HomeKOP

by

Vineela Kunapareddi, Oreofeoluwa Oyelowo, and Briana Padgett

Submitted to
the Faculty of the School of Information Technology
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

Vineela Kunapareddi, Oreofeoluwa Oyelowo, Briana Padgett — April 15th, 2019

Vineela Kunapareddi, Oreofeoluwa Oyelowo, Briana Padgett — Date

Ryan Moore — April 29th, 2019

Ryan Moore, Faculty Advisor — Date

University of Cincinnati
College of
Education, Criminal Justice, and Human Services

February 2019

HomeKOP

Prepared by:

Vineela Kunapareddi, Project Manager and Software Developer
Oreofeoluwa Oyelowo, Network Engineer
and Briana Padgett, Security Analyst

Students of
University of Cincinnati
College of Education, Criminal Justice, Human Services and Information Technology
cech.uc.edu/it

April 2019

Table of Contents

List of Illustrations

Abstract

Ten billion IoT devices will be added to consumer home networks by 2020 (Leuth, 2018), with little regard for security. Users are unaware of what it takes to secure their networks and there are currently no security standards in place to hold manufacturers accountable. HomeKOP raises awareness of security issues amongst users and equips them with the right tools to secure their smart home networks. We conducted a vulnerability assessment of smart home networks, gauged consumer awareness using surveys, and created a set of standards for IoT devices. Based on the set of standards, we developed a risk score calculation system that helps users visualize risk. We then built onto the Mozilla Web of Things Gateway that employs a user-friendly dashboard to monitor these devices as they are added to a network, creates a risk score based on how well these devices meet the HomeKOP standards and walks users through securing their networks. HomeKOP is revolutionizing the world of security by putting the user back in control.

1. Problem Statement

1.1 Introduction

Picture this – you wake up in the morning and turn off your alarm. This triggers your curtains to open and your coffee machine starts brewing. Your friend Alexa knows to control the temperature of your home. Even an action as simple as grabbing your keys signals to a system intuitive enough to know to turn off the air conditioning and start your car. This is the world integrated with IoT.

Now imagine losing control of these devices. It probably won't matter much if your curtains don't open or your temperature control is haywire. But, try to fathom a hacker hijacking your smart car while you are still in it or even tampering with a pacemaker in you or your loved ones and draining the battery. Frightening? We think so, too.

This isn't a far-fetched nightmare, this is the reality of a sliver of the vulnerabilities that the world of IoT brings with it. In October 2016 Mirai botnet caused a massive distributed denial of service (DDoS) attack that left much of the internet inaccessible across the world. Mirai is a malware which once implanted in a device, can scan the network for the IP addresses of IoT devices and proceed to hack into them with default credentials.

1.2 Project Description

Research and develop a set of standards, a risk score and visualize it in a Network Access Control System (Mozilla Web of Things Gateway) to secure Smart Home Networks. Millions of IoT devices are being added to consumer home networks every day, with little regard for security. Users are unaware of what it takes to secure their networks and device manufacturers are making

use of “security through obscurity” by releasing devices with known vulnerabilities in hopes that these vulnerabilities will not be exploited.

Some IoT devices only have a stripped-down version of the Linux OS and not enough storage for updates, posing a security threat to any networks they are connected to. For example: The Mirai Botnet attack is one of the most prominent events that has shown the importance of securing IoT devices. It is crucial to make users aware of these issues and equip them with the tools that are necessary to secure their IoT devices and by extension, their home networks. The end product will be research findings and a tool to enforce the best practices for securing IoT devices.

1.3 Problem

IoT devices and smart home networks entail a massive exchange of information. If compromised, the threat posed would be colossal causing a lot of damage from both network and societal perspectives. Imagine losing control of your own home or even a hacker tampering with a defibrillator in you or your loved ones. It is important to ensure secure practices when using IoT devices, but the extent of vulnerabilities is yet to be discovered and a set of secure practices and guidelines are yet to be developed.

1.4 Solution

To combat the vulnerability of IoT devices and Smart Home Networks we propose a three-step process:

a. Vulnerability assessment in a simulated Smart Home environment.

We propose a research study where we conduct a vulnerability assessment on IoT devices connected to the same network to simulate a Smart Home environment. Through testing and set-

up, we will familiarize ourselves with the installation and network configuration process and expose common vulnerabilities of these IoT devices. Additionally, we will conduct a requirements analysis of the network itself. We will then come up with a set of guidelines for end-users that we will disseminate in the form of research findings. Finally, we will create a network access control system with a visual dashboard.

b. Raise awareness amongst the user base about security issues stemming from said devices and networks.

The findings obtained from the research will be shared with both businesses and end-users to help them understand the implications of vulnerabilities. We will also share a set of guidelines to assist users in securing their smart home networks and devices.

c. Network Access Control System to guide users through best practices when connecting Smart Home devices to the network.

Additionally, based on the research findings, we will build onto a tool (Mozilla's Web of Things Gateway) that will work in collaboration with devices to walk users through securing any device that is added to the wireless network and continue to monitor it during its lifetime. This tool will include a user-friendly visual dashboard.

1.5 Overview

The remainder of the report describes what we have done to fill the gap in standardization of IoT devices, HomeKOP aims to research and establish a set of standards. Based on these standards and how well devices meet the standards, a risk score (scale 1-10, 1 being low risk and 10 being high risk) will be calculated to help users understand how safe and secure their devices are. This risk score is packaged with the Mozilla Web of Things Gateway which can be physical

(Raspberry Pi) or cloud-based. The risk score will be depicted on top of the icons for each device on the dashboard and will be color coded to signify the level of risk, green indicating low risk, yellow indicating medium risk and red indicating high risk. The report includes the following sections: user profile, use case diagram, budget, objectives/deliverables, project schedule and timeline, research component, productized solution, visuals, test plan, and conclusions and future work.

1.6 User Profile

Table 1: User Profile contains a collection of data associated to the target user. All potential user types are included. This is to keep the end-user in mind throughout the development of the product and follow user-focused design.

User Profile Form
Application HomeKOP
Potential Users - Technological Users - Non-technological Users
Software, Interface and Related Experience HomeKOP is targeted towards the average consumer who does not have a lot of technological know-how. This is the consumer that purchases and connects a smart home device to their home network without making considerations for security. We seek to provide this user with a solution that would not only raise awareness, but also enable them to protect their home networks in a way that is simple. Our technological users would understand the impact of these issues and have the literacy to protect themselves. HomeKOP will be designed with the non-technological user in mind. We plan to keep our design simple enough for non-technological users to understand but intricate enough for technological users to appreciate.

Experience with Similar Applications
Our non-technological users have experience setting up smart home devices and adding them to their network. This is as simple as connecting a device to their Wi-Fi network. However, these users do not have much experience with taking security precautions such as changing the default password of a smart device.

Our technological users have experience with both setting up smart home devices and following security protocols. They also have experience with monitoring tools for home networks and smart home devices.

Task Experience
Step 1- Setup
When the Mozilla Web of Things Gateway with the HomeKOP risk score integration is implemented on a user network, the user will access a visual dashboard that helps them visualize the devices on their network and manage permissions. Setup also allows users to determine and set rules for devices.

Step 2 - Manual Scan
Once HomeKOP has been setup, the user will be able to perform a monitor their smart home network. This brings up a list of IoT devices that are currently on the network, performs security assessments and gives users a risk score for each of the devices based on the HomeKOP standards. HomeKOP then offers suggestions on any security protocols to implement.

Step 3 - Adjusting Settings
Once a user is aware of the vulnerabilities of a device, they have the option to turn off certain devices. For example, a user who does not wish to update the software on a device has the option to turn off notifications for potential updates. This prevents HomeKOP from flagging the device each time it scans the network. However, this does not alter the risk score of the device. We expect this feature to be most relevant to our technological users who understand the risks associated with such decisions.

Step 4 - Continuous Monitoring
After the initial setup, HomeKOP scans the network periodically depending on the user's settings. It proceeds to show risk scores and offers suggestions on how to secure devices. Additionally, once a new device is added to the network, HomeKOP performs a scan of the device and shows the user the results of the scan on the dashboard.

Frequency of Use
We expect the use-case of the device to follow the following format
- Scans network after setup
- Scans new devices as they are added to the network
- Monitors network in background to notify users of updates and vulnerabilities
- Scans network periodically depending on user's settings and notifies users of vulnerabilities

Key Interface Design Requirements that the Profile Suggests

- Interactive, user-friendly interface
- Training wizard for average consumer to understand relevance of tool
- Visual dashboard/monitoring tool, which includes color coded results for users to easily understand risk levels
- Mobile/Web-based application for easy management of smart home network

Table 1: User Profile

1.7 Use Case Diagram

Figure 1: Use Case Diagram is a visual representation that depicts how the users that will interact with the system as well as technologies used to develop the product.

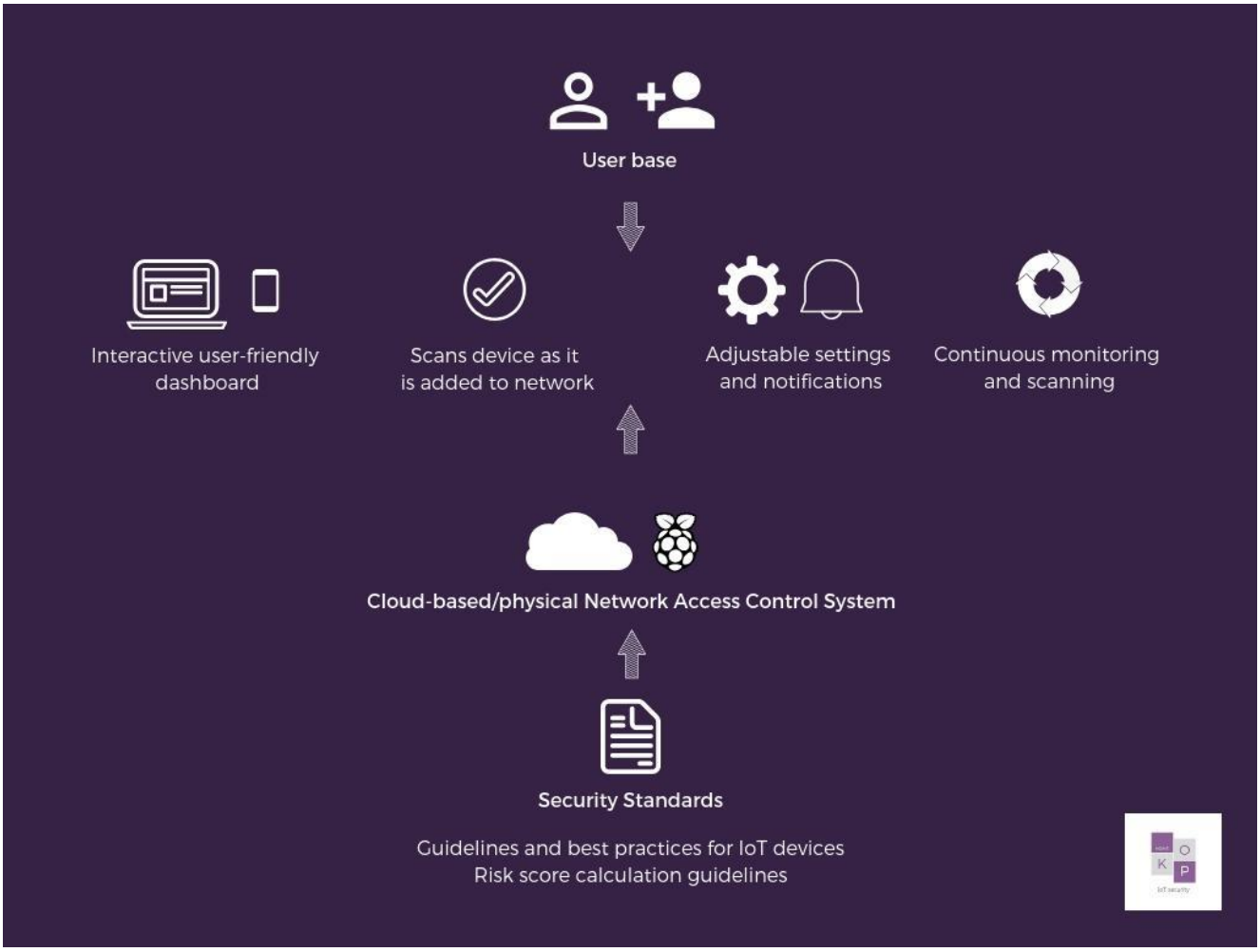

Figure 1: Use Case Diagram

2. Project Management

2.1 Budget

Table 2: Project Budget outlines the budget for this project. It is broken up into three categories - research, technical, and labor. For our research, we will be accessing peer-reviewed journals and articles through the University of Cincinnati Libraries students' free access. We will also conduct our survey using the paid version of Qualtrics (free to students through UC). We will be making use of our personally owned IoT devices, and we will host our standards in a publicly-accessible database. Lastly, we would assume wages of $20/hour per team member and a full-time work schedule for a duration of 4 months to estimate the labor costs. This labor cost will not be factored into the project costs because the project is being completed for free as part of the University of Cincinnati's Information Technology Senior Design Project/for the procurement of a Bachelor of Science degree in Information Technology.

Category	**Item**	**Description**	**Expected Cost**	**Total Cost**
Research	Peer-reviewed journals	Previously published research on IoT vulnerabilities available through UC libraries and other free journals	$0	$0
	Qualtrics Survey Tool	A paid online website for administering the survey, collecting results and analyzing data - free for UC students	$0	$0
	Survey Incentive	A gift card to motivate more users to respond to survey	$25	$25
Technical	Hardware	List of smart devices that	$0	TBD

		we would be connecting to the network		
	Software	AWS cloud storage for housing our standards in a publicly-accessible database (Free for the first year)	$0	TBD
	Platform	Mozilla Web of Things Gateway (open source)	$0	$0
Labor	Simulated Wage Costs*	The predicted wages that would be distributed if we were hired by our sponsor to work on the project. We will assume 40 hours of work/week for 4 months with a pay of $20/hour per team member	$28,800	TBD
Total Cost			$25	TBD
**simulated wages are not factored into product costs*				

Table 2: Project Budget

2.2 Objectives/Deliverables

Table 3: Objectives/Deliverables contain major deliverables and associated due dates for the completing of the project itself, as well as the dates for submission for the senior design class.

FALL OF 2018 MILESTONES			
Research	12/11/18	Team Contract	9/24/18
		Project Abstract Draft	10/15/18
		Fall Report	11/26/18
SPRING OF 2019 MILESTONES			
Development	3/11/19	Abstract	2/18/19
Testing	3/18/19	Tech Expo	4/9/19

Table 3: Objectives/Deliverables

2.3 Project Schedule

Table 4: WBS contains the work breakdown structure of the project with broken down milestones.

HomeKOP WBS			
START DATE	**END DATE**	**TASK DESCRIPTION**	**DURATION**
8/27/18	10/12/18	**1. Project Management**	46
8/27/18	9/3/18	1.1. Assignment 0 and Individual Blogs DUE	7
9/3/18	9/24/18	1.2 Assignment 1: Team Contract DUE	21
10/8/18	10/15/18	1.3 Assignment 2: Project Abstract for Tech Expo DUE	7
10/8/18	10/15/18	1.4 Assignment 3: Team Contract Resubmission DUE	7
10/15/18	10/22/18	1.5 Assignment 4: User Profile DUE	7
10/15/18	10/22/18	1.6 Assignment 5: Use Case Diagram DUE	7
10/22/18	11/5/18	1.7 Assignment 6: Draft Report DUE	14
11/5/18	11/26/18	1.8 Assignment 7: Fall Semester Report DUE	21
1/14/19	2/11/19	1.9 Spring Assigment 1: Testing Plan/Report DUE	28
2/11/19	2/18/19	1.10 Spring Assigment 2: Abstract DUE	7
2/18/19	3/4/19	1.11 Spring Assignment 3: Draft Tech Expo Poster DUE	14
3/4/19	3/18/19	1.12 Spring Assignment 4: Final Poster DUE	14
8/27/18	12/11/18	**2. Research**	106
8/27/18	10/1/18	2.1 Research Smart Home Networks	35
8/27/18	12/10/18	2.2 Research commonly used IoT devices and security measures using a survey	105
8/27/18	11/10/18	2.21 Develop Survey	75
11/10/18	11/20/18	2.22 Administer Survey	10
11/20/18	12/31/18	2.23 Analyze Results of Survey	41
8/27/18	10/8/18	2.3 Research known vulnerabilities and solutions	42
10/8/18	10/15/18	2.4 Set up simulated environment	7
10/15/18	10/22/18	2.5 Conduct vulnerability testing	7
10/22/18	11/12/18	2.6 Document findings	21
1/1/19	3/11/19	**3. Development**	69
1/1/19	1/21/19	3.1 Develop set of standards for secure IoT devices based on the risk score	20
1/21/19	2/4/19	3.2 Research existing technological solutions	14
2/4/19	2/18/19	3.3 Propose technological solution	14
1/1/19	2/18/19	3.4 Develop technological solution	48
2/18/19	3/18/19	**4. Testing**	28
2/18/19	3/4/19	4.1 Create test scenarios and test cases	14
3/4/19	3/18/19	4.3 Deploy to users and survey results of standards	14

Table 4: WBS

Figure 2: Gantt Chart contains the milestones with due dates mapped out against time in the form of a Gantt Chart.

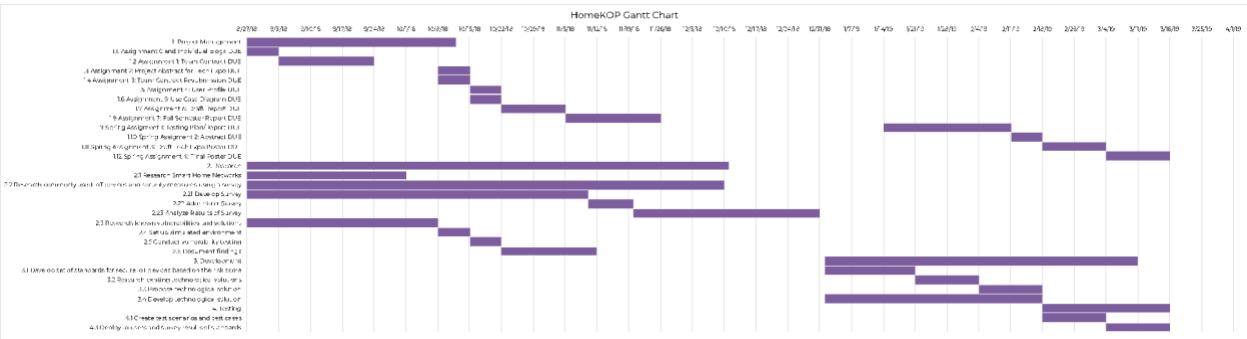

Figure 2: Gantt Chart

3. Technical Elements

3.1 Research Component

A key component of our project is researching common IoT vulnerabilities and the current solutions to them. Our research focused on understanding smart home networks, knowing the current devices consumers are purchasing and using, and understanding the security practices being exercised by said consumers. Below are summaries of our findings that contributed to our security standards and end product.

Smart Homes:

Smart homes, or home automation, is the idea and practice of using a centralized device or hub to control multiple aspects of your home. This is intended to make home operations easier and more efficient for users. Though this seems like a new concept, it has been around for over a decade. The popularity of IoT devices for personal uses has grown tremendously and is projected to hit over 20 billion devices by 2020 (Gartner, 2017). With the increase of connected homes, we face an increase in privacy, safety, and security issues.

The increase in risks is not the only cause for concern; it is accompanied by a gap in understanding how home networks work and the dangers associated with connecting home devices to the Internet. In 2016, a report found that more than 60% of users were concerned for

the security of their home devices (Rouse, 2018). That said, manufacturers still have yet to do anything to educate their customers on the security of their devices. It has now become a user's responsibility to protect themselves. Most users know that they need to secure their devices, but how? Currently there are no recommended products or standards for IoT devices, so users are left to hope that their network won't be targeted.

Known Vulnerabilities:

The problem with securing these devices is not just user error but also neglect on the part of the manufacturer. The devices they create have vulnerabilities that do not get patched, default passwords that do not get changed, and small processors that cannot run secure applications. It has been found that some devices display usernames and passwords as plaintext with no encryption and have tokens that don't expire, so they can be used multiple times by multiple people. All of these components create different opportunities for hackers to exploit the machines and network. Staying proactive as a user to combat these vulnerabilities is vital to protect yourself.

Best Practices:

The best way to do this is for users to update all passwords to be complex and unique as default passwords can easily be hacked and common passwords can also be guessed or cracked quickly. A study found that 5% of devices connected to the Internet have weak or common passwords (Pascu, 2018). Users also need to stay up to date with any software/firmware updates as this is the current way the manufacturers release patches for their devices. It is also important for users not to share any personal or device information with anyone, such as IP addresses and serial numbers. These steps are very simple to follow but make a huge difference on the security of home networks and connected devices. Unfortunately, a lot of users are unaware of this.

3.2 Productized Solution (Development)

Based on the research findings and key components that characterize IoT device security, we are putting together a Risk Score calculation system that can signify if a device is safe, unsafe or somewhere in between. In order to make this into a digestible product for regular users, we have added this onto Mozilla's Web of Things Gateway that can either sit in the cloud or on a Raspberry Pi. The risk score will be incorporated into the Gateway to show users the risk levels of their different devices and in turn govern the usage and security.

The risk score calculation will be based on current practices, user awareness and ongoing research throughout the sphere of IoT. To gauge the above stated measures, we have developed a survey to be administered through Qualtrics. We are hoping to survey anywhere between n=50 to n=100 people. This survey aims to collect a list of devices that users utilize as well as verify if they use any devices from the list we have compiled from our research.

4. Visuals

4.1 User Interface

Figures 3, 4, 5 and 6 below show the dashboard of the Mozilla Web of Things gateway we aim to incorporate the risk scores into as well as the progress of visualizing the risk score on the dashboards.

Figure 3: Dashboard depicts what the initial dashboard looks like before the incorporation of the risk score on the device icons. This dashboard allows users to turn devices on/off from a web-based application.

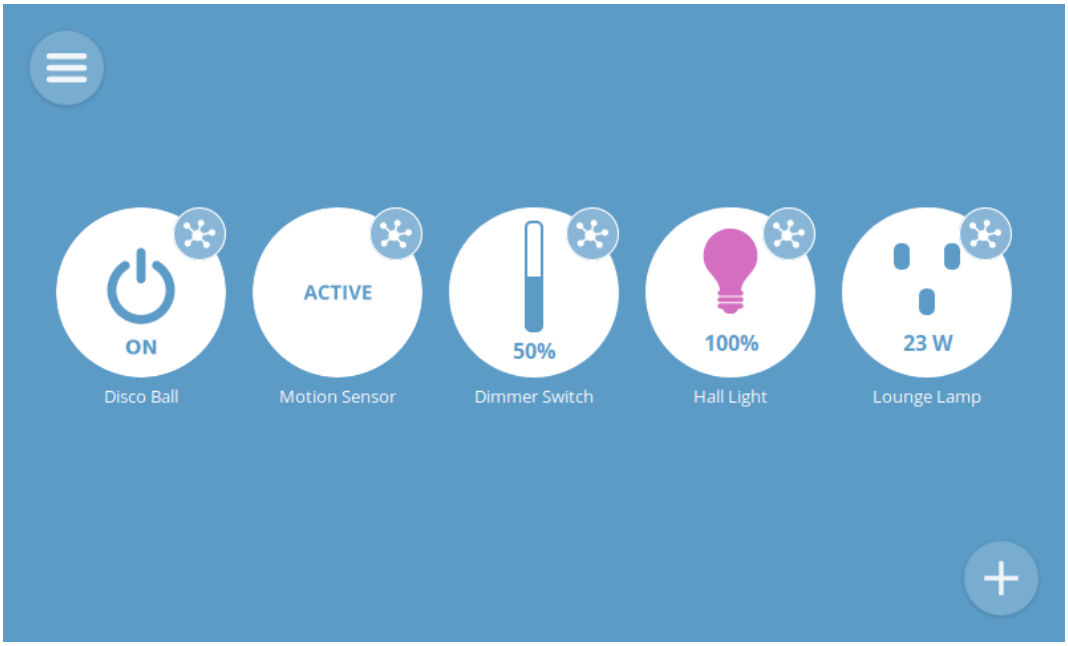

Figure 3: The landing page of a Mozilla Web of Things Gateway (Things Gateway)

Figure 4: Rules Screen depicts the process of setting up rules for each device using simple *if* and *while* conditional statement.

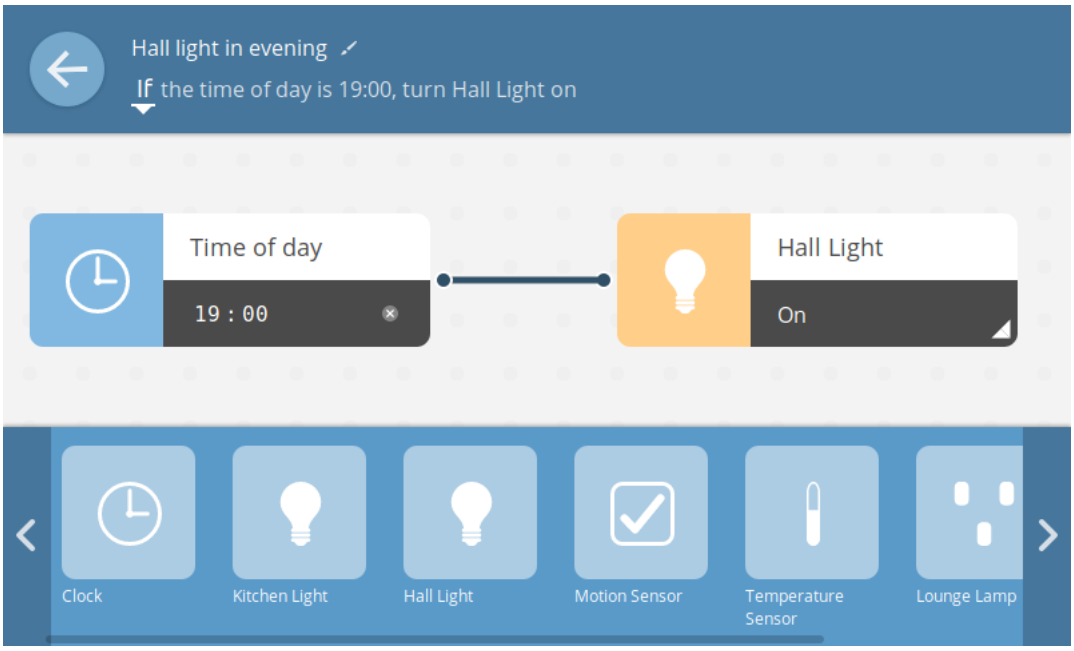

Figure 4: An example of setting up rules through the Mozilla Web of Things Gateway (Things Gateway)

Figure 5: Layout Screen depicts the layout of the home environment with the devices listed in respective rooms. This will allow users to understand where their devices are situated and help them lock things down in case of emergencies in certain areas of the home.

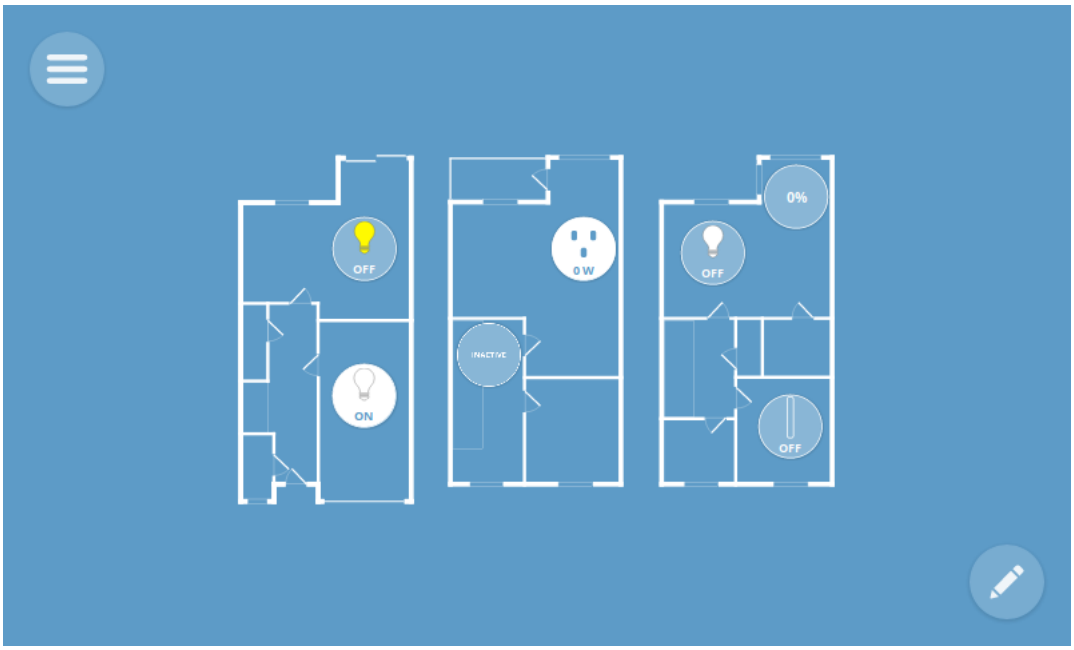

Figure 5: An example of a residence layout with devices depicted in a gateway (Things Gateway)

Figure 6: Risk Score Implementation depicts what the risk score will look like for a device on the network. The circle with the number is colorized to indicate risk level.

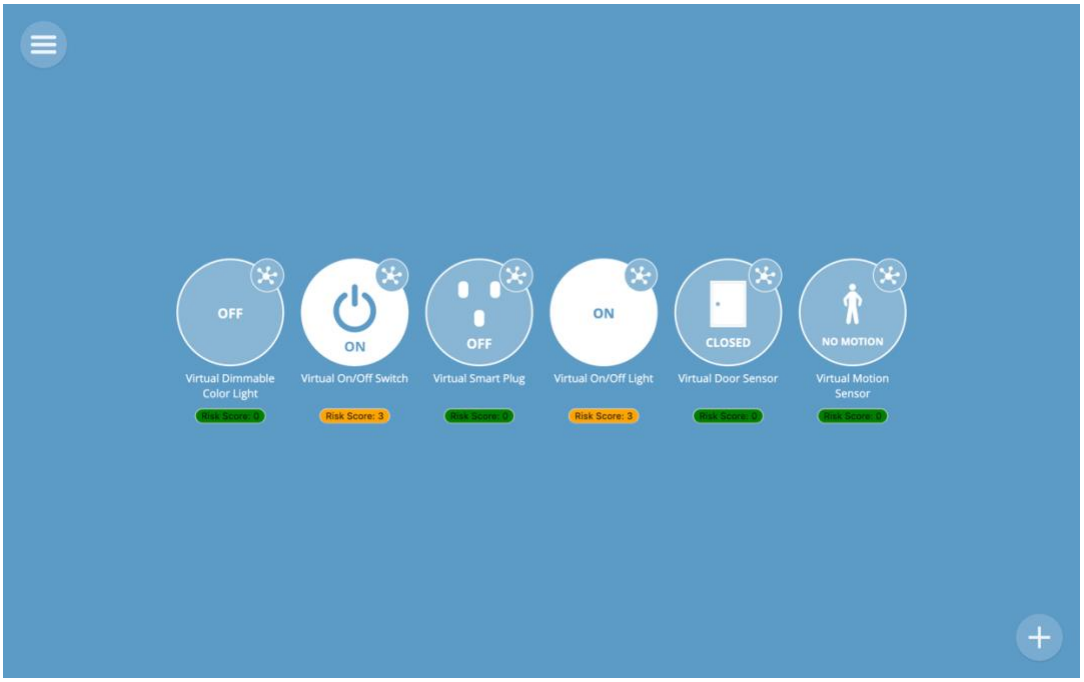

Figure 6: Depiction of the risk score below the devices listed in a WoT dashboard

5. Test Plan

5.1 Overview

This section will explain the testing methodology of the HomeKOP risk score and should be used as a guide. Once the risk score calculation is solidified, the dashboard and the risk score will undergo user acceptance testing to verify that users understand the liability of devices and what the risk score and guidelines indicate. The following individuals should use this section:

- Developers
- Project Managers
- Network Engineers
- Security Analysts
- End-users

5.2 Scope

The scope of testing the HomeKOP risk score will be limited to the web-application on Google Chrome browser. The test will be structured based on the requirements of the application.

5.3 Objective

The objective is to find any discrepancies that come up through development and implementation of the product and to expedite bug and issue fixes before proceeding with rolling out the product and publishing research findings. The objective is also to ensure that users understand how to use the application.

5.4 Test Cases

The test cases are determined based on the functionality of the final product. The test cases mainly focus on the usability of the product.

5.5 Entry and Exit Criteria

Entry Criteria:

- Environment set-up complete
- Devices added onto the interface
- Scan of device properties and risk score population complete

Exit Criteria:

- All tests are run
- Bugs and issues are documented and fixed

5.6 Logging Test and Reporting

In the event of a bug discovery, an issue will be created on the Github project to notify the developers of the application. The developers will discuss and execute a plan to fix the application and other members of the team will provide quality assurance by testing the bug fix.

5.7 System Testing

The HomeKOP application and risk score will be tested as a whole in one unit. Any usability issues detected will affect the overall use of the application and therefore need to be fixed for the application to be considered stable.

5.8 Testing Procedures

The following prerequisites are required to be completed for testing to take place:

- Document all test scenarios and use cases
- Document instructions for testing and reporting bugs
- Report bugs in the correct format

Tests to be performed:

- Stability test: This test will verify whether the HomeKOP application loads glitch free on a Google Chrome browser on the end-user's machine.
- Launch test: This test will verify whether the HomeKOP application loads all the devices as they are added to the interface and loads the risk score.
- User Interface Test: This test will focus on the usability of the HomeKOP application and any aesthetic issues that may arise.
- Functionality Test: This test will focus on whether all parts of the web-application are clickable and return some amount of feedback to the user.

5.9 Pass/Fail Conditions

The tests will be considered successful if all listed test scenarios pass. If they do not pass, test will fail and will need to be recorded in issue list.

5.10 Schedule of Team Member Testing

The schedule of team member testing is listed below:

Team Member	Timeline to be Completed	Frequency
Developers	2/28/2019 to 3/28/2019	weekly
Security Analysts	2/28/2019 to 3/28/2019	weekly
Network Engineers	2/28/2019 to 3/28/2019	weekly

Table 5: Schedule of Team Member Testing

5.11 Schedule of Round Table Testing

The schedule of round table testing is listed below:

Round Table	Timeline to be Completed	Frequency
Tech savvy end-users	3/28/2019 to 4/4/2019	weekly
Non tech savvy end-users	3/28/2019 to 4/4/2019	weekly

Table 6: Schedule of Round Table Testing

5.12 Risks

Factors impacting the feasibility of the testing process:

- Availability of the application server
- Availability of end users
- Delay in bug fixes

5.13 Issues Encountered and Solutions

Through the development of the HomeKOP solution, there was one continuous issue affecting the availability of the application – lack of space on the server. The Mozilla Web of Things Gateway was installed on a Macbook Pro with under 20GB of space left. The server kept

crashing because of the volume of requests being made. We increased the amount of free space available on the server to avoid crashes.

6. Tech Expo

On April 9, 2019 the annual Tech Expo was held from 9AM to 1PM. We were able to display our application and Qualtrics survey results throughout the Expo. Users were able to view and toggle the risk score on the Gateway without any issues. Users were also able to use the web-based risk scoring system on the HomeKOP website. Below is an image of the poster displayed at our booth at Tech Expo.

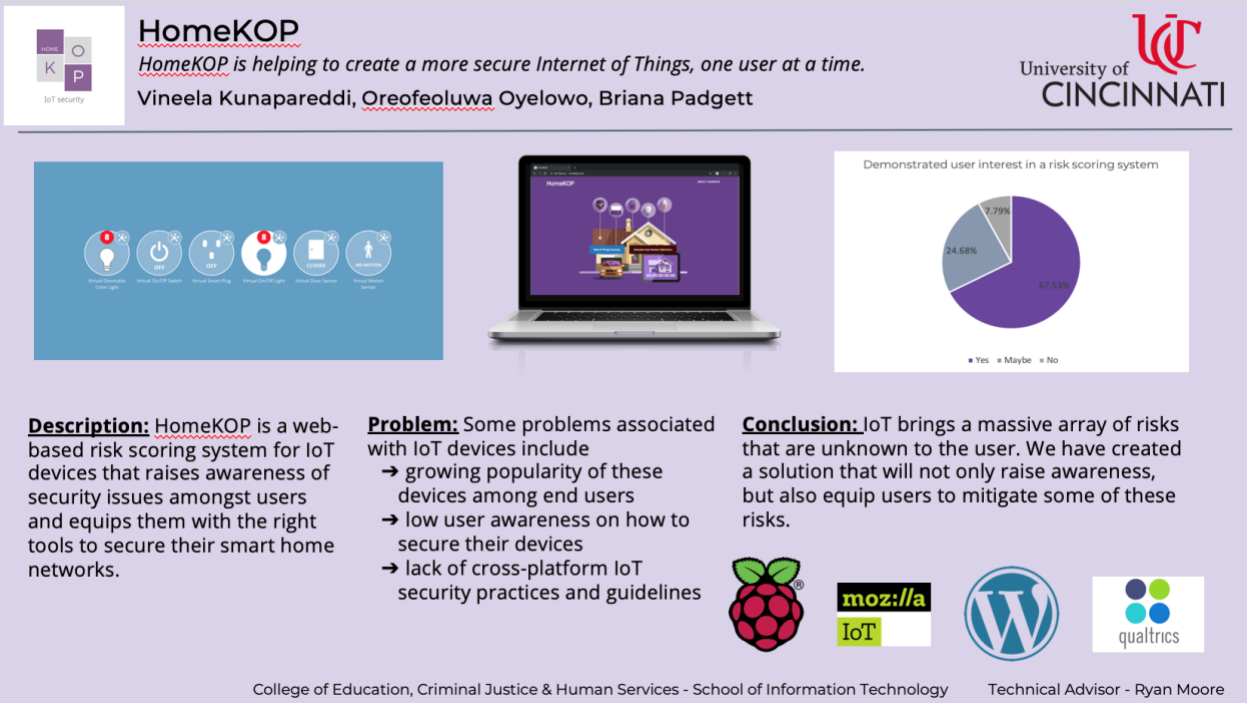

Table 7: Poster

7. Future Recommendations

In terms of further development of the HomeKOP application, some changes can be made before carrying out a usability study. A tooltip may be added to the risk score button on the Mozilla Web of Things Gateway to point exactly which properties are causing the risk to rise. One of the

most major challenges with the project was using an open source gateway built in pure TypeScript without a frontend framework. Hiring a developer with more experience in TypeScript would be helpful with the frontend changes that need to be made. Additionally, obtaining funding for IoT devices in place of using the Virtual Things adapter to assess more properties could benefit with taking the application to market. Once these changes and further work is completed, the application can be modified to work on mobile devices.

8. Conclusion

8.1 Fall Semester 2018

Our goal this semester was to conduct research to get a better understanding of the problem with securing IoT devices as well as the implications of this issue. This is being done through the administration of a survey amongst IoT device users. Based on our research findings and meetings with IT professionals in the industry we have established a good understanding and grasp on the extent of the issue and have begun focusing more on our productized solution. Our solution entails assigning a risk score to devices to signify the level of security of the device. The risk score will be calculated on protocols followed at many different layers of the device. To make this risk score easily available to users, we are attempting to add it on as a layer to Mozilla's Web of Things Gateway.

For the duration of the semester we will be finishing up our research by creating and distributing a survey to the UC community, conducting penetration tests on common devices used as found in the survey, developing our standards and risk score calculation systems, and working towards our reach goals. These activities will continue into the spring 2019 semester.

8.2 Spring Semester 2019

We completed compiling our survey results and finalized the requirements of our productized solution. We surveyed a total of 98 users using the Qualtrics survey tools. Based on the survey results, we gauged interest in the product and collected a list of most popularly used IoT smart home devices. Based on availability and affordability, we conducted additional research through literature reviews and penetration testing to assess device vulnerabilities.

We found that in the cyber-physical risk posed by IoT devices, the more concerning threat is posed by physical vulnerabilities. To address the physical and cyber risks, we developed a two-part solution. One addresses the physical vulnerabilities by informing the user of the risk level based on physical properties of the devices. This is productized through the open source Mozilla Web of Things Gateway. We modified the front end of the application to display a risk score that is dynamically calculated based on physical properties of the device such as state, temperature, use of usernames and passwords. The second part of the solution is to educate users on vulnerabilities based on their existing practices. For this, we created a website that incorporates a web-based risk score calculator that provides users with a risk score and a general set of guidelines on how to better secure their smart homes.

There is hope for a future usability study to study the viability of the product and to collect additional requirements for a more robust application based on the prototype.

References

Fruhlinger, Josh. "The Mirai Botnet Explained: How IoT Devices Almost Brought down the Internet." CSO Online, CSO, 9 Mar. 2018, www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html.

"Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent From 2016." *Gartner IT Glossary*, Gartner, Inc., www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016.

Lueth, K. L. (2018, August 8). State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. Retrieved from https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

Moffitt, Tyler. "Source Code for Mirai IoT Malware Was Recently Released." *Webroot*, 10 Oct. 2016, www.webroot.com/blog/2016/10/10/source-code-mirai-iot-malware-released/.

Pascu, L. (2018). The IoT Threat Landscape and Top Smart Home Vulnerabilities in 2018 [Bitdefender Whitepaper].

Rouse, Margaret. "What Is Smart Home or Building (Home Automation or Domotics)? - Definition from WhatIs.com." *IoT Agenda*, internetofthingsagenda.techtarget.com/definition/smart-home-or-building.

Things Gateway by Mozilla. (n.d.). Retrieved from https://iot.mozilla.org/gateway/

Woolf, Nicky. "DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say." The Guardian, Guardian News and Media, 26 Oct. 2016, www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

Appendix

Testing Reports

Stability Test - This test will verify whether the HomeKOP application loads glitch free on a Google Chrome browser on the end-user's machine. Below is a list of initial and final test results.

Tester	Date	Item#	Expected	Actual	Pass/Fail	Bug
Tech savvy end-user	2/28/2019	1.1 Google Chrome Stability	Application runs on port 4443 without interruptions	Application ran, but pulls a blank page	Fail	Frontend components not loading
Non tech savvy end-user	2/28/2019	1.1 Google Chrome Stability	Application runs on port 4443 without interruptions	Application ran, but pulls a blank page	Fail	Frontend components not loading
Non tech savvy end-user	2/28/2019	1.1 Google Chrome Stability	Application runs on port 4443 without interruptions	Application ran, but pulls a blank page	Fail	Frontend components not loading

Table 8: Stability Test #1

Tester	Date	Item#	Expected	Actual	Pass/Fail	Bug
Tech savvy end-user	4/1/2019	1.1 Google Chrome Stability	Application runs on port 4443 without interruptions	Application runs and loads all components	Pass	
Non tech savvy end-user	4/1/2019	1.1 Google Chrome Stability	Application runs on port 4443 without interruptions	Application runs and loads all components	Pass	
Non tech savvy end-user	4/1/2019	1.1 Google Chrome Stability	Application runs on port 4443 without interruptions	Application runs and loads all components	Pass	

Table 9: Stability Test #2

Launch test - This test will verify whether the HomeKOP application loads all the devices as they are added to the interface and loads the risk score. Below is a list of all first and final tests.

Tester	Date	Item#	Expected	Actual	Pass/Fail	Bug
Tech savvy end-user	2/28/2019	2.1 Loading devices on screen	All six devices load correctly	All six devices loaded	Pass	
Non tech savvy end-user	2/28/2019	2.1 Loading devices on screen	All six devices load correctly	All six devices loaded	Pass	
Non tech savvy end-user	2/28/2019	2.1 Loading devices on screen	All six devices load correctly	All six devices loaded	Pass	

Table 10: Launch Test #1

Tester	Date	Item#	Expected	Actual	Pass/Fail	Bug
Tech savvy end-user	4/1/2019	2.1 Loading devices on screen	All six devices load correctly	All six devices loaded	Pass	
Non tech savvy end-user	4/1/2019	2.1 Loading devices on screen	All six devices load correctly	All six devices loaded	Pass	
Non tech savvy end-user	4/1/2019	2.1 Loading devices on screen	All six devices load correctly	All six devices loaded	Pass	

Table 11: Launch Test #2

User Interface Test - This test will focus on the usability of the HomeKOP application and any aesthetic issues that may arise. Below is a list of all usability tests of initial prototype.

Tester	Date	Item#	Expected	Actual	Pass/Fail	Bug

Tech savvy end-user	2/28/2019	3.1 Usability Feedback	Feedback on interface design	The risk is looks out of place.	N/A	Change position of the risk icon to below the device.
Non tech savvy end-user	2/28/2019	3.1 Usability Feedback	Feedback on interface design	Unsure what the number over the device represents.	N/A	Add a label "Risk score" before risk score.
Non tech savvy end-user	2/28/2019	3.1 Usability Feedback	Feedback on interface design	Would like to see more information on how to fix the risk level.	N/A	Add tooltip over risk score button to make the information more apparent.

Table 12: Usability Test

Functionality Test - This test will focus on whether all parts of the web-application are clickable and return some amount of feedback to the user. Below is a list of all first and final tests.

Tester	Date	Item#	Expected	Actual	Pass/Fail	Bug
Tech savvy end-user	2/28/2019	4.1 Device On/Off	Device turns on and icon is updated	Device turned on	Pass	
Non tech savvy end-user	2/28/2019	4.1 Device On/Off	Device turns on and icon is updated	Device failed to turn on	Fail	The Virtual Things Adapter expired, need to reinitiate
Non tech savvy end-user	2/28/2019	4.1 Device On/Off	Device turns on and icon is updated	Device turned on	Pass	
Tech savvy end-user	2/28/2019	4.2 Dynamic Risk Score	Risk score is calculated and updated	Risk score is calculated and updated	Pass	

Non tech savvy end-user	2/28/2019	4.2 Dynamic Risk Score	Risk score is calculated and updated	Risk score is calculated and updated	Pass	
Non tech savvy end-user	2/28/2019	4.2 Dynamic Risk Score	Risk score is calculated and updated	Risk score is calculated and updated	Pass	

Table 13: Functionality Test #1

Tester	Date	Item#	Expected	Actual	Pass/Fail	Bug
Tech savvy end-user	4/1/2019	4.1 Device On/Off	Device turns on and icon is updated	Device turned on	Pass	
Non tech savvy end-user	4/1/2019	4.1 Device On/Off	Device turns on and icon is updated	Device turned on	Pass	
Non tech savvy end-user	4/1/2019	4.1 Device On/Off	Device turns on and icon is updated	Device turned on	Pass	
Tech savvy end-user	4/1/2019	4.2 Dynamic Risk Score	Risk score is calculated and updated	Risk score is calculated and updated	Pass	
Non tech savvy end-user	4/1/2019	4.2 Dynamic Risk Score	Risk score is calculated and updated	Risk score is calculated and updated	Pass	
Non tech savvy end-user	4/1/2019	4.2 Dynamic Risk Score	Risk score is calculated and updated	Risk score is calculated and updated	Pass	

Table 14: Functionality Test #2