# Simplifying Home Network Security

Ryan McAfee

Austin Bolstridge

Benjamin Churchill

# Abstract

Computer Network Security is an incredibly important area of research and study. According to the 2015 Verizon Data Breach report, in 2015 there were 79,790 security events, 2122 confirmed data breaches and more than 80% of these breaches were by external actors (Verizon). 99.9% of the vulnerabilities exploited have been compromised for more than a year after a CVE has been published (Verizon). With that said, do you feel comfortable sleeping at night? The short answer is you shouldn't. The above statistics were from enterprises, imagine what the statistics would be when taken from consumer devices that don't receive regular updates! Millions of residential home routers are connected to the internet and according to Avast as much as an estimated 50% of residential routers use default username and password combinations. Home Network Security is a serious area of concern in most households across the world, and most home users are not even aware of the problem. This paper will address ways in which home users can simplify their home network security, increase their home network security, and ultimately give them increased online security.

We have developed plans for home users to deploy a cost affordable secure home network that gives them insight into what's happening within their networks. We're aiming to keep users up to date with their networks and bring enterprise level features to homes across the country at a sub $100 price and as a package that even Grandma can understand. We're aiming to simplify home network security and increase consumers' confidence in their online security and privacy.

# Introduction - The Problem

There is a very large number of insecure end user firewalls and networking gateways connected to the internet that are prone to cyber security attacks. Through research of enterprise level technology as well as open source projects, there is an apparent lack of a simple home network security solutions that can be used by the layman. Why isn't there a plug and play solution that my grandma can use? Good network security practices are currently limited to enterprises and to tech savvy individuals who can understand complicated cyber security concepts needed to properly put a secure firewall solution in place. Private individuals are not always the target of the large scale DoS attacks or more targeted attacks like spear fishing. There is however, an increasing level of cyber-attacks every year against large companies and data centers as well as the individual home user. As of the current time, the end user is most vulnerable in their own home network. Current ISP providers do not provide any sort of cyber considerations. A current home internet setup from an ISP would include a modem, which connects to a wireless router. Sometimes these devices are contained on the same device. In other cases the cable modem is combined with a router as well as home phone connection. While these setups are cheap and easy to implement as well as maintain, there is little protection from targeted cyber-attacks. User's software and firmware upgrades are often not always up to date with the latest security patches. Users who are not able to upgrade their own firmware/ software are even more vulnerable to targeted attacks. Enterprise users have dedicated cyber teams that monitor and respond to incoming attacks and malicious activity. They are able to respond to cyber threats instantly to keep their data safe and hacker free. The end user should have the comfort that they are going to have a secure network. While hiring a team of cyber professionals is not reasonable, a small upfront cost as well as a small monthly fee may be an acceptable solution for the individual or small business. Such a service would have to provide a small scale IDS/ IPS as well as keep up to the minute updates for such a system. In order to provide such a solution we would need to do the processing and definitions remotely. Remote analysis of the aggregate data from the in home sensors of a large

number of customers would allow for new cyber threats to be made known quickly. This paper will explore the design of such a system aimed at simplifying and increasing home network security for the end user.

# Proposed Solution

Network security is incredibly important in today's world. However, home network security has been swept under the rug by many companies, who instead focus on developing solutions for enterprise customers who can pay more. A major contributing reason to the lack of home network security is the cost of secure systems and the skill involved in configuring such a system. Many home users aren't willing to pay above $100 dollars, as there are routers, gateways and firewalls that provide them with a working internet setup for less than $50. Given this price constraint, how can a secure router/gateway/home network be deployed and set up by the end user? We think we have the solution.

The beauty of our solution lies within continual software updates, open source software, off the shelf hardware, and innovative system integration. Our solution involves having the user replace their firewall with a system that will receive automatic security updates and send packets to an optional secondary monitoring system. The optional monitoring system will be a dedicated piece of hardware that will connect to a subscription based service that provides in depth analysis of network signatures and provides updated firewall and filtering rules to the client. The client monitoring system would communicate with the firewall and update rules as new definitions are released and updated by the core cloud analysis engine.

The firewall will be powered by the *Ubiquity Edge Router X* and the monitoring system will use the *Raspberry Pi 3*. This design is very modular and allows a user to have a fully functioning network, yet add a monitoring solution if they desire the additional security on their home network. Our total MSRP for such a system would be less than $100.

# Hardware Overview

***Ubiquiti EdgeRouter X - Router, Firewall and Gateway***

https://dl.ubnt.com/datasheets/edgemax/EdgeRouter_X_DS.pdf

**Main Features**

**Interface/ Encapsulation** - Ethernet, 802.1q, VLAN Bonding (802.3ad)

**Addressing** - Static IPv4/IPv6 Addressing, DHCP/DHCPv6

**Routing** - Static Routes, OSPF/OSPFv3, RIP/RIPng, BGP (with IPv6 Support)

**Security** - ACL, Zone-Based,, NAT, Deep Packet Inspection

**VPN** - OpenVPN, IPSEC, PPTP, L2TP

**Services** - DHCP, Dynamic DNS, DNS Forwarding, Automatic Updates

**Management** - Web UI, SSH, SNMP, Netflow, NTP, Logging

**Hardware Specs**

**Processor**: Dual-Core 880 MHz, MIPS1004Kc

**System Memory**: 256 MB DDR3 RAM

**Storage**: 256 MB NAND

**Ports**: 5 Gigabit Assignable Ports

***Raspberry Pi 3 - Monitoring engine, IDS, IPS***

https://www.raspberrypi.org/magpi/raspberry-pi-3-specs-benchmarks/

**Main Features**

**Interface: Ethernet**

**Hardware Specs**

**SoC:** Broadcom BCM2837

**Networking:** 10/100 Ethernet, 2.4GHz 802.11n wireless

**Bluetooth:** Bluetooth 4.1 Classic, Bluetooth Low Energy

**Processor:** 4× ARM Cortex-A53, 1.2GHz

**System Memory:** 1GB LPDDR2

**Storage:** SD Card, Varies.

**Ports:** 4 USB

# What do we wish to accomplish?

Enterprise customers who can afford cyber security specialists have had access to advanced cyber security network defenses for years, however home network users are far behind the curve. We are attempting to bring enterprise data monitoring and data analysis to home users to increase their home network security and ultimately increase their confidence in their privacy and security. We're developers and advocates of open source software projects. We think the best things in the world are free and developed by a community of creative, passionate and intelligent individuals. Our goals are this:

1) Utilize preexisting off the shelf hardware to create a powerful firewall and monitoring solution for home users.
2) Develop a centralized logging service and analysis engine that parses network data and continually creates refined security rules. This is our Open Source Cyber Threat Exchange Community.
3) Keep the client monitoring solution in sync with the Cyber Threat Exchange Community for the best protection against emerging cyber security threats.
4) Update the firewall from the monitoring client when new definition updates are received from the open source cyber threat exchange community.
5) Give user the ability to receive daily/ weekly reports about their network and receive emails if any suspicious activity is detected.

# How It Works

Users will be running an Ubiquiti Edge Router X as their router within their home network. Conventional routers do not receive regular security updates. However, EdgeOS uses an automatic signature update mechanism to ensure that the router is up to date. In addition, we have added the Debian core package repositories to EdgeOS and wrote a cron job to update core security packages as tracked in the Debian security releases repository. This increases the security of the system and mitigates the likelihood of a system being susceptible to a known published vulnerability.

The system we have developed is modular in nature and uses off the shelf components. The Ubiquiti Edge Router X has all the features your standard home user will want. The Edge Router X is running a variant of an open source router operating system called Vyatta which Ubiquiti repackaged as EdgeOS. In order to capture data packets, we will be using nProbe. NProbe is a software package developed by the ntop project. NProbe captures packets on a host and emits the packets via the ZeroMQ distributed messaging protocol as json to a data collector on the Raspberry Pi that will be running ntopng. Ntopng is a high speed web based traffic analysis and flow collection tool. Ntopng is based on libpcap and works very well. We decided to use ntopng because it gave us the following main features (NProbe):

- Sort network traffic
- Show network traffic
- Produce reports about network metrics (throughput, application protocols, etc.)
- Geolocation of hosts
- Discovery of application protocols by using nDPI
- Display IP Traffic Subnet matrix (who’s talking to who?)
- Low Memory Usage
- Extensible
- Integrates with Elastic Search, Logstash and Kibana

After the data is received by the collector that is running ntopng, the data is logged to the local device in the syslog.

Next, after being authenticated via a OAuth2 token, the data is filtered with syslog-ng and sent over to the central data collection API that is powered by Logstash in intervals of 5 minutes, the data is then further reduced and analyzed using Elastic Search and displayed in Qbana, which is a fork of the Kibana project that focuses on the display and analysis of network data.

Users will be able to log into the cloud dashboard, view their data associated with their account, manage their subscription and opt in/out of notifications.

Our application utilizes a client server architecture in order to relay network data to the cloud analysis server to be further processed and to provide users with updated network signature definitions. This centralized data collection allows us to collect large amounts of network data which we will cross compare and analyze to determine relationships, heuristics and to help with the formation of new and updated network signature rules for use in Intrusion Detection and Prevention Systems.

# System Components

## Sensor (Raspberry Pi)

### Software running on sensor

**Syslog-ng** - This is a program that combines syslog with http/https and offers a way to send collected syslog data through the internet through conventional web communication protocols.

**Ntopng -** This is a network traffic data analysis engine and framework that allows us to visualize network data and get additional insight into a network

### Security

**How is this secure?**

Data that sent over the public internet is secure in transit to prevent the snooping of information by an unauthorized third party. We also verify the public key of our web server to ensure we are communicating with the correct host to prevent a Man in the Middle attack.

**How do we address privacy concerns of user?**

A user may opt out of our cloud subscription service if they do not wish to contribute data for processing to our open source cyber threat exchange community. Also, we remove any personally identifiable information when creating aggregated data sets for use in the cyber threat exchange. Personally identifiable information is tied to a user's account and only showed when a user is viewing their personal network data.

### System Configuration

**What's the operating system and why?**

We are using Arch Linux as the Raspberry Pi Operating System due to minimal resources on the device, it allows us to optimize our security and to optimize performance.

**What does the system do?**

The Raspberry Pi is our traffic analysis engine. The PI is running Ntopng which provides the base network traffic analysis, which is then relayed to our cloud analysis engine using syslog-ng if the user is signed up for it. This data is visualized and gives the user additional insight into what is occurring within their networks.

# Server

## Software running on server

**NodeJS -** Node JS is a JavaScript framework built on Google's V8 engine. It uses event driven non-blocking I/O to make an efficient runtime. Its package management system, npm is considered one of the largest in the world. The npm has recently been updated to make the updating and pulling of packages more secure. The Node Environment has been selected for this project for a many reasons. It can provide quick and efficient development as well as even more efficient runtime. It is capable of running backend for even the largest websites, it is scalable above all else. The npm ecosystem is very active and vibrant, any packages that are used during development (i.e. Express) will be consistently updated and considered to be secure without any editing before deployment. Node is not only simple to use and easily scalable, but the rich development environment mean that there can be continued support for many years. NodeJS is powering our custom SIEM - Security Information Event Management (NodeJS).

**Logstash -** This is an open source software developed by Elastic that powers our centralized data collection API.

**Elastic Search** - This is a data analysis engine that has been developed by Elastic, we use this in our cloud analysis engine in order to compare collected data and to create new network signatures and signatures to keep clients protected.

**Qbana** - This is a fork of the Kibana project by Elastic that focuses on the display and analysis of network data

## Security

**How is this secure?**

1) We scan our systems regularly for vulnerabilities by using the Nessus vulnerability scanner.
2) We use asymmetric cryptography for all data in transit between client and server.
3) We regularly check our systems for updates.

4) We strip personal data out of the data you report to us, you only report to us key metadata we need to develop heuristics and relationships.
5) We store your data encrypted on disk while in rest
6) We rotate our logs and periodically clear our data
7) We give you the option to clear your collected data or to turn off reporting and data collection
8) We use OAuth2 authentication for communication between the monitoring system and the cloud analysis engine.

**How do we address the privacy concerns of our users?**

1) We listen to our users and consider each case on a case by case basis.

## System Configuration

**Operating System**

Centos 6.7 - Based off of Redhat. Enterprise Level Security.

**Security Policies**

1) We use Security Enhanced Linux to increase security on our server and to prevent unauthorized access.
2) We disallow username/ password via ssh.
3) We only allow public/private key to connect via ssh.

## Features

**What does the system do?**

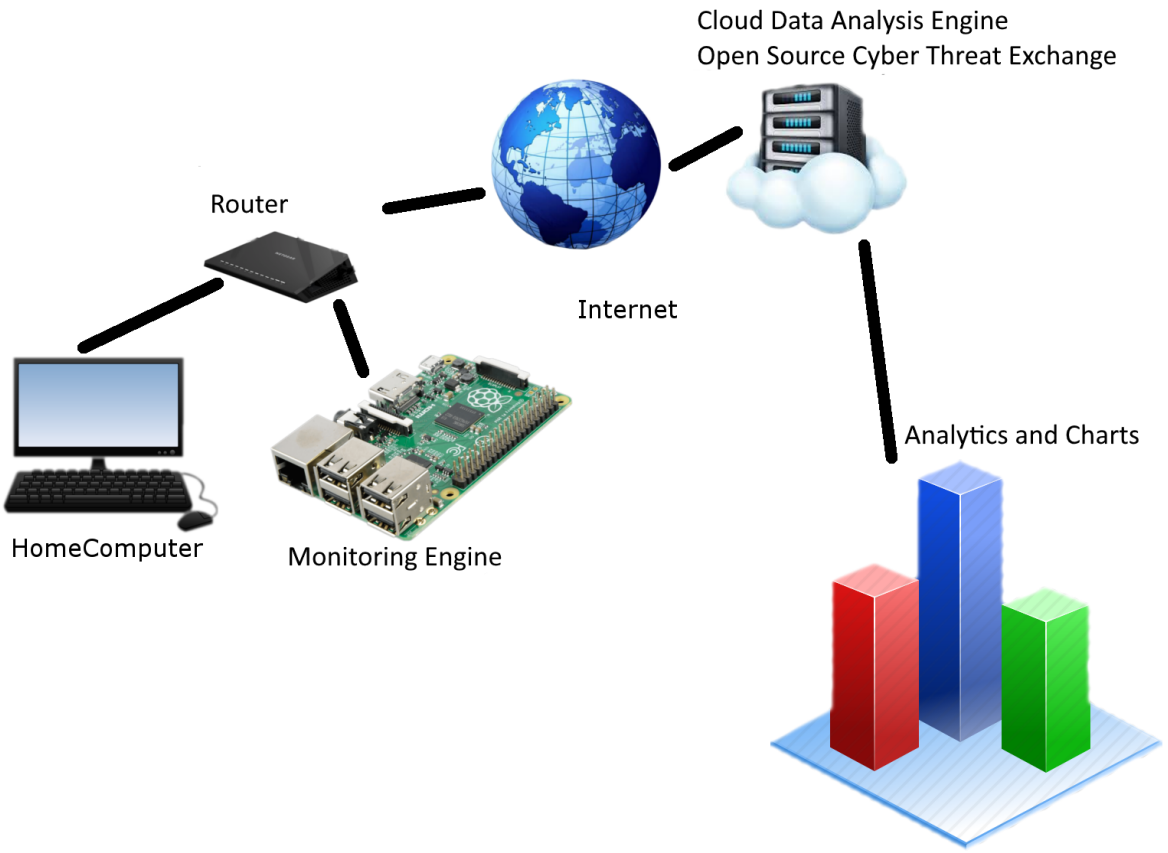
1) Collects data
2) Analyzes data
3) Creates updated network signatures/ rules
4) Visualizes network data in user dashboards

# Technologies

- ELK Stack - Open source data analysis engine by the smart guys over at Elastic
    - Elastic search - Data analysis engine
    - Logstash - Data collection engine
    - Kibana - Data visualization engine
- Apache Hadoop - Distributed processing of data
- Syslog-ng: Syslog + http/https - Allows for sending the data to collecting agent
- NodeJS - Used to create SIEM (Security Information and Event Management) web app that gives user insight into network
    - Express - NodeJS web development framework
    - Passport - User authentication
    - Interacts with Kibana/ Qbana to display custom data
- Raspberry Pi
    - Cost effective hardware to run monitoring solution for home network
    - The First Raspberry Pi model was released early in 2012, its invention came from the foundation's want to make a computer science education available to everyone around the world. While it serves this purpose, making programming available to practically everyone due to its $35 price point, the Pi has been used by independent developers to make everything from sensor networks to automated robotics. There are a myriad of resources available for developers wanting to use the Pi for their own projects. The Foundation and community is always in favor of new open source projects using the technology. We decided on the raspberry pi for this project for a lot of these reasons. Its price point makes the hardware affordable for our purposes (less than $100). Its hardware is also a good selling point, the Raspberry pi 3's quad core processor running at around 1200 mHz is considered adequate for packet sniffing of a residential network (around 100 mbps). On top of this, the pi will only draw about 4 W of power. Having adequate

hardware and affordable price point make the Pi a good choice for a project like this. The power usage will even appeal to the budget conscious users as well as 4 W is considered minimal.

# Architecture



# Privacy Concerns

While the lay user may not be comfortable with a third party looking at and receiving their internet traffic, a solution that requires data to be aggregated in real-time and update network signature definitions and rules would need to have off site processing if using a small system with limited processing power. We test our systems with vulnerability scanners and regularly keep our systems patched and updated.

Furthermore, it would seem unlikely that an inexperienced user would be able to run and maintain a large scale system as it is very uneconomical. As covered in previous sections, we designed the system to continue to function even after the user opted out of data collection. They will still be able to receive remote updates from the main server (or server cluster) and from that be protected with up to date definitions. There would need to be programs in place that can encourage the average user to opt into the data aggregation. On top of this we will need to make sure that the client side sensor system can still function without any connection to the internet (aside from periodic updates). For very privacy conscious users, we will need to produce a security appliance that contains all of our software as an all in one device. This package will make sure that the power user to the enterprise level user can do all of their processing on site and make sure that all of their confidential/ proprietary data can be kept completely private and secure. This solution will allow the user to still opt into remote processing (as load balancing or as a way to contribute to the open source community.) but it will be disabled by default (unlike the light solution). The heavy solution will also provide, inherently by its nature, a faster way of receiving updates to network signature definitions. While the light solution (which combines the cloud analysis engine and client sensor) would be considered more prone to security flaws due to its design, the heavy solution provides increased security because the data processing is all performed locally on an end-user's own hardware. Our standalone all in one security appliance is more secure than our hybrid security appliance, however it should be stressed that both systems are secure and tested, the hybrid system just has more attack surfaces, therefore it would be more targeted by attackers. Lastly, it should be noted, having a security system deployed is much safer then no security

system at all. Would you leave your front door unlocked? No? You should probably think about adopting a secure home network solution.

# Conclusion

In our paper we addressed the topic of Home Network Security. We realized through research that nearly 80% of all residential users connect to the internet through a router are at risk of an attack (Avast). The internet and home network security is very insecure. We have suggested a recommendation and solution to end users that is easily affordable, intuitive, easy to setup, increases home network security and gives a user additional insight into the status of their network. This paper focused on the design and architectural planning for such a system. Future work will entail the implementation of the work discussed in this paper.

# References

84 Fascinating & Scary IT Security Statistics | Cool Solutions. (n.d.). Retrieved April 26, 2016, from https://www.netiq.com/communities/cool-solutions/netiq-views/84-fascinating-it-security-statistics/

2015 Data Breach Investigations Report. (n.d.). Retrieved April 26, 2016, from http://www.verizonenterprise.com/DBIR/2015/

Home Network Security. (n.d.). Retrieved April 23, 2016, from https://www.us-cert.gov/Home-Network-Security

Home Router CERT. (n.d.). Retrieved April 26, 2016, from https://www.us-cert.gov/sites/default/files/publications/HomeRouterSecurity2011.pdf

Your home network is at risk of cybersecurity attacks. (n.d.). Retrieved April 26, 2016, from https://blog.avast.com/2014/11/05/your-home-network-is-at-risk-of-cybersecurity-attacks/

Node.js. (n.d.). Retrieved April 24, 2016, from https://nodejs.org/en/

NProbe. (2011). Retrieved April 26, 2016, from http://www.ntop.org/products/netflow/nprobe/

Raspberry Pi - Teach, Learn, and Make with Raspberry Pi. (n.d.). Retrieved April 25, 2016, from https://www.raspberrypi.org/