projectcanary™

by

Jarrod Calhoun, Paul Galyen and Daniel Glover

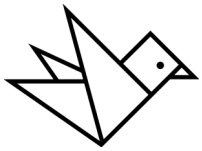
Submitted to
the Faculty of the School of Information Technology
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

Jarrod Calhoun	October 31, 2016 Date
Paul Galyen	October 31, 2016 Date
Daniel Glover	October 31, 2016 Date
Bo Vykhovanyuk, Faculty Advisor	October 31, 2016 Date

University of Cincinnati
College of
Education, Criminal Justice, and Human Services

November 2016

Table of Contents

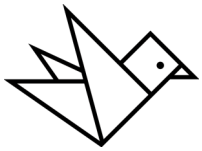


FIGURES

Number

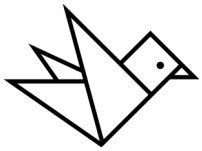
Acronyms and Abbreviations

PHP	Hypertext Preprocessor
MySQL	My Standard Query Language (Open Source Data Management System)
IP	Internet Protocol
SANS	System Administration, Networking and Security Institute
USB	Universal Serial Bus
OS	Operating System
SSID	Service Set Identifier
MAC	Media Access Control address



Abstract

Project Canary is a pre-programmed standalone home DNS and DHCP Server. Project Canary has provided the user with an intuitive graphical user interface (GUI), which made administration procedures and set up easier. The Canary leveraged a Raspberry Pi, PHP, BASH and Pi-Hole, which provided the novice user with a simple home monitoring solution. Cybersecurity products mainly targeted the business market, which do not transition well to the home. An overall reduction of user awareness, time, and skills characterizes the home market. This device has been used to help increase cybersecurity awareness and bridge the gap between the business and home products. Project Canary has provided the average homeowner the ability to white and blacklist devices and websites; as well as designed for other SANS 20 Critical Security Controls to be introduced. Project Canary will raise awareness and security in the home.

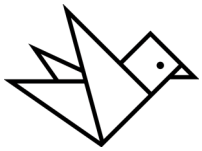


1.0 Problem Statement

There is a lack of cybersecurity technology available for the home network and the home user. The current technology does not port well from the business world to the home network. This created a niche market for a device like Project Canary. Project Canary provides the user a sense of security past the already available anti-virus or malware removal tool. Canary is a turnkey solution to these problems by allowing the homeowner to plug the device in and select what devices can connect to their WiFi. This will allow the user to determine if a device can stay on the network, what websites the device can access while on their network, and will provide security to the devices from known malicious sites.

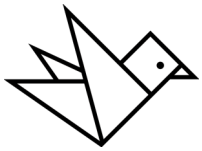
1.1 Introduction

Cybersecurity is, astonishingly, a relatively new endeavor for businesses. The media has brought to light some of the biggest corporate information network intrusions to date. While businesses have invested millions of dollars in securing a way of doing business that increases productivity and keeps costs low, homeowners have yet to embrace techniques that safeguard their information. Developing products that provide novice users with appropriate tools is difficult. While much of the tools are available online, most individuals aren't aware they exist, and don't have the expertise to use them. In many cases, no graphical user interface can surmount the lack of knowledge. To create a new market, and provide the novice user with security on their home networks, products like Canary will introduce people to new techniques by meeting their needs and slowly making new features available.



1.2 Project Description

Project Canary is a Raspberry Pi that connects to the homeowner's WiFi. Once the device connects to the WiFi, the user will be asked to connect to it using a desktop, tablet or IPad. Once they connect to it (like a typical WiFi) they will be asked to go to the IP address; 172.24.1.1. Once at this screen, the user will be asked to follow a set of instructions. This simple set up process will ask the user; how they want to be notified concerning devices connecting to their network and their user's name. Then, it will provide a current list of devices on their network and give the options to allow, block, or temporarily allow each device on the network.



1.3 Problem

Project Canary allows the homeowner to increase their home network security without opening them up to more vulnerability. Using this device, the homeowner will supplement their current security, antivirus, or malware removal tool. This device will greatly increase the security of the home network for the user by allowing the owner to see who, what, and when a device is connected to their home network.

1.4 User Profile

The targeted user(s) for Project Canary, a home network intrusion alert device, are average people with novice level experience and a basic level of understanding concerning information technology. Our user(s) will possess basic knowledge to operate and use devices, applications, laptops, smartphones, WiFi, Internet, and social media sites. In addition, as the users' experience increases, so does their concern for security. As they read on the Internet or hear on TV, they learn that their information is not secure on their home computers or on their own home WiFi network. The user(s) will be able to install, set-up, modify, and run the Project Canary device via an easy to use web interface. Once installed, the user(s) will see a list of devices currently connected to their home WiFi network. The user's interface, although simple and intuitive, will offer the user the ability to then allow, temporarily allow, or decline each device's current connection to the network. With any subsequent device connection established thereafter, the user will receive an alert concerning this new connection. Alerts will only be generated when a device has no previous recognition or has been previously declined

connection to the network. Below, figure 1 outlines in more detail, how the user will interact with and what role they will have with the Canary in their home environment.

1.4.1 User Profile Description

Potential User(s): Average Home Owners and Average Technology User(s)
User Experience and Understanding: The typical Project Canary user has novice experience using computers and computer applications. The typical Project Canary user has basic understanding of technological devices and Internet connectivity.
User Experience with Similar Applications: Typical Project Canary user(s) are familiar with connecting mobile devices to various WiFi networks in other locations such as, at work, at school, or at Starbucks.
Task Experience: The user(s) will be comfortable with and capable to monitor a provided, real-time list of devices connected to their home network, receive alerts for new connections, and actively allow or deny connectivity to their home WiFi network.
Frequency of Use: Continuous.
Key Design Requirements that the Profile Suggests: Simple and intuitive User Interface Easily accessible navigation tabs/buttons Basic and logical user guide

Figure 1. User Profile

1.5 Use Case Diagram

Figure 2 displays what the homeowner can achieve on the Canary. The homeowner can set up a home security system, which will alert the user to notify them when someone logs on to their network for the first time. Once they receive the alert they can grant access to the user, decline access to the user or grant temporary access to the user. The network user has the generic abilities of browsing the internet and logging into the WiFi if they are granted access to it.

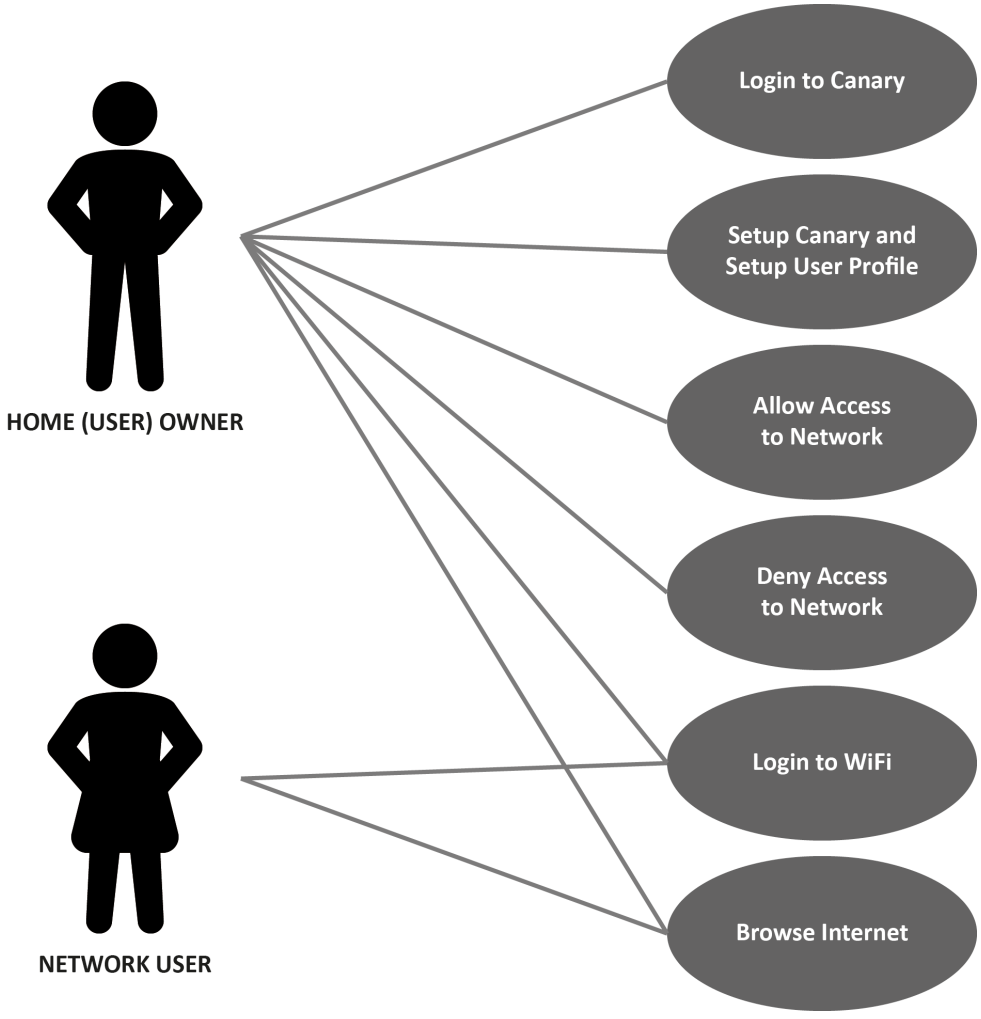
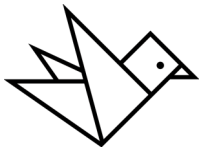


Figure 2. Use Case Diagram



2.0 Technical Elements

There are several issues with introducing a product to the average user. Primarily, it must be simple to use. Canary is meant to be an out of the box product that can be setup by nearly anyone. Subsequently, it must be a cost-effective solution, it must address issues that network owners deal with daily; and, it must not fall into the conundrum of allowing excessive security practices which inhibit user experience. Canary also must be modular to augment scalability. More importantly, it must not introduce more cybersecurity concerns into a network.

2.1 Device Description

We are currently using the Raspberry Pi 3 Model B, which is the third-generation Raspberry Pi. It is an inexpensive computer, with a cost of approximately $30. It comes with an internal WiFi that will communicate with the router, or be an intermediary with the router. We will utilize a second WiFi dongle allowing Canary to connect to itself as an access point. This offers direct device connectivity while only requiring a power source. The user will then be able to connect to the Canary, visit the static IP address, and enter its setup procedure without need of a network.

2.2 Software

We have installed a Debian OS, which is commonly referred to as Noobs with Apache Server, MySQL and PHP. This works well in the Linux environment. Most the setup will be done by a simple web application that uses PHP to run command line code and execute Ruby and Bash

scripts. The Canary is also building on existing open source software called Pi-Hole. This software had many of the features that were desired for everyday users. The additional features that we created for Pi-Hole were for IP blocking, filtering and integrating of malware lists to the known malicious site lists.

3.0 Testing

3.1 Overview

This section will define the testing approach employed during the development of Project Canary.

3.2 Scope

The scope of testing is to test the installation, set-up, and usage of the Canary device. Each test will be administered within the confines of the requirements of the device.

3.3 Objective

The objective of testing is to verify that a process, feature, and the device itself, executes as expected. These tests are designed to test subjects in isolation or as a whole.

3.4 Entry and Exit Criteria

Entry Criteria:

- Build complete
- Self-testing complete
- Test environment is established

Exit Criteria:

- All tests are run
- Glitches are documented and fixed

3.5 Logging Test and Reporting

If an anomaly is found during testing, the individual glitch will be documented. The designers will meet after the test and decide if the glitch reported is an anomaly or a feature that is not functioning as it was intended. Once the glitches are decided on, then the designers will fix the glitches based on a combination of severity and usability.

3.6 System Testing

Project Canary will be tested as a complete entity with all its features tested as one item. This will help identify the defects (glitches) that will only show when the complete device is tested. It is intended to verify that the device performs as one working unit.

3.7 Testing Procedures

The following are the steps required for testing which consist of:

- Create all the test scenarios and test cases;
- Prepare a record of the steps used to conduct the test and any expected results; and
- Specify the glitches in the correct report.

Below are the tests that will be performed:

1. **Internal Test** – This test will focus on the proper operation and execution of the buttons and features of Project Canary.
2. **Launch Test** – This test will focus on the ease of ability for a novice user to properly install, start, and configure Project Canary.
3. **User Interface Test** – This test will focus on the user interface of Project Canary and its level of intuitiveness to the novice user.
4. **Functionality Test** – This test will focus on all features that are included and implemented with Project Canary and that they perform in concert as expected.

3.7.1 Pass/Fail Conditions

It will be expected that Project Canary must pass all tests in every category to be successful. If it does not pass, the tester will record the matter.

3.7.2 Schedule of Team Member Testing

The schedule of the team member testing is summarized in table 1 below.

Team Member	Timeline for Completion	How Often?
Developer	01/07/2017 – 03/20/2017	Weekly
Project Manager	01/07/2017 – 03/20/2017	Weekly

Table 1. Team Member Testing

3.7.3 Schedule of User Testing

The schedule of the user testing is summarized in table 2 below.

User	Timeline for Completion	How Often?
Novice	01/07/2017 – 03/20/2017	Once per month (3 times)
Advanced Novice	01/07/2017 – 03/20/2017	Once per month (3 times)

Table 2. User Testing

3.8 Risks

The following will impact the test cycle:

- Wi-Fi availability/connectivity;
- Programming expertise;
- Designing around current foundation;
- A delay in glitch fixes; and
- Schedule/availability of a specified user for testing.

3.9 Testing Reports

Internal Test – This test focused on the device and application being stable on various

platforms such as, an Android device, iPhone device, iPad device, and an Apple Mac Pro when

using a particular web browser. Please note that the Android used Firefox (1.1), the iPhone (1.2), iPad (1.3) and Mac Pro used Safari (1.4).

3.9.1 Internal Test: Round One

Below, table 3 displayed the results of the first round in the last test prior to expo performed on these devices. It was expected that the website would display the administration website properly and function as expected.

Tester	Date	Item	Actual	Pass/Fail	Glitch
J. Calhoun	1/23/17	1.1	Worked as expected	Pass	-
J. Calhoun	1/23/17	1.4	Worked as expected	Pass	-
P. Galyen	1/23/17	1.2	Worked as expected	Pass	-
D. Glover	1/23/17	1.1	Worked as expected	Pass	-
D. Glover	1/23/17	1.2	Worked as expected	Pass	-
D. Glover	1/23/17	1.3	Worked as expected	Pass	-
D. Glover	1/23/17	1.4	Worked as expected	Pass	-

Table 3. Internal Testing – Round One

3.9.2 Results/Notes

The one issue that was noted in every environment was latency between adding and deleting websites from the lists and the time the change took to propagate. In addition, the footer is displaying differently in Safari. Further investigation will be needed.

3.9.3 Internal Test: Round Two

This test round considered several new sections to the website. While a few new style guides were added, they had very little impact on the overall HTML. Regardless, it was important to test the website again after the upgrade. The following table, table 4, displays this testing round.

Tester	Date	Item	Actual	Pass/Fail	Glitch
J. Calhoun	1/30/17	1.1	Minor issue with footer	Pass	CSS
J. Calhoun	1/30/17	1.4	Minor issue with footer	Pass	CSS
P. Galyen	1/30/17	1.2	Minor issue with footer	Pass	CSS
D. Glover	1/30/17	1.1	Minor issue with footer	Pass	CSS
D. Glover	1/30/17	1.2	Minor issue with footer	Pass	CSS
D. Glover	1/30/17	1.3	Minor issue with footer	Pass	CSS
D. Glover	1/30/17	1.4	Minor issue with footer	Pass	CSS

Table 4. Internal Testing – Round Two

3.10 Results/Notes

The newest page has a default setting that allows the user to see activity real-time. There is a script that is essentially an auto-scroll. The page automatically scrolls to the bottom of the page with this setting regardless of the amount of data showing. For a more appropriate user experience, either turn this initial setting to off, or add functionality that determines there being enough data to warrant scrolling feature. With the upgrade, the propagation delay has become acceptable; and, there is now a disable button, which allows users to bypass the device altogether in certain situations.

Launch Test – The focus of this test was to observe the user performing an initial setup of the device. Given the instructions, can the user set the device up (2.1), and can they access it (2.2)?

3.11 Launch Test: Round One

Table 5 is displaying the first round of testing. It was expected that the user would be able to setup the device and subsequently access Canary's web administration with the user's preferred device.

Tester	Date	Item	Actual	Pass/Fail	Glitch
User A	1/24/17	2.1	Difficulty	Pass	Instructions
User A	1/24/17	2.2	Difficulty	Pass	Instructions
User B	1/24/17	2.1	Moderate	Pass	-
User B	1/24/17	2.2	Accessed	Pass	-

User C	1/24/17	2.1	Easy	Pass	-
User C	1/24/17	2.2	Accessed	Pass	-

Table 5. Launch Testing – Round One

3.11.1 Results/Notes

User A is an older individual. User A had difficulty conceptualizing what the device was and how it was going to work opposed to following the instructions. To overcome this issue, insert either a brief excerpt about the device (with a diagram), or perhaps, include a link to a promotional video. This user also struggled in grasping that the web administration could be accessed from any device and the necessity of connecting to the Canary Wi-Fi. This issue was not the case concerning the other user testers.

3.12 Launch Test: Round Two

The previous tests were somewhat concerning. As a solution for this, we crafted straightforward IKEA style instructions, which helped the novice user setup the device with ease. The current process requires the user to; give Canary power, connect to Canary Wi-Fi, and then access Canary's web administration using a browser and the default IP address.

Tester	Date	Item	Actual	Pass/Fail	Glitch
User A	1/31/17	2.1	Moderate	Pass	-
User A	1/31/17	2.2	Accessed	Pass	-
User B	1/31/17	2.1	Easy	Pass	-
User B	1/31/17	2.2	Accessed	Pass	-
User C	1/31/17	2.1	Easy	Pass	-
User C	1/31/17	2.2	Accessed	Pass	-

Table 6. Launch Testing – Round Two

3.12.1 Results/Notes

The IP address is causing some issues. We may need to simply have an address like "localhost" or "canary". New issues may occur to due novice user's expectation of URLs ending with ".com" or the like. The ideal situation would pop-up the main page once the browser is launched (while connected to the Canary Wi-Fi).

We may need to revisit this test later. We will be adding a new settings page that will certainly add complexity for the target user; but, will also add meaningful functionality. So then, we will

have to determine what is necessary and what complicates the overall experience for the most novice of user. Making a robust cybersecurity device that hovers at the level of the lowest common denominator is something we should avoid. We should strive for offering advanced functionality to promote and appeal to higher level users, but is still effective in its basic default state.

3.13 User Interface Test – This test focused on the usability of Canary's interface and how it appealed to the user. We asked users to perform certain tasks and graded the task on pass or fail. We felt timing these assignments would be unnecessary since redundancy would reinforce familiarity. We would be concerned if the task could not be performed. We asked the user to blacklist a website – facebook.com (3.1), and blacklist a device that is listed (3.2). The user should be able to navigate to the page and add the website or device.

3.13 User Interface Test: Round One

Below is the first round and the last round of test performed on the web administration.

Tester	Date	Item	Actual	Pass/Fail	Glitch
User A	1/25/17	3.1	Found page, added facebook.com	Pass	-
User A	1/25/17	3.2	Found page, clicked plus symbol	Pass	-
User B	1/25/17	3.1	Found page, added www.facebook.com	Fail	cues
User B	1/25/17	3.2	Found page, clicked plus	Pass	-

			symbol		
User C	1/25/17	3.1	Found page, added http://www.facebook.com	Fail	cues
User C	1/25/17	3.2	Found page, clicked plus symbol	Pass	-

Table 7. Interface Testing – Round One

3.13.1 Results/Notes

Our users could find the pages easily. Each added the web address differently. This is going to be problematic. Adding specificity to the URL narrows the scope of what will be blocked. In some cases locations such as mail.facebook.com would not be blocked, for example. Some of these issues may need to be handled programmatically by removing "www.", or "http://www.". Another solution may be to add videos that are hosted on YouTube.

3.14 User Interface Test: Round Two

Below is the second round and the final round of test performed on the administration. We added a cue to the website to exclude "http://www.", which helped immensely.

Tester	Date	Item	Actual	Pass/Fail	Glitch
User A	2/1/17	3.1	Found page, added facebook.com	Pass	-
User A	2/1/17	3.2	Found page, clicked plus symbol	Pass	-
User B	2/1/17	3.1	Found page, added	Pass	-

			facebook.com		
User B	2/1/17	3.2	Found page, clicked plus symbol	Pass	-
User C	2/1/17	3.1	Found page, added facebook.com	Pass	-
User C	2/1/17	3.2	Found page, clicked plus symbol	Pass	-

Table 8. Interface Testing – Round Two

3.14.1 Results/Notes

The CSS cues helped the user understand that they did not need to add 'http://www', thereby standardizing input. The user easily found the page that provides device blocking and could block the device we specified. Our proposed (feature) additions may require further testing. Users will be able to schedule how they block web addresses and devices. We will try to draw on existing layouts to make this feature more easily accomplished.

Functionality Test – This test is to determine if the website functions as expected. Project Canary team members easily conducted this test.

3.15 Functionality Test: Round One

For this test, we will be analyzing the addition of blacklisting websites (4.1), whitelisting websites (4.2), blacklisting devices (4.3), and whitelisting devices (4.4). Not only did we want to make sure the programming works, but the device controlled the access of a website (4.5), or device (4.6). Table 9 displays the Pass/Fail results and testing information for the first functionality test.

Tester	Date	Item	Actual	Pass/Fail	Glitch
J. Calhoun	1/26/17	4.1	Worked	Pass	-
J. Calhoun	1/26/17	4.2	Worked	Pass	-
J. Calhoun	1/26/17	4.3	Worked	Pass	-
J. Calhoun	1/26/17	4.4	Worked	Pass	-
J. Calhoun	1/26/17	4.5	Accessed	Fail	Code
J. Calhoun	1/26/17	4.6	Device access	Fail	Code
P. Galyen	1/26/17	4.1	Worked	Pass	-
P. Galyen	1/26/17	4.2	Worked	Pass	-
P. Galyen	1/26/17	4.3	Worked	Pass	-
P. Galyen	1/26/17	4.4	Worked	Pass	-
P. Galyen	1/26/17	4.5	Worked	Pass	-

P. Galyen	1/26/17	4.6	Device access	Fail	Code
D. Glover	1/26/17	4.1	Worked	Pass	-
D. Glover	1/26/17	4.2	Worked	Pass	-
D. Glover	1/26/17	4.3	Worked	Pass	-
D. Glover	1/26/17	4.4	Worked	Pass	-
D. Glover	1/26/17	4.5	Worked	Pass	-
D. Glover	1/26/17	4.6	Device access	Fail	Code

Table 9. Functionality Testing – Round One

3.15.1 Results/Notes

Jarrod noted some situations where the website that had been added was still accessible if "www" was changed to something else or omitted. In every case, the device that was listed to be blocked was not being blocked. We will expect making the Canary a DHCP may fix this issue.

3.16 Functionality Test: Round Two

After making a few changes to the programming, we decided to test it again. This time we focused solely on the device's ability to control the access of a website (4.5) and a device (4.6). Table 10 displays the Pass/Fail results and testing information for the fsecond functionality test.

Tester	Date	Item	Actual	Pass/Fail	Glitch
J. Calhoun	2/2/17	4.5	Worked	Pass	-
J. Calhoun	2/2/17	4.6	Device access	Fail	Code
P. Galyen	2/2/17	4.5	Worked	Pass	-

P. Galyen	2/2/17	4.6	Device access	Fail	Code
D. Glover	2/2/17	4.5	Worked	Pass	-
D. Glover	2/2/17	4.6	Device access	Fail	Code

Table 10. Functionality Testing – Round Two

3.16.1 Results/Notes

We will continue to focus on the issues discovered from testing. We are working with a programmer to resolve these issues, but at this point, they are not completely resolved. We are, however, confident they will be resolved within a week.

4.0 Project Management

4.1 Objectives & Deliverables

We intend to introduce a product that will bolster cybersecurity in a vulnerable segment of society. By providing individuals with technology that can first provide them tools that are relevant to their lives and then introducing easy to manage add-ons, and ultimately more complex modules.

The first hurdle was getting the OS installed. Next, Upgrade the OS. Then make it so the Raspberry Pi broadcasts a WiFi SSID. Figure 3 below is the Raspberry Pi that we used to create our Canary. We then created and manufactured a hard cover to place over the Pi so that it would not be exposed and potentially damaged.

Figure 3. Raspberry Pi

4.2 Budget

Figure 4 is the budget that we had for the entire fall and spring semester while working on Project Canary. The components were all bought at a local computer store here in Cincinnati and priced accordingly. We based our hourly price on the average dollar amount on a typical developer pay and of intrusion analyst salary, which the medians are between $65,000 and $75,000.

No.	Item	Unit, Each	Unit Price, $	Line Item Total
		Labor		
1	Collaboration	15	$35.00	$525.00
2	Research & Development	25	$35.00	$875.00
3	Project Management & Documentation	50	$35.00	$1750.00
4	Acquisition of Components	10	$35.00	$350.00
5	Production of Prototype/POC	70	$35.00	$2450.00
6	Marketing	15	$35.00	$525.00
Subtotal		185		$6475.00
		Components		
7	Raspberry PI	1	$30.00	$30.00
8	Raspberry PI Case	1	$10.00	$10.00
9	WiFi Dongle	1	$10.00	$10.00
10	Micro SD Card	1	$15.00	$15.00
11	Ethernet Cord	1	$2.00	$2.00
12	Mini USB Power Cord	1	$7.00	$7.00
Subtotal		6		$74.00
Total		**$6475.00 (labor)**	**$74.00(parts)**	**$6549.00**

Figure 4. Budget

4.3 Fall Semester Deadlines

Figure 5 and Figure 6 are the deliverables and timelines that our team set up for Project Canary. We wanted to make sure that all of the tasks that we set for ourselves had clear achievable goals and had specific end points to keep us on task and moving forward throughout the semester(s).

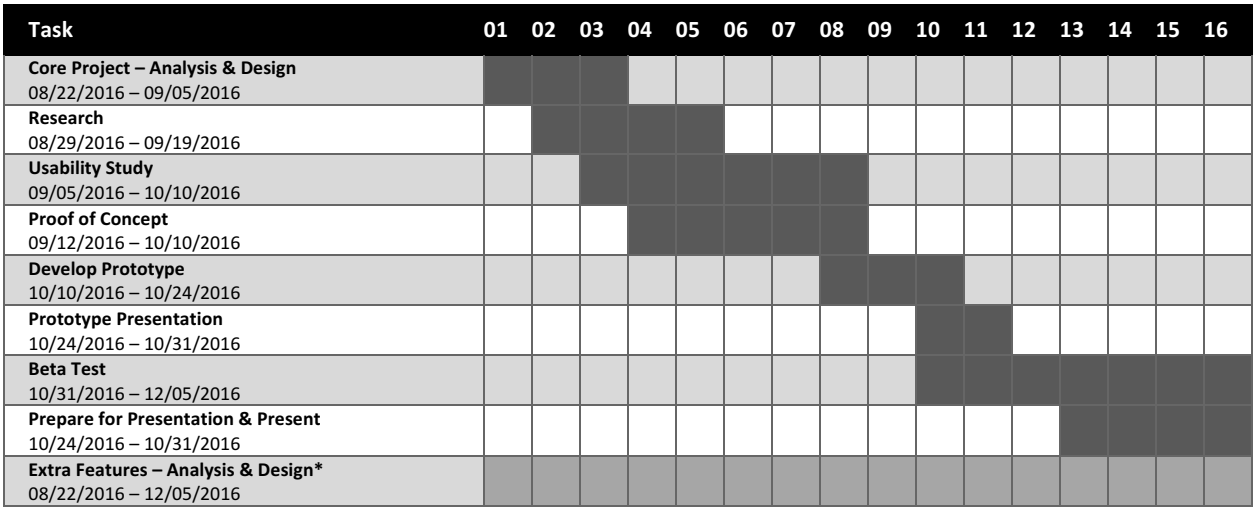


Figure 5. Fall Semester Deliverables **time permitting*

Task / Deliverables	Weeks	Corresponding Dates
Core Project – Analysis & Design Request Virtual Machine Test Virtual Machine Install Security Onion	01-03	08/22/2016 – 09/05/2016
Research Determine required application Remove superfluous applications	02-05	08/29/2016 – 09/19/2016
Usability Study Focus group, Use case model Wireframe any design features	03-08	09/05/2016 – 10/10/2016
Proof of Concept Prototype feasibility & Cost analysis Purchase hardware	04-08	09/12/2016 – 10/10/2016

Develop Prototype Setup prototype, Initial test	08-10	10/10/2016 – 10/24/2016
Prototype Presentation PowerPoint & Speech	10-11	10/24/2016 – 10/31/2016
Beta Test Extensive testing and revisions	10-16	10/24/2016 – 12/05/2016
Prepare for Presentation & Present Test production model, & Practice speech	10-11	10/24/2016 – 10/31/2016
Extra Features – Analysis & Design* Research and development	01-16	08/22/2016 – 12/05/2016

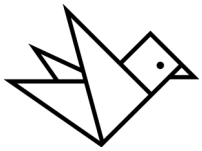
3.4 Spring Semester Deadlines

Task	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
Securing the Canary 01/09/2017 – 01/23/2017																
Securing the Code in the Canary 01/16/2017 – 02/06/2017																
Enhancing the Canary 01/23/2017 – 02/27/2017																
Beta Test 01/30/2017 – 02/27/2017																
Focus groups 02/27/2017 – 03/13/2017																
User Testing 03/13/2017 – 03/20/2017																
Rebuild / Redesign Based on Findings (1st) 03/13/2017 – 04/24/2017																
Focus Group / Test (2nd) 03/13/2017 – 04/24/2017																
Rebuild / Redesign Based on Findings (2nd) 04/03/2017 – 04/24/2017																
Extra Features – Analysis & Design* 01/09/2017 – 04/24/2017																

Figure 6. Spring Semester Deliverables **time permitting*

Task / Deliverables	Weeks	Corresponding Dates
Securing the Canary Test Security of the device	01-03	01/09/2017 – 01/23/2017
Securing the Code in the Canary Check the code for security flaws	02-05	01/16/2017 – 02/06/2017
Enhancing the Canary Revise usability	03-08	01/23/2017 – 02/27/2017

Beta Test Test the device in the real world	04-08	01/30/2017 – 02/27/2017
Focus Groups Discuss features target audience expects	08-10	02/27/2017 – 03/13/2017
User Testing Test among target audience	10-11	03/13/2017 – 03/20/2017
Rebuild / Redesign Based on Findings (1st) Address concerns that can be met in time allotted	10-16	03/13/2017 – 04/24/2017
Focus Group / Test (2nd) Create production model	10-16	03/13/2017 – 04/24/2017
Rebuild / Redesign Based on Findings (2nd) Develop presentation and talking points	13-16	04/03/2017 – 04/24/2017
Extra Features – Analysis & Design Research and development	01-16	01/09/2017 – 04/24/2017



5.0 Conclusion

In conclusion Project Canary is an out of the box home network security device; utilizing an intuitive graphical user interface for a simplified setup and administration. Project Canary has helped to bridge the technology gap between the business world and homeowners. Further research and work into this product can help bring this product into a greater position with integrating it into non-expensive home router, such as one provided by an Internet service provider. The main purpose of the project was to get everyday homeowners more cyberaware and to increase their overall cyber awareness. This issue is one that is continually to grow and Project Canary is a device to help your average homeowners think about this growing problem.

Bibliography

Desmond, Michael. "What You Should Know About Firewalls." *PC World.* November 25, 2004. http://www.pcworld.com/article/117557/article.html (accessed January 5, 2017).

Gibbs, Samuel. "Antivirus software is dead, says security expert at Symantec." *The Guardian.* March 6, 2014. https://www.theguardian.com/technology/2014/may/06/antivirus-software-fails-catch-attacks-security-expert-symantec (accessed January 5, 2017).

Miessler, Daniel. "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack." *Hewlett Packard.* July 29, 2014. https://community.hpe.com/t5/Protect-Your-Assets/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.WLu8mhiZNsP (accessed January 5, 2017).

NIST. *Risk Management Guide for Information Technology Systems.* Technical Report, U.S. Department of Commerce, National Institute of Standards & Technology, Gaithersburg, Maryland: National Institute of Standards & Technology, 2002, 55.

Oppenheimer, Priscilla. *Top-Down Network Design.* Indianapolis, Indiana: Cisco Press, 2011.

Pagliery, Jose. "Money." *CNN.* May 28, 2014. http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/ (accessed January 5, 2017).

Ponemon Institute. "2016 Cost of Data Breach Study: United States." Research Department, Ponemon Institute, Travrse City, Michigan, 2016, 24.

Raspberry Pi Foundation. *Raspberry Pi 3 Model B.* February 21, 2016. https://www.raspberrypi.org/products/raspberry-pi-3-model-b/ (accessed October 12, 2016).

Sanders, Chris, Chris Randall, and Jason Smith. *Applied Network Security Monitoring.* Waltham, Massachusetts: Syngress, 2013.

SANS. *Critical Controls for Effective Cyber Defense .* Bethesda, Maryland: SANS, 2008, 89.

Smith, Richard E. *Elementary Information Security.* Burlington, MA: Jones & Bartlett Learning, 2013.

Appendix A

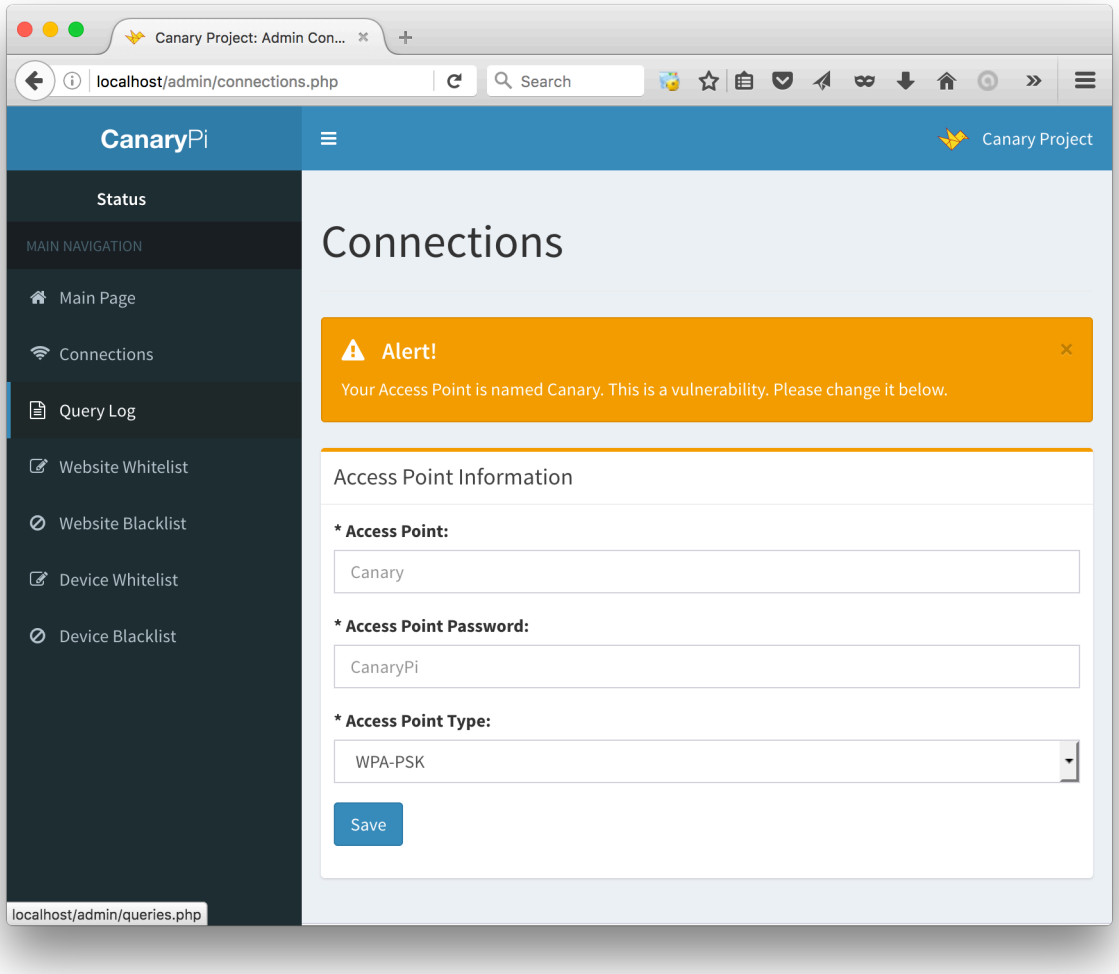


Figure 7. Access Point Customization

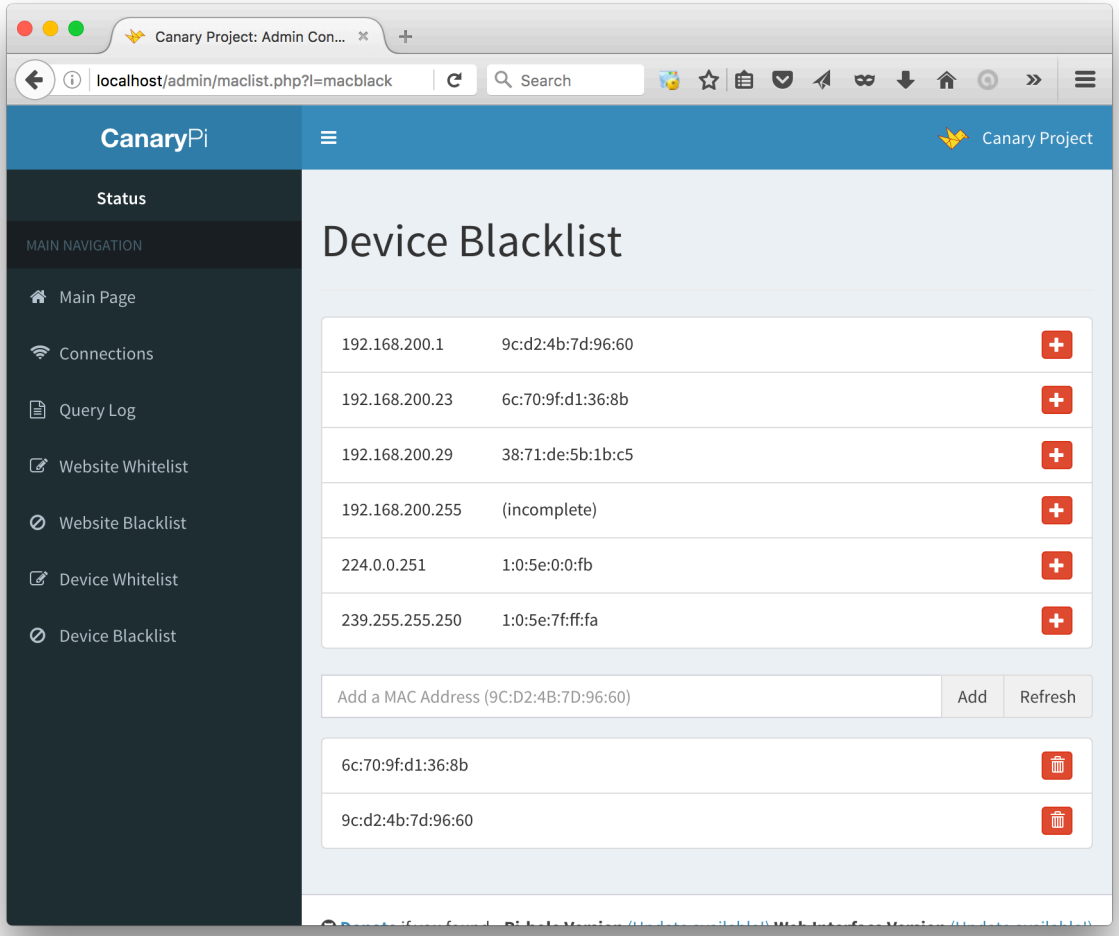


Figure 8. Blacklist Devices by MAC Address

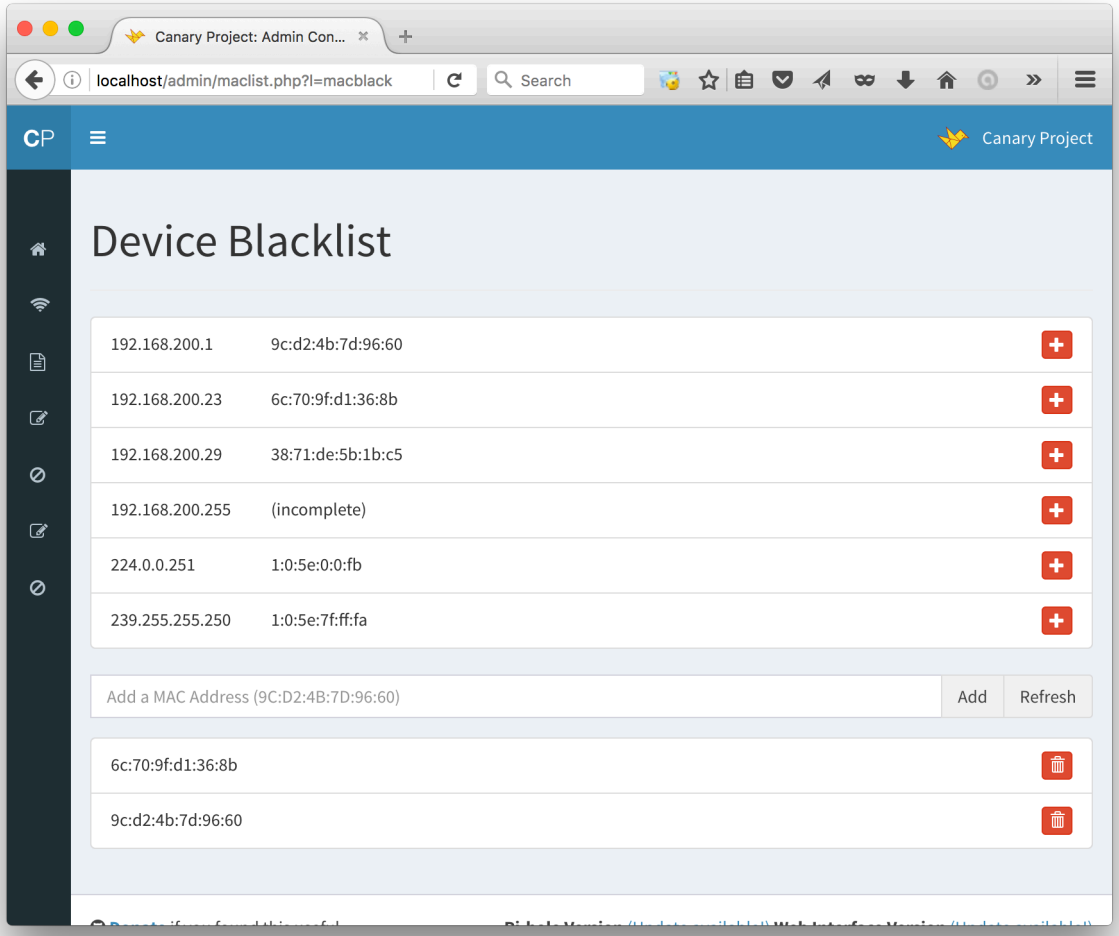


Figure 9. Responsive Design - Tablet Ready

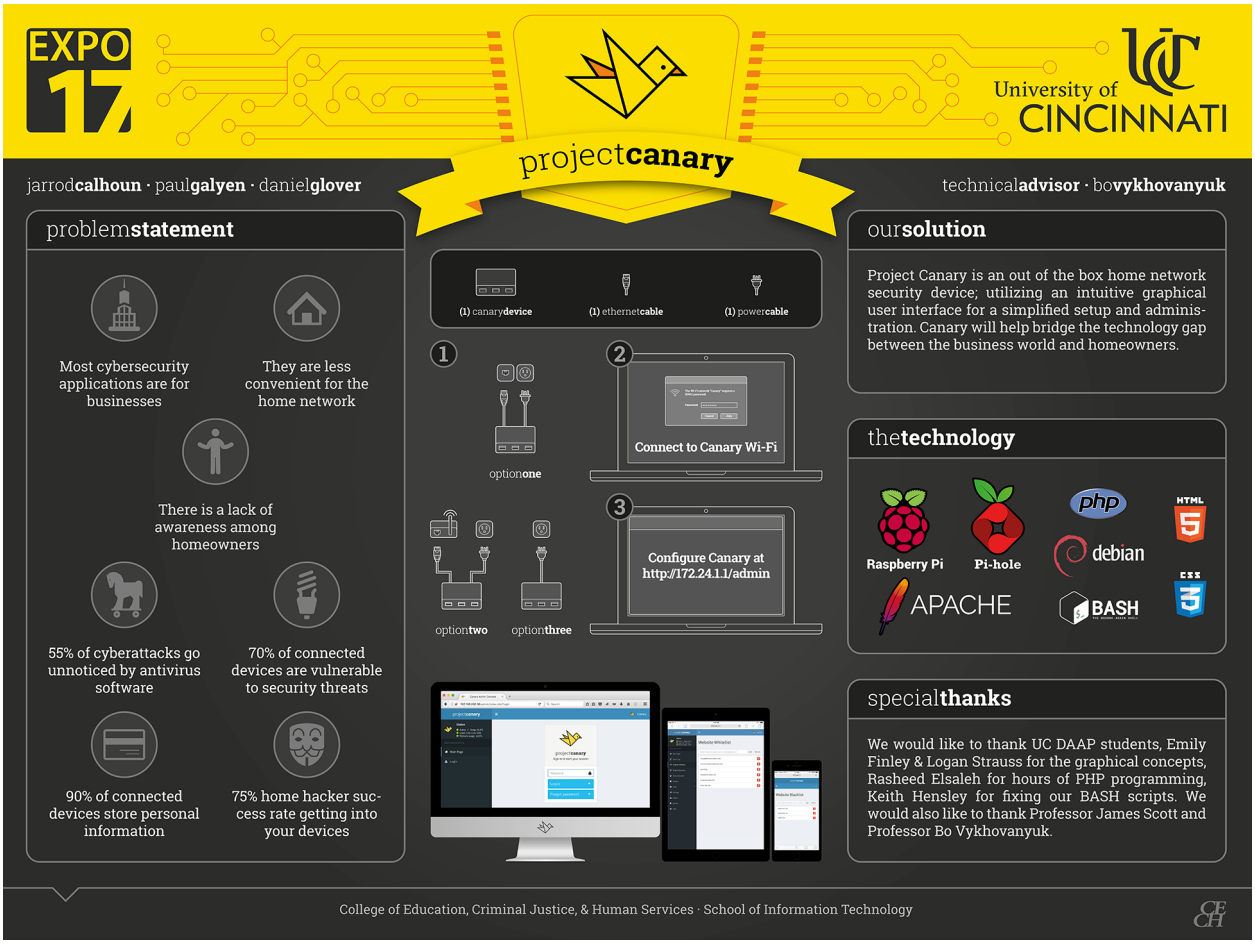


Figure 10. IT Expo Poster

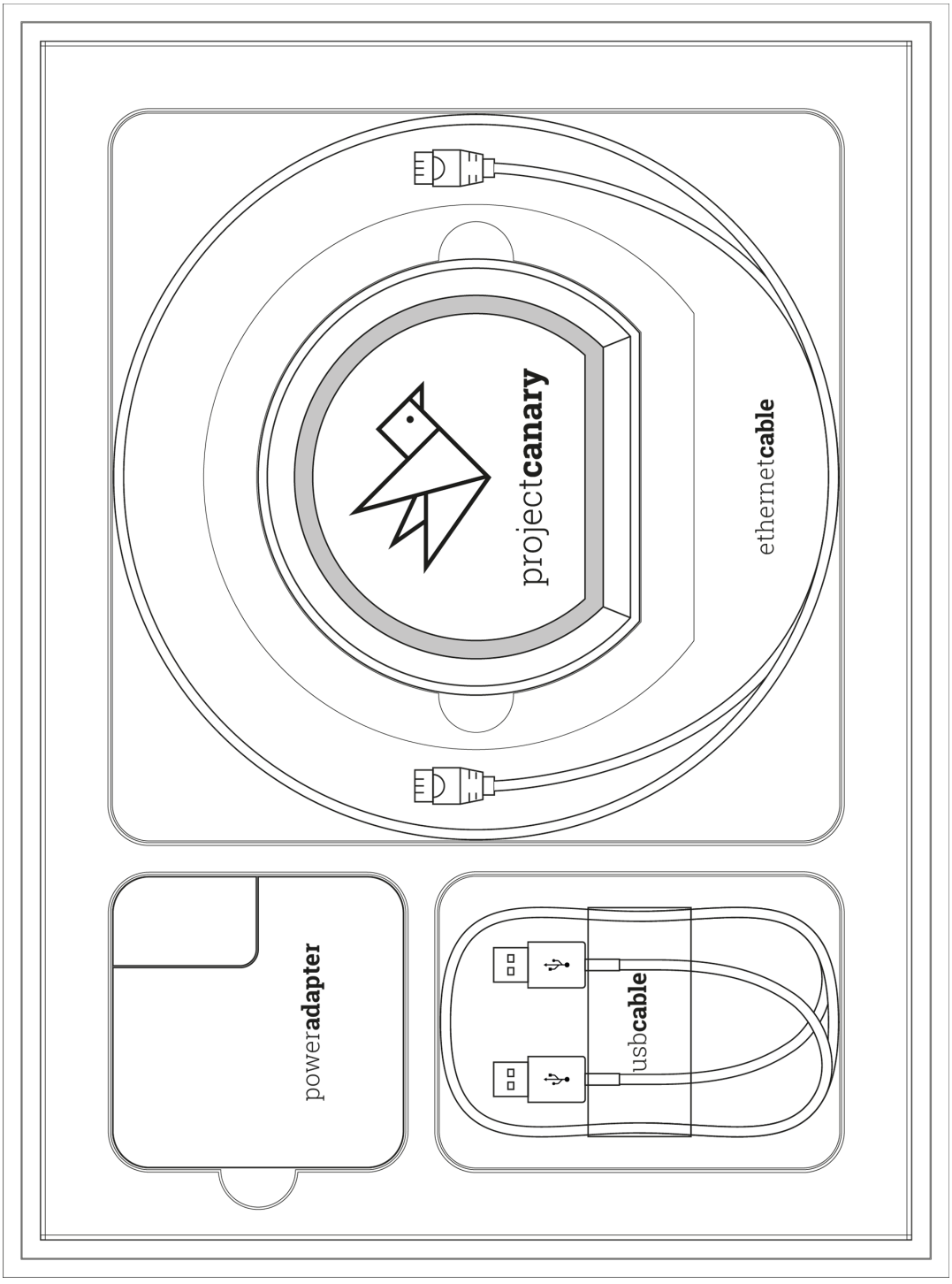


Figure 11. Packaging Concept