Lab 2 – Black Bear Home Guardian Product Specification

Katie Taylor

Old Dominion University

CS411W

Professor Janet Brunelle

28 March 2021

Version I

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). 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 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. 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). In addition, 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). Hypothetically, a homeowner could create a custom virtual local area network (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.

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 VLANs. The architecture of the VLANs along with multi-factor authorization (MFA), for new users or devices attempting to join the network, 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.

1.1 Purpose

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.

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 goal for market acceptance of 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.

1.2 Scope

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 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 of the prototype is for it to replace the user's current home network router.

The Black Bear Home Guardian prototype is dependent on the router hardware that was selected for development and it implements the functional features of the Real World Product (RWP). The Black Bear Home Guardian prototype demonstrates the convenience and security provided by the RWP. User authentication and authorization as well as user roles are demonstrated in the prototype. Other key features demonstrated in the prototype include segmented VLANs and multi-factor push notifications for new users or devices. Both the web portal and the mobile application are available with the prototype. Features relating to metadata, analytics, reports, and customizable user preferences are not included in the prototype. Data models for simulated events, such as a MFA request, are included in the framework for the sake of testing and demonstrating.

[This space intentionally left blank.]

1.3 Definitions, Acronyms, and Abbreviations

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

Application Programming Interface (API): A software intermediary that allows two applications to talk to each other.

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 User 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.

Ethernet: The traditional technology for connecting devices in a wired local area network (LAN) or wide area network (WAN), enabling them to communicate with each other via a protocol.

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 VLAN for a limited time period as authorized by the Administrative User.

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

Hypertext Transfer Protocol (HTTP): The protocol used to transfer data over the web. It is part of the Internet protocol suite and defines commands and services used for transmitting web page data.

Institute of Electrical and Electronics Engineers (IEEE) 802: A family of IEEE standards for local area networks (LAN), personal area network (PAN), and metropolitan area networks (MAN).

IEEE 802.3: A set of standards and protocols that define Ethernet-based networks.

IEEE 802.11: Specifies the set of medium access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) computer communication.

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.

Multi-Factor Authorization (MFA): A security mechanism to determine access levels or user/client privileges related to system resources including files, services, computer programs, data and application features.

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 multi-factor confirmation by an Admin or Standard User.

Power User: A user of a computer system or program whose skills and expertise are more advanced than most other users, especially a person in an organization who is assigned additional administrative rights and responsibilities for that system or program.

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.

Remote Procedure Calls (RPC): A computer program causes a procedure (subroutine) to execute in a different address space (commonly on another computer on a shared network), which is coded as if it were a normal (local) procedure call, without the programmer explicitly coding the details for the remote interaction.

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.

Transmission Control Protocol (TCP): A communications standard that enables application programs and computing devices to exchange messages over a network. It is designed to send packets across the Internet and ensure the successful delivery of data and messages over networks.

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.]

1.4 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/

Hedge, 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-sector s/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/

Taylor, K. (2021, March 1). Lab 1 – Black Bear Home Guardian product description. Old Dominion University Department of Computer Science. https://www.cs.odu.edu/~411red/index.html#labs

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/

[This space intentionally left blank.]

1.5 Overview

The hardware and software configurations as well as the external interfaces of the Black Bear Home Guardian prototype are provided in this product specification. Figures 1 and 2 are provided to further illustrate the prototype's architecture. The key features and capabilities along with their implementations for the prototype are also outlined in this document and listed in Table 1.

2 General Description

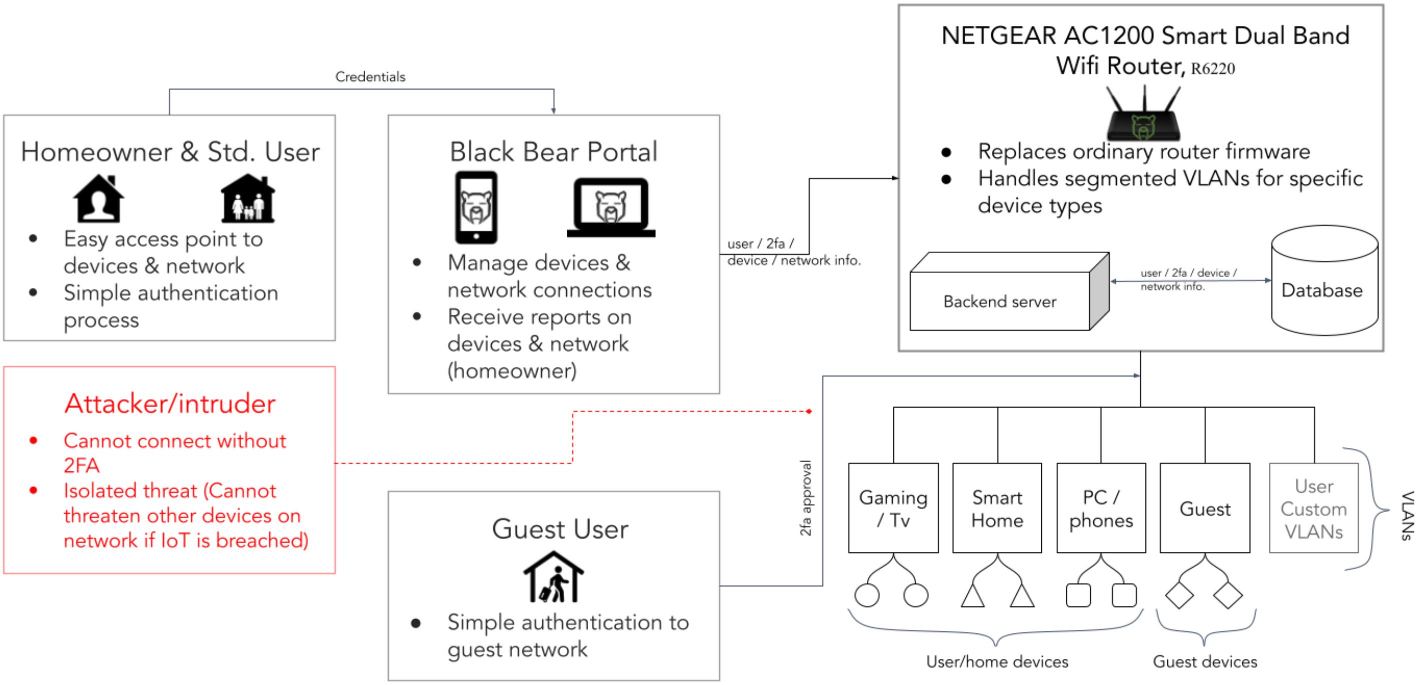
The Black Bear Home Guardian prototype demonstrates the overall functionality of the RWP by implementing a subset of its features. Black Bear's core functionalities include internet access, a straightforward initial setup process, convenient network organization, and inherent network security. Primary features for device management, such as user interfaces and segmented VLANs, are implemented in the prototype. Additional key features that deliver convenience and security, like receiving push notifications for new devices, are also implemented in the prototype. The prototype demonstrates the user interfaces for the advanced networking and metadata reporting features, but does not include their functional implementations.

2.1 Prototype Architecture Description

The most apparent difference between the architecture of the 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, is the specific host hardware used for the Black Bear prototype. OpenWrt is open-source router firmware that has the ability to handle customized router features, such as MFA, as well as advanced networking features like configurable VLANs. The database baked into OpenWrt 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. As shown in Figure 1, the prototype 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 because they are meant to guide the user with segmenting their devices on the network.

Figure 1

Black Bear Prototype Major Functional Component Diagram (MFCD)


Credentials
Homeowner & Std. User
Easy access point to devices & network
Simple authentication process
Black Bear Portal
Manage devices & network connections
Receive reports on devices & network (homeowner)
NETGEAR AC1200 Smart Dual Band Wifi Router, R6220
Replaces ordinary router firmware
Handles segmented VLANs for specific device types
user / 2fa / device / network info.
Backend server
user / 2fa / device / network info.
Database
Attacker/intruder
Cannot connect without 2FA
Isolated threat (Cannot threaten other devices on network if IoT is breached)
2fa approval
Guest User
Simple authentication to guest network
Gaming / Tv
Smart Home
PC / phones
Guest
User Custom VLANs
VLANs
User/home devices
Guest devices

The prototype includes both the web portal and iOS 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. The Black Bear web portal replaces the default frontend web portal provided by the OpenWrt image. Python and Lua scripting aided in interfacing the portal with OpenWrt. The web portal interface was built using ReactJs, WebPack, and Babel for compilation. NodeJs and ExpressJs are utilized to accomplish front-to-backend communication. Additionally, all Registered Users are able to access their Black Bear user account through the Black Bear mobile application with their Black Bear credentials. The Black Bear iOS application maintains feature parity with the Black Bear web portal while also offering the convenience of network management remotely from one's mobile device. Software tools required for the development of the iOS mobile application included SwiftUI, Combine, and Xcode. The primary deployment method for the iOS application is through the Xcode simulator. In addition to the router, the product is also packaged using Docker containers and being tested 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.

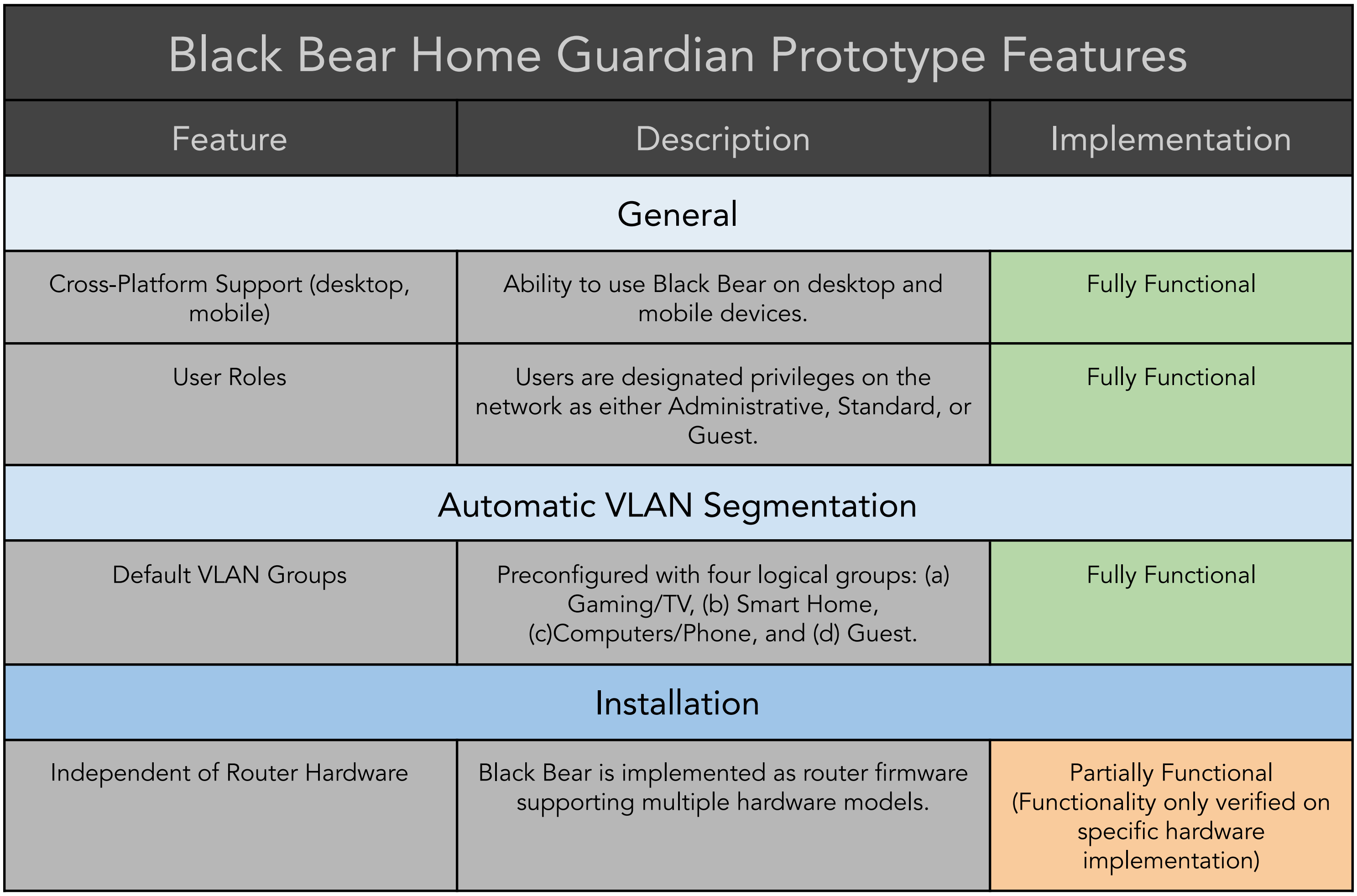
2.2 Prototype Functional Description

The frontend components of Black Bear, the web portal and mobile application, provide end-user functionalities for user account creation, user account management, user login, device management, network management, push notifications, and user profile management. Administrative User account creation is facilitated through the web portal after the router setup process is complete in the user's home environment and connected to the local network. The web portal prompts for customization of Administrative User credentials if none exist in the database. Standard User registration with Black Bear is facilitated by the Administrator User through their web portal. Temporary credentials are generated by the Administrative User which are to be customized by the requesting Standard User in order to receive access to the network.

Authentication for all Registered Users is performed using an email and password provided to the login page. Once authenticated into the portal with their customized credentials, Registered Users can access web pages to view, add, or remove devices from their home network along with editing their profile settings and preferences. Furthermore, Administrative Users have the ability to modify the network name and personal identification number (PIN) as well as configure additional VLANs through web pages accessible from the portal. Push notifications for new users or devices joining the home network are facilitated through the mobile application interface and are sent to all Registered User devices for approval or denial on the network.

Table 1

Black Bear Prototype Features Table



Black Bear Home Guardian Prototype Features

Feature	Description	Implementation
General		
Cross-Platform Support (desktop, mobile)	Ability to use Black Bear on desktop and mobile devices.	Fully Functional
User Roles	Users are designated privileges on the network as either Administrative, Standard, or Guest.	Fully Functional
Automatic VLAN Segmentation		
Default VLAN Groups	Preconfigured with four logical groups: (a) Gaming/TV, (b) Smart Home, (c)Computers/Phone, and (d) Guest.	Fully Functional
Installation		
Independent of Router Hardware	Black Bear is implemented as router firmware supporting multiple hardware models.	Partially Functional (Functionality only verified on specific hardware implementation)

Administrative Credential Setup	Ability to customize administrative user credentials upon installation using the provided access code.	Fully Functional
Authentication		
Standard User Registration	Create a Standard User account (or an additional Admin User account). *(Admin User only)*	Fully Functional
Authorized User Login	Access an existing Black Bear account.	Fully Functional
Multi-Factor Notifications	Send push notifications to Black Bear Registered User(s) requiring approval for new Standard Users and devices on the network.	Fully Functional
Guest Device Authorization Span	Devices assigned to Guest VLAN are authorized and connected to the network for a default or customized period. After which the device is unauthorized and disconnected from the network.	Partially Functional
Account Management		
Update Profile Information	Ability to update Registered Black Bear User's general information.	Fully Functional
Configure Weekly Reports	Ability to customize the frequency and content of metadata reports on the network and its devices. *(Admin User only)*	Partially Functional
Device Management		
Manage Devices (Edit / Remove)	Ability to edit or remove devices on the network.	Fully Functional
Search Devices	Ability to search for previously or actively connected devices on the network.	Fully Functional
Network Management		
VLAN Management	Ability to create, edit, and remove VLANs other than the four default. *(Admin User only)*	Fully Functional
Basic Router Configuration	Registered Users can update basic router settings such as wireless encryption, SSID, and Wi-Fi password. *(Admin User only)*	Fully Functional

Continuous Monitoring	Allows for metadata reporting, device searching, and log auditing.	Fully Functional

The backend component, the router firmware, provides functionalities for push notifications, VLAN segmentation, data storage and management, as well as supporting the frontend components. Basic router functions, such as routing and forwarding, are preserved in the prototype's firmware along with the key function of providing Internet access to all authorized devices. OpenWrt, the customizable router firmware selected for development, is configured to run scripts for interfacing the push notification service as well as creating the default VLANs on the local area network (LAN). The Guest VLAN is configured with a default authorization span of twenty four hours after which the device is automatically unauthorized and disconnected from the network. The database baked into OpenWrt is configured to store the designated user role for each Black Bear account so that the frontend components can present the appropriate web resources to that user depending on their privileges. The backend component is interfaced with the web portal frontend component mainly through remote procedure calls (RPCs). The functionality implemented for all features in the Black Bear prototype can be seen in Table 1.

2.3 External Interfaces

There are four main external interfaces used within and by the Black Bear prototype that contribute to its overall functionality. The hardware interface required for the Black Bear prototype is the physical router hardware in which the software interface, the router firmware, is installed. There are also two user interfaces used by the prototype for interacting with the network.

2.3.1 Hardware Interfaces

The portal for the Black Bear prototype is available on any desktop computer with the appropriate web browser installed. The mobile application for the Black Bear prototype is available on any Apple iPhone device.

Figure 2

NETGEAR AC1200 Smart Dual Band Wifi Router, R6220

As displayed in Figure 2, the prototype firmware is available on the NETGEAR AC1200 Smart Dual Band Wifi Router and provides the necessary router services, like Wifi and Ethernet connections, to the Black Bear prototype.

2.3.2 Software Interfaces

OpenWrt is open-source router firmware that supplies basic router functionality as well as allows for the configuration of the Black Bear prototype's custom features, including the push notification service and the default segmented VLANs. OpenWrt also provides the interface for the prototype's database. RPCs are the main protocol used to interface the Black Bear portal with OpenWrt.

2.3.3 User Interfaces

The two user interfaces for the prototype are a desktop computer and an iOS device. The web portal user interface can be viewed in any modern web browser and it is hosted locally at https://blackbear-router.com. The web portal user interface cannot be accessed from outside the home network. However, the iOS user interface can be accessed from outside the home network to allow for remote management of the network. The iOS user interface maintains feature parity with the web portal and runs on any Apple iPhone device.

2.3.4 Communications Protocols and Interfaces

Standard Internet protocols such as hypertext transfer protocol(HTTP) and transmission control protocol (TCP) are used in the Black Bear prototype to retrieve web pages for the web portal as well as to retrieve data for both the web portal and the mobile application using a RPC application programming interface(API). Standard Institute of Electrical and Electronics Engineers (IEEE) 802.3 is used to define Ethernet communication and standard IEEE 802.11 is used to define the communication for our wireless LAN. Standards IEEE 802.3 and IEEE 802.11 are both operated by OpenWrt.

[This space intentionally left blank.]

3 Product Requirements

A separate document titled “Lab 2 Section 3 – Black Bear Home Guardian Product Requirements” defines Black Bear Home Guardian’s requirements. This document outlines the functional, performance, and non-functional requirements for the product as well as assumptions and constraints. Figures and tables are used to further demonstrate the capabilities of Black Bear.

[This space intentionally left blank.]