Covid-19: Application of Machine Learning for Wireless Security during a Pandemic

Gerso Guillen[1], Jorge Campuzano[1], Adan Guadarrama[1], Joshua Dare [1]

Vahid Emamian[2], Senior IEEE Member

[1]Computer Science Department

[2]Electrical Engineering Department

St. Mary's University, San Antonio, TX

Our team has decided that we take care of the low hanging fruit when it comes to wireless network security for homes. We figured that was a good topic since most of us are at home or working from home. Taking on the default insecurities meant that we could use this project to ensure that our home network was secure and any other system that we might visit, be it a friend or family member. We planned to get a data set of all home routers that we could get our hands-on. We might target one brand name of routers or at least the most common ones. We gathered known security configurations commonly known for security issues. We then researched some ML (Machine Learning) algorithms that could help this project out. AI Machine learning will permit for quicker identification of anomalies on any given network, which will then provide us the ability to check if the router has those presets enabled and if the router is vulnerable or not. We can provide lots of relevant information and finish with some useful concrete algorithms already created.

My name is Gerso Guillen, and I am the team leader for this team. My specialty is hardware repair, desktop engineering, programming with Python, Visual Basic, Java, and C Sharp. I also have excellent communication skills as I have been in the customer service industry for banking, internet service, and retail sales for Fry's electronics. My hobby is tinkering with the raspberry pi and various microcontrollers. I also am very skilled with video and sound editing as I have the right eye for how the human eye perceives body language. I recently created a desktop for work that has only one task it has to do. It is an SMB server that allows the printer to scan files to that desktop, and it is attached to my job SharePoint, making it quite easy for us to digitize all the paper documents we get. For a law firm, that is an excellent help as paperwork is all digital due to this bridge I created. The printer company wanted to charge us thousands to license their software that does what I made with hardware, saving us some hard-cold cash.

My name is Adan Guadarrama, and I am a team member for this team. I currently work for Credit Human Federal Credit Union as an IT Specialist. I am currently studying for the Master of Science in Cyber Security from St Mary's University. I also received my bachelor's from St Mary's University in Computer Science and am proficient in multiple programming languages including Java and Python. I do not really have a lot of hobbies outside of spending as much time as I can with my family. I have worked in the IT industry for close to 14 years now, only professionally for the past 4 years. I felt that going for my master's now was the best case for me because I did not want to get lost in work and forget to do this degree especially since it is a growing field.

My name is Jorge Campuzano, and I am a team member of this team. I am originally from Torreon Coahuila, Mexico; I am 24 years old, and I recently completed my undergraduate studies as a Computer Information Systems degree. I decided to start my master's degree instead of following the regular path because it will open more doors in the future. Since I will focus 100% of the time on my job instead of having to divide my time between going back to school and keeping up with my career, I can confidently say that I like to focus on Databases, Microservices, Data-Analysis, and Testing. From my five years and a half in computer science, I have always focused my projects on related or based on those categories because they are the ones that I have always been pull towards since I was younger. In the end, I think this plan will have paid off since I now have a job as a data analyst at General Motors. My hobby is playing tennis and spending time with my family.

My name is Joshua Dare. I am a team member of this team. I am a computer engineer. I work at the Technical Support Centre in St. Mary's University as a graduate assistant. I am studying for a master's in cyber security. I am proficient in python programming language. Outside my current employment, I have worked in different sectors of the IT industry as a software developer for a company that provides service to Pension Fund Administrators and as an implementation and support staff to an EMR company. I have no prior experience working in the US. I decided to study cyber security as the next step in my career because I have a keen interest in security in general, so I decided to follow my passion.

ABSTRACT.

First, we will flesh out why we are engaged in low hanging fruit when securing a home network's default settings in the following sections. Demonstrate best-known security protocols by prominent security agents currently out on the field now. Quickly identify security configurations for home security to be as tight as possible but functional for home use. Share the

prototype of the potential applications process. Finally, explain AI algorithms used in the applications' API and the working behind each algorithm, and what each one does.

1. Introduction

Recently because of the pandemic, the world witnessed a drastic change in the way work. We go from going into the office every single day to work to just working from home altogether. Once that happened, the entire world changed in a single day. Due to this unexpected pandemic, companies figured out how to remotely operate for call centers, others for banks and credit unions. Those whose jobs solely depend on customer interaction were scrambling to make sure they chose to lay off employees because of excess due to this pandemic. Others had no idea how to handle the infrastructure changes. Unprepared for what happened, and no one prepared for how to feel the difference when it happened. One thing that suddenly got thrust to the front of the line is the following question we are about to discuss: security assessment of a wireless home network. In other words, make sure that home networks are safe for employees working from home and connecting to their company's domain.

Prime example, Credit Human Federal Credit Union in San Antonio, Texas, experienced this hard and learned many valuable lessons throughout the way. What happened to them was the following. Management granted employees VPN access to work from home to meet their duties. That started to strain out the IT department to its last limits. Then, while they were doing all they could to prepare for this, the most challenging part was with VPN's phone system. No one fully knew how the network would handle many people working from home vs. just about a few hundred or so working from home because of personal reasons. The City mandated Credit Human to figure out without knowing the full detail about what was about to happen to their network to deal with a new standard for Credit /Human's systems.

There were always security training videos and proper security practices made available throughout the company. However, when Covid-19 forced a lot of things to change, the security practice became that much harder. For example, how do you change a network password through a VPN when changing their password? What happens when someone makes the mistake of going to the wrong website while connected to a VPN? How do we stop someone who is sniffing the home network for passwords to discover the home network's password? Not that many companies are VPN ready.

These are a lot of questions that got thrust into the limelight and made IT. Information security is stressed to the limit because while it is easier to control a potential security threat inside the network, what happens when you no longer have that available to you because of how VPN traffic follows. A great solution is Wireless Sensor networks, WSN. While there are others out there, the first thing we will discuss is WSN and its capabilities.

2. Background

WSNs have distributed networks of tiny sensor nodes that extend depending on its environment from close location. They are useful for IoT, the Internet of Things, home applications, and data transmission through a wireless medium. A few things to note about this is what the security requirements are. They require authentication, trustworthiness, data freshness, confidentiality and privacy, secure localization, integrity, non-repudiation, availability, and access control. Interestingly, many security principles that WSN's use are also the same as current security practices that are becoming more commonly known for fundamentals. How do we know you are who you say you are? How do we make sure that the network is safe to access on a VPN? How can we make sure that you still have the same access you have in the office while at home?

While yes, you are secure in VPN connection to your local company or business, what about making sure not to create a strain on the network, so everybody has the same access simultaneously, and the system remains available to everybody? For example, Credit Human experienced this the hard way when its employees first started working from home. What originally started happening was that there was no sure way to know what compatible application would work with a VPN. One application was in serious question as to if it would work from a remote location as it can be done regularly in the office on the network. So, how many people could work from home during the pandemic is one of the first questions that needed to get answered before addressing security concerns were what the company was prioritizing during that time.

Rather than focus on making sure that the VPN network would still be secure working from a remote environment, the challenge became how work would become uninterrupted while working from home. Different security protocols are making sure networks are safe at home. Wi-Fi Protected Setup, WPS, is a perfect example of this. With Spectrum, there are these protocols listed on the router to use, but how many other ISPs, Internet Service Providers, also provide the same security type. More importantly, what kind of protocols are currently being utilized by all these ISPs? Are they using AES encryption or any encryptions standards? What about making sure that people in their homes have a strong password to protect their home network? If that gets compromised, where do they go from there? How do they fix it in the event their home network does get compromised?

That is why home networks that are now home offices to most that are part of the work from a home shift that lately is happening should be a priority to get such systems secured. Yes, VPN is supposed to ensure the company's network all the time; it does not always fall-proof. VPN, at times, can forget to block specific sites that are not approved by companies. If you access a malicious site via a VPN and successfully loads, you put yourself in a vulnerable position where an attacker might have a more leisurely foothold. The only fail-safe way to ensure that the company's network is protected is to ensure that the employee's home network is protected.

3. Best Practices

Attacking a home network is one of the surest ways to target a particular person to access that person's private/confidential information. Most people are most comfortable in their homes and therefore do not follow strict rules as they would in an office space, for example. Because of these reasons, they may be more vulnerable in their own homes than they would be outside.

Even when there is security in place, an attacker can still take advantage of the user's lack of understanding/proper enforcement to access their home network. And because the system is trusted, the attacker may be privy to sensitive information. For these reasons, we have decided to develop best practices and implementations to ensure that security is a home network is maintained.

3.1 Router Information

Nowadays, at home without the internet is something weird in society. Everyone needs access to the internet. People need the internet for work, school, to shop, and pretty much everything else. But because all this information is going through the network, it is vital to keep you and your family safe from intruders to your system looking to steal required information or spy on people. To have the internet, you need to have a service from an internet provider. Many companies offer this service, but among the top 3 providers in the United States are ATT, Google Fiber, and Spectrum.

All these companies offer full service. Full service means that they provide the connection, and it comes with a router. The router allows the users to connect to the internet wirelessly as long as you have the right credentials to access this router that can also be considered an access point. Each company has different routers that specific for their use with varying speeds and connections offered. Typically, out of the box routers come pre-set with a username for the network, a password for it, and some internal software that allows the router to do its job. A study made to 1000 people in the UK showed that at least 85% of the people know that their network requires protection, but only 22% of them went into the settings and made the changes necessary to meet their needs (the length of a password with which you can feel secure). When a user does not change this password, it is a security hazard because hackers already know, on average, the strength of those passwords. With time these pre-set passwords have become more secure because they introduce capital letters and numbers, but that only helps. The best way to tackle this problem will be to go into your router's settings and change the pre-set password to one of your own containing numbers, symbols, and capital and lower-case letters. Another way to go even further would be to set your router to not appear as available, and the only way to access it then will be to search for your network with the specific name manually. These are some of the measurements that you can take to protect your house from outside intruders. Another smart thing to do would be to set up a guest network.

Another way to protect yourself and your house and family would be to set up your router to activate a guest network. A guest network is a separate network created by your router using different credentials for the username and password while using the same LAN connection. This information is helpful because it contains the use of the network within the network itself. It will keep internal LAN information not visible by the exterior. You are lowering the rate of a possible future attack. Without being inside your house, they can get into the network and look at your history.

3.2 Home Entertainment Devices recommendations

Home Appliances:

Consider all your home appliances. Differentiating the “smart” ones from the others and take the following steps in securing them.

NOTE: Smart devices include: WiFi enabled printers, cars, cameras, fridges, mobile phones, computers, laptops, etc. (Read about internet of things)

Update to latest Operating system: A smart home user should always make sure that all devices on the network stay up to date. Every new OS version provides new security features that previous versions lacked. It is important to stay updated, as vendors may be putting out updates in reaction to a security vulnerability found in previous versions. On the other hand, attackers take advantage of the vulnerabilities found on older versions. Therefore, smart home users should ensure that devices auto update as soon as a new OS version is detected.

This also applies to software installed on home devices, as attackers may also exploit vulnerabilities in outdated software applications. If automatic software updates are not available in a particular application, find products that are built to constantly check software applications’ health/status. These mostly notify the user when an update is available for an application. Users must disable third party software installations and developer mode.

Install a security suite: In addition to the default security measures that may come with home devices, it is also a good idea to install an anti-virus or anti-phishing or host-based intrusion prevention, firewall, etc. as applicable to each device. Alternatively, the smart home user may get a cloud-based reputation service for detecting malware and preventing its execution.

Passwords: Users should avoid using a general password for all devices. As much as possible, passwords should be unique to each device and difficult to guess. (avoid passwords with patterns because they can easily be guessed. For example: “device1, device2, device3”)

Admin Account: A smart home user should limit admin account use solely to actions that require privilege (running updates, installations, general maintenance). The user should create a non-privileged user account for normal activity like checking emails, social media, web browsing, etc. This is because most malwares are only as powerful as the environment they are executed in. If a malware gets executed in a privileged environment, it can cause more damage to the entire system as it is not restricted by access.

Entertainment Devices: In a comprehensive security set up, home entertainment devices are not overlooked as is often the case in regular security systems. Home entertainment devices include game consoles, Blu-Ray players and video players (streaming). If not looked after, these devices can become the weak link in the smart home network. Ensure that entertainment devices are behind the home router/firewall to protect it from unauthorized access. Also use strong passwords on these devices, as most of these devices require some kind of sign up process in order to access online services or link with social media accounts.

3.3 Social Media sites

There is a personal element to every social media account. It is a convenient means to share personal information with family and friends. Every social media account is tailored to the preference of the individual that created/owns that account. The amount of information divulged, the level of activity and the security of the account, all boils down to the person in charge of the account.

It is no news that user interaction/behavior (especially on social media) is highly valuable information in today's market, as companies track users in order to appeal to customers by making targeted advertisement and luring them. These ads pop up based on the user's history of click, interactions and previous websites visited. The bad news is that if these companies have access to all this information, then so does an attacker. In order to avoid revealing sensitive information, the smart home user(s) should abide by these guidelines when access social media pages.

Authentication: The smart home user should employ the use of multi-factor authentication, when signing into social media accounts. Multi-factor authentication include secondary confirmation of a login attempt through phone or email, or even an OTP device in high security cases. These should be employed by the user whenever possible.

The smart home user(s) should disable features that allow websites or programs to remember passwords. Many sites engage password recovery questions to help users recover forgotten information. During sign-up for these questions, the smart home user(s) should purposely provide a false (but memorable) answer to these questions. This prevents an attacker from leveraging personal information to answer those questions.

Privacy policy: The smart user should pay attention to the privacy policy of the sites that are being visited. Nowadays, social media sites usually put up a summarized version of their privacy policies, with all the disclaimers that may vindicate them in the event where user information may be mishandled. For this reason, when a user is registering for a social media account, it is best to quickly look through the privacy policy of the site, checking for what information they would take and how that information may be used. This gives the individual a better understanding of how much information to divulge and what to hold back, when using that site or application.

Take precautions: Avoid posting information like home or current address, phone number, place of work, and other personal information that may be a tool for potential harassment or social engineering.

Social accounts should be set to "private" or "friends only" and opt out of anything that may expose information to search engines and third-party applications. User should avoid opening unsolicited attachments or links. Double check the identity of the sender through secondary methods, and delete the message if verification fails. When accessing social media accounts, access the website directly by its well-known web address, or search for the site in a search engine, using precise key words.

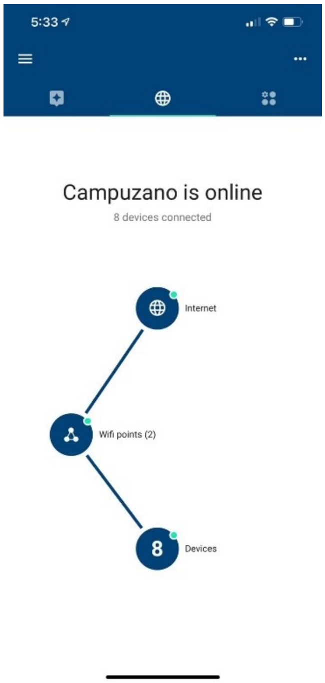
Public hotspots/WiFi: Public WiFi should be avoided. Many public places like coffee shops, hotels, aiports offer free WiFi for public consumption. These are easy targets for attackers because most of these public WiFi lack any form of encryption. This means that data is sent over the channel in plain text, unencrypted. Any attacker on the network using simple tools can easily have access to log-in credentials like username and passwords. The worse part, these tools are available for free on the internet!! It is therefore a good idea to avoid public WiFis. If the user must use public WiFis the user should employ caution and access sites that do not require sensitive information, or the user may employ VPN.

Home and Work: Exchanging information between home systems and work systems through removable media or emails may jeopardize work systems or increase the risk against them. When working away from the office, user should not use home equipment or accounts. Rather, user(s) should use organization-provided equipment and accounts. User may use a personal device if the user is connected to a remote desktop inside the corporate network. User should always use a VPN to connect to corporate networks to ensure data security.

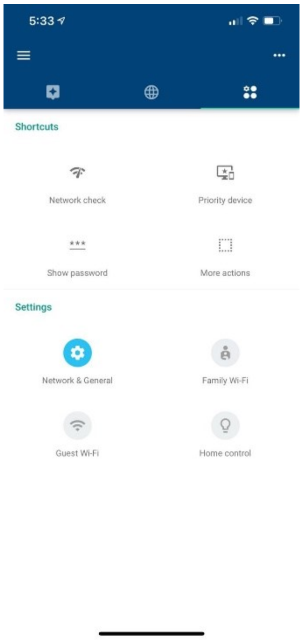
3.4 Parental Controls

Nowadays parental controls can be found in multiple devices like laptop computers, tablets, phones, routers, and even TV's. Setting this control in all your devices is important if you are trying to protect yourself and your family, especially the kids. Since there are many websites that have content that it will not be appropriate for certain ages, but most importantly because people that do not surf the web safely can get into websites that have trojan horses. This means that they ask permission to download a file that you think is safe but this file will grant them access to the webcam, the microphone and even in some cases control of your entire computer and the information that it is in it.

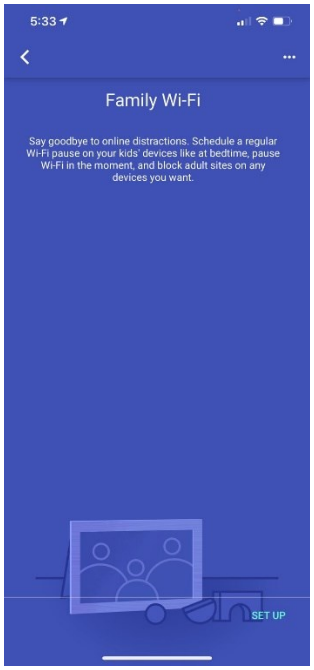
As mentioned before many devices have this feature but if you want to protect your wireless network and with this create the first wall of protection you should go ahead to the settings of your router and set it up there. In this case I will show you the process of a google router.



In this picture to the left you can see my private network and how it is set up, I changed the settings to name it to my particular name and I changed the password to a longer and harder one using lower and uppercase letters numbers, and multiple symbols. To proceed you will need to click on the right 4 icons in the upper right corner of the options

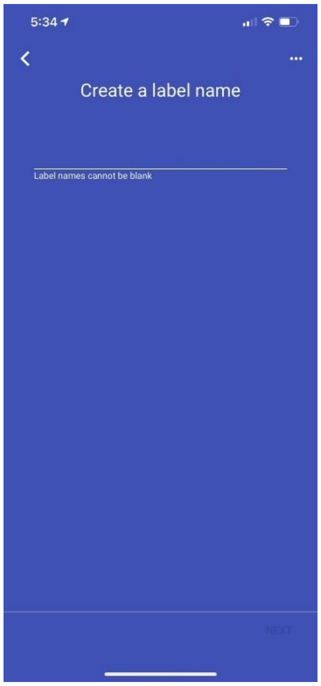


This is the page that will appear once you go into the settings, here the next step would be to go into "Family WI-FI".



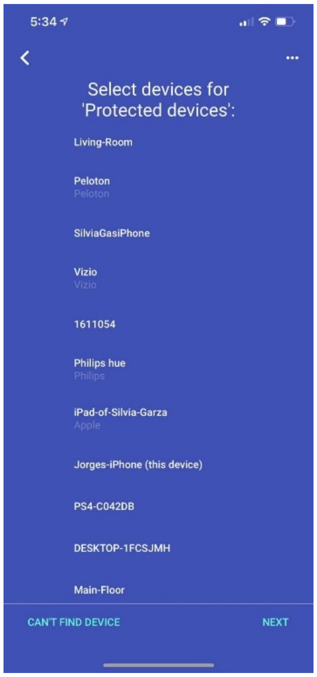
Say goodbye to online distractions. Schedule a regular Wi-Fi pause on your kids' devices like at bedtime, pause Wi-Fi in the moment, and block adult sites on any devices you want.

After clicking in "Family WI-FI" it will give a simple explanation and of what you can expect and then the user should go ahead and click "Set Up"



Label names cannot be blank

The next step would be to give a name to the list that you want to create, this name will help you put the specific devices into this category.



Select devices for 'Protected devices':

Living-Room

Peloton
Peloton

SilviaGasiPhone

Vizio
Vizio

1611054

Philips hue
Philips

iPad-of-Silvia-Garza
Apple

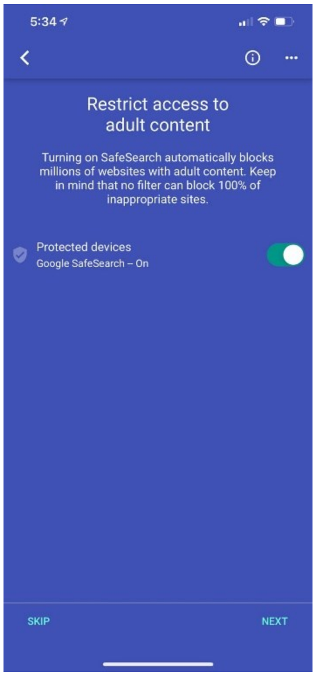
Jorges-iPhone (this device)

PS4-C042DB

DESKTOP-1FCSJMH

Main-Floor

Once you have named the list of devices, you will be able to go ahead and select the specific devices that you would want to put in this protected list that will block them from getting into specific or restricted websites. Once you are finished selecting the devices click on “Next”



Restrict access to adult content

Turning on SafeSearch automatically blocks millions of websites with adult content. Keep in mind that no filter can block 100% of inappropriate sites.

Protected devices
Google SafeSearch – On

In this next screen you need to make sure that this option is tuned on. This function will also block any searched that the users try to make in those devices that are not considered to be safe or appropriate. Then you need to click “Next”.

From the instructions above you can see how easy it is to set up parental controls from a google router, it is practically the same thing for any big brand of routes and this can help you protect you and your family.

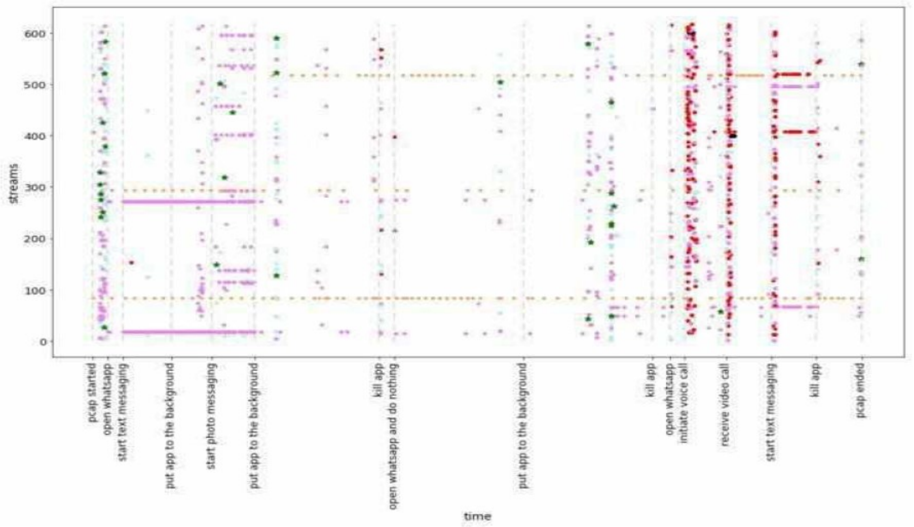
3.5 Securing it all with CUJO AI

Ever wondered if what you are doing at your home network ever open to possible security risks or worse. It is surprising to see that consumers of network routers for home internet don't follow through with such devices' configuration. The filler line of defense might be teaching AI to eliminate the low hanging fruit with small brute force common admin router admin username and password dictionaries. Using a Machine Learning algorithm is a requirement to combat the frequently changing Virtual Reality world, we called the Internet. With the Internet of Things trending and start-up companies pumping out so many new devices, only AI would have the leverage needed to be as secure as a secure consumer may be. CUJO AI has done just that and could be a model to build on with the four services they provide, which are Sentry, Incognito, Compass, and Explorer.

Device Sentry and Web Sentry are part of the CUJO AI Sentry algorithm that mainly detects unusual behavior based on analyzing packet headers in the network traffic. The Web Sentry uses a feature that classifies web addresses catching even zero-day malicious sites.

CUJO AI Incognito uses Machine-Learning based browser fingerprinting using two classifiers, one static and one dynamic. The static classifier checks JS files to see if they have any indicators of typical fingerprinting. The dynamic classifier analyzes the behavior of the JS files calling on its function tree but taxes the processor more, so it does decrease processing performance while browsing. Combing both of these algorithms obfuscates any known attempts for entities to collect telemetry history.

CUJO AI Compass uses a Semiautomatic Rule-based System approach to keep the account holder at the bay of unusual application usage by a bad actor. It first gives suggested best practices for specific applications, and the account holder sets the rules customed peruse. Automation of application usage happens after the end-user has agreed to guide best practice rules as shown here:



Visualization of the network streams observed during a WhatsApp session. The horizontal axis is time; the vertical axis enumerates the streams by their index. Each dot represents network activity. Stars are TLS handshake events. In the first interval of activity (from "start text messaging" to "put an app to the background"), the bulk of communication can be associated with two streams. Afterward, the pattern is less regular. This figure illustrates that app usage detection is a challenging task because the signal is mixed with a significant amount of noise.

Finally, the CUJO AI Explorer uses extensive data sets to compare various possible new devices with different languages to get multiple hits on the latest IoT devices. In conclusion, Machine-Learning based methods require far less maintenance and make sense. As CUJO AI's various algorithms learn from the network traffic and device behavior, it puts the control back in the consumers' hands.

4.0 Conclusion

In conclusion, thanks to Covid-19 and the world sending us to work from home, these are a lot of the security concerns that can often be overlooked because of the simple fact that we believe our home network is safe. These are just some of the potential fixes and resolutions that will make us feel a lot safer working at home. Through first understanding of what type of changes need to occur and being able to find a way to up the practices of security at home treating it as if you were at the office, we can ensure that everything will be protected. The simple technologies and practices that we once used to think was not a necessity has now become the most critical. If we can protect to the best of our abilities our work environments, then we should take those same precautions also to our home-office work environments.

References

Constantin, L. (2016, July 8th). *hot to secure your router and home network*. Retrieved from pcworld.com: https://www.pcworld.com/article/3093362/how-to-secure-your-router-and-home-network.html

cujo.com. (2020, November 16). *CUJO AI contributes to World's economy*. Retrieved from www.cujo.com: https://cujo.com/newsroom/cujo-ai-contributes-to-wef-oxford-report/

dni.gov. (2016, September). *NSA guide to keeping home networks secure*. Retrieved from dni.gov: https://www.dni.gov/files/NCSC/documents/campaign/NSA-guide-Keeping-Home-Network-Secure.pdf

Rijnetu, I. (2019, April 18). *12 steps to maximize your network security*. Retrieved from www.heimdalsecurity.com: https://heimdalsecurity.com/blog/home-wireless-network-security/

valient technologies. (2018). *Wireless Security Assessment*. Retrieved from www.valiant-technologies.com: https://www.valiant-technologies.com/wireless-security-assessment