Lab 1 – Black Bear Home Guardian Product Description

Kathleen Taylor

Old Dominion University

CS411W

Professor Janet Brunelle

01 March 2021

Version II

Table of Contents

List of Figures

List of Tables

1 Introduction

Internet of Things (IoT) devices are defined as "web-enabled smart devices that use embedded systems, such as processors, sensors and communication hardware, to collect, send and act on data they acquire from their environments" (Rouse, 2020). In the context of a home network environment, data is shared locally between related devices on the network. Most IoT devices are installed in households for the purpose of convenience and typically require little human interaction. As the number of devices installed around the home expands, the amount of unencrypted data being transferred over the network increases which in turn escalates the potential for an attack. With little to no security standards defined, the lack of information security and encryption protocols for IoT devices are what makes them so vulnerable.

Despite their apparent security flaws, homeowners appreciate the value of having IoT devices installed in their homes. In fact, according to Smart Energy International (2020) the market is expanding rapidly for "connected products that can deliver convenience, energy efficiency, and greater security." The expanded revenue generated over the next nine years from the smart home and IoT device market is expected to increase by approximately $83.5 billion (Nhede, 2020).

The number of IoT devices being installed by homeowners is increasing at an exponential rate (Hegde, 2017). In the year 2019, U.S households had an average of 11 connected devices (Spangler, 2019) and it is projected that this average will increase to 50 by the end of the year 2020 according to Economic Times (Phadnis, 2016). With that many devices connected to the network, it will become extremely inconvenient for homeowners to manage all these devices and connections whether it is starting from setup and installation to dealing with maintenance and security monitoring.

The biggest threat to IoT device security is an exploit. For instance, a zero-day is where the attacker capitalizes on an unknown security vulnerability in the system before it is detected by the developer or the developer has had the opportunity to create a patch. Malware, such as ransomware, where a user is threatened to have their data exposed unless the attacker is paid, consists of 33% of the threats to IoT devices. In addition, 26% of threats to IoT devices are the result of poor user practices, for example neglecting to change the default password preconfigured for the device (O'Donnell, 2020). A hacker can often look up the default password for a specific IoT device online and thus breach any home network using the IoT device as a backdoor (Wired Brand Lab, 2017). The severity of the attacks recorded on IoT home devices range from ransomware on a smart coffee pot (Goodin, 2020), to a hacker watching a 8-year-old girl in her bedroom through a home security camera (Burke, 2020).

Unfortunately invasion of household privacy occurs more often than expected: security camera systems comprise 46% of IoT devices that are hacked; the remaining majority of commonly hacked IoT devices consists of smart home hubs and Network Attached Storage (NAS) systems (Help Net Security, 2020). Although security camera systems are the most commonly hacked IoT device, there has been a notable increase in the number of attacks on all IoT devices. Researchers from the Palo Alto Networks Unit 42 team found that 98% of all IoT device traffic is unencrypted, exposing personal and confidential data on the network, which means more than half of all IoT devices are vulnerable to medium or high-severity attacks (O'Donnell, 2020). Sensors are one of the most targeted IoT devices by hackers since they can be attacked using various methods such as sending infrared signals to cameras or sending ultrasonic sounds to voice-control systems (Spencer, 2018).

Hypothetically, a homeowner could create a custom VLAN system to monitor their IoT devices, but this often proves to be a difficult task when selecting the correct configurations unless the user has knowledge in network security. Furthermore, the user will ultimately find themselves spending a significant portion of their money on specialized equipment.

The average homeowner cannot mutually solve the inherent security concerns and inconveniences associated with the increasing number of connected devices installed within their home. Black Bear Home Guardian ships as a multi-vendor router firmware that effortlessly replaces the homeowner's standard firmware preinstalled on the router provided to them by their Internet Service Provider (ISP). This alleviates the stress of needing to upgrade one's hardware in order to protect their home network with Black Bear. Black Bear is equipped with software defined networking through preconfigured segmented virtual local area networks (VLANs). Before homeowners assign new devices to the appropriate VLAN in which they will reside on the network, they can configure to have push notifications sent to their mobile device that requires their approval for all device connections to the home network; this requires no knowledge of network security from the Black Bear user. The architecture of the VLANs along with two-factor authentication (2FA) isolate and shield devices from threats. Black Bear users manage their home network and all its device connections through the convenience of the Black Bear web portal and mobile application.

2 Black Bear Home Guardian Product Description

Black Bear Home Guardian is a home network solution for conveniently managing IoT and smart home devices while providing security through VLAN segmentation. Black Bear eliminates the need for managing multiple passwords for numerous smart devices by requiring a password and a push notification for user authorization to the portal or mobile application,

where they can then manage their devices and home network. By receiving a push notification for every new user and device connection, Administrative Users are able to control which users are granted access to their network, assign which VLAN the user's device is connected to on their network, and set the span of time for which the user's device remains connected to their network. Furthermore, network segmentation of the devices through VLANs isolates any threat or security vulnerability that may occur on one VLAN from affecting other devices on other VLANs.

The objective of Black Bear Home Guardian is to provide homeowners with a convenient and secure way to manage their IoT and devices residing on their home network. Black Bear alleviates the stress of needing knowledge in network security in order to protect one's home network and its devices. The goal for market acceptance of the Black Bear Home Guardian is to develop the customer base through an Internet Service Provider (ISP). Black Bear Home Guardian seamlessly replaces the firmware on any standard router provided by ISPs that is found in 90% of U.S. households (Moore, 2015). By packaging Black Bear in the form of router firmware, homeowners can easily update their home network system when necessary while ensuring compatibility between the firmware and their hardware is maintained. Older router hardware that is able to support custom firmware will also have the ability to install Black Bear. Aftermarket routers will not have access to installing the Black Bear firmware since the Black Bear customer base is solely being established through an ISP.

2.1 Key Product Features and Capabilities

Currently, there is no router on the market with preconfigured IoT security features that are offered by Black Bear Home Guardian. Black Bear Home Guardian is custom router firmware configured to allow for VLAN segmentation and can be installed on any standard WiFi

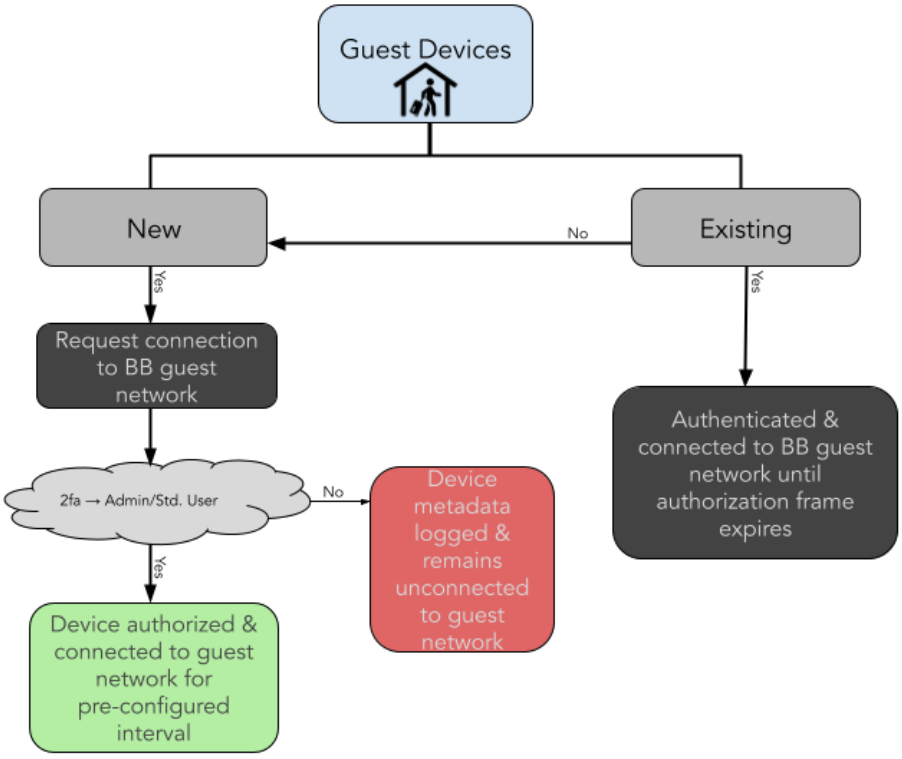
router. Although mobile applications do exist for managing one's smart home devices, there are not any applications on the market that offer the same functionality as Black Bear in regards to both device and network management. The core functionalities of Black Bear include: simple installation, authentication, network management, device management, and user role specific profile management.

Users are provided with a quick-start pamphlet to assist with set up and installation of Black Bear into their network. Administrative Users are prompted with credential customization immediately after completing the installation and set up process. To access the web portal, Administrative Users are provided with a link after completing installation that directs them to the portal login page. Using an Apple device, users can scan the quick response (QR) code found in the pamphlet for easy navigation to the mobile application.

After customizing the default administrative credentials, Administrative Users are subsequently authorized access to the web portal or mobile application with their updated credentials. The head of household, also referred to as the Administrative User, can authorize other household members through a push notification to create a Black Bear Standard User account where they can then connect and manage their own devices along with Guest User devices. Standard Users are emailed temporary credentials that must be customized through the provided link which will direct them to the portal or mobile application where they can then also customize their Black Bear user profile. Standard Users also have the ability to authorize Guest User devices to the Guest network with a push notification sent to their associated device. As displayed in Figure 1, anytime a Guest User's device attempts to connect to the network, a 2FA notification is sent to active, Registered Users for approval before being authorized to the network.

Figure 1

Black Bear Guest User Process Flow Diagram



If the Guest User's device is denied, the Administrative User has the option to block this specific device from requesting future connections.

With the current user process flow, all user devices are connected on the same network. Users must either manage passwords on all of their smart devices or have knowledge in network security to configure custom VLANs for their home network. If an attack occurs, the intruder has full access to the network and all of its connected devices. Black Bear is equipped with four default preconfigured VLANs set up for the user to which they can easily designate their devices. Through the architecture of VLAN segmentation, the VLANs and their devices remain isolated from attacks on another VLAN. This ensures that devices with weak security protocols, such as a light bulb, cannot be used as a backdoor to more serious devices like a home security camera

system. Homeowners who have their home network protected by Black Bear Home Guardian have the ability to easily manage their devices through push notifications sent directly to their iPhone. 2FA approval for device connections prevents unauthorized users and devices from connecting to the network even in the case of an intruder hijacking the network password. If the device is approved, it is assigned to one of the preconfigured VLANs by the Black Bear Administrative User.

Administrative Users are provided full privileges with their portal to the home network which can be accessed through their desktop or mobile phone. Administrative Users have the ability to view and identify all devices actively connected to the home network by their user-given name as well as any devices that may be offline. The administrator also has the ability to view logs of all connection and disconnection history on the home network as well as search all previously or currently connected devices to the home network. Additional features provided to administration include the ability to edit and remove all devices on the home network along with the ability to manage these devices' connections to the network. Standard Users are provided limited access with their portal to the home network which can also be accessed through their desktop or mobile phone. Similarly to Administrative Users, Standard User can view and identify their associated devices by their user-given name along with their devices that are offline. However, Standard Users are only able to manage Guest User devices and their connections on the network.

Administrative Users can view the status of their network along with metrics on network speed, data traffic, and usage per VLAN through their web portal or mobile application. Report frequency on device and network analytics sent to the administrator can be configured through the administration profile page. These reports include notifications of devices not connected

within the last several months, unresponsive devices, and abnormal connection activity. "Normal" activity of the household is recorded monthly as a baseline.

2.2 Major Components (Hardware/Software)

The Black Bear Home Guardian system consists of software components, the Black Bear web portal and iPhone operating system (iOS) application, as well as a hardware component, a Smart WiFi Router. Black Bear Home Guardian utilizes software defined networking through segmented VLANs and can be installed on any smart WiFi router that supports custom firmware. An Apple smartphone device is required for access to the mobile application.

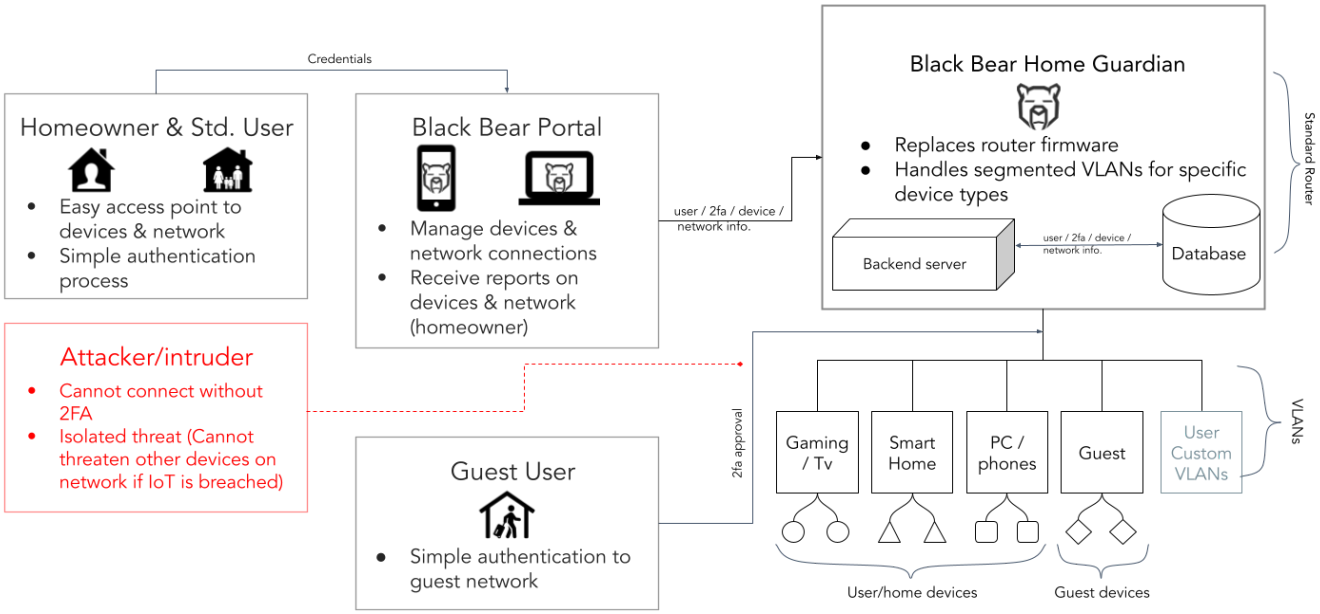
Registered Users are provided with a Black Bear web portal account in which they are authorized to access with their Black Bear credentials. Through their portal they can manage their devices, network connections, and user profile preferences. Additionally, all Registered Users can access their Black Bear user account through the Black Bear mobile application with their Black Bear credentials.

As seen in Figure 2, the Black Bear router firmware is preconfigured with four default VLANs for the Administrative User to assign devices. These default VLANs are: (a) Computers and phones, (b) Smart Home, (c) Gaming and Television, and (d) Guest. These four VLANs cannot be removed and have no editing capabilities. Administrative Users have the ability to create and name new VLANs for device assignment along with the ability to remove any of these additionally created VLANs. For each device assigned to the VLANs there are details stored in the database upon its authorization to the network such as the device's user-given name, which user added the device, the role of the user who added the device, and other metadata on the device's connection.The Black Bear database stores data related to each individual Black Bear

user profile and preferences, their device information, their device connection activity, their network connection activity, VLAN information, and network metadata.

Figure 2

Black Bear Major Functional Component Diagram



The most important end user of Black Bear Home Guardian is the Administrative User. As shown in Table 1, the Administrative User is granted full access in regards to managing the home network, its devices and its users, which is conveniently done through the Black Bear web portal or mobile application. Guest Users must have each of their devices approved to the Guest network through a 2FA notification sent to Registered Users. Guest User devices are only authorized and connected to the Guest network for the authorization period configured by the Administrative User. When the authorization span for the connection ends, the device is automatically disconnected and unauthorized from the network.

Table 1

Black Bear Access Control Table

	USER ROLE		
ACTION	Guest	Standard	Admin
Access portal from desktop or mobile device		✓	✓
Provided credentials for portal access		✓	✓
View & identify devices on the network		✓	✓
Manage devices on the network (edit, remove)		✓	✓
Authorize new devices to the network		✓	✓
Authorize new Standard users to the network			✓
Authorize new Guest users to the network		✓	✓
Manage VLANs on the network (create, edit, remove)			✓
View logs of all connection/disconnection activity on network			✓
Search all previously & currently connected devices			✓
Weekly/monthly metadata reports on network			✓
View analytics on network			✓
Configuration of advanced network features			✓

If an intruder were to hijack the Guest network password, they would still need approval sent by the Administrative User with a push notification. If an attack on the Black Bear home network were to occur, the threat would remain isolated within the targeted VLAN--therefore leaving the remaining VLANs and their connected devices shielded from the threat.

3 Identification of Case Study

Black Bear Home Guardian is designed for average, highly connective households typically utilizing 10 or more IoT and other smart devices on their home network. Not only does Black Bear Home Guardian allow for simple management of one's IoT and all other smart home devices, it also ensures the security of these devices and one's information through easy to use,

preconfigured VLANs. Homeowners that install Black Bear Home Guardian on their router will have a separate VLAN specifically for Guest User devices to further isolate any threats from the home network and its devices. Through either the Black Bear web portal or mobile iOS application, homeowners along with their household members can conveniently and securely manage the devices on their home network.

The selected case study for the Black Bear Home Guardian Prototype are homeowners. Family and highly interconnected households containing multiple technologically-dependent household members, including the homeowner, will be chosen. Each homeowner will assign all of their IoT and other smart devices residing on their home network to one of the four default VLANs preconfigured with Black Bear. Homeowners are encouraged to authorize all devices not belonging to the homeowner or household onto the Guest VLAN requiring 2FA approval. A malware honeypot will be built to explore possible vulnerabilities in the system. Each homeowner will observe the overall security of Black Bear segmenting the devices on their home network. The necessary feedback to be solicited by the case study to further prototype development is: (a) the convenience of assigning devices to their appropriate VLAN, (b) the convenience of the push notification system, (c) the convenience of the privileges assigned to each user role, and (d) the security of the 2FA approval required for new devices and users.

Black Bear Home Guardian expects to cater to small business owners who have highly connected businesses or offices. Business owners need to ensure the security and confidentiality of their customers' information along with the transactions occurring on their network. Future implementations of Black Bear Home Guardian for small business owners would include preconfigured VLANs for security camera systems, electronic payment systems, customer devices, etc.

4 Black Bear Home Guardian Prototype Product Description

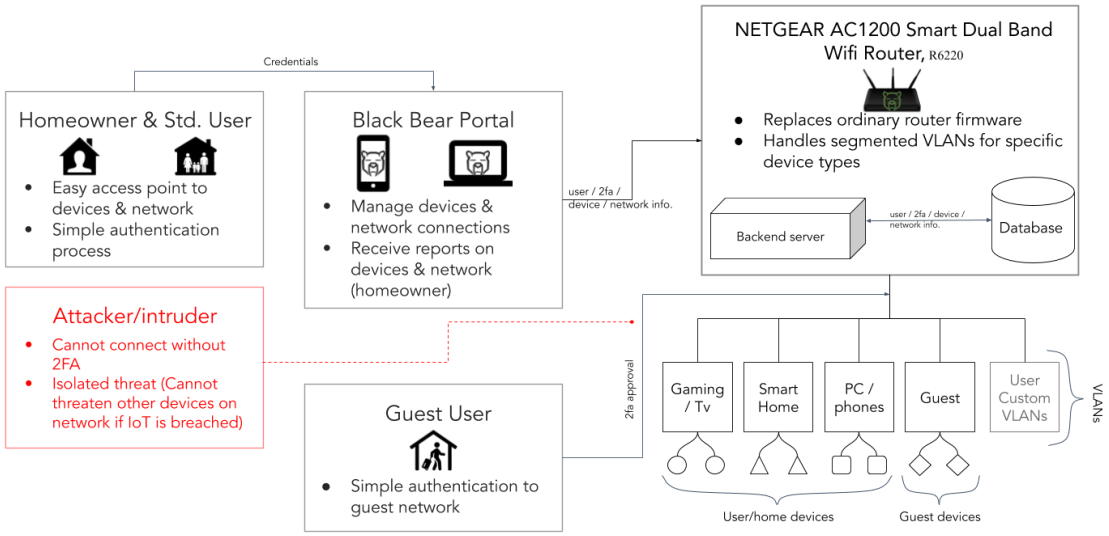
The Real World Product will be implemented as router firmware and will replace the homeowner's existing standard router firmware. The Black Bear Home Guardian prototype will be dependent on the router hardware selected for development and will implement the functional features of the Real World Product. Features relating to metadata, analytics, reports, and customizable user preferences will not be included in the prototype. Data models for simulated events, such as a 2FA request, will be included in the framework for the sake of testing and demonstrating.

4.1 Prototype Architecture (Hardware/Software)

The most apparent difference between the architecture of the Real World Product (RWP) compared to the prototype is the hardware component that is introduced. For proof of concept a Netgear AC1200 Smart Dual Band Wifi Router configured with OpenWrt, the router firmware necessary for development, will be the specific hardware used for the Black Bear prototype. In addition to the router, the product will also be packaged using Docker containers and developed in a virtual environment. An Apple iOS device is required for use of the mobile application but not necessary for the overall functionality of Black Bear.

Figure 3

Black Bear Prototype Major Functional Component Diagram



With respect to the RWP, the architecture of the software components for the Black Bear prototype will be relatively the same. The prototype will include both the web portal and iOS application. Python and Lua scripting will aid in interfacing the portal with the router firmware. The web portal interface will be built using ReactJs, WebPack, and Babel for compilation. NodeJs and ExpressJs will be utilized to accomplish front-to-backend communication. Software tools required for the development of the iOS mobile application include SwiftUI, Combine, and Xcode. The primary deployment method for the iOS application will be through the Xcode simulator. The same four default VLANs that are utilized in the RWP will also come preconfigured with the prototype as shown in Figure 3. Administrative, Standard, and Guest User roles will all exist within the prototype as well. Since the prototype contains a subset of features from the RWP, information stored in the database will be limited in scale in comparison to the RWP.

4.2 Prototype Features & Capabilities

The Black Bear Home Guardian prototype demonstrates the convenience and security provided by the RWP. User authentication and authorization as well as user roles will be demonstrated in the prototype. Other key features demonstrated in the prototype include segmented VLANs, two-factor push notifications, the web portal, and the mobile application. The main objective of the Black Bear prototype is to simplify device management on one's network while providing extra security.

Black Bear Home Guardian's real world application includes additional advanced features for users that have an intermediate level of experience with network security. These features include: honeypots for detecting attacks on the network, blocking networking traffic from specific countries, and secure shell (SSH) server for configuring the router through the

command line. As displayed in Table 2, advanced network configurations will not be incorporated into the Black Bear prototype. Another feature that is not included in the prototype is the ability for the Administrative User to configure complex user permissions for other Standard Users in the home network. For example, the Administrative User may want to limit the bandwidth of another device or authorize a Standard User to approve other users on the network. Additionally, the prototype will not display device and network analytics to users through their portal or mobile application. However, the Administrative User will have the ability to configure a weekly and monthly subscription for receiving reports relating to their network metadata and analytics.

The Black Bear Home Guardian RWP is in the form of router firmware rather than an actual router such as the Netgear AC1200 Smart Dual Band Wifi Router R6220 that is being utilized for the prototype. This ensures forward compatibility of Black Bear with any standard router hardware thus not requiring the user to purchase new hardware when updates are released.

Table 2

Table of Comparison Between Real World and Prototype

Features	Real World Product	Prototype
Software-Defined Networking	**Fully Functional**	**Fully Functional**
Automatic VLAN Segmentation	**Fully Functional**	**Fully Functional**
Independent of Router Hardware	**Fully Functional**	**Partially Functional**
Web Portal	**Fully Functional**	**Fully Functional**
iOS Application	**Fully Functional**	**Fully Functional**
Optional 2FA Device Authorization	**Fully Functional**	**Fully Functional**
Metadata Collection / User Notifications	**Fully Functional**	**Partially Functional**
Advanced Config (SSH Server / Honeypot / IP Blocking)	**Fully Functional**	**Not Included**
Admin-Granted User Privileges	**Fully Functional**	**Not Included**

Not only will the Black Bear Home Guardian prototype allow for simple management of IoT and all other smart devices, it will also ensure the security of these devices and information through easy to use, pre-configured VLANs. Segmented VLANs further isolate any threats from the network and its devices in the case of an attack. Through either the web portal or mobile iOS application, users can conveniently manage their devices and network. Success of Black Bear Home Guardian will ultimately be demonstrated by delivering a prototype that is scalable.

Mitigations have been developed for each risk associated with the development of the Black Bear prototype. By preconfiguring the prototype with four logical groups, the risk of congestion and thus bottlenecking is reduced. In the case of an intruder having physical access to the router, passwords will be presented in the form of a quick response (QR) code rather than cleartext for all to see. The necessary documentation will be developed for installation and set up of Black Bear Home Guardian to improve the user's experience with the frontend interfaces.

The expected functionality produced by the prototype is convenient and secure management of smart home devices through software defined networking. One of the main objectives for Black Bear Home Guardian is for it to cater to users of varying levels of knowledge, especially those lacking knowledge in the field of network security. The goal of the prototype is for it to replace the user's current home network router.

4.3 Prototype Development Challenges

Although one may assume that Black Bear Home Guardian is a relatively simple concept to implement, there are several challenges to overcome with the development of the prototype. An initial concern with prototype development was having a single Netgear router for which code could be developed and tested on; therefore, code will be developed locally and run in virtual environments using Docker containers to thus allow for efficient collaboration.

Furthermore, the Netgear router used in prototype development may have insufficient or limited computational resources necessary for running the code. An additional concern with prototype development is interfacing the web portal and mobile application with the router firmware through Python and Lua scripting. Perhaps one of the biggest challenges for prototype development will be implementing two-factor notifications offline. In other words, it is difficult to implement push notifications without either an Internet connection or cellular data which presents an issue with installation of Black Bear in one's home. Lastly, as with any system designed to enhance security, ensuring user authentication is secure is a prime concern of Black Bear Home Guardian.

[This space intentionally left blank.]

5 Glossary

Administrative User (Admin / Homeowner): A user who most likely purchased the router then completed initial install and set up of Black Bear Home Guardian to protect their home network (e.g. head of household).

App Store: The official digital distribution platform for iOS and iPadOS applications which is both developed and maintained by Apple.

Authentication: Black Bear Registered Users are able to access their portal and be authenticated using their Black Bear credentials (username and password).

Authorization Period/Span: The period of time configured by the Administrative User for which Guest Devices are authorized access to the Guest VLAN.

Babel: A Javascript transpiler that converts code written in modern versions of the language into an older, more widely supported version. This allows developers to use the latest features of Javascript without needing to worry about browser compatibility.

Combine: Apple's “reactive” framework for handling events over time.

Device Management: The ability for Registered Users to view and manage their devices (edit, remove) on their network.

Docker: A set of platform as a service products that use OS-level virtualization to deliver software in packages called containers.

Exploit: Code that takes advantage of a software vulnerability or security flaw.

ExpressJs: A web application framework for NodeJs.

Graphical User Interface (GUI): A form of user interface that allows users to interact with electronic devices through graphical icons.

Guest User: A user that briefly visits the home network guarded by Black Bear, and whose

devices are granted access only to the guest network for a limited time period as authorized by the Administrative User.

Honeypot: A computer or computer system intended to mimic likely targets of cyberattacks.

Integrated Development Environment (IDE): A software application that provides comprehensive facilities to computer programmers for software development.

Internet of Things (IoT): Describes the network of physical objects—"things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet.

iPhone Operating System (iOS): A mobile operating system created and developed by Apple Inc.

Local Area Network (LAN): A computer network that interconnects computers within a limited area.

Lua: A scripting language used in game development and embedded systems.

Major Functional Components Diagram (**MFCD):** A diagram that displays the software and hardware architectural components of a system.

Media Access Control (MAC) Address: A unique identifier assigned to a network interface controller for use as a network address in communications within a network segment.

Metadata: Data that provides information about other data, such as device connection data that provides information about the device.

MySQL: A popular, open-source relational database management system.

Network-Attached Storage (NAS) Systems: A storage device connected to a network that allows storage and retrieval of data from a centralized location for authorized network users and heterogeneous clients.

Network Management: The ability for Administrative Users to manage their network name and PIN, along with the ability to manage the VLANs (create, edit, remove) on their network.

NodeJs: A Javascript runtime environment.

OpenWrt: An open-source operating system used in routers and other embedded applications.

Personal Identification Number (**PIN):** A simple string of numbers used as a password that must be entered by an individual attempting to connect to a Black Bear router. This takes place before the two-factor confirmation by an Admin or Standard User.

Profile Management: The ability for Registered Users to view and edit their personal profile information and preferences.

Python: An interpreted, high-level and general-purpose programming language.

Quick Response (QR) Code: A machine-readable code consisting of an array of black and white squares, typically used for storing URLs or other information for reading by the camera on a smartphone.

ReactJs: A popular Javascript framework.

Real World Product (RWP): The fully-featured version of the product which, in contrast to the prototype, is sold in the real world.

Registered User(s): Administrative and Standard User(s) that have been authorized to the home network and possess valid Black Bear credentials for accessing the portal. A Guest is not considered a registered user.

Secure Shell (SSH): A network communication protocol that enables two computers to communicate and share data.

Simple Installation: Homeowners are provided with a quick-start pamphlet to guide them through the installation and setup process for equipping their home network with Black Bear.

Small Network: A LAN in a home or small business with less than 100 connected devices. This is the type of network targeted by Black Bear.

Smart Home Hub: Hardware or software that connects devices on a home automation network and controls communications.

Standard User: A user that resides within the home network guarded by Black Bear but is granted limited access in regards to managing the network and its devices (e.g. children of admin).

Swift: The programming language used to write software for Apple products.

SwiftUI: A Swift framework for designing user interfaces.

Two-Factor Authentication (2FA): A method of establishing access to an online account or computer system that requires the user to provide two different types of information. A factor in this context simply means a way to convince a computer system or online service that a user is who they are claiming to be so the system can determine if the user has the rights to access the data services that they are trying to access. The most common authentication factor in use today is the username/password pair. Users are required to both provide a password and prove their identity in order to gain access.

Virtual Local Area Network (VLAN): A custom network created from one or more existing local area networks (LAN) that enables groups of devices from multiple networks (both wired and wireless) to be combined into a single logical network. The result is a virtual LAN that can be administered like a physical local area network.

Virtual Machine (VM): A virtual environment that functions as a virtual computer system with its own CPU, memory, network interface, and storage, created on a physical hardware system (located off or on-premises).

VLAN Segmentation: The practice of placing device connections into categorized virtual local area networks (VLANs) to remove access to one another from logically separate devices.

WebPack: JavaScript module builder.

Web Portal: The graphical user interface of the Black Bear application which can be accessed from a web browser.

Xcode: Official IDE for Mac OS and iOS.

Zero-Day Exploit: These exploits are considered "zero-day" before and on the day that the vendor is made aware of the exploit's existence, with "zero" referring to the number of days since the vendor discovered the vulnerability. "Day zero" is the day the vendor learns of the vulnerability and begins working on a fix.

[This space intentionally left blank.]

6 References

Burke, M. (2020, January 16). *Man hacks Ring camera in 8-year-old girl's bedroom, taunts her: "I'm Santa Claus."* NBC News. https://www.nbcnews.com/news/us-news/man-hacks-ring camera-8-year-old-girl-s-bedroom-n1100586

Goodin, D. (2020, September 26). *When coffee makers are demanding a ransom, you know IoT is screwed.* Ars Technica. https://arstechnica.com/information-technology/2020/09/how-a hacker-turned-a-250-coffee-maker-into-ransom-machine/

Hegde, Z. (2017, October 30). *Smart home will drive Internet of Things to 50 billion devices, says Strategy Analytics.* IoT Now. https://www.iot-now.com/2017/10/30/70040-smart-home-will-drive-internet-things-50-billion-devices-says-strategy-analytics/

Help Net Security. (2020, February 26). *Shadow IoT: A growing threat to enterprise security.* Help Net Security. https://www.helpnetsecurity.com/2020/02/26/shadow-iot-enterprise/

Ilchenko, V. (2020, August 13). IoT cybersecurity risks and solutions. *ByteAnt.* https://www.byteant.com/blog/iot-cybersecurity-risks-and-solutions/

Moore, J. (2015, July 6). *IHS: 90% of households will get Wi-Fi routers from ISPs by 2019.* FierceTelecom. https://www.fiercetelecom.com/installer/ihs-90-households-will-get-wi-firouters-from-isps-by-2019

Nhede, N. (2020, July 15). *Smart home IoT devices market to record 18% growth despite pandemic.* Smart Energy International. https://www.smart-energy.com/industry-sectors/iot/global-smart-home-iot-devices-market-to-record-18-growth-despite-pandemic/

O'Donnell, L. (2020, April 22). *More than half of IoT devices vulnerable to severe attacks.* Threatpost. https://threatpost.com/half-iot-devices-vulnerable-severe-attacks/153609/

Phadnis, S. (2016, August 19). Households have 10 connected devices now, will rise to 50 by

2020. *Economic Times.* https://cio.economictimes.indiatimes.com/news/internet-ofthings/households-have-10-connected-devices-now-will-rise-to-50-by-2020/53765773

Rouse, M. (2020, February 11). *Internet of Things (IoT).* IoT Agenda. https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

Spangler, T. (2019, December 10). U.S. households have an average of 11 connected devices — and 5G should push that even higher. *Variety.* https://variety.com/2019/digital/news/u-s-households-have-an-average-of-11-connected-devices-and-5g-should-push-that-evenhigher-1203431225/

Spencer, R. (2018, October 22). 10 IoT security and privacy trends to watch. *Lanner.* https://www.lanner-america.com/blog/10-iot-security-privacy-trends-watch/

Williams-Grut, O. (2018, April 15). Hackers stole a casino's high-roller database through a thermometer in the lobby fish tank. *Business Insider.* https://www.businessinsider.in/Hackersstole-a-casinos-high-roller-database-through-a-thermometer-in-the-lobby-fish-tank/articleshow/ 63769685.cms

Wired Brand Lab. (2017, June 21). IoT is coming even if the security isn't ready: here's what to do. *Wired.*
https://www.wired.com/brandlab/2017/06/iot-is-coming-even-if-the-security-isnt-ready-heres-what-to-do/