Old Dominion University

Engineering Management and Systems

Engineering Department

Capstone Project Final Report

Home Network Security Improvements

Robert E. Litts

8-1-2022

Executive Summary

The objective of this project is to research and implement the appropriate techniques and procedures needed to increase the security of a private home network. A home network in the context of this project is defined as all devices that fall within the local network behind an Internet Service Provider's modem in a residential household. Greater than 85% of households in the United States have a broadband internet subscription and therefore maintain some form of a home network. Exponential production and widespread adoption of Internet of Things (IoT) devices such as smart televisions, appliances, and monitoring tools are now connected to the networks in over 70% of households. The addition of these devices without scrutiny introduces significant risk into the home network infrastructure. According to the NSA, all networks are at risk of compromise and require administrators to secure devices, applications and information; failure to do so leaves homes open to vulnerabilities, exploit, digital theft, and spying. In the residential environment, physical security and maintenance responsibilities rest on the homeowner; network administration and security are no different.

To accomplish this project, a thorough literature review of home network vulnerabilities, cybersecurity best-practices, and secure network architecture was conducted. Additionally, a home network security survey was provided to family, friends, and coworkers and established a realistic cross-section of data for existing home network security practices. This research showed that over 50% of respondents are not taking basic security measures to protect their home network. The literature review provided an understanding of current threats and defensive strategies which aided in the development of requirements for a secure home network. To put these requirements into practice, I developed a secure home network architecture modeled after my own residential network, procured necessary equipment, and integrated these devices into my

home network as designed. At a cost of only $348, this exercise allowed me to demonstrate the key challenges and benefits of adding a firewall and layered segmentation into my own home network. This project utilized knowledge obtained throughout my studies and directly aligns with several key Engineering Management principles including project management, analysis of organizational systems, information science, and cost estimating/financial analysis.

This project identifies important areas of focus for homeowners to increase the security of their home network. These strategies start with the basics of creating strong access credentials with multi-factor authentication whenever possible. Additionally, individuals should keep software/firmware updated and use strong wireless network encryption such as WPA2 at all times. To further harden their network, homeowners should additionally configure a strong firewall and restrict all external access, ensuring no TCP/UDP ports are available to conduct remote administration. Several high-profile cyber-security attacks took advantage of a simple vulnerability such as this to gain network access and device control. Finally, creating a segmented network which separates IoT devices from personal devices provides security in depth and hardens the overall security posture if an attacker gains access to an insecure device.

The contributions of this project are applicable to Engineering Managers across all disciplines. The principles detailed in this report are based on enterprise level cybersecurity guidance and are completely scalable from small businesses all the way to large corporations and government agencies. By starting with home networks, this project aims to develop a culture of understanding and mitigating strategies against the real risks that exist on the computers and devices used on a daily basis. By reading this report, following the security steps provided, and improving upon network architecture, engineering managers can better protect their data and ensure cybersecurity is a fundamental part of all projects.

Table of Contents

Table of Figures

Table of Tables

Acknowledgements

I would like to thank my wife Kristy for providing me with the time to complete this second Master's degree during an adventurous first year with our son Charlie. I would not be here today without her love, support and guidance. Thank you to my son Charlie for always waking up with a big smile on your face! And to our second child, we are looking forward to meeting you next year! I am very appreciative of the knowledge I have gained during my studies and am looking forward to the future with my family!

Disclaimers

This project was conceived as an expansion on my hobby of home networking, privacy, and security; the intersection of these three areas of interest provided the perfect venue to conduct further research and expand my knowledge. As an Electrical Engineer with a focus on computers and communication systems, I have always had an interest (and fear) of networking because it seemed like complicated magic. However, the greatest successes in life come when you step out of your comfort zone and try to learn something new. I have taken considerable personal time to setup a more secure home network in an effort to take control of my family's digital data, which was previously spread out between a number of commercial cloud providers. Throughout this journey, I have learned a significant amount about networking but also understand that I have just scratched the surface of this field. The work contained in this project should be viewed as a framework for others to take control of their own networks. However, consulting with manufacturer documentation and official guides should always be the first step when configuring hardware or software. I hope this paper will be helpful to anyone that comes across it, but note that I am not a professional network engineer.

Introduction & Background

General Focus

Home network security is a topic of fundamental interest to every internet connected household in the United States, yet many individuals are blissfully unaware that they can and should take action to increase their defensive posture to prevent cyber security attacks. “Security controls are defined as the safeguards or countermeasures employed within a system or an organization to protect the confidentiality, integrity, and availability of the system and its information and to manage information security risk” (National Institute of Standards and Technology, 2020). Failure to implement even the most basic security controls often leave households as the prime target of rogue cyber actors with bad intentions to exploit these vulnerabilities, gain access to the network and cause digital vandalism, theft, or ransomware attacks. The 2016 Mirai botnet is a prime example of basic security controls being exploited to amass several hundred thousand home network devices into an army of offensive weapons targeting political and private targets. Additional attacks and subsequent data breaches by retail stores such as the 2013 Target attack which leaked 11GB of data including millions of consumers credit card data, indicate that cyber security breaches by a single insecure device can have devastatingly widespread impact (Rothrock, 2018). The goal of this project is to provide home network administrators with the resources to implement strong security controls and harden their networks against bad-faith cyber actors.

Organization and Target of Study

The target of this study are residential households with a broadband internet connection. The U.S. Census Bureau has been tracking internet usage since 1997 and has noticed steady growth

in both computer ownership and internet access. As of 2018, which is the most recent American Consumer Survey, 92% of households had at least one computer and 85% had a broadband internet connection (Martin, 2021). For the purposes of this project, households who meet the above criteria have a home network, even though this may be as simple as an Internet Service Provider (ISP) supplied modem, router, and one computer or smart phone. For the vast majority of households, the home network is much more involved and includes devices such as a wireless router providing wireless internet access, smart phones, laptops, gaming systems, and various Internet of Things (IoT) devices such as televisions, thermostats, cameras, and appliances. No matter the size of the network, the principles addressed in this project will be applicable.

Importance

It is impossible to put a price or metric on an individual's personal information and digital data, so it is imperative that initial steps are taken to put up layers of defense to protect home networks against compromise. With over 26 million IoT devices in U.S. households, caution must be exercised on the level of access and control these notoriously vulnerable devices are provided (Davis, Mason, and Anwar, 2020). As the world becomes more internet-connected, it is easy to allow devices access to one's home network without much thought. This project aims to challenge that the existing mindset and ensure individuals consider access control and network segmentation before new devices are allowed to communicate with private devices. Additionally, there are a number of basic security steps that every home network administrator should review without any financial commitments or advanced computer knowledge. Failure to take these steps could leave home networks as ripe targets for exploitation by cyber criminals.

Project Definition

Purpose

The vast majority of U.S. households utilize a home network and should understand the vulnerabilities present and have strategies at their disposal to defend their data and devices from exploitation by adversaries. The purpose of this project is to develop a strategy which households can use to increase the security of their home networks. This strategy will include three tiers of guidance: basic, intermediate, and advanced security practices which households can incorporate into their home networks no matter how much money or computer networking expertise they have.

Specific Objectives

To accomplish this project, the following objectives will need to be completed. First, I completed a literature review of the existing cybersecurity vulnerabilities present in home & business networks. Next, I conducted research on best-practices for setting up a secure network based on enterprise infrastructure guidance and developed a secure home network architecture plan. Finally, I put these best-practices into use by upgrading the security of my own home network. This included purchasing additional hardware such as a separate router/firewall, layer 3 switch, and wireless access points. Additionally, I configured network parameters to include setting up Virtual Local Area Networks (VLANs) for network segmentation as well as advanced firewall rules to prevent lateral network movement by guests or IoT devices. Finally, I completed several tests to ensure that my network meets the requirements as defined by the applicable guidelines and references.

Scope

Limitations

1. There will be no penetration or cybersecurity testing done to validate the inherit security of my network once implemented.
2. The research conducted and data obtained is readily available for free on the internet or contained within a research database; no studies or publications will be purchased or accessed using Government intranet.
3. Implementation of hardware/software will only be at the level I am comfortable administering on the network.
4. Internet Service Providers will not be involved in this project.
5. There will be no Information Technology (IT) guides, tutorials, or instructions associated with this report.
6. There will be no walkthroughs of configurations or device parameters.

Assumptions

1. Any needed equipment will be available for purchase using Amazon or similar "next day delivery" services.
2. Funding for this project will be solely provided by myself.
3. Equipment will be in working order.
4. Internet and power will be available to my home for the duration of this project.
5. Testing will be conducted using the command line on Linux/Windows; no further sophisticated networking tools will be utilized.

6. I have a background and interest in Computer Networking and IT and enjoy tinkering with my home network.
7. I have hardware configurations and backups of all my critical data.
8. I have redundant network equipment and detailed guidance which will allow me to revert my network setup to pre-test conditions without any interruptions to my hardware/software.

Project Significance

Local Level Impact

This project will provide households with the requisite knowledge and techniques to better secure their home network from digital threats. Since digital networks are an inherently complex topic, the tiered guidance provided by this report provides recommendations which are approachable by anyone regardless of existing knowledge. This project also ensures households begin considering the existing cybersecurity risks and make them more conscious of the security choices (or lack thereof) in their digital lives. While most people are trained to lock their doors when they are away, this report shows that locking down digital networks is just as important. This report demonstrates to households that networks are vulnerable, provides actionable guidance on how to secure their own network, and details my actual implementation of advanced home network security controls which can easily be replicated if desired. These guidelines provide increased awareness to advance the cybersecurity conversation both at home and into individual's professional lives.

Application of Engineering Management Knowledge

This project provided me the opportunity to exercise several of the key facets of ENMA knowledge gained throughout the program. First, Project Management (ENMA 604) was used to

develop the initial plan and schedule which was decomposed into tasks using a Work Breakdown Structure (WBS). This allowed me to ensure my goals were realistic within the time frame allowed. Next, information from Organizational Systems (ENMA 601) was incorporated when conducting the home network security survey. This data allowed me to compare the information found during the literature review with data obtained from a diverse set of friends, family, and co-workers. Information Science for Systems and Engineering Management (ENMA 646) was used to analyze my survey results to determine if there are any trends within the data. Cost Estimating and Financial Analysis (ENMA 600) & Economic Analysis of Capital Projects (ENMA 700) were both fundamental when I created an initial budget for this project and helped me analyze the viability of costs associated with the proposed security for the majority of U.S. households.

Extension of Project Beyond Local Level

One can easily apply the results and findings of this project to their business or professional lives. Cyber security should no longer be an afterthought, but is something that should be considered from the very advent of a digital or network connected device/system. The security controls described in this project are enterprise grade and as such, they are scalable to smaller or larger environments. The fundamental principles do not change, but management and enforceability become more difficult as the network and number of participants grows. Therefore, I believe that this project should spark the cyber security mindset into individuals who were not already considering these risks as part of their planning or budgeting cycles. Additionally, understanding just how easily a cyber-criminal can attack a simple home network and wreak havoc should increase the concern and awareness that business owners and engineering professionals have when considering their own endeavors. Regardless of the type of

engineering conducted, cyber security and network controls should always be a fundamental part of the conversation.

Project Approach

Project Design Overview

The overall idea behind this project is to take a look at the technical resources and security practices recommended by cyber security authorities and apply them to individuals home networks with a goal of providing increased security. To accomplish this, I conducted a literature review and also completed a survey of personal and professional contacts to see current vulnerabilities and how they are being exploited. Using this data, I presented a straight-forward methodology that home network administrators can use to increase their security controls, regardless of the level of expertise they currently have. By presenting this information in a logical manner, individuals will be able to take action in their own homes. Additionally, the principles can be used by engineering managers in their business and professional lives since cyber security and network vulnerabilities exist throughout many facets of the workforce.

Specific Project Design

Project Approach

The following sections outline the specific approach taken to accomplish this project, including the method of data collection, plans for data analysis, and the expected outcomes.

Data Collection

To accomplish this project, the approach utilized was a combination of literature review, survey of friends, family, and co-workers, and physical implementation of network security hardware with associated software controls. The first step was to conduct a background literature review which consisted of reviewing technical documentation from the major U.S. Government cyber

security entities. These entities included the National Security Agency (NSA), Department of Homeland Security: Cybersecurity and Infrastructure Security Agency (CISA), and National Institute of Standards and Technology (NIST) publications. Additionally, I conducted a review of both home and corporate network security papers on Google Scholar and Institute of Electrical and Electronics Engineers (IEEE) Xplore. Once I gathered this documentation, I reviewed the applicable home network security controls and used this research to create the "Home Network Security Survey." Simultaneously, I compiled a diverse list of survey participants from myself and my wife's personal and professional contacts. This list contained approximately 50 people from throughout the country and ranged in age from 18-65. This survey was then input into a Google Form and sent out to the participant list and would automatically compile anonymous results. The final data that needed to be collected was the hardware necessary to implement advanced home network security controls in my own network. I conducted market research across a range of consumer and small business grade networking equipment, including TP-Link, Ubiquiti, Cisco, Netgear, and Juniper. The goal of this market research was to obtain an independent firewall/router, layer 3 switch (which allows VLAN configuration) and wireless access points with layer 3 VLAN capability.

Plan for Data Analysis

Following the initial research, I then compiled my technical results into two main documents. The first is the "Home Network Security Best Practices" document (Appendix C), which included a summary of the major guidelines presented by CISA, NSA, NIST security controls. This literature review also allowed me to develop the "Secure Home Network Architecture" diagram (Appendix B), since many of the advanced security controls were beyond simple administrative changes to software or firmware. The anonymous results from the home network

security survey were output into an excel spreadsheet which I fed into the program R to generate bar graphs of the major survey areas. These graphs can be seen in Appendix A. This allowed me to better visualize the results and present them as an artifact for this project. Finally, my market research allowed me to purchase the necessary equipment to implement my version of the "Secure Home Network Architecture" (Appendix B). I then configured my network and integrated these new devices using applicable manufacturer guidance.

Results of Data Collection

The literature review highlighted some common areas of vulnerability that many individuals can correct immediately. A Joint Cybersecurity Advisory published by CISA in conjunction with the NSA and several partner nations identifies that poor cyber hygiene practices are the root cause of many criminals' ability to gain access to home networks (Cybersecurity and Infrastructure Security Agency, 2022a). The initial areas of concern include under-utilization of multi-factor authentication, particularly with Remote Desktop Protocol (RDP) or similar applications. The next area of concern is keeping software and firmware up-to-date with the latest versions. Manufacturers typically release patches to harden software/firmware against known vulnerabilities and bugs, so individuals should always ensure that devices in their network are kept updated. This is often a very simple process, and many modern computers and devices will notify you via e-mail when an update is available. Another common area of concern to address is the use of vendor-supplied default usernames and passwords. Although this sounds simple, changing the default username and password of network-connected devices is a fundamentally important step that many individuals simply overlook; survey results indicate that 50% of individuals fail to take this precaution. Default credentials can allow an attacker to easily gain access to a device and make lateral movements within a network, conduct man-in-the-middle

attacks, spy, or steal personal information. These results were captured and included in the "Home Network Security Best Practices" deliverable. Every home network administrator should read through this document and take immediate action to review and update their devices. Based on the results of the home network security survey, many individuals are either unaware of the risks, lack the information, or simply have not taken even the most basic steps to harden the cyber security controls. A review of the report, deliverables, and guidance should be sufficient to get everyone on the right track toward protecting their network.

Project Management

Schedule

The detailed project schedule with major milestones identified provided an easy method to ensure I stayed on track throughout the semester. Table 1 identifies the major milestones identified to be completed for the project, including the proposed completion date and the actual completion date. These major milestones were used to generate a more detailed Gant Chart in Figures 2 and 3. This Gant chart provides a visual breakdown of the individual work items as well as the predecessors. A network diagram was also created and can be seen in Figures 4-6 and easily visualizes the critical path for the project.

The methodology I followed was Waterfall Project Management. This traditional form of project management allowed me to conduct sequential planning with clear goals since there is a defined scope and limited client interaction. As I worked through the different stages of the project, events built upon the knowledge and information gained from the previous tasks and allowed me to make progress. I utilized a small amount of informal Agile Project Management while integrating the hardware and software updates into my home network, but this

encompassed only a small portion of the overall project. The waterfall methodology was adequate for this project and allowed me to complete the project during the semester as required.

Major Milestones		
Milestone	Proposed Completion Date	Actual Completion Date
Home Network Security Survey Released	6/08/2022	06/09/2022
Project Proposal Submission	6/12/2022	6/12/2022
Research & Literature Review	6/20/2022	6/18/2022
Home Network Best Practices Guidance	6/27/2022	6/23/2022
Secure Home Network Architecture Diagram	6/28/2022	6/27/2022
Hardware Market Research	6/30/2022	6/25/2022
Home Network Security Survey	6/30/2022	6/30/2022
Hardware Delivery	7/6/2022	7/1/2022
Secure Home Network Hardware & Software Installation	7/12/2022	7/3/2022
Final Repot Submission	8/1/2022	7/31/2022

Table 1: Major Milestones

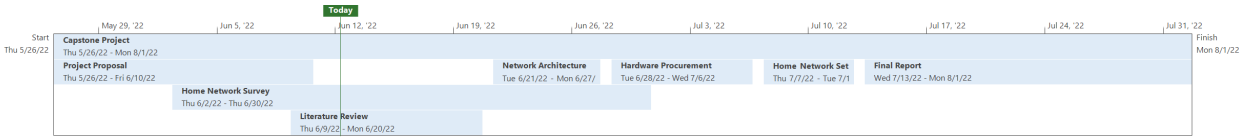


Figure 1: Schedule Overview

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors
1		**Project Proposal**	**12 days**	**Thu 5/26/22**	**Fri 6/10/22**	
2		Executive Summary	2 days	Thu 5/26/22	Fri 5/27/22	
3		Intro & Background	3 days	Mon 5/30/22	Wed 6/1/222	
4		Project Approach	2 days	Thu 6/2/22	Fri 6/3/22	2,3
5		Project Expectations	3 days	Mon 6/6/22	Wed 6/8/222	3,4
6		References	2 days	Thu 6/9/22	Fri 6/10/22	5,3,4
7		**Home Network Survey**	**21 days**	**Thu 6/2/22**	**Thu 6/30/22**	3
8		Research	3 days	Thu 6/2/22	Mon 6/6/22	
9		Gather List of Peopl	1 day	Thu 6/2/22	Thu 6/2/22	
10		Develop Survey Que	2 days	Tue 6/7/22	Wed 6/8/228	
11		Release Survey	0 days	Wed 6/8/22	Wed 6/8/228	9,10
12		Wait for Survey Res	14 days	Thu 6/9/22	Tue 6/28/22	11
13		Survey Closed	0 days	Tue 6/28/22	Tue 6/28/22	12
14		Analyze Results	2 days	Wed 6/29/2	Thu 6/30/22	13
15		**Literature Review**	**8 days**	**Thu 6/9/22**	**Mon 6/20/22**	11
16		Vulnerabilities	5 days	Thu 6/9/22	Wed 6/15/2	
17		Infrastructure	3 days	Thu 6/16/22	Mon 6/20/22	16
18		Best Practices Guidanc	5 days	Tue 6/21/22	Mon 6/27/22	15
19		**Network Architecture**	**5 days**	**Tue 6/21/22**	**Mon 6/27/22**	15
20		Rough Draft	3 days	Tue 6/21/22	Thu 6/23/22	
21		Final Network Diagr	2 days	Fri 6/24/22	Mon 6/27/22	20
22		**Hardware Procuremer**	**7 days**	**Tue 6/28/22**	**Wed 7/6/22**	19
23		Market Research	3 days	Tue 6/28/22	Thu 6/30/22	
24		Order	2 days	Fri 7/1/22	Mon 7/4/222	23
25		Shipping	2 days	Tue 7/5/22	Wed 7/6/222	24
26		Delivery	0 days	Wed 7/6/22	Wed 7/6/222	25
27		**Home Network Setup**	**4 days**	**Thu 7/7/22**	**Tue 7/12/22**	22

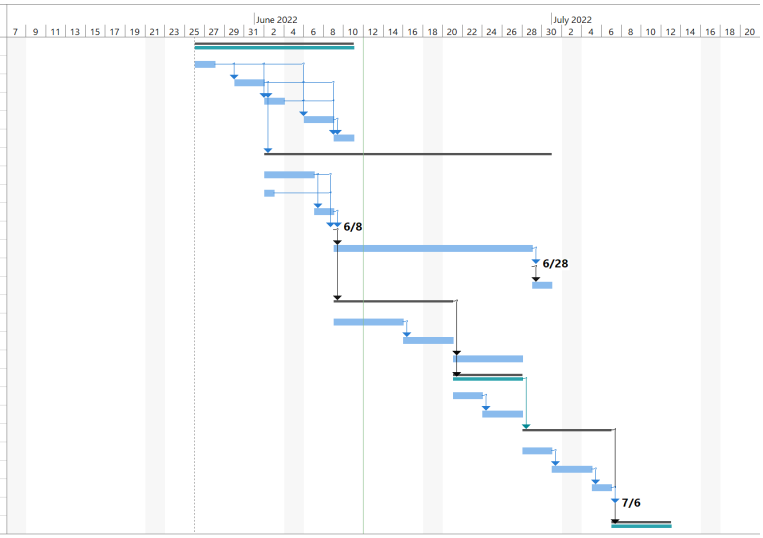


Figure 2: Gant Chart Part 1

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors
27		**Home Network Setup**	**4 days**	**Thu 7/7/22**	**Tue 7/12/22**	22
28		Configure Router Sc	1 day	Thu 7/7/22	Thu 7/7/22	
29		Configure Switch	1 day	Fri 7/8/22	Fri 7/8/22	28
30		Configure Access Pc	1 day	Mon 7/11/22	Mon 7/11/22	29
31		Hook Up Hardware	1 day	Tue 7/12/22	Tue 7/12/22	30
32		**Final Report**	**14 days**	**Wed 7/13/22**	**Mon 8/1/22**	27
33		Finalize Results	5 days	Wed 7/13/22	Tue 7/19/22	
34		Discuss Deliverables	5 days	Wed 7/20/22	Tue 7/26/22	33
35		Recommendations	3 days	Wed 7/27/22	Fri 7/29/22	34
36		Biographical Data	1 day	Wed 7/13/22	Wed 7/13/2	
37		References/Append	1 day	Wed 7/13/22	Wed 7/13/2	

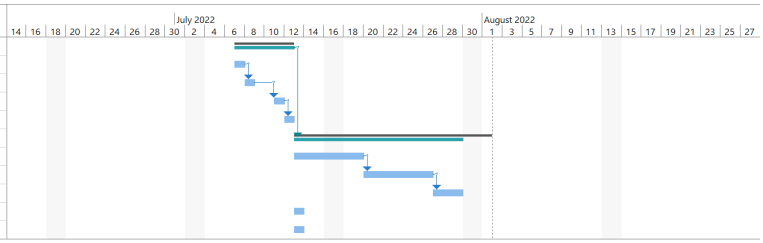


Figure 3: Gant Chart Part 2

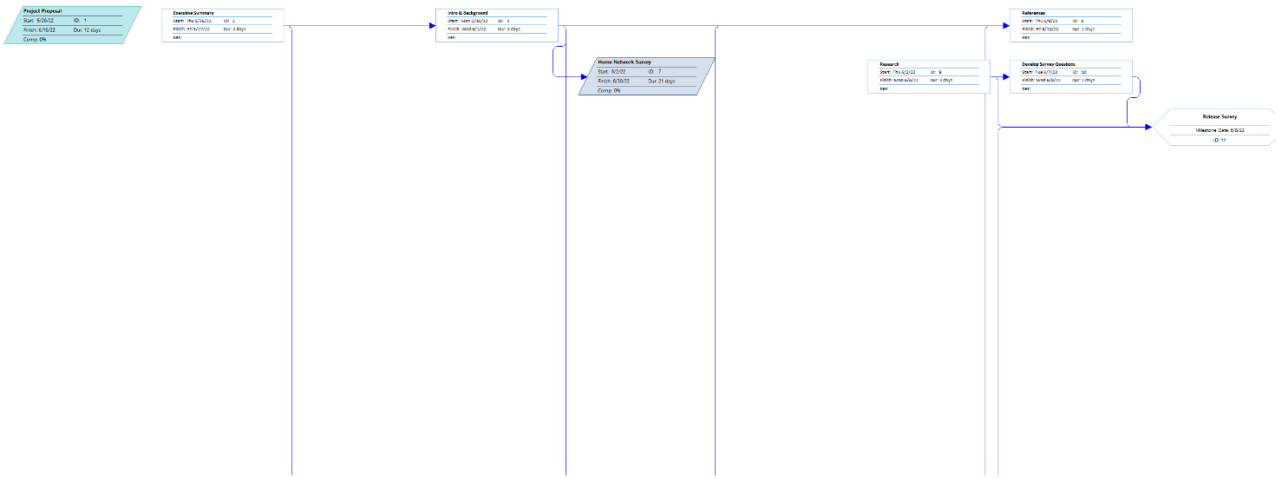


Figure 4: Network Diagram Part 1

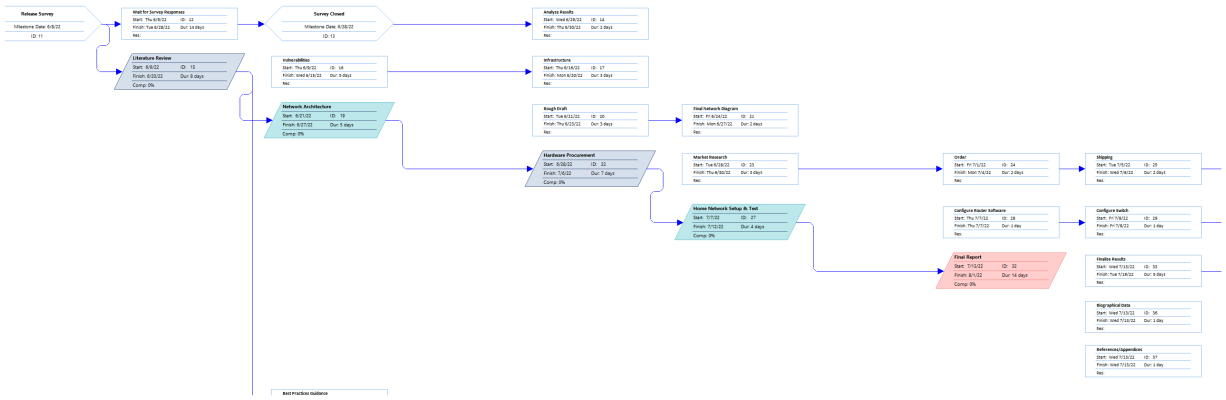


Figure 5: Network Diagram Part 2

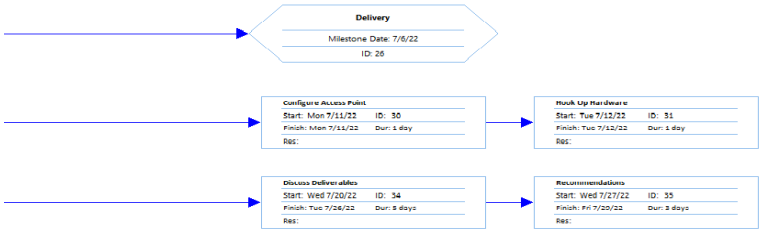


Figure 6: Network Diagram Part 3

Deliverables

The deliverables created for this project included the following:

1. Literature Review of Home Network Vulnerabilities (addressed in "Project Results and Implications – Interpretation of Data")
2. Home Network Security Survey Results (Appendix A)
3. Secure Home Network Architecture Diagram (Appendix B)
4. Secure Home Network Best Practices Guidance (Appendix C)
5. Results & Lessons Learned of Advanced Home Network Installation (addressed in "Project Results and Implications – Interpretation of Data")

Controls

Since this project was functionally run by myself and included limited interaction with any outside entities, I was able to maintain the scope and schedule fairly rigidly without issue. The initial project proposal helped me lay out a clear vision with a reasonable timeline, schedule of events, actionable milestones, and realistic goals. Since I have a personal passion for networking, I had to limit myself to "over-engineer" a solution when working on software configuration. The method I used to do this was by reviewing the schedule and ensuring that my individual tasks followed the Gant Chart and did not deviate from the scope of work outlined. Aside from this, it was fairly straightforward to complete this project on schedule/budget and limited controls were necessary to remain on task.

Project Design Issues

I did not encounter any significant design issues or required modifications throughout the project lifecycle. I ran into some minor complications when configuring my home network but these were overcome by reviewing equipment manufacturer documentation. For example, configuring an "IoT VLAN" on my TP-Link switch required significant consultation from the TP-Link website because each manufacturer of layer 3 switches provides their own interpretation of the IEEE 802.1Q standard. I did not encounter any issues conducting my home network security survey or with the literature review. Overall, the project flowed fairly smoothly and accomplishment met the plan as set forth in the proposal.

Project Results and Implications

Interpretation of Data

Literature Review of Home Network Security

A thorough literature review was conducted of U.S. Government publications from CISA, DHS, NSA, and NIST, along with academic papers to establish a credible, technical background for the recommendations provided in this project. It is abundantly clear that weak security controls are often the culprit of most cyber-attacks. Technical advisories from the U.S. Government state that a lack of multi-factor authentication and a combination of default/vendor supplied passwords and incorrectly applied privileges are often exploited for initial network access (Cybersecurity and Infrastructure Security Agency, 2022a). Once inside the network, cyber-criminals can utilize known vulnerabilities in outdated software to conduct surveillance and steal data, money, or hold files hostage and demand a sum of money for their safe return. Misconfigured VPNs, remote desktop protocol (RDP), and other remote network access mechanisms are also frequently exploited to gain access to a private network.

One of the most well-known IoT cyber-attacks is known as the Mirai botnet. In 2016, the Mirai botnet took the world by storm when it infected over 600,000 IoT devices and generated a peak 600Gbps distributed denial of service (DDoS) attack which crippled several high-profile company networks (Antonakakis et al., 2017). Mirai conducted rapid scanning of internet-accessible Telnet TCP ports 23 and 2323 and conducted brute-force login attempts with a pre-configured list of known, weak credentials, also known as a dictionary attack. Once a login attempt was successful, the program logged the IP address and downloaded malware which deleted processes, shut down further access to the device, and silently awaited commands from an external control server. This phase of the attack was a massive, brutal recruitment of solider devices, amassing a steady state force of between 200,000 to 300,000 rogue devices which would later be used to conduct offensive operations. During the five-month period where the

Mirai botnet was active, over 15,000 DDoS attacks were conducted using techniques such as volumetric resource exhaustion, TCP state exhaustion, and application-layer attacks. Victims of these attacks included game servers, telecoms, and even political websites. The most high-profile victim was Lonestar Cell, the largest telecom operator in Liberia, where the botnet substantially deteriorated the company's network (Antonakakis et al., 2017). Overall, the Mirai botnet exploited the lack of basic security best practices on IoT devices and makes it abundantly clear that action must be taken to prevent basic security holes from exploitation. As shown in this attack, an individual's home network may just become a solider in an army of devices targeting thousands of different web servers around the world.

As shown by the Mirai botnet, IoT devices represent a ripe target for cyber-attacks, yet the average home network simply adds these devices to their network without much thought. 120 new IoT devices are connected to the internet every second, and despite the features and convenience they bring to households, there is a lack of industry security standards in place for these devices (Davis, Mason, and Anwar, 2020). Many IoT devices have known vulnerabilities and can be exploited using Man-In-The-Middle attacks, cross-site scripting, and information spying. Several well-known smart thermostat brands such as Google Nest and Honeywell have the ability to deduce home network Wi-Fi passwords and their software can expose cross domain access information. Smart light bulbs such as Philips Hue are susceptible to replay attacks, DNS spoofing, and can access secret keys. Well-known vendors such as Philips or GE are more likely to patch known vulnerabilities, but there are thousands of lesser-known IoT devices out there which may continue to stack up vulnerabilities without remediation (Davis, Mason, and Anwar, 2020). In the enterprise environment, over 1 billion IoT transactions are being completed each month but have also seen an increase in 14,000 malware attempts per month, indicating that the

IoT field is being heavily targeted as a cyber security attack vector. Enterprise risks indicate that 83% of IoT transactions are not using TLS encryption, but are instead sending traffic over plain text which could significantly compromise passwords and data (Zscaler, 2020).

Further issues in the consumer device market involve weak default credentials which enhance exploitability. Admin/Admin are the most commonly used default account credentials in 88% of weak File Transfer Protocol (FTP) and 36% of weak Telnet devices (Kumar et al., 2019). TP-Link (the most popular home router in the world, comprising 15% of the market) home routers also support FTP by default in 62.8% of devices and 9.3% open the FTP port on the firewall by default. Additionally, a number of these routers expose HTTP, Telnet, FTP, or SSH access to the internet with default credentials and vulnerabilities present (Kumar et al., 2019).

NIST defines security controls as the safeguards and protection capabilities appropriate for achieving the security/privacy objectives of the organization (National Institute of Standards and Technology, 2020). Controls should be implemented early in the development of a system, and in the case of home network security, we have the opportunity to "redesign" our networks to take these important security controls into consideration. Appendices B and C provide an overview of important security controls that must be implemented in order to enhance home network security. These controls were developed from a combination of publications and document the most important steps necessary to enhance cyber security in the home. Figure 7 depicts the "layered" network approach, which includes multiple firewalls and increases attackers' difficulty of access as one moves from the internet to the heart of the network.

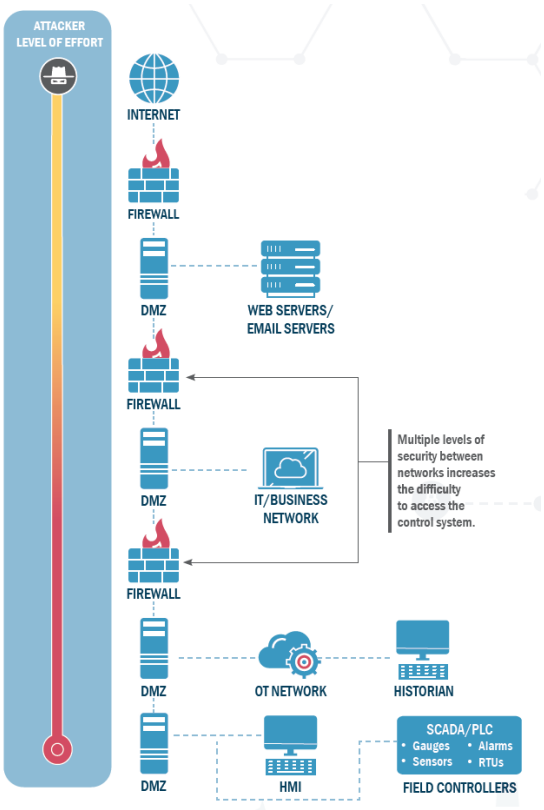


Figure 7: Layering Network Security (Cybersecurity and Infrastructure Security Agency, 2022b)

Appendix B provides a similar architecture to Figure 7, but only utilizes one firewall and segmentation principles where IoT devices are segregated to their own network. This means that even if an attacker were to gain access to an IoT device using an exploit, they would only have access to other IoT devices and no private information. Appendix C offers many security features that an individual should enact to harden the security controls on their network. These controls include changing default credentials, disabling external administrative capabilities, and employing a hardened firewall. By taking the most basic steps to implement security controls at home, networks will become much more capable of resiliency against attack.

Results & Lessons Learned of Advanced Home Network Installation

To implement the architecture shown in Appendix B, I had to purchase a few additional devices for my network. Previously, I had a typical network setup as you would find in most homes: a

single Netgear Nighthawk R6700 combination Wi-Fi access point/switch/router. All my home devices were connected directly to this device (wireless and wired) and this was connected to my Verizon ONT to provide internet access. To enhance my home network security, I needed to purchase a dedicated firewall/router, layer 3 switch, and a new wireless access point.

My market research began with the dedicated firewall/router. For router/firewall software, I decided to utilize the free and open source pfSense Community Edition (CE), which is made by Netgate. This software can be run on any computer, but you must have at least 2 ethernet ports on the device's network interface card (NIC). My research found that refurbished small form factor (SFF) enterprise computers consume minimal power, often have multiple ethernet ports, and are fairly inexpensive to purchase. I decided to purchase a HP T620+ computer with a quad-port NIC for $160. This device had plenty of computing power to run pfSense and with the four ports I would be able to have three separate LANs (the fourth port is used for the WAN connection).

Next, I searched for layer 3 switches which are capable of VLAN segmentation. Powerful switches can run into the $100-$200+ range, but for my basic home needs I decided on a 16-port TP-Link SG116E for $79. This device is VLAN capable using a web interface that is slightly complicated to configure. I had to consult several online forums and videos to understand how to properly configure a VLAN on this switch, and in retrospect I would not recommend anyone purchase this device. However, the price of this device was unmatched by anything else I found with similar specifications.

Finally, I wanted to purchase a new wireless access point that was also VLAN capable so that I could create wireless network segmentation along with physical segmentation at the switch. Logically, this works exactly the same as the switch but the access point itself must be

capable of tagging traffic since all data returns through the same physical port which must be distinguishable beyond layers 1 & 2. I decided to purchase the TP-Link EAP 245 V3 access point for $79. This device is part of TP-Link's Omada line and can be managed via a web interface or using a software controller installed on a network device. I decided to install the software controller on my NAS drive since that device is a high-availability item in my house and is connected to an uninterruptable power supply (UPS).

In total, I spent $318 on hardware and another $30 on CAT6 ethernet cables, making this project's cost a grant total of $348. This was well within my budget of $500 as set out in my project proposal and allowed me to effectively establish a much more secure home network. The customization and security offered by the pfSense firewall/router allows for significant enhancements from my previous setup. I was able to configure a Wireguard VPN server, network logging and monitoring, and ad-blocking all within this one device. Additionally, adding a switch and access point capable of segmenting VLAN traffic allowed me to establish four separate subnets within my home, which directly falls in line with CISA layered network security guidance (Cybersecurity and Infrastructure Security Agency, 2022b).

Discussion of Deliverables

Home Network Security Survey Results

The Home Network Security Survey was sent out to just over 50 people and received 37 responses, resulting in a 74% response rate. There were two initial questions included to establish demographics: age and household size. 37% of respondents were between the ages of 29-35, 35% between ages 18-28, and 19% over age 45. There was only one respondent between age 36-45 and one declined to provide their age. 56% of respondents live in a household with 2-3

people and 16% live with 4-5 people, indicating that the average respondent has at least 6-12 personal devices connected to their home network (phones, computers, and/or tablets).

65% of respondents utilize their ISP provided router and 83% of responses indicate that this device acts as an "all-in-one" router/switch/wireless access point. This means that a company such as Verizon, Cox, or AT&T supplies the hardware and associated software to control access to and from the internet, route all traffic, and allow wireless connection to the internet. This is an indicator that the majority of respondents do not take the time to procure and configure a more feature-rich router/firewall and/or network segmentation and simply utilize the easiest solution available. The easiest solution from the ISP (and most heavily marketed to customers) is to use the provided router/access point. Although this is not itself an indication of poor security controls, ISP provided equipment is inherently limited in customization because you are "renting" the device. Additionally, the availability of software or firmware updates may be transparent to you, which could either mean that the ISP is taking care of that, or nobody is. Either way, this element of security would be out of your control and thus create an additional vulnerability in your home network.

Only one respondent indicated that their wireless network does not have a password. This is by far the most basic preventative security measure that an individual can take to protect their wireless network, and almost all devices come pre-configured with a password set by default so this statistic is not surprising. Unfortunately, 50% of respondents did not change the default wireless password and also failed to change the default administrative credentials to their router. Utilizing the default credentials to both wireless access points and administrative accounts provides a false sense of security and indicates an extremely weak security posture overall. The most fundamental security control is to change default credentials and put in place strong

passwords and enable multi-factor authentication when available. Additionally, enabling the most up-to-date wireless encryption is important, and over 50% of respondents were unsure what version of encryption they were using. This can easily be configured by logging into the wireless access point and selecting at least WPA2 or higher.

Another important security control is to keep hardware and software updated with the manufacturer's latest patches. This ensures that any security vulnerabilities, bugs, or exploits are removed and cyber attackers cannot gain backdoor access to the network. Since most respondents indicated that they are using an "all-in-one" router/wireless access point, security updates should be easily accomplished by logging into the device and looking for the "check for updates" tab. 75% of respondents indicated that they are either not sure how to do this, or have never done this, or have simply forgotten how.

Network segmentation ensures that even if a cyber attacker gains access into the network through an insecure device or security control, they will be unable to move laterally into more important devices such as personal computers or servers. 55% of respondents indicated that they do not have any network segmentation, which is typically accomplished through different LANs or VLANs. 60% of respondents were also unaware if they had a firewall running, which is the first line of defense against rogue access to the network and also used to provide access control between LANs. A properly configured firewall typically does not allow any access from outside the network, but allows devices inside the network to reach out to the public internet. Additionally, the firewall would also allow a management device to access the IoT LAN/VLAN but would restrict any IoT devices from accessing any other part of the network, confining them to a limited access box that can only access the internet.

There were several advanced network security questions that became available if the respondent selected a certain response on an earlier survey question. Only 12 respondents reached these questions, which went a bit further in depth into network segmentation techniques. 66% of these respondents indicated they utilize a Guest Wi-Fi network, but only 33% utilize a separate network for IoT devices. 66% also indicated that they do not use firewall rules to restrict access between LANs and also do not have any VLANs configured.

The results of this survey indicate that the majority of home networks do not adhere to the most basic network security controls and improvements can be made immediately. Individuals should take basic precautions to change default credentials, keep their devices up-to-date, and limit access to privileged administrative accounts. Additionally, advanced network segmentation techniques such as utilizing a Guest WiFi network and implementing VLAN segregation could provide even better security in depth should an attacker gain access to the network.

Secure Home Network Architecture Diagram

Appendix B showcases the Secure Home Network Architecture diagram which takes into consideration guidance from NIST, CISA, and the NSA. First, a dedicated router/firewall is in place with hardened rules to block all traffic emerging from outside the network. This ensures that only authorized traffic that was initiated by a device on the network would be able to reach the internet and break the firewall. I setup a pfSense firewall/router which is an open-source software based on FreeBSD. This software allows for advanced customization and utilization of packages to monitor traffic and review logs. There is only one approved method to enter the home network from outside in the public internet and bypass the firewall, and this is by using a

private VPN. In my case, I setup a Wireguard VPN server on my router which is an advanced encryption technology that provides a secure UDP tunnel via asymmetric encryption between an end point device (laptop or cell phone) and the home network. A device configured to utilize this private VPN would appear as if its IP address is inside the home network despite physically being located outside of the home.

From a network segmentation perspective, there are 3 physical LANs each with their own IP subnet range. One LAN is dedicated to a network attached storage (NAS) device which stores backup files for important devices on the network, including photos, contacts, and documents. The next LAN is dedicated to a trusted wireless access point for authorized devices such as personal computers and cell phones. Finally, the last LAN is setup for the 16-port switch, which has a combination of servers and IoT devices connected. To further segment this switch, some ports are configured to provide VLAN tagging, which provides logical segmentation of a physical device. This essentially creates a fourth subnet (VLAN 20) within the home network that is dedicated solely to guest WiFi and IoT devices, such as Ring Home Security, Nest Thermostat, Roku TV, etc. Firewall rules prevent any devices originating in VLAN 20 from communicating with devices in any other subnet. Additionally, only certain approved devices are able to access the NAS subnet.

The Secure Home Network Architecture Diagram provides for layered access which ensures that even rogue access would be unable to cause significant harm or loss of digital property; IoT devices would only have access to other IoT devices. The most important element in this diagram is a strong firewall with verified rules which prevent unintended access to sensitive devices. Open-source firewall software such as pfSense provides for professional-grade customization and can be run on a variety of low powered computers without any cost.

Community driven upgrades and response to vulnerabilities ensures exploits are removed expeditiously. Alternatively, consumer routers from Netgear or Linksys can utilize custom Operating Systems such as OpenWRT or DDWRT which provide similar levels of customization and control without the need to procure another physical device. Once the basic security controls are verified and in place, advanced users should take steps to segment their network by using multiple LANs or VLANs to compartmentalize devices into risk categories and provide least-access where possible.

Secure Home Network Best Practices Guidance

Appendix C provides the top-ten most important "best practices" that individuals should review and implement within their own home networks immediately. This guidance is segmented into Basic, Intermediate, and Advanced categories and provides pointed areas to consider when assessing home network security. These controls should be implemented in order from basic to advanced, since some controls build on those completed earlier.

Items within the basic category can be completed with no additional hardware/software and center mostly around ensuring access control to devices is limited to those with a "need-to-know". Default, or vendor supplied, credentials are an extremely common tool that hackers use to gain access to network devices, so proper housekeeping to simply change these passwords can stop the vast majority of attacks (Cybersecurity and Infrastructure Security Agency, 2022a). Along with this advice, re-use of the same "complex" administrative password can be just as bad as default credentials, since this provides an attacker with the ability to brute force access to one weak device and then have access to everything else on the network. Instead, individuals should

utilize a password manager to avoid the hassle of memorizing and tracking numerous complex passwords. Ensure multi-factor authentication is enabled wherever possible.

Intermediate category guidance may require some additional hardware or advanced networking knowledge, such as a dedicated firewall and the understanding of implementing firewall rules. Although this step may seem technically daunting at first, a strong firewall provides exponential security improvements to a home network since it is literally the device that resides between the hostile public internet and your internal network. Individuals who complete all basic guidance should take time and effort to research firewall implementation by either purchasing a router/firewall combination or installing an open-source firewall software such as pfSense Community Edition or OPNSense onto a dedicated computer.

Finally, the advanced guidance is aimed at those who have gained advanced networking knowledge and are able to purchase additional network hardware that is capable of logical network separation. This usually requires dedicated VLAN capable access points or a layer 3 network switch. Additionally, network segmentation requires router/firewall configuration so completion of the Intermediate guidance must be accomplished before moving onto these advanced tips. By reaching this stage in securing the home network, individuals should be confident that access to their devices is secure, the weakest devices are not even on the same network as management/administrative devices, and any suspicious activity will automatically alert the network administrator that something strange is happening.

Recommendations & Project Results

Local Level Implications & Recommendations

This project demonstrates that it will not be long before every household in the U.S. has broadband internet access, yet the majority of households are still not implementing basic security controls which provides ripe targets for cyber security attacks. The survey results provided in Appendix A show that individuals should review the best-practices from Appendix C and immediately conduct a security audit of their home network. This would include basic steps such as obtaining administrative access to the router/wireless access point and replacing default credentials with a secure username/password combination. Additionally, individuals should maintain the latest versions of software/firmware on devices and periodically check to enforce this standard. Finally, the network architecture in Appendix B should be implemented wherever possible to provide another layer of security for home networks. Although Appendix B may require some advanced networking knowledge, the benefit of segmenting similar devices to their own network is crucially important as more devices become internet enabled without commensurate security considerations. Unfortunately, this project indicates that IoT devices are severely lacking in security updates, have been the source of major cyber security attacks, and pose a security risk that may provide cyber criminals with unauthorized access to the home network. Therefore, it is recommended that these devices be configured on their own LAN or VLAN as soon as possible once basic security controls are completed.

Local Level Issues Identified

There were very minor local issues that emerged as a result of this project, and mainly centered around device-specific configuration procedures. Appendix B and C recommend

utilizing VLANs to segment IoT devices, but it may be challenging for individuals to actually complete this configuration. I utilized an inexpensive TP-Link “smart” switch, but the process to configure a VLAN required more than just the basic user manual to control and also required router-level configuration to ensure devices with the same VLAN tag can communicate and traffic is routed properly. This is explained at a basic level in the TP-Link documentation, but is not as obvious as it should be given the significance of the configuration required. Therefore, VLAN configuration on inexpensive devices may be more challenging than advertised and should be approached with caution. Fortunately, many routers have default setup for a Guest Wi-Fi network which essentially acts as a VLAN and segments traffic from the main wireless network. If VLAN configuration at the switch/router level becomes too difficult, individuals may alternatively utilize this Guest Wi-Fi network as an impromptu IoT network and obtain the same benefits of network segmentation as explained previously.

Similar to VLAN configuration, wireless access point and router configuration can be quite complex and misconfigured devices could prevent internet access to the network. Fortunately, the default configuration settings on most consumer devices provide the best combination of security and control, so there may not be significant manual setups required. However, pfSense can be advanced once certain settings are enabled so there must be careful consideration and a backup plan in place should one decide to go this custom software route. There is a strong community on the pfSense forums that is willing to support user-submitted questions, and similar communities can be found around other open-source projects such as OpenWRT or DD-WRT. I encourage individuals to proceed with caution when making configuration changes, but offer reassurance that the community support is extremely beneficial should problems arise.

Project Implications Beyond Local Level

Cybersecurity within the corporate environment is becoming increasingly complex and the need to provide tighter security controls is necessary. There also appears to be a dichotomy in our modern business world, where the desire to advance cloud, AI, and IoT technology is met without the requisite cybersecurity posture. “Digitally enhanced connectivity is the mother of all double-edged swords. It opens us to unprecedented levels of opportunity and exposes us to equally unprecedented levels of risk” (Rothrock, 2018). According to a cyber risk report, 88% of C-level executives consider digital trends in these areas as relevant to their business, yet 83% also stated that their own company is not prepared to handle digital threats (MunichRE, 2022). This paper provides the Engineering Management field with the knowledge necessary to start considering cybersecurity within their corporate strategy and risk management framework to ensure that our increasingly digital world is adequately prepared to handle modern threats. Although this paper was aimed at home network security, the concepts are modeled after enterprise infrastructure security practices which can easily be scaled to fit any size home or business. After reviewing this project, individuals should be thinking about cybersecurity as not just a philosophy, but foundational knowledge that must be considered in their daily lives. By providing this foundational knowledge to the Engineering Management field, we can all become better stewards of the data that we want to protect, or are tasked with protecting from shareholders and the public.

References

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K. and Zhou, Y., 2017. Understanding the Mirai Botnet. *Proceedings of the 26th USENIX Security Symposium*,.

Cybersecurity and Infrastructure Security Agency, 2022a. *Weak Security Controls and Practices Routinely Exploited for Initial Access*. Joint Cybersecurity Advisory. [online] Available at: https://www.cisa.gov/uscert/ncas/alerts/aa22-137a.

Cybersecurity and Infrastructure Security Agency, 2022b. *Layering Network Security Through Segmentation*.

Davis, B., Mason, J. and Anwar, M., 2020. Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study. *IEEE Internet of Things Journal*, 7(10), pp.10102-10110.

Kumar, D., Shen, K., Case, B., Garg, D., Alperovich, G., Kuznetsov, D., Gupta, R. and Durumeric, Z., 2019. All Things Considered: An Analysis of IoT Devices on Home Networks. *Proceedings of the 28th USENIX Security Symposium*,.

Martin, M., 2021. *Computer and Internet Use in the United States: 2018*. American Community Survey Reports. [online] United States Census Bureau. Available at: https://www.census.gov/content/dam/Census/library/publications/2021/acs/acs-49.pdf.

Munich RE, 2022. *Global Cyber Risk and Insurance Survey 2022*.

National Institute of Standards and Technology, 2020. *Security and Privacy Controls for Information Systems and Organizations*. NIST Special Publication 800-53. [online] Available at: https://doi.org/10.6028/NIST.SP.800-53r5.

National Security Agency, 2022. *Network Infrastructure Security Guidance, PP-22-0266*. Cybersecurity Directorate.

Rose, S., Borchert, O., Mitchell, S. and Connelly, S., 2020. *Zero Trust Architecture*. NIST Special Publication 800-207. [online] Available at: https://doi.org/10.6028/NIST.SP.800-207.

Rothrock, R., 2018. *Digital Resilience: Is Your Company Ready for the Next Cyber Threat?*. New York: American Management Association.

U.S. Department of Homeland Security, 2016. *Threat to Network Infrastructure Devices, Binding Operational Directive BOD-16-02*. Washington, DC.

U.S. Department of Homeland Security, 2017. *A Guide to Securing Networks for Wi-Fi (IEEE 802.11 Family)*. U.S. Department of Homeland Security Cybersecurity Engineering.

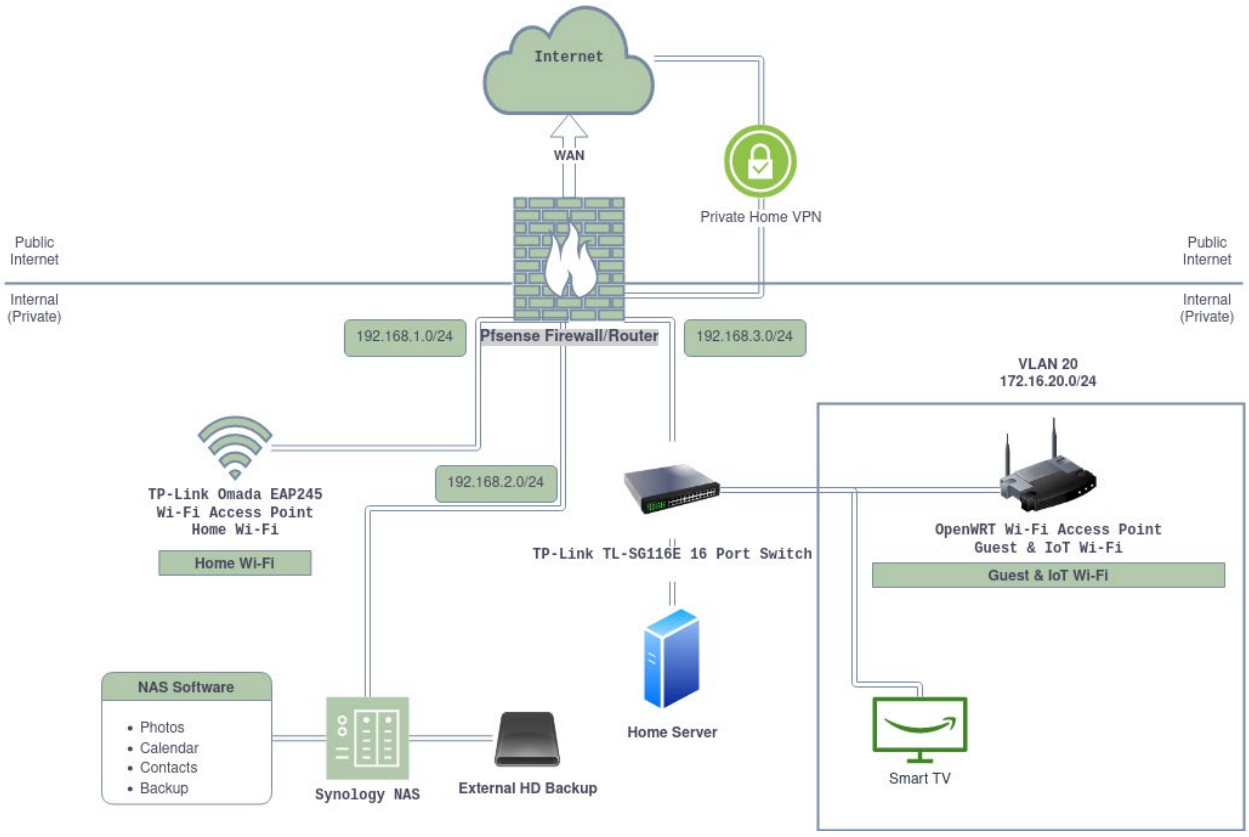
U.S. National Security Agency, 2018. *Best Practices for Keeping Your Home Network Secure*.

Zscaler ThreatLabZ, 2020. *IoT in the Enterprise: Shadow IoT Emerges as Security Threat*.

Appendices

Appendix A: Home Network Security Survey Results

Appendix B: Secure Home Network Architecture Diagram



Appendix C: Secure Home Network Best Practices Guidance

BASIC

1. **Administrative Access**: Obtain administrative access to all network routers, switches, and access points. This is often as simple as consulting the manufacturer's manual for the device. However, in most cases just type the IP Address of the device into a browser search bar. You will need this to both ensure these devices are properly secured and kept up-to-date.
2. **Default (Vendor Supplied) Credentials**: Change the default, or vendor supplied, username and passwords to all network devices including routers, switches, access points, computers, servers, Wi-Fi networks, and IoT devices.
3. **Password Manager**: Generate random, complex passwords using a password manager such as Bitwarden or Keepass. This also serves as a secure "vault" to store all passwords.
4. **Multi-Factor Authentication (MFA)**: Enable Multi-Factor authentication wherever possible, including access to the password manager and devices. NOTE: DO NOT RE-USE THE SAME ADMIN PASSWORD ACROSS ALL DEVICES; ENSURE EACH DEVICE HAS A UNIQUE PASSWORD.
5. **Keep Devices Updated**: Login to each device and ensure the software/firmware is running the latest version (consult the manufacturer's website to validate the version number if not listed on the device).
6. **WiFi Encryption**: Ensure your Wi-Fi network is setup to use Wireless Protected Access 2 (WPA2) at a minimum along with a strong, unique password.

INTERMEDIATE

7. **Firewall**: Ensure your home network is protected by a firewall which includes Network Address Translation (NAT) to segment your home network from the public internet. Disable all external access to the firewall. If external access is required, setup a secure VPN tunnel using OpenVPN or Wireguard.
8. **Disable Remote Admin Access**: Disable remote administration of network devices & ensure Universal Plug-n-Play (UPnP) is turned off on all devices. Conduct all network admin either within your network or using a VPN. UPnP can allow individual devices to open ports in the firewall without your knowledge. As indicated by tip #4, external access across the firewall should be disabled by default and no ports should be opened without advanced knowledge.

ADVANCED

9. **Network Segmentation**: Practice network segmentation by separating critical devices on your network from guest or IoT devices. Ideally, place all IoT devices on their own LAN or VLAN and use firewall rules to restrict their LAN/VLAN from accessing any other segments of your network.

10. **Logs**: Implement log collection and retention policies within your network so that suspicious activity can generate alerts and data is available for review. Utilize a security information and event management (SIEM) tool for automation.

Biographical Data

Robert E. Litts received the B.S. Electrical and Computer Engineering from the United States Coast Guard (USCG) Academy, New London, CT in 2013 and M.S. Electrical and Computer Engineering from Old Dominion University in 2021. Robert completed 6 years at sea aboard U.S. Coast Guard Cutter WAESCHE (WMSL 751) in Alameda, CA, USS McCAMPBELL (DDG 85) in Yokosuka, Japan and U.S. Coast Guard Cutter DEPENDABLE in Virginia Beach, VA. He is currently an active-duty Lieutenant Commander at the Command, Control, Communications, Computers, Cyber Intelligence Service Center (C5ISC) in Portsmouth, VA. His current job is the Communications Product Line – Short Range Systems Branch Chief, responsible for VHF/UHF communications and the shore-based Rescue 21 system for the USCG. Robert and his wife Kristy have a 1-year-old son Charlie and are expecting their second child in early March 2023.