Raspberry Pi 3 Home Network Monitoring Tool

Garen Kutukian*
California State Polytechnic University, Pomona
3801 W Temple Ave
Pomona, CA 91768
gkutukian@cpp.com

Mohammad Husain, PhD†
California State Polytechnic University, Pomona
3801 W Temple Ave
Pomona, CA 91768
mihusain@cpp.edu

ABSTRACT

A network monitoring device can be a very beneficial add-on to one's home network. As more devices are becoming smart devices and the world of Internet-of-Things are taking over home networks, it is important for owners to be notified of new devices entering their network and to have the ability to conveniently revoke any unwanted device without affecting the entire network. Unwanted devices that have entered a network without consent can cause a lot of damage. The aim for this research and project is to understand the importance of network monitoring tools and to propose a cost effective network monitoring tool that takes into account a network made of smart devices. By looking at the different network monitoring tools from software-based and hardware-based approaches, a concept Raspberry Pi 3 Home Network Monitoring Tool is proposed and implemented, which provides a network owner the ability to detect new devices and revoke unwanted ones.

1. INTRODUCTION

1.1 Motivation

As simple home networks are slowly evolving into complex smart networks, people seem to be less aware of what is connected to their home network. A few years ago, a simple home network would include a few devices, such as smart phones, computers, laptops, or printers. In addition to these devices, a simple home network now consists of thermostats, kitchen appliances, laundry appliances, televisions, surveillance devices, and even vacuums. All of these devices are now being made into smart devices, allowing a person to connect to them through their home network. These smart devices are also identified as Internet-of-Things (IoT). While some of these devices make our daily lives easier, they also make our home network insecure and prone to attacks. With so many devices connected to a home network, cyber-criminals try to exploit the vulnerabilities of these devices. Over the years, it has become even harder for a person to keep track of the many devices connected to their home network. There are different network tools and scanners that a person can use to try to maintain and keep track of the devices on their home network, but they are either hard to use or lack important features.

1.2 Problem Description

With so many smart devices connected to a home network, owners can be overwhelmed if they would like to know information or keep track of the different devices that are connected. Individuals can download different network monitoring tools that can scan and show the different devices on their network. If they would like to revoke a device from their network that has connected without their knowledge, they will need to login to the router's configuration utility page and block the device directly from there. There is no easy way for the home owner to be able to revoke or remove any unwanted devices from accessing the network without logging into the router's configuration utility page. This can become an annoyance to users and may even be a security issue when users have to constantly log into the router's interface. Users can also face challenges in receiving notifications for new devices that have joined the network or trying to look at current or previous devices that are or have been on the network. Network monitoring tools are usually installed directly on a computer, with the computer needing to be on all the time for the tool to work. Without spending a lot of money on professional network monitoring tools, expensive firewalls, or expensive smart routers, home network owners do not have a quick and easy method to discover any unwanted devices on their network and conveniently block those unwanted devices.

2. BACKGROUND AND HISTORY

2.1 Internet-of-Things

With the evolution of advanced wireless technologies, people are exchanging simple home appliances with smart devices. A smart device is not actually a new concept, as the idea has been seen around the industry as early as 1982 [8]. When a simple device becomes a smart device, it gains the ability to collect and exchange data easily with other

*Master's Student.
†Associate Professor.

ICNS '16 Nakagyo-Ku, Kyoto-shi, Kyoto

smart devices. A single smart device that is able to connect to the Internet with a unique IP address is considered an Internet-of-Thing device. Multiple smart devices working together, with each one having a unique IP address, are categorized as a network of Internet-of-Things. Analysts from Gartner, Inc. forecast that there will be about 20.8 billion Internet-of-Thing devices by 2020 [8]. As people start buying more and more Internet-of-Thing devices, they start to lose count of how many devices are connected to what was previously a simple home network.

As each Internet-of-Thing device is introduced to a person's home network, the security risk gets bigger and the home network gets weaker. Hackers and criminals try to exploit the weaknesses of consumer devices that have not been made with security in mind. Consumers of these devices do not understand the security risks that they take by purchasing insecure products. Even though the product itself might be working properly and not show any signs of malicious tampering, criminals can still be lurking around home networks. Hackers and cyber-criminals who do get a hold of a device on a person's network usually make the device a malicious spamming machine without the consumer's knowledge. Hackers and cyber-criminals may start sniffing and collecting network activity using the exploited device. They may join the exploited device into a distributed denial-of-service attack, or they may even use the exploited device to damage or exploit other connected devices on the home network. As more and more devices are connected to a home network, network owners can and should keep track of the devices using network monitoring tools. For any unwanted devices on the home network, network owners should be able to easily prohibit the device's access.

2.2 Network Monitoring Tool

There are many network monitoring tools out there for all levels of users and operating systems. Some network monitoring tools that contain many features are designed with network administrators in mind, while other simple tools that contain minimal features are designed for non-tech-savvy users. Most of these monitoring tools need to be constantly monitored themselves or otherwise need constant user interaction. Monitoring tools designed with home users in mind are usually meant to be installed on a computer, such that the network monitoring tool becomes useless if the computer is turned off. There are also smart routers and hardware firewalls that have network monitoring capabilities, but they are usually harder to set up and very expensive. For a non-tech-savvy person, setting up home network firewalls may be a nightmare. Network monitoring tools aimed for non-tech-savvy people need to be designed to be easy to set up and easy to use, with minimal monitoring capabilities. Network monitoring tools should be designed not only to be able to function independent of a computer, but also to work for mini-computers such as ODROID [12], HummingBoard [16], CubieBoard [3], Arduino [2], or Raspberry Pi [13].

2.3 Raspberry Pi

The Raspberry Pi has been around since 2006, and in 2016, the Raspberry Pi Foundation revealed that they had sold over 8 million Raspberry Pi devices [13]. The Raspberry Pi is an affordable mini single-board computer that hobbyists, enthusiasts, and curious people wanting to learn how to program have come to love. The Raspberry Pi is a perfect ARM-based mini-computer for a home network monitoring system. The ability to install different operating systems allows one to install an ARM-based Kali Linux. Kali Linux is a Debian-derived Linux distribution containing over 600 network penetrating tools [15]. Using some of the tools available on Kali Linux will allow a programmer to put together a useful network monitoring tool. The Raspberry Pi consumes very little power in comparison to a traditional computer, so one will not need to worry about turning the Raspberry Pi off to save power. Some models of the Raspberry Pi come with a built-in 10/100 wired Ethernet, which can be easily configured when being used for a home network monitoring tool. The Raspberry Pi can be designed to be a powerful smart firewall, but it may be confusing for a non-tech-savvy user. The design of the network monitoring tool on a Raspberry Pi should be focused on simplicity and ease of use.

2.4 Dojo-Labs - Dojo

Dojo is a smart hardware firewall designed for home networks. Dojo is designed to detect and prevent threats on the home network. Dojo is also designed to be a home network monitor, notifying users of what is going on in their home network. Dojo has three parts: Dojo (the device), Dojo Cloud (the intelligence), and Dojo App. Dojo is a hybrid form of a smart hardware firewall and a home network monitor. With the ability to act as a firewall, Dojo is able to analyze data easily. It is able to apply machine-learning algorithms to the data going in and out of the network to inform the user if it detects any malicious activity. Being in the middle allows Dojo to block any network activity that it perceives to be a privacy risk. The activity information that is sent back to Dojo-Labs is metadata of the traffic going in and out of the network and does not contain private information [5]. Dojo notifies a user of the activity on the home network, which is the network monitoring portion of the device. Dojo allows the user to be able to select which devices will get access to their home network, to the internet, or to other connected devices [5]. Dojo also allows the user to create temporary devices and treat those devices differently. Setting up Dojo typically takes a few minutes with guided installation provided with the software [5]. No additional software is needed to operate Dojo.

2.5 SoftPerfect Network Scanner

SoftPerfect Network Scanner is a free multi-threaded IPv4/IPv6 scanner [17]. It is designed for both system administrators and general users. SoftPerfect Network Scanner pings the network for devices. It scans the network for TCP/UDP ports and discovers shared folders, including system folders and hidden folders [17]. SoftPerfect Network Scanner utilizes network protocols and gets information through WMI, SNMP, HTTP, and NetBios. It can also retrieve host names and auto-detect the local and external IP address range [17]. SoftPerfect Network Scanner has a lot of features. A non-tech-savvy person will still be able to use most of the features that it offers without getting confused. One useful feature of SoftPerfect Network Scanner is a ping sweep of all devices on the home

network, which is a feature that all network scanner tools should have. SoftPerfect Network Scanner supports both IPv4 and IPv6. A unique feature of SoftPerfect Network Scanner is that it has a MAC-address detection of devices across different routers. It will detect both internal and external IP addresses on a device. SoftPerfect Network Scanner will allow a user to mount and explore devices that are shared. It also shows detailed information about users that are logged on to those devices.

2.6 F-Secure Sense

Sense is a cyber defense solution for smart homes that combines hardware and software in a home network [6]. It is an advanced and secure high-speed router. Sense creates a secure home network with its ability to monitor all of the traffic going in and out of a home network. With the Sense app, users can monitor the security and privacy status of their home network and devices. Sense utilizes cloud computing by analyzing the data on the cloud and using machine-learning algorithms to learn the reputation and behavior of the devices [6]. A device's traffic is sensed instead of scanned [6]. Sense is a hardware router that sits in between the modem and the connected devices in a home network [6]. It supports both cabled and Wi-Fi connections. Sense also has the user install a Sense anti-virus/security application on devices for extra protection. "With the lightweight Sense app installed on [the] devices, managing and maintaining . . . device security is made much easier. Sense protects all of [a user's] devices in [a] present home network, as well as any new devices [the user] may add in the future [6]." Sense protects both inbound and outbound traffic, acting as a security gateway [6]. Using cloud computing and machine-learning algorithms, Sense ensures that the latest protection is always available on the home network.

2.7 Cujo

Cujo is a smart hardware firewall that keeps a home network safe from cyber threats [4]. Cujo allows the home network to be secure and private too. Being in the middle of the router and modem allows Cujo to be able to constantly analyze all the network traffic coming in and out of the home network. Cujo can easily set any specified home network security rules because it relays traffic. Cujo can also play a form of an anti-virus being able to recognize large sets of cyber threats and block them. "CUJO analyzes your local network traffic data locally and in real time. It then sends statistics on that data to the cloud for further analysis. For your privacy as well as performance reasons, we don't send the contents of those packets to the cloud. If a threat or suspicious activity is detected, CUJO will tell the cloud what it has blocked so you can receive a notification on your mobile app to confirm it [4]."

3. STRUCTURE OF THE SYSTEM

All elements of a network monitoring tool were taken into consideration during the research. Different platforms, operating systems, function and usability, and U/I were looked at. Different types of systems were considered in the research as well. The cost of the tool was also taken into consideration. After all the research was completed and different tools were looked into, formation of the thesis and system began. It was decided that emphasis on the user's overall usability and easiness of the device was going to be heavily taken into consideration. Four goals were conceived during the formation of the thesis and the system: the device, the U/I, the denial, and the usability and easiness.

3.1 First Goal: The Device

During the research of different network monitoring tools and systems, it was noticed that the actual device itself was often not taken into consideration. The existing network monitoring tools were mostly designed to be installed on the user's computer and were rarely considered to be a separate hardware addition to the user's existing network. Taking into consideration that a network monitoring tool is most useful when it is monitoring throughout the whole day, the Raspberry Pi home network monitoring tool is designed to be a separate hardware addition to the network. We also took into consideration the amount of time the user would be dealing and interacting with the actual device itself by making sure to emphasize the overall usability and easiness of the user's experience.

3.2 Second Goal: The User Interface

Looking through the different types of network monitoring tools, it was seen that the U/I's look and feel were always taken into consideration and that a great deal of time was put into them. Some network monitoring tools had a lot of different buttons and tabs and some were simple. Some also included information that a non-tech-savvy user would have trouble understanding. It was observed that the developers presumed that the user who was going to be using the network monitoring tool was also the same person who had installed and configured the network monitoring tool, so a person without a technical background would have a lot of trouble using the device to the fullest. In the System Architecture and System Evaluation sections, more information will be given about the U/I of the Raspberry Pi home network monitoring tool and how a non-technical user can easily use the monitoring tool without having trouble.

3.3 Third Goal: The Denial

During the research, it was seen that when the network monitoring tool was not a firewall or a smart router, the user would not be able to deny access to an unwanted device from the network monitoring tool itself. Network owners would be able to see a device's information, but they would need to login to the router's configuration utility page in order to deny access to that device. Also, most network monitoring tools do not have the ability to detect spoofed MAC devices or warn for possible spoofed MAC devices. In the System Architecture and System Evaluation sections, more information will be given about how the denial works, what tools were used to be able to deny, and what possible denial techniques were considered and taken into measures.

3.4 Fourth Goal: The Usability and Easiness

When researching the different types of network monitoring tools on different platforms and with each one having different goals in mind, usability and easiness for the overall system was seen to be observed. In the device area, we looked to see if the actual device was easy to use and install and if any technical background was needed

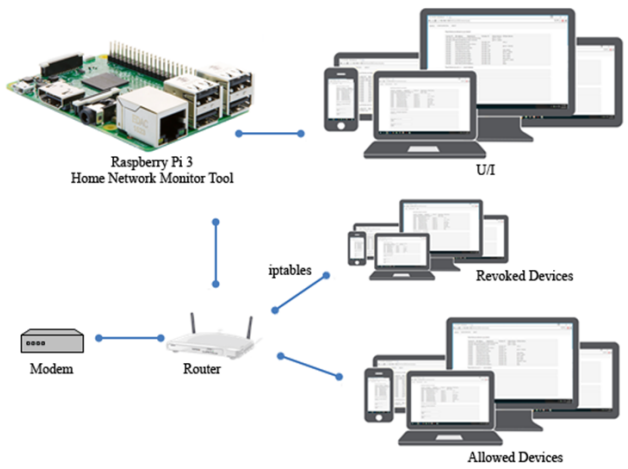

Figure 1: Structure and architecture of the Raspberry Pi 3 Home Network Monitoring Tool

once the device was configured. For the U/I, we looked to see if it was a smooth experience and if a non-technical user would be able to get around the interface. For the denial portion, we looked to see if the monitoring tool would easily allow the user to block an unwanted device. We also looked to see if the way the revoking was being implemented would have an effect on the allowed users. In the System Architecture and System Evaluation sections, more information will be given about the usability and easiness for each part.

Figure 1 represents the structure and architecture of the Raspberry Pi 3 Home Network Monitoring Tool. The Raspberry Pi 3 is connected to the router via a wired or wireless connection. The homeowner can access the Raspberry Pi 3 Home Network Monitoring Tool with any device on the network. If the home network owner would like to revoke a device, a rule would be added to iptable by the Raspberry Pi 3 Home Network Monitoring Tool connecting to the router via SSH. All allowed devices on the network will also be connected to the home router.

4. SYSTEM ARCHITECTURE

The overall usability and ease of use for non-tech-savvy users is heavily stressed for each part of the Raspberry Pi Home Network Monitoring Tool.

4.1 The Device

The Hardware Used.

The network monitoring tool was configured on a Raspberry Pi 3. There are many varieties of single board computers out in the market now but the Raspberry Pi was selected because of the large community support it has. The Raspberry Pi also allows for configuration of various operating systems, so it was deemed the ideal candidate. After researching the different operating systems that can be installed on the Raspberry Pi, Kali Linux was selected.

The Operating System Used.

Kali Linux was selected because of the vast tool set it provides for a network monitoring tool. Being open source, it also has a huge community support system, which is always useful when questions arise and answers are needed. Raspbian [14], Raspberry Pi's official operating system was also considered to be used as the operating system. After testing out Raspbian and installing different tools to see how they worked, we realized that some tools were either not compatible with Raspbian or were compiled differently and did not provide all the features. Because Kali Linux for the Raspberry Pi is compiled based on ARM architecture, an image with the network monitoring tool configured can be easily transported to and configured on other ARM-based systems. Kali Linux also contains over 600 network penetrating tools [15].

The Different Tools Used.

The tool set that Kali Linux provides is rich with network-oriented scripts and applications for penetrating and exploiting weaknesses. With each tool focused for a specific purpose, we had to test different tools to see which one would be best suited to efficiently be integrated in the network monitoring tool. All the tools used for the Raspberry Pi home network monitoring tool are open source.

For the detection portion, NMAP [10] is used. NMAP is a security network scanner that scans the entire network and provides useful information for each system. NMAP can accept different forms of commands and allows the user to select the type of scan to perform, from simple to fully informative. After analyzing different commands and comparing the scans on different routers, we decided that it would best for the scan to not be too simple and not be fully informative due to the restraints from different routers. The length of the scan was also taken into consideration. The different information provided by NMAP that are being used are: IP address, MAC address, and network device manufacturer.

For the denial portion, a few different tools and methods were taken into consideration. In the mini denial-of-service attack, Nping [9] was taken into consideration to be used. Nping is an open source tool that allows customization of network packets to be generated. In the implementation of the denial-of-service attack, if the Raspberry Pi was generating too many packets during a mini denial-of-service, the system would crash. A denial-of-service attack is not the main method for denying a user from the system in the Raspberry Pi home network monitoring tool. For the denial portion, iptable configuration is implemented. Iptable is an open source application that allows the configuration of the Linux kernel firewall table. When network owners decide to revoke an unwanted device from their network, they will send the MAC address to a file. A program will be triggered to use SSH and SCP to transfer that file over to the router. The router will need to be configured for SSH connection to successfully implement an iptable revoke method. On the router section, a small script is written for

the router and will need to be running in order to work. The script will look at a certain file that has the MAC address of the revoked user, which will then be inserted into the iptable. If network owners are not able to configure their router to connect with SSH, they will still be notified that a device who is on the revoked list is back on their network, at which point they will need to login to the router's configuration utility page and revoke the device from there.

The back-end of the network monitoring tool uses several different programming languages: Bourne Shell, Perl, and PHP. The main portion of the network monitoring tool is written in Bourne Shell. Perl is used for the back-end user interface. The back-end user interface gives network owners ability to allow devices, remove devices from the allowed list, revoke devices, and remove devices from the revoked device list. PHP allows the front-end user interface to interact with the back-end. PHP also triggers a few Bourne Shell scripts.

The notifications are triggered via email. SSMTP Server and mailutils are used for the email configuration. The different scripts will trigger the appropriate emails that are sent to the network owner as notifications.

The front-end of the network monitoring tool is written with HTML, Bootstrap, and JavaScript. The front-end communicates with the back-end via PHP. In order for users to be able to see the network monitoring tool via any web browser on their network, Apache2 [1] is configured. Apache2 is a web server. Also, in order for only the network owner to be able to use the tool, htpasswd is configured, requiring a user name and password. Htpasswd is an Apache2 utility that allows for user name and password authentication.

It is important to be able to utilize all the open source tools available for the different Linux operating system distributions.

4.2 Network Monitoring Tool

Network Monitoring Tool.

The main tool used for the Raspberry Pi home network monitoring tool is NMAP. With NMAP, we get the current IP address, the MAC address, and the network device's manufacturer. The user can choose and configure the scan time. By default, it scans every one minute. Once the scan finishes, it creates a temporary file with all the information for each device.

The temporary file is then parsed and separated into the following categories: existing allowed online devices, existing allowed offline devices, missing old devices, missing new devices, revoked devices, and spoofed devices. It then appends the existing allowed online devices with the existing allowed offline devices to create one file for allowed devices. Devices logging on to the network for the first time will be put on the missing new devices file and an email will be sent to the network owner to provide notification that a new device has logged on to the network. If an existing new device is still online and there are no new devices, an email will not be sent. This is to prevent spamming the network owner's email with notifications. If network owners are logged on to the Raspberry Pi home network monitoring tool through a web browser, they will only be able to either allow a new device or revoke a new device. They will be allowed to view all the lists but will not be able to edit any of them. If owners would like to edit and revoke an existing allowed device or remove a revoked device from the revoked list, they will need to use the back-end Raspberry Pi home network monitoring tool utility. Depending on how owners will be able to deny an unwanted device, network owners will be notified every one minute of an unwanted device that is on the revoked list still connected to their network. For spoofed devices, the Raspberry Pi home network monitoring tool checks to see if an existing online device appears twice on a list with a different IP address. It checks the MAC addresses of all the devices and if there are two of the same MAC addresses, that means a device is being spoofed.

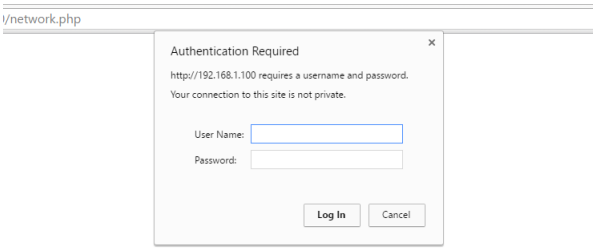

Figure 2: Login Page for Raspberry Pi Home Network Monitoring Tool

The network owner will be able to interact with the Raspberry Pi Home network monitoring tool via any device that has a web browser and is on the network. The network owner will need to provide a user name and password in order to access the Raspberry Pi home network monitoring tool. An Apache2 web server, configured on the Raspberry Pi 3, gives owners the ability to interact with the Raspberry Pi home network monitoring tool via any device on their network. The U/I is designed to be very simple and straightforward. When owners log on, they will see the devices that are allowed and also new devices that have joined the network. If they would like to see revoked devices or spoofed devices, they can click on the configuration tab, which will allow them to select the appropriate section. The about section will give information about the monitoring tool.

The owner will also be able to interact with the Raspberry Pi home network monitoring tool via command line. The command line version of the Raspberry Pi home monitoring tool provides the user with more features, including the ones provided via the browser version. Owners will be able to remove allowed devices off the allowed list and also off the revoked list. The command line utility network monitoring tool is straightforward, just like the browser-based network monitoring tool.

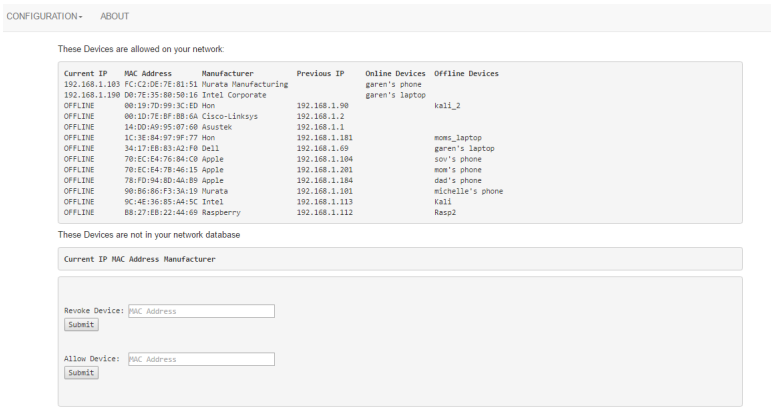

Figure 3: Main Page for Raspberry Pi Home Network Monitoring Tool

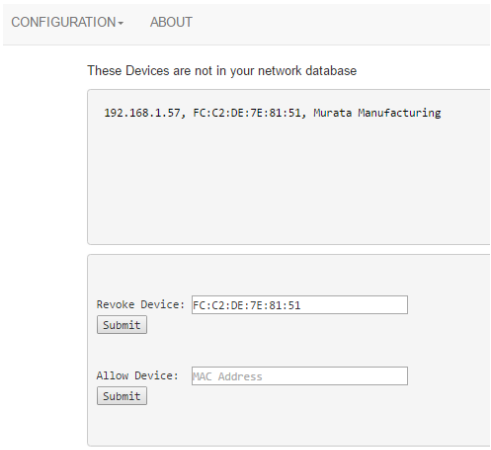

Figure 4: Missing Page for Raspberry Pi Home Network Monitoring Tool

The network monitoring tool is designed to be simple and easy to use. The configuration steps might be a little confusing if not all the appropriate Linux tools are installed, but once installed and configured, it is very easy to use.

4.3 Revoking

In the beginning of the research and beginning parts of implementing the project, a denial-of-service attack was an idle method to slow and eventually kick off an unwanted device. When small denial-of-service attacks were performed, the Raspberry Pi and the network monitoring tool worked fine. When multiple devices were on the network and a denial-of-service attack was performed, the effects were not the same. The intended device did not feel the effect and, if the packet size or speed of the denial-of-service was increased, the entire network and system would crash. Also, some devices are configured in a way that they do not accept any packets and a denial-of-service attack does not affect them. In order to fully implement an unwanted device to not be able to access the network, we focused on the router and how we can use the router to our benefit.

The router plays an important factor in the network. We looked to see if the router could be connected to through command line and whether there was any possible way of sending commands without logging into the router's configuration utility page. If the router has the capabilities of accepting signals through the command line, a complete denial of the unwanted device is possible. A small script was written and placed on the router. The script reads a specific file, which includes the unwanted device's MAC address, sent by the network monitoring tool. It takes the MAC address and adds it to the iptable's rule for revoking all forms of connection. This way, the device that is associated to the MAC address is not able to access the network. If the unwanted device decides to spoof the MAC address to an allowed device's MAC address, the network monitoring tool will detect that it is being spoofed because there are two of the same MAC addresses on the network. The network monitoring tool also looks at the manufacturer of the device and compares that as well. Network owners are notified if a spoofed device is on the network. In addition, if the revoked device is able to still use the network, the network owner would be notified that a revoked device is still on the network. That way, the network owner can log in to the router's configuration utility page and revoke the user there.

	RP3 H.N.M.T	Dojo	Cujo	F-Secure Sense	SoftPerfect Network Scanner
Type	Monitoring Tool	Smart Firewall	Smart Firewall	Smart Router	Monitoring Tool
Standalone	Yes	Yes	Yes	Yes	No
Notification System	Yes	Yes	Yes	Yes	No
Spoofing Notification	Yes	No	No	No	No
PC or Phone App	Both	Phone App	Phone App	Phone App	PC
Released	No	No	Yes	No	Yes
Cost	$35 RP3	$99 Dojo $99 Service	$99 Cujo $99 Service	$99 Sense $99 Service	Free

Figure 5: A comparison table for a few different network monitoring tools and devices

The importance of not disturbing or disrupting the quality of service to the allowed devices is very essential. We also thought about a full distributed denial-of-service, but we considered that to not meet the quality of service for which an allowed device would look.

Figure 5 shows a comparison table for some of the devices that were researched and looked into. The comparison is for both network monitoring tools and devices and also includes the proposed Raspberry Pi 3 Home Network Monitoring Tool.

5. SYSTEM EVALUATION

We evaluated the Raspberry Pi 3 Home Network Monitoring Tool in two parts. The first evaluation was done on my home network by me. The second evaluation was done on my girlfriend's network by her.

5.1 First Evaluation

The way the system was evaluated for the ease of use was to first time and see how long it took me to set up the network monitoring device and to begin the scanning. The Raspberry Pi 3 was already configured with the network monitoring tool. The appropriate email tools were also configured to be able to send notifications. I first read the README file, which gave me step by step direction on how to configure the network monitoring tool. I had to get the IP address of my router and device, which the README file guided me on how to find. After getting the appropriate IP address, I had to put it in the network monitoring tool. I then put the email address at which I wanted to be notified and I defined how often the network monitoring tool should scan. After completing and saving all of the required parts of the file, I went to the next step, which was to configure my router for CLI commands.
My router at home is an ASUS RT-AC68W. After a simple Google search, I was able to change a few settings on my router, which then let me be able to connect to the router with CLI commands. I was then able to connect to the router and put the file that was configured to revoke unwanted devices. In the README file, the appropriate commands give the correct privileges to the file that is going to be executed. Once that was done, I was ready to start the network monitoring tool on the Raspberry Pi 3. The total time it took me to appropriately configure the network monitoring tool and my router was about 20 minutes. The longest interval therein was spent on connecting to the router and making sure that no exploitable weaknesses were opened by changing configuration settings. I put the appropriate notes and a link in the README file for those who have an ASUS router and need to configure their router. It seems that setting up the device and connecting the router would be a bit challenging for a non-tech-savvy person and would therefore take someone with less technical background to set it up a little longer than 20 minutes.
Once the network monitoring tool was running, I was able to log on to the browser and was able to see all my devices that were on the network. I also received an email stating that there are devices on my network that are new. I then added each device and let the monitoring continue. I then added an additional device and tested the revoking of the device. Before revoking, I was able to search the web with that device. Once the device was set to be revoked, I was no longer able to search the web. I then logged on to the router and removed the rules to allow that device to continue being able to communicate with the router. I received an email notification stating that a device on the revoked list has returned. Everything was easy and straightforward. A person without a technical background would easily be able to move around the interface. I also decided to use the command line network monitoring tool and wanted to see how easy that was. The tool is straightforward and a person of a non-technical background can easily use it without any confusion.

5.2 Second Evaluation

I set up the network monitoring tool on another Raspberry Pi 3 and asked my girlfriend to see if she could easily configure the tool with the README file. She is not as technical as I am but knows computers so she did not need a lot of help to configure the network monitoring tool. She was able to easily follow the directions and was ready to move on to the router. The router configuration is where she and I struggled. Her router was a different ASUS model than mine. The configurations were a bit different than my router and we were struggling to be able to configure the router for command line communication. After reading a few different articles and trying different suggestions, we were finally able to configure the router and put the appropriate file to allow the denial of an unwanted device. It took us about an hour and half total for the configuration of the network monitoring tool and the configuration of the router. She was ready to test the network monitoring tool.
She was able to easily use the network monitoring tool and was able to understand what to do without my help. She also tried the command line network monitoring tool and it was a bit confusing for her. She did not feel comfortable with the command line and she did not like that she was stuck to the Raspberry Pi and could not work comfortably on a web browser. She allowed the network monitoring tool to monitor her network for about two weeks. In those two weeks, she was able to give me appropriate feedback and suggest future changes. She was also able to detect an unwanted device and appropriately revoke the device from her network. She was overall very satisfied with the device and the ability to easily see new devices and to be able to conveniently revoke unwanted ones.

6. FUTURE WORK AND CONCLUSION

6.1 Future Work

It is important for network owners to own their network and to easily see essential information about their network. Future work for this system can vary from the usability and easiness aspects to the security aspect.

Even though the setup of the network monitoring tool is not hard, configuring the device and router can be a bit tedious. Future work should aim to see if it is possible to make the configuration of all devices smoother. Maybe a package installer or an easier configuration would be helpful. The importance placed on ensuring that non-technical people can easily configure and use the network monitoring tool should continue to be emphasized in future work.

Network owners' ability to easily see essential information about their network is important but may not be enough. Future work should aim to see if additional information can be included, including, for example, a log of each user's connection history or a log of each user's traffic. The importance of keeping the quality of service should not be taken lightly during logging.

Even though the network monitoring tool does provide a form of security by warning for new devices, unwanted devices, or spoofed devices on the network, focus should be

placed on other forms of security as well in the future work. For future work, it would be an improvement in the overall security of the system if the Raspberry Pi could be converted into a hybrid smart router within which the network monitoring tool would be integrated as a firewall.

6.2 Conclusion

With the network monitoring tool, network owners can easily and quickly be notified of any unwanted devices on their network and conveniently kick them off. Network owners will no longer need to connect to their router's configuration utility page in order to prevent any unwanted devices. The focus for the research and project was to provide non-technical people with a cost-effective solution to own their network, and such a device was successfully created.

Making a network secure with firewalls and smart routers can be very expensive and may even require a technical background to configure and setup. The network monitoring tool is proven to be the exact opposite. With only a $35 investment in a Raspberry Pi 3 and a simple configuration of the network monitoring tool, everyone can make their network a little more safe and secure.

As more and more smart devices are added to home networks, it is very important for owners to make sure that they are secure and safe without relying heavily on vendors providing paid-for services and securing their products. Having the Raspberry Pi 3 Home Network Monitoring Tool connected to their home networks will allow owners to take a positive step in keeping their home network safe from intruders.

7. REFERENCES

[1] Apache2. Apache2. https://httpd.apache.org/.
[2] Arduino. Arduino. http://www.arduino.cc/.
[3] CubieBoard. Cubieboard. http://cubieboard.org/.
[4] Cujo. Cujo. https://www.getcujo.com/.
[5] Dojo-Labs. Dojo. https://www.dojo-labs.com/.
[6] F-Secure. Sense. https://sense.f-secure.com/us.
[7] Famatech. Advanced-ip-scanner. http://www.advanced-ip-scanner.com.
[8] I. Gartner. Internet of things. http://www.gartner.com/it-glossary/internet-of-things.
[9] L. Gordon. Nping. https://nmap.org/nping/.
[10] G. Lyon. Nmap. https://nmap.org/.
[11] S. N. Management. Softperfect wifi guard. https://www.softperfect.com/products/wifiguard.
[12] Odroid. Odroid. http://www.hardkernel.com/main/main.php.
[13] R. Pi. Raspberry pi 2 model b. https://www.raspberrypi.org.
[14] Raspbian. Raspbian. https://www.raspbian.org/.
[15] O. Security. Kali linux. https://www.kali.org.
[16] SolidRun. Hummingboard. https://www.solid-run.com/freescale-imx6-family/hummingboard/.
[17] S. N. M. Solutions. Softperfect network scanner. https://www.softperfect.com/products/networkscanner.
[18] Wireshark. Tshark. https://www.wireshark.org/docs/man-pages/tshark.html/.