Home Network Security & Monitoring

Benjamin Rader
IUPUI
Purdue School of Engineering & Technology

1 Introduction & Literature Overview

Most consumers and even advanced IT workers perceive the home network as a less appetizing target to the average attacker. This results in a lack of focus on home network threats and vulnerabilities because the money simply is not there. The dilemma of home network security exists since most attacks are not reported with the average home user not knowing the first thing about cyber attacks, most home users do not have visibility into their networks, and most home network attacks are simply not of interest to the general public.

1.1 Recent Home Network Threats

Networking is one of the most complex parts of cybersecurity. Most users do not know where to begin or even what to search online to begin protecting their home networks [8]. The Internet itself was designed to solve complex issues with distributed computing and communication that relies on a relatively narrow set of protocols. Most businesses have a difficult time with information technology and networking problems because of the complexities of various heterogenous systems having to operate in very unique ways. On the contrary, most home networks do not necessitate complex protocols, unique topologies, or expensive network hardware to operate. Implementing security in different-sized companies can reveal a dynamic that applies to home networks. Anecdotes from the corporate environment suggest that security is easiest to implement in the smallest and largest businesses but hard to pull off in small to medium-sized enterprises. This is explained by the fact that businesses like the Fortune 100 have refined security processes and architectures which makes them more secure, and the smallest businesses have networks that are small enough so that coverage of weaknesses is straightforward with simple approaches. Although small businesses may potentially have good security on average, research conducted in this paper suggests that home networks specifically have unaddressed wide-reaching weaknesses. These weaknesses and threats do not include other forms of human error like the fact that the most common password is still ”12345” [16]. The real problem originates at the home and personal front.

Despite much work, research, and legislation for cybersecurity with businesses, more work needs to be done for home networks which, on a practical level, operate like small enterprises. When breaches occur at people’s companies, most people are not motivated to make behavioral and personal security changes [10]. Findings in recent years also show that individuals are just as harmed by these cyberattacks as businesses that are affected. It is estimated that 42% of the total losses experienced due to cyber attacks on U.S. municipalities are losses on the individual [33]. In other words, the average home user is surely being harmed by cybercrime, and yet, there is a lack of pragmatic solutions for home networks. ”There is no lack of technological means and advice to ensure secure operation of systems, but it is usually people with a technical background who define these concepts only/mainly based on technical reasoning. The actual users are rarely figured in, which increases the probability that security measures are not practical. [5]” Although there are not a lot of stats on actual attacks against home networks, conducted pentests on home network topologies show gold mines of vulnerabilities and weaknesses [29]. There are other avenues of solutions that would not focus on the user, but rather on home network hardware manufacturers such as home routers. Technical work at the manufacturer level could do the trick but supply chain and business problems can be more difficult to solve than securing a home network with third-party tools and solutions. A lot of work would need to be done to change the business and supply chain problems that surround creating inherently secure home networks as they are deployed by Internet Service Providers (ISPs) [19]. Yet, even the third-party approach to securing a home network could use a more holistic framework. A lot of the research is quite segmented [2].

1.1.1 Internet of (Vulnerable) Things - IoT

The growth of Internet of Things (IoT) devices is perhaps one of the most pivotal changes for home networks. By 2030, the growth will have doubled from 2022 [35]. The risk of not getting these various IoT products out into the market is seen as larger than the risk of developing insecure IoT devices. Furthermore, domestic network architectures do not seem to be on a lot of the IoT device makers’ minds [29]. Consumers love the innovation and solutions that come out of IoT, but they are not aware of the potential misuse or weaknesses of such systems. California even made an IoT law (California’s SB-327 IoT law) that prohibited password defaults and other poor password security practices for these devices. Some of the bad practices simply happen because of operational misalignment where the product development team is not interacting enough with the security engineers. Gafgyt is an example of an IoT botnet that has targeted 32,000 SOHO (Small office/home office) routers which technically can qualify as IoT devices. This exploit was used to do a DDoS (distributed denial of service) attack on gaming servers [6]. These attacks tend to be specific to the device, but they are simple to pull off with a bit of tinkering or investigation with the IoT device firmware. Most IoT devices are unencrypted - 98% of them in fact and 57% of IoT devices have medium to high severity vulnerabilities on them. That does not include all of the likely unknown vulnerabilities. Most of the attacks that have been observed occur on security cameras and printers. However, research on IoT in the healthcare industry shows that most hospitals or healthcare organizations do not handle IoT security seriously. One of HIPAA's (Health Insurance Portability and Accountability Act) defining requirements is that certain networks are segmented which can be done with VLANs (virtual local area networks). These are basic logical separations of networks that make it difficult for attackers to pivot across network devices if one is compromised. Data shows that most of the healthcare industry does not segment medical IoT devices from other devices such as personal computers on the networks [6]. The same idea goes for IoT devices at home. If the devices are not segmented, then attackers can easily find vulnerabilities, laterally move in the network, or even creates DoS (denial of service) attacks using the IoT devices so that none of the devices can use the network. It does not take long for attackers to find these devices and exploit them either. Studies show that IoT devices can be hacked just minutes after they're connected [16]" Segmentation is the best way to go because it ignores the individual IoT device implementations. Trying to create solutions for every IoT device would be a huge lift for society. Simply segmenting devices on the networks stop attackers from doing anything that can damage home network operations.

1.1.2 Remote Work

Work-life will never be the same since the Coronavirus pandemic. Remote work is now the norm. Some argue that cybersecurity helped make this possible [8], and although this might be true every great development can come with its issues. "More than half (60%) of consumers reported an increased concern for data safety due to the COVID-19 pandemic [16]" Users noticed that moving all of their work to their homes creates a new attack surface practically overnight, and organizations had to follow suit. Setups and remote-enabling systems were deployed quickly, and approaches differed from organization to organization just as much as each user's "cyber hygiene" [5]. Studies revealed that most remote workers associated remote work with ample benefits such as flexibility and time-saving efficiencies, despite the consequences of decreased social interactions. Cyberattacks increased and changed to match the tone of the pandemic, but some teleworkers reported that they "did not experience cyberattacks in unprecedented volume [25]." Incidents, by nature, may not be reported in their entirety to the public, but data shows that many cyber attacks during Covid relied on weaknesses that presented themselves with remote work changes. This manifested itself in the form of increased ransomware attacks which leveraged RDP (remote desktop protocol) connections and phishing [13]. Users tend to use personal accounts a lot for work, and since some organizations do not require VPN (virtual private network) usage to tunnel traffic to the internal network, then most phishing attempts, malware, and other attacks can bypass detection and security controls.

1.1.3 LAN & WLAN Vulnerabilities

In terms, of non-application protocol-based attacks, Wi-Fi is generally still an issue since most home networks do not solely use ethernet. Using WPA3 or forms of hardening can fix these issues [1]. Most home networks rely on wifi now, but SOHO routers are still generally attached to the home network modem. Most small businesses don't configure their routers correctly either when they don't have a network team [30]. In other words, routers will be an issue until solutions are developed to cover the large risk surface. Studies show that most home routers and WLAN networks are prone to various attacks: "Deauthentication, Dictionary and Bruteforcing Attack, ARP Poisoning, etc [4]." A 2020 study on home router security from a German research group showed that even some of the more secure routers have around 20 critical CVEs (common vulnerability enumeration) and around 350 high-rated CVEs. Practically, all home routers are easy to exploit [37].

1.2 Research Goals - A Solution for Home Users

It has been shown in research that home networks have value to malicious actors on the Internet. Moreover, home networks generally have poor security and a lack of visibility which also makes it hard to obtain data showing that home networks are being consistently attacked daily. This project attempts to implement a solution to home network visibility which is the first step towards better home network security. In the corporate world of security, visibility and "mapping" is vital to understanding the network and where to direct security efforts. Without a fundamental understanding or ontology of the home network, there will always be low-hanging fruit for the average hacker. Various methods for home network security monitoring will be presented which are supported by research and experience in enterprise security operations.

2 Implementation

Network security monitoring is an area of cybersecurity that requires more curation of knowledge and methods. Soon after performing search queries on the subject, one will only find super technical research or biased articles from network device manufacturers. The language used to describe such methods and systems is also too technical for the average home user. There are only a few official or professional resources for network security monitoring that are not trying to sell the reader. This problem also roots itself in the problem of business is more of a focus than home networks, and so one arrives at a crossroads where they either learn networking concepts or they do not obtain visibility into their home networks.

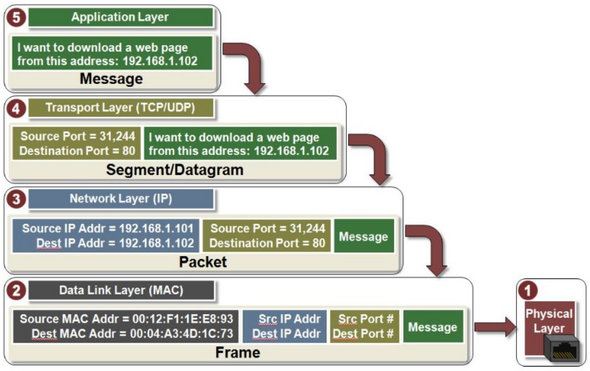

5
Application Layer
I want to download a web page from this address: 192.168.1.102
Message
4
Transport Layer (TCP/UDP)
Source Port = 31,244
Destination Port = 80
I want to download a web page from this address: 192.168.1.102
Segment/Datagram
3
Network Layer (IP)
Source IP Addr = 192.168.1.101
Dest IP Addr = 192.168.1.102
Source Port = 31,244
Destination Port = 80
Message
Packet
2
Data Link Layer (MAC)
Source MAC Addr = 00:12:F1:1E:E8:93
Dest MAC Addr = 00:04:A3:4D:1C:73
Src IP Addr
Dest IP Addr
Src Port #
Dest Port #
Message
Frame
1
Physical Layer

Fig. 1. 5-Layer TCP/IP model showing the encapsulation of data as various headers are appended in the transmission process over the internet.

2.1 TCP/IP Model & How the Internet Works

The best way to understand difficult concepts may be to use a ”mental model” for the concept. The most prevalent conceptual models in the networking world are the OSI (Open Systems Interconnection) model and the 5-layer TCP/IP (Transmission Control Protocol/Internet Protocol) model. In experience, most argue that the TCP/IP model is the most sensible model for applying consistently to realistic networking problems. The process of ”data encapsulation” is visualized in Figure 1. As data leaves an application or operating system (Layer 5), it is formed into segments or datagrams which allow the data to retain its shape and usability once it arrives at the sender (Layer 4). In Layer 3, the data arrives at the network interface of the sender where IP addresses of the sender and receiver are appended to packets or pieces of the data segments from layer 4. These packets now travel separately over various routers and switches, while also crossing back and forth various ISP networks and WANs (wide area networks). Layer 2 involves MAC addresses and usually switches or wireless transmissions. Layer 1 is the physical medium that the data travels on such as wires of over-the-air as a wireless signal. Soon enough, the data is decapsulated at the receiver and can be used by some applications. This is how all networking works, and the TCP/IP model allows people to frame various network problems in ways that are easy to understand. In the case of home network monitoring, packets and frames (layer 2) will be monitored at layers 2 and 3 in a home network LAN (local area network) or WLAN [20] [12].

2.2 Home Network Monitoring Methods

All monitoring will be done at layers 2 and 3 of the TCP/IP model. In layman’s terms, this means that packets and frames will be observed which are pieces of data that have IP addresses (layer 3) or MAC addresses (layer 2). Routers operate at layer 3 of the model and use IP addresses whereas switches practically operate with MAC (media access control) addresses which are installed into devices at manufacture time. Wireless networks also have MAC addresses involved and operate in a similar manner. However, WLAN is easy to monitor because over-the-air traffic can easily be sniffed. Methods for monitoring ethernet traffic at various points in the network will be reviewed and tested.

2.2.1 *Ways to Passively Monitor Networks*

There numerous ways to monitor a network in an enterprise setting, but the home network arguably has **5 methods**:

1) SPAN (Switch Port Analyzer) / Mirrored Ports
2) Network/LAN Taps
3) Switch/Router Log Dumping (Netflow or sFlow)
4) Passive Wireless Sniffing
5) **ARP Cache Poisoning / ARP Spoofing**

All of these methods passively observe network traffic. Therefore, the network topology is likely to be paramount in the effectiveness of the monitoring method. In other words, the traffic has to pass by the viewer for it to be seen. This dynamic is equivalent to a man-in-the-middle (MITM) attack. Switch port analyzers or mirrored ports duplicate the traffic which can be directed using an ethernet cable to a machine that will ingest and do analysis on the incoming packets. Local area network taps are the epitome of man-in-the-middle methods. Taps are put between two network cables, and the traffic is duplicated or observed via. a 3rd cable. Log dumping or Netflow requires a switch or router to have storage that holds all of the observed traffic on it, which is sent to an external machine over the internet or other means to be analyzed. The method which is tested in this project involves ARP (address resolution protocol) poisoning or ARP spoofing (equivalent meaning)BHIS) [27] [14] [32] [18].

2.2.2 *SIEMs Mentioned in Research*

Various SIEMs (Security Information & Event Managment) and IDS (intrusion detection systems) were mentioned throughout research such as Suricata, Snort, Zeek/Bro, Security Onion, and the ELK stack (Elasticsearch, Logstash, KQL). These are not as important as setting up network monitoring, but each have their strengths and weaknesses is what they can be used to detect. Research should be done to determine what sort of security detection engineering stack should be used for a home network. It is apparent that advanced attacks require DNS (domain name system) or website level analysis for detection. However, even these sorts of attacks require the primary step of setting up ingestion and monitoring of network traffic [23] [7] [21].

2.3 ARP Spoofing for Monitoring

One of the most unorthodox methods for network security monitoring is to use ARP spoofing to redirect network traffic to a machine that will be used for analysis. ARP is a protocol that is used at Layer 2 of the TCP/IP model. It allows devices that operate at Layer 3 to figure out the MAC addresses of devices on the same LAN. The process goes as such. Host A wants to communicate with Host A, but it only has its IP address and not its MAC address. Host A could be a personal computer and Host B could be the gateway router, and there is a switch (layer 2) between them. Host A sends out an ARP request asking for the device with the right IP address to give its MAC address to it. The switch forwards this request to every attached device. All

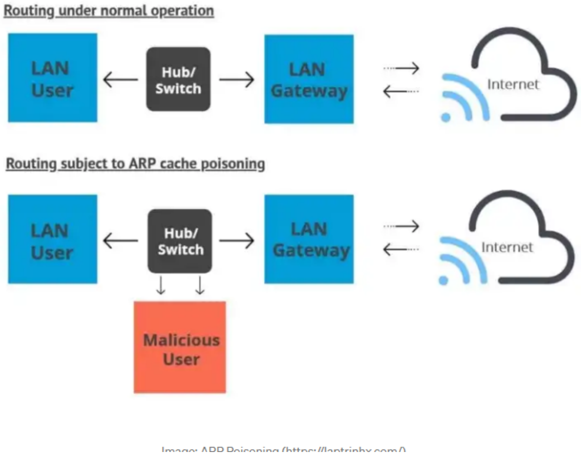
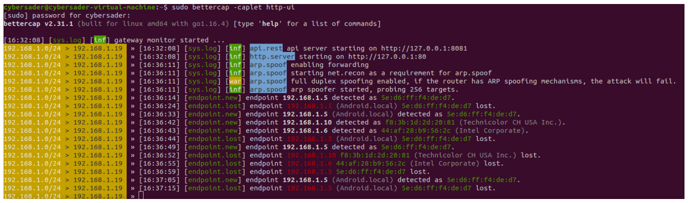


Image: ARP Poisoning (https://laptrinhx.com/)

Fig. 2. Diagram of address resolution protocol cache poisoning at Layer 2 of the TCP/IP model.

operating systems maintain this sort of table with IP and MAC addresses. The switch has a table with MAC addresses and and the ports that those devices are plugged into on the switch device. However, if a malicious actor wants to trick all other devices to send traffic to it, all the device has to do use ARP to tell all the other devices that it has the MAC address of the gateway router. Then, this malicious device forwards all of the gathered traffic to the gateway router. The device also has to trick the gateway router to send it all traffic for monitoring to see incoming and outgoing traffic as shown in Figure 2 [7] [36].

2.3.1 *Bettercap using Ubuntu 20.04*

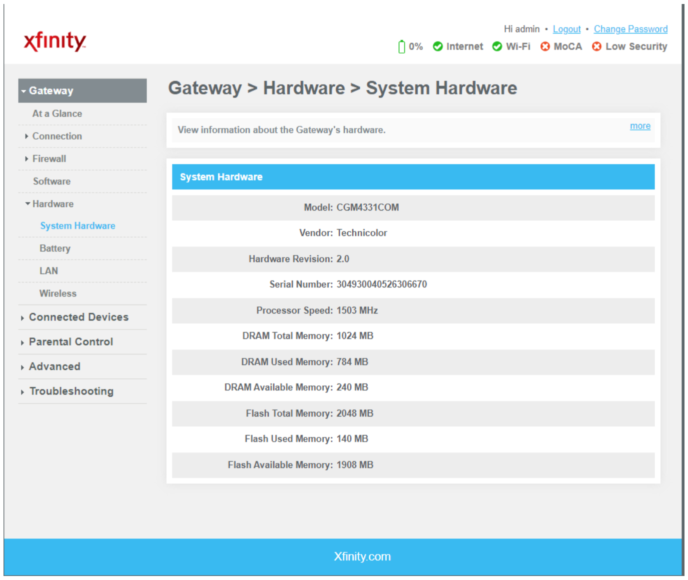


```
cybersader@cybersader-virtual-machine:~$ sudo bettercap -caplet http-ui
[sudo] password for cybersader:
bettercap v2.31.1 (built for linux amd64 with go1.16.4) [type 'help' for a list of commands]

[16:32:08] [sys.log] [inf] gateway monitor started ...
192.168.1.0/24 > 192.168.1.19  » [16:32:08] [sys.log] [inf] api.rest api server starting on http://127.0.0.1:8081
192.168.1.0/24 > 192.168.1.19  » [16:32:08] [sys.log] [inf] http.server starting on http://127.0.0.1:80
192.168.1.0/24 > 192.168.1.19  » [16:36:11] [sys.log] [inf] arp.spoof enabling forwarding
192.168.1.0/24 > 192.168.1.19  » [16:36:11] [sys.log] [inf] arp.spoof starting net.recon as a requirement for arp.spoof
192.168.1.0/24 > 192.168.1.19  » [16:36:11] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechanisms, the attack will fail.
192.168.1.0/24 > 192.168.1.19  » [16:36:11] [sys.log] [inf] arp.spoof arp spoofer started, probing 256 targets.
192.168.1.0/24 > 192.168.1.19  » [16:36:14] [endpoint.new] endpoint 192.168.1.5 detected as 5e:d6:ff:f4:de:d7.
192.168.1.0/24 > 192.168.1.19  » [16:36:24] [endpoint.lost] endpoint 192.168.1.5 (Android.local) 5e:d6:ff:f4:de:d7 lost.
192.168.1.0/24 > 192.168.1.19  » [16:36:33] [endpoint.new] endpoint 192.168.1.5 (Android.local) detected as 5e:d6:ff:f4:de:d7.
192.168.1.0/24 > 192.168.1.19  » [16:36:42] [endpoint.new] endpoint 192.168.1.10 detected as f8:3b:1d:2d:20:81 (Technicolor CH USA Inc.).
192.168.1.0/24 > 192.168.1.19  » [16:36:43] [endpoint.new] endpoint 192.168.1.6 detected as 44:af:28:b9:56:2c (Intel Corporate).
192.168.1.0/24 > 192.168.1.19  » [16:36:44] [endpoint.lost] endpoint 192.168.1.5 (Android.local) 5e:d6:ff:f4:de:d7 lost.
192.168.1.0/24 > 192.168.1.19  » [16:36:49] [endpoint.new] endpoint 192.168.1.5 detected as 5e:d6:ff:f4:de:d7.
192.168.1.0/24 > 192.168.1.19  » [16:36:52] [endpoint.lost] endpoint 192.168.1.10 f8:3b:1d:2d:20:81 (Technicolor CH USA Inc.) lost.
192.168.1.0/24 > 192.168.1.19  » [16:36:55] [endpoint.lost] endpoint 192.168.1.6 44:af:28:b9:56:2c (Intel Corporate) lost.
192.168.1.0/24 > 192.168.1.19  » [16:36:59] [endpoint.lost] endpoint 192.168.1.5 5e:d6:ff:f4:de:d7 lost.
192.168.1.0/24 > 192.168.1.19  » [16:37:05] [endpoint.new] endpoint 192.168.1.5 (Android.local) detected as 5e:d6:ff:f4:de:d7.
192.168.1.0/24 > 192.168.1.19  » [16:37:15] [endpoint.lost] endpoint 192.168.1.5 (Android.local) 5e:d6:ff:f4:de:d7 lost.
192.168.1.0/24 > 192.168.1.19  » 
```

Fig. 3. Bettercap ineffectively ARP spoofing in an Ubuntu 20.04 VM inside of VMware workstation 17. The red lines are failures.

ARP spoofing is simple to do with Linux systems such as Ubuntu 18 and 20.04. Bettercap is the most popular application for ARP spoofing traffic, and it is the same tool that is used by the penetration testing firm that streamed a tutorial on networking monitoring with Bettercap. VMware Workstation 17 is used to load up an Ubuntu 20.04 virtual machine, then steps are taken to install Bettercap along with it various libraries and manual symbolic links for the Linux file system. Bettercap is the most popular because it has a graphical user interface and also allows for full duplex spoofing. The VM had to also be set in ”bridged” mode so that it had an actual attachment to the physical network and its own IP address for spoofing and redirection of traffic. Figure 3 shows Bettercap running properly, detecting the gateway, attempting to ARP spoof and actually losing out. I was not able to get ARP spoofing to work [7].



Gateway > Hardware > System Hardware

View information about the Gateway's hardware.

System Hardware

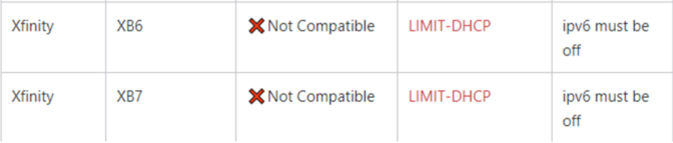
Model: CGM4331COM
Vendor: Technicolor
Hardware Revision: 2.0
Serial Number: 304930040526306670
Processor Speed: 1503 MHz
DRAM Total Memory: 1024 MB
DRAM Used Memory: 784 MB
DRAM Available Memory: 240 MB
Flash Total Memory: 2048 MB
Flash Used Memory: 140 MB
Flash Available Memory: 1908 MB

Fig. 4. Configuration and model of Xfinity router.

2.3.2 *ARP Spoofing Fails*

It was determined that I had a mesh wireless network and two different APs (access points) which could be used. I tried ARP spoofing with every possible configuration and target on the network, but to no avail. Figure 4 shows the configuration of the modem, and I also looked into the routers themselves to try doing mirrored traffic but this also failed. The question is why did it fail?

3 EVALUATION



Xfinity	XB6	✗ Not Compatible	LIMIT-DHCP	ipv6 must be off
Xfinity	XB7	✗ Not Compatible	LIMIT-DHCP	ipv6 must be off

Fig. 5. Firewalla consumer firewall (uses ARP spoofing) showing that my router makes it impossible to conduct an ARP spoofing attack (Support Team).

There exists a consumer firewall hardware called ”Firewalla” that does the same method of ARP spoofing for network monitoring, but they refer to it as ”simple mode.” The documentation for the device was thoroughly researched, and an explanation was found. Figure 5 shows a line in the ”Simple and DHCP Mode Compatibility with Routers” table for the Firewalla device. My router was listed in the Xfinity settings as the ”CGM4331COM” model, but upon further research, this is equivalent to the ”XB7” gateway listed on their website. This is shown to be incompatible with ARP spoofing with the Firewalla, so this was likely the culprit. Some devices use ARP differently or have protections. I did not have a tap, router or switch with a SPAN port, or any other device to help so this was as far as the research could go [7] [36].

3.1 Why Home Network Monitoring is Complex

Home network monitoring is complex due to the fact of network topology and the sheer variety of functionalities in routers (especially gateways for ISPs) and switches. Various network protocol implementations and setups of routers and sometimes swithces can drastically affect the setup necessary for monitoring. In the case of this project, the network topology and choice of modem made it impossible to conduct packet analysis and deeper observation into home network traffic. The placement of the monitoring device (personal computer with a VM in this case) will vary based on the method and hardware being used on the network.

3.2 Network Setup & Monitoring Strategy for Home

Since network monitoring ability is drastically affected by the modem or gateway router being used, then starting with the method is vital. If a tap is being used, then any router or setup can be used as long as the network tap is placed in a spot on the network where all traffic will pass, such as right in front of the gateway router. With ARP spoofing, the buyer should consider a gateway router that works with ARP spoofing via. a resource such as Firewalla. It is also important to note that ARP poisoning is a type of attack, but network monitoring can be used to detect other devices performing the attack. In the case of log dumping and mirrored ports on a router, then the gateway router should have the ability to do those things. Wireless sniffing is simple, but there are unique problems with trying to monitor all traffic with that approach [7].

Here is an example of some known devices utilizing various approaches:

- **Plug'n'Play ARP spoof**– Firewalla
- **Manual ARP spoof** – Run Linux with Bettercap on PC or Raspberry Pi
- **Network Taps** – throwing star LAN tap from Hak5
- **Consumer PnP Firewalls** –Ubiquiti Unifi
- **Advanced Consumer Options** – pfsense routers - Protectli vault.

4 Conclusion

My report starts by looking at literature and research that is relevant to home network security and widespread issues related to home users, remote work, IoT, and home network device vulnerabilities and exploits. It is determined that the best way to approach and solve home network security issues which are evolving with new threats, is to deploy a network monitoring solution at home which can then be used to prioritize network security problems and understand the unique characteristics of certain network configurations and topologies. Various network monitoring methods are proposed to analyze home network traffic, but the peculiar approach of ARP (address resolution protocol) spoofing is tested and evaluated using Bettercap in Ubuntu 20.04 and an Xfinity modem. Solutions and a general consumer approach are explained which can be used to setup a home network which enables for security visibility and use of a SIEM (security information & event management) system. Home network security can be improved in people put just a little bit of effort into understanding their traffic.

References

[1] *Hardening applied over a WLAN SOHO environment for mitigation of vulnerabilities*, 2018.

[2] *Cybersecurity in SMEs: The smart-home/office use case*, 2019.

[3] *Consumer Perspectives on Loss of Support for Smart Home Devices*. 6th Workshop on Technology and Consumer Protection (ConPro '22), San Francisco, CA, US, 2022.

[4] *Penetration test on home network environments: A cybersecurity case study*. Association for Computing Machinery, 2022.

[5] 2022 IEEE 31st International Symposium on Industrial Electronics (ISIE). *Cyber Security at HomeWhat Really Matters to People*, 0.

[6] Unit 42 Palo Alto. 2020 unit 42 iot threat report 2020 unit 42 iot threat report, 03 2020.

[7] BHIS. Webcast: No span port? no tap? no problem!, 07 2021.

[8] Mary Bispham, Sadie Creese, William H. Dutton, Patricia Esteve-Gonzalez, and Michael Goldsmith. Cybersecurity in working from home: An exploratory study, 08 2021.

[9] Marco Borza. Cyber security is everyone's responsibility, 03 2021.

[10] Shelby R Curtis, Jessica Rose Carre, and Daniel Nelson Jones. Consumer security behaviors and trust following a data breach. *Managerial Auditing Journal*, 33:425–435, 01 2018.

[11] Bernd Debusmann. Why remote working leaves us vulnerable to cyber-attacks. *BBC News*, 07 2021.

[12] DNSStuff. Ultimate guide to network monitoring, 05 2019.

[13] Tiberiu Georgescu. A study on how the pandemic changed the cybersecurity landscape. *Informatica Economica*, 25:42–60, 03 2021.

[14] Gigamon. Tap vs. span: Which option is right for you? — gigamon.

[15] Samuel Ho, Hope Greeson, and Umit Karabiyik. Smart home forensics: Identifying ddos attack patterns on iot devices. *Annual ADFSL Conference on Digital Forensics, Security and Law*, 01 2022.

[16] Bojan Jovanovic. Better safe than sorry: Cyber security statistics and trends for 2020, 11 2019.

[17] Kaspersky. 1 in 4 wi-fi hotspots just waiting to be hacked, kaspersky lab stats show, 05 2021.

[18] Keysight. Taps vs spans.

[19] Derek McAuley, Jiahong Chen, Tom Lodge, Richard Mortier, Stanislaw Piasecki, Diana Andreea Popescu, and Lachlan Urquhart. Human-centred home network security. 2022.

[20] Microchip. Tcp/ip five-layer software model overview - developer help, 2019.

[21] Yasir Faraj Mohammed, Paul Cronan, Brajendra Panda, and Qinghua Li. *Network-based detection and prevention system against DNS-Based attacks*. PhD thesis, 2021.

[22] Sunny Valley Networks. Best hardware firewalls for home and small business networks - sunnyvalley.io, 2022.

[23] Ikechukwu C Nwosu. *Intrustion Detection in Soho Networks using Elasticsearch SIEM*. PhD thesis, 2021.

[24] Nandita Pattnaik, Shujun Li, and Jason R.C Nurse. A survey of user perspectives on security and privacy in a home networking environment. *ACM Comput. Surv.*, 2022.

[25] Aaron Piper, Alan B. Watkins, Stephen Campbell, Uros Trnjakov, Maurice Turner, Michael K. Wicks, Robin Regnier, Aaron Wilson, Phil Langlois, and Joshua M. Franklin. Cis controls telework and small office network security guide, 202.

[26] Dimas Febriyan Priambodo, Amiruddin, and Nanang Trianto. Hardening a work from home network with wireguard and suricata. *2021 International Conference on Computer Science and Engineering (IC2SE)*, 11 2021.

[27] Profitap. Comparing network monitoring tools - tap vs. span, 05 2017.

[28] Khurram Salman. *Assessing work from home security packages vulnerabilities*. PhD thesis, 2022.

[29] Karen Seaman. *Good cybersecurity starts at home*. PhD thesis, 05 2022.

[30] Chris Selph. How soho routers and networks differ from ordinary ones, 07 2021.

[31] Serhiy Shkarlet, Anatoliy Morozov, Alexander Palagin, Dmitri Vinnikov, Nikolai Stoianov, Mark Zhelezniak, and Volodymyr Kazymyr, editors. *Architecture of Distributed Blockchain Based Intrusion Detecting System for SOHO Networks*. Mathematical Modeling and Simulation of Systems, Springer International Publishing, 2022.

[32] Viavi Solutions. Tap vs span.

[33] Rebecca Spiewak. *Overlooking the Little Guy: An Analysis of Cyber Incidents and Individual Harms*. PhD thesis, 05 2022.

[34] Smiljanic Stasha. Smart home statistics: 2021 update — policy advice, 2020.

[35] Statista. Iot: number of connected devices worldwide 2012-2025 — statista, 2012.

[36] Support Team. Router compatibility: Simple and dhcp mode, 12 2022.

[37] P. Weidenbach and J. Vom Dorp. Home router security report 2020, 2020.

[38] Jing Yang and Laura Linkeschová. *Remote working and cybersecurity in the pandemic: Research on the employee perceptions of remote work and cybersecurity in an international organisation during COVID-19*. PhD thesis, 2021.