The procedure that is used to install the latest updates for the IoT smart home device firmware.	Permission required (Push mode), Manual (Pull Mode), Automatic.	
4	Exposed service		Total number of services that a user of the smart home device could access using a local network connection to this device.	video, audio, temp, presence, carbon monoxide (fire).	
5	Firmware Vulnerabilities		The shortcomings in the mini system running on the IoT smart home device.	Password Exploitation, Rogue Recordings, Outdated Software.	
6	Protocols		The set of rules that format the data transmission over the local network and Internet.	non-standard (custom protocol, 3rd party DNS, UDP, HTTPS, NTPv),	
7	Network encryption		Encryption techniques or procedures that are used in the data transmission in the IoT smart home ecosystem network.	Device to Cloud, Mobile Application to Cloud, Mobile Application to Device.	
Data sensor practices					
Type	Symbol	Data storage location	Data retention time	Shared or sold	Collection recurrence
Camera					
Microphone					
fire					
Temperature					
Movement/Location					
Technical specifications					
Specifications		Description			
Power and max power consumption					
SDRAM or Flash Memory					
Combined Applications					
Smart Assistance					
Connectivity Information					
Label Barcode			Privacy Policy		
			www.Privacy.sa		

Q5. In the summarized label, which section do you think would help you the most in purchasing decision?

- General information section
- The Factors score table
- The final score bar graph

Q6. Based on the information provided by the summarized label, if all security, privacy and firmware features about an IoT smart home device matches what you need, would you still look for the detailed label or would you directly make a purchasing decision instead?

- I will make a final purchasing decision without looking for the detailed label
- I will look for the detailed label to make a better purchasing decision

Q7. There are four sections in the detailed label. Which section are you going to look for the most in this label?

- Security, Privacy and Firmware factor scoring table
- Data sensor Practices section
- Technical specifications section
- Privacy policy section

Q8. When purchasing an IoT smart home device, will you look for the product's detailed label?

- Definitely not
- Probably not
- Might or might not
- Probably yes
- Definitely yes

Q9. Will you trust a IoT smart home devices label if it was created by: (Select all that apply)

- A government authority such as SASO
- A technical or computer devices distribution companies such as best buy, Extra, Jarir, Walmart
- An IoT smart home devices manufacturers
- Other: _____

Q10. If you own a smart doorbell that is equipped with a camera and microphone sensors, how often do you think these sensors would sense or collect information?

- Always sense or collect information
- Sense only when someone is present
- Sense only when I press a button
- Not sure how the device works

Q11 If you see that an IoT smart home device has a full score on its security, privacy and firmware attributes, how confident would you be in your purchasing decision?

- Not At All Confident
- Somewhat Confident
- Very Confident

SECTION 3 IoT smart home devices purchase decisions

Q12 What IoT smart home devices are you willing to buy? (Select all that apply)

- Security camera
- Smart TV.
- Smart light or bulb.

- Smart Thermostats
- Smart doorbell
- Other: _____

Q13 What privacy, security, or firmware issues are you most afraid of when purchasing an IoT smart home device?

Selling my personal information to other companies

Breach of personal information to be used for blackmail

Recording video or audio without consent

Other: _____

Q14 How do you typically research for IoT smart home devices that you purchase?

- I read the information presented on the package.
- I ask the salesperson at the store.
- I watch a YouTube review about the product.
- I read the device's user manual.
- Other: _____

Q15 Please order the factors that you usually consider when purchasing IoT smart home devices?
(1st factor is the highest priority in the list)

_____ Price

_____ Warranty

_____ Software update lifetime.

_____ Brand name

_____ Easy installation

_____ advertisements on social media or TV

Q16 If the device that you are about to purchase is in the right budget range and comes from a well-known manufacturer, but it does not have trustworthy security and privacy characteristics, will you still purchase this IoT smart device?

- Definitely not
- Probably not
- Might or might not
- Probably yes
- Definitely yes