Borderless Asset Recovery Systems [B.A.R.S]

by

Leo Adams, Alex Smith, Tyler Stewart

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

Leo Adams, Alex Smith, Tyler Stewart — Date: 18 April 2016

Bogdan Vykhovanyuk
Faculty Advisor — Date: 18 April 2016

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

2016

Table of Contents:

Table of Figures:

Table of Tables:

Abstract:

Borderless Asset Recovery Systems [B.A.R.S] is a solution which has leveraged Security Incident and Event Management (SIEM) and log management technologies to enhance the location and recovery of lost and stolen electronic information systems. This is a feat which is easily achievable on a single network. Physical and logical network borders currently make locating and recovering electronic information systems improbable. By integrating technology and collaboration, personnel responsible for separate networks share information and data effectively removing those borders. Technologies have been configured to enable easy implementation of the [B.A.R.S] system on any network. Integration with existing log management and SIEM solutions has simplified the automation of alerts and updates for stolen and lost electronic information systems. Subscription to the service is affordable and simple for users of any network size.

Introduction:

Problem:

Very frequently, Electronic Information Systems (EIS) are lost or stolen. The assets themselves have varying value to their owners. More concerning is the value of the data on EIS's. The breach of confidentiality, integrity or availability of intellectual property, personally identifiable information, or other data which is difficult to recreate (ie. research data) can cause significant impacts to individuals and organizations. Recovery of EIS's and the data on them can potentially return value to people and organizations, whether it be in the form of time or money.

Solution:

Develop an Electronic Information System (EIS) repository which will allow law enforcement and IT staff to provide information about stolen/lost EIS information through a web application. Organizations will be able to pull the list of stolen/lost EIS Media Access Control (MAC) addresses from the repository for ingestion into their SIEM environments. When a stolen/lost EIS MAC address is located on an organization's network, the web application will receive notification from the organization's SIEM and will provide contact information for the network in which it was found to the original investigating source. Organizations can choose how often they receive updated repositories of stolen devices to match the bandwidth and capacity limits on their networks. Organizations can configure their SIEM solution(s) to produce an alert whenever a stolen/lost MAC address is detected on their network.

For example, a University of Cincinnati Police detective would work with UC's Office of Information Security to determine the MAC address for a stolen MacBook Pro with highly confidential research data. Together, they would then enter the MAC address and physical descriptive data into the web application. The web application would add the

record to a database which would be ingestible by any organization's SIEM environment through a web service. Once the Mac Book Pro is detected, the SIEM would trigger an alert that would connect with the [B.A.R.S] web service to update the database with a notification that the EIS has been found on a network. Contact information for UC's police department and OIS would be provided to the IT staff at the organization at which the EIS was located to coordinate further refinement in EIS location and retrieval of the EIS.

Project Goals:

- Increase the likelihood and improve the ability of organizations to recover lost and stolen electronic information systems through the use of available technologies in order to preserve the confidentiality, integrity, availability, and accountability of their potentially sensitive data.
- Provide a system to collect and share lost/stolen electronic information system identification details from customers in a mostly-automatic manner via secure network transportation technologies.
- Ensure robust security of systems for storage of sensitive customer data to meet any applicable compliance standards per NIST frameworks.
- Foster integration between our system and customer SIEM implementations by providing a variety of output formats and methods.
- Provide seamless user-experience through both the web interface and the data outputs to foster adoption of the system and increase its usage.

Discussion:

Project concept:

Using existing methodologies for recovery lost/stolen asset (i.e. Scrap Metal, Vehicles, Pawn Shops) and existing technical capabilities to create a system for recovery of lost/stolen electronic information systems.

Design Objectives:

Interface

- Account management
- User Management
- Asset Management
- Simple, guided implementation across other networks

Backend

- Integrates seamlessly and dynamically with the interface
- Securely transports and stores data

Methodology and Technical Approach:

Database Server:

1. Communicate with Web Application Server on Port 1521.
2. Store and maintain data integrity of [B.A.R.S] Database.
3. Up to date and free of any known or existing vulnerabilities.

Web Application Server:

1. Communicate with Database Server on Port 1521.
2. Host [B.A.R.S] Web Application, RESTful Web API and email services.
3. Up to date and free of any known vulnerabilities.

4. Maintain availability and reliability for customers and internal processes.

5. Secure communication between Web Application Server and RESTful Web API that communicates with [B.A.R.S] Splunk application.

Procedures:

Subscriber Registration

1. Navigate to barsrecovery.com.
2. Select the Login/Register navigation link.
3. Select the Signup button.
4. Complete the following fields:
    a. Organization Name
    b. Organization ID
    c. Contact First Name
    d. Contact Last Name
    e. Street Address
    f. Street Address 2
    g. City
    h. State
    i. Zip Code
    j. Country
    k. Email Address
    l. Password
5. Select the Complete Registration Button.
6. Confirm your email.
7. Login to [B.A.R.S] with your initial Subscriber account.

User Creation

1. Navigate to barsrecovery.com.
2. Select the Login/Register navigation link.
3. Select login and enter your credentials.
4. On the left navigation bar, select Administration.
5. Select Add User.
6. Complete the following fields:
    a. Username
    b. Contact First Name
    c. Contact Last Name
    d. Email Address
    e. Password
    f. Permission Level
7. Select the Complete Registration Button.
8. Confirm the email.
9. Login to [B.A.R.S] with the new user account.

Adding Devices

1. Navigate to barsrecovery.com.
2. Select the Login/Register navigation link.
3. Select login and enter your credentials.
4. On the left navigation bar, select Assets.
5. Select Add Asset.
6. Complete the following fields:

a. Asset Type

b. Asset Manufacturer

c. Asset Model

d. MAC Address(s)

e. Notes

7. Select monitor local if you wish to alert on occurrence of the device locally.

8. Select Add Another Asset or Complete.

Splunk App

1. Navigate to http://splunkbase.splunk.com

2. Search for and Download the [B.A.R.S] app

3. Install the [B.A.R.S] app in your Splunk instance, follow documentation for stand alone or cluster

4. Test the app's functionality by waiting 30 minutes, then go to the lookup table directory of the app and check for content in the app's lookup table. If this is populated, the app is functioning.

Testing:

Overview

This test plan will cover which aspects of the [B.A.R.S] system need to be tested prior to production roll-out. The scope, objectives, and requirements to meet the project's vision are outlined to guide the testing process through to completion.

Scope

[B.A.R.S] is made up of a complex backend with many moving parts which then translates into a very simple front end for Subscribers and Users. By making the system easy to use, organizations are more likely to subscribe for service and contribute to the overall success of the system. The testing will involve end to end testing of the web application and all subsequent functionality. This will also verify the functionality of the back end infrastructure.

Objective

Sharing data is the overall goal of [B.A.R.S]. Taking existing data and applying an alternate and practical use for it is the underlying principal. Making the system seamless to the users, and low-maintenance for the administrators is key for scalability and efficiency. The testing will verify the integrity of the source code.

Criteria

- Seamless connectivity between web-app and database
- Network connectivity seamless for users
- Roll-out to proof of concept customers
- Front end functionality requirements met
- Back-end functionality requirements met
- Database functionality requirements met
- Web-app functionality requirements met

System Testing

1. The system should allow access only to authorized users.
    a. Passwords should be at least 8 characters long.
    b. Passwords must include one number, one special symbol, one upper case, and/or one lowercase letter.
    c. Passwords must not be visible on screen when entered.
    d. Unauthorized users should not be able to gain access to the system.
    e. Error messages should be properly displayed.
    f. Depending on the user privileges, menu availability should vary.
    g. General users should not be able to modify subscriber information.
2. User should be able to view, add, and remove devices.
3. The subscripting user should be able to add, remove users.
4. Splunk App should install on client system correctly.
5. Connection to subscribers should be able to receive files from [B.A.R.S].
6. Subscribers should be able to send an alert to [B.A.R.S].

Budget (Implementation + Annual):

[B.A.R.S] Estimated Annual Budget			
Labor			
Position	**Hourly Rate**	**Hours**	**Total (Annual)**
Web Developer	$40	400	$16,000
Security Architect	$40	400	$16,000
Project Manager	$40	400	$16,000
Total	$120	1,200	$48,000
Equipment			
Hosted Virtual Environment			$500
Web Application Server			$650
Database Server			$650
SSL Certificate			$50
Domain Name			$25
Marketing			$1,000
Total			$2,875
			$50,875

Table 1: Budget

Task List:

Task	Duration	Start	End
Submit Project Proposal	3 days	M 8/24/15	W 8/26/15
Weekly Team Meeting: Fall	75.38 days	T 8/25/15	T 12/8/15
Complete Functionality Requirements	20 days	T 9/8/15	M 10/5/15
Find Corporate Sponsors	16 days	T 9/22/15	T 10/13/15
Develop Process Flow	6 days	T 9/22/15	T 9/29/15
Determine Functionality Requirements	11 days	T 10/6/15	T 10/20/15
Secure 3 Committed Customers	26 days	T 10/13/15	T 11/17/15
Build Virtual Test Environment	16 days	T 10/13/15	T 11/3/15
Develop [B.A.R.S] Web Service	16 days	T 10/20/15	T 11/10/15
Build Virtual Servers	21 days	M 12/7/15	M 1/4/16
Migrate from Test to Production Environment	30 days	M 12/7/15	F 1/15/16
Enable and Enforce SSL on Web Server	5 days	M 1/11/16	F 1/15/16
Update Gantt Chart	5 days	M 1/11/16	F 1/15/16
Weekly Team Meeting: Spring	70 days	W 1/13/16	M 4/18/16
Secure Production Environment	12 days	F 1/15/16	F 1/29/16
Establish Desired UI, Begin Build	5 days	T 1/19/16	S 1/24/16
OS Vulnerability Scan, Fix	5 days	M 1/25/16	F 1/29/16
Progress on UI	5 days	M 1/25/16	F 1/29/16
Begin Test Plan/Report	5 days	M 1/25/16	F 1/29/16
Prepare for Deliverables Presentation	5 days	M 1/25/16	F 1/29/16
Draft of UI Complete	5 days	M 2/1/16	F 2/5/16
Begin Draft of Documentation	5 days	M 2/1/16	F 2/5/16
Test Functional Solution with Test Data	5 days	M 2/8/16	F 2/12/16
Fix Issues, Clean Code and Website	5 days	M 2/15/16	F 2/19/16
Open Solution to Outside UC Network	5 days	M 2/15/16	F 2/19/16
Package and host Splunk App for [B.A.R.S] on Splunk Base	5 days	M 2/15/16	F 2/19/16
QA Test - Systems	6 days	M 2/22/16	M 2/29/16
Fix Issues, Clean Code and Website	5 days	M 2/22/16	F 2/26/16
Import Production Data for UC, Complete Live Testing	5 days	M 2/29/16	F 3/4/16
Roll Solution out to POC Participants with Documentation	5 days	M 2/29/16	F 3/4/16
Prepare Solution for Final Presentation	5 days	M 2/29/16	F 3/4/16
Finalize User Interface	29 days	W 3/2/16	S 4/10/16
QA Test - User Experience	14 days	W 3/2/16	S 3/20/16
Complete Testing, Fully Functional	5 days	M 3/7/16	F 3/11/16
Clean-Up, Maintain, Expand Solution	5 days	M 3/14/16	F 3/18/16
Incorporate Customer Data	10 days	M 3/21/16	F 4/1/16
Finalize Presentation Plan	6 days	M 3/21/16	S 3/27/16

Present at IT Tech Expo	1 day	T 4/12/16	T 4/12/16
PROJECT COMPLETION	5 days	M 4/18/16	F 4/22/16

Figure 1: Task List

Timeline:

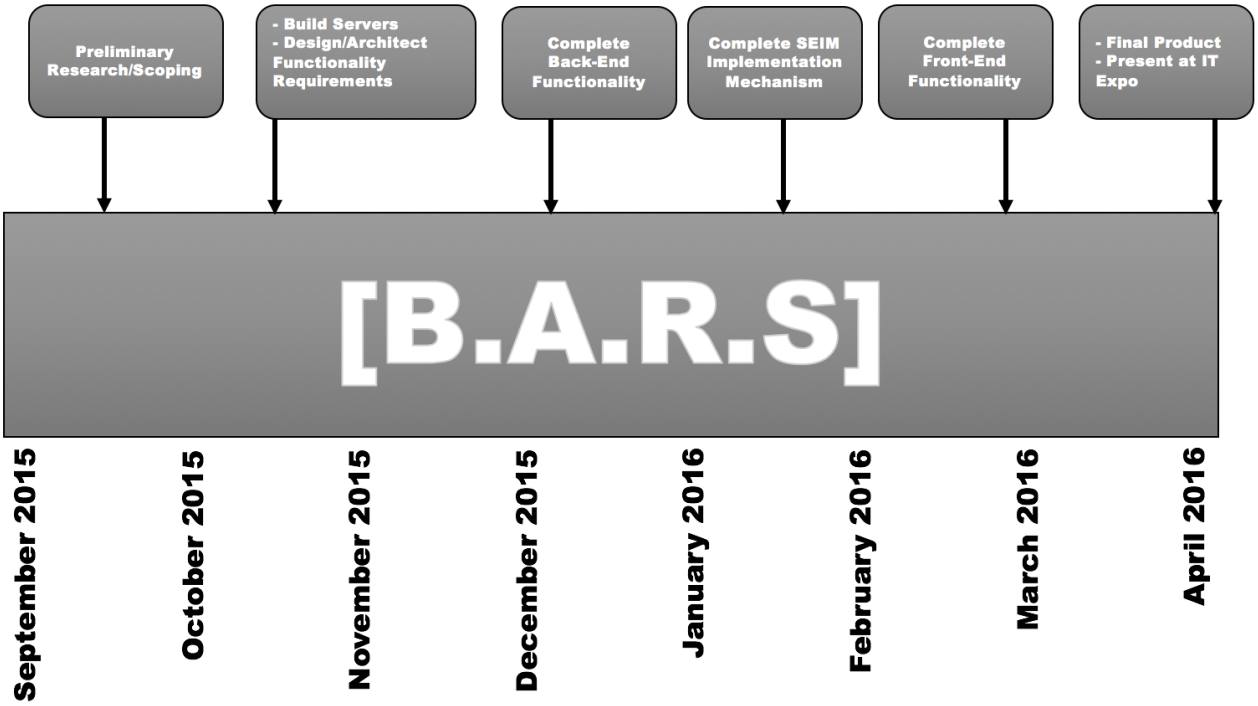

Figure 2: Timeline

Lessons Learned:

Concerns:

Are MAC Addresses Unique?

- Technically no. They can be spoofed and in rare cases MAC address collision can occur. However, MAC addresses are designed using a scheme enabling uniqueness and assigned as needed to network interface card vendors. There are over 281 trillion unique possible values for a standard 48-bit MAC address.

Not every network has log management.

- No, but the large networks where the majority of Electronic Information Systems

(EISs) will inevitably be found likely do. In cases that it is not existing, management can provide documentation and sources for implementation of the [B.A.R.S] solution in an ad-hoc manner.

Law Enforcement has higher priorities.

- In some instances, this may be the case. For example, it may not be worth the time and effort an officer in a busy city to recover a lost cell phone. However, there are a variety of uses. The solution in theory could be used to track down a criminal or a missing person. In some cases, recovery of very expensive hardware, valuable data or a large quantity of hardware may be worthwhile.
- Law enforcement may not always be required for recovery/identification. In some use cases maybe an organization purchases used hardware only to discover it is stolen property, or an employee does the same and connects to the network.

Challenges:

Implementation outside of the university network.

- This will cost approximately $1,875 per year. For a solution that has not yet monetized this is not easily recovered. Migrating to a cloud service would allow for more flexibility in hardware, naming and other important variables.

Effectiveness/coverage and monetization.

- [B.A.R.S] is not a catch-all solution. However, it has potential to be close to a catch-all. [B.A.R.S] is very dependent on coverage and participation. In addition, with more users, more powerful hardware will be required. To support sustainability and scalability the solution must be monetized. This is awkward because until coverage is achieved, the solution holds limited value to the users.
- A subscription charging model could in theory be put in place with a free tier, an

extended free tier for networks who monitor, then paid tiers and a reduced price paid tiers for networks which monitor data.

Conclusion:

Problems Encountered and Analysis of Problems Solved:

- Thus far the primary problem is finding potential partners to help test the project. After asking four IT entities with relatively large networks, Miami University has agreed to participate. With their assistance we can complete the testing phase and have a successful proof of concept. Pending the positive experience, they may help spread the word to others.
- The technical portion of the [B.A.R.S] solution is quite complex and difficult to explain and demonstrate in a short amount of time. [B.A.R.S] will be built out for a very quick Splunk implementation. Many entities use Splunk as a means of log management. The ease of use should increase adoption rates for the solution.

Future recommendations/Recommendations for Improvement:

- Functionality is yet to be implemented on the front-end. However, back-end functionality and a completely successful process flow for the solution has been proven.

References:

1. “RFC 7042 - IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters” last modified October, 2013, http://www.iana.org/assignments/ethernet-numbers/ethernet-numbers.xml.
2. “Stolen car detection system and method”, Grant: US 5568406 A, publication date October 22, 1996, https://www.google.com/patents/US5568406.

Appendix A: User Profiles

User Profile Form
Application: Borderless Asset Recovery Systems [B.A.R.S]
Potential User: Admins
Software and Interface Experience: Admins will require back-end access to both the Database and Web Application Server. They should understand how the system works and be able to manage accounts, updates, code and underlying data.
Experience with Similar Applications: Oracle Databases. Web Application Servers. REST-APIs. SIEM/log management solutions.
Task Experience: System Administration (updates, configurations, troubleshooting). Development (Web App, REST APIs, Oracle DB). Security (SIEM Alerting/Reporting and management, IPTables, IDS/IPS, account management).
Frequency of Use: Daily.

Key Interface Design Requirements that the Profile Suggests: Does not apply to this profile. Management can all be handled on the back end of the application.

User Profile Form
Application: Borderless Asset Recovery Systems [B.A.R.S]
Potential User: Subscribers
Software and Interface Experience: Can add/remove electronic information system data through the application. Can add additional users with limited access to organization data (users). Can configure settings for their organization, their account, and user accounts. Installation/configuration of system on local resources.
Experience with Similar Applications: Active Directory. Windows Explorer. Other Web Applications.
Task Experience: Enterprise Application Management. User Management.
Frequency of Use: Can range from daily to monthly or less frequently.
Key Interface Design Requirements that the Profile Suggests: Login Page Configure - Organization settings. - Account settings. - Subordinate settings. Information - FAQ. - Installation Instructions/Documentation. - Support. Data Management - Add/Remove/Edit electronic information systems. - View/Report on electronic information systems.

User Profile Form
Application: Borderless Asset Recovery Systems [B.A.R.S]
Potential Users Users
Software and Interface Experience: Can add electronic information system data through the application. Can remove data they have added. Can configure their own account settings.
Experience with Similar Applications: Social media. Any web application (front end). Database entry.
Task Experience: Data entry.
Frequency of Use: Can range from daily to monthly or less frequently.
Key Interface Design Requirements that the Profile Suggests: Login Page Configure - Account settings. Information - FAQ. - Support -> Redirect to their subscriber. Data Management - Add electronic information systems to organization. - Remove/Edit their own entries. - View/Report on electronic information systems.

Appendix B: Use Case Diagram

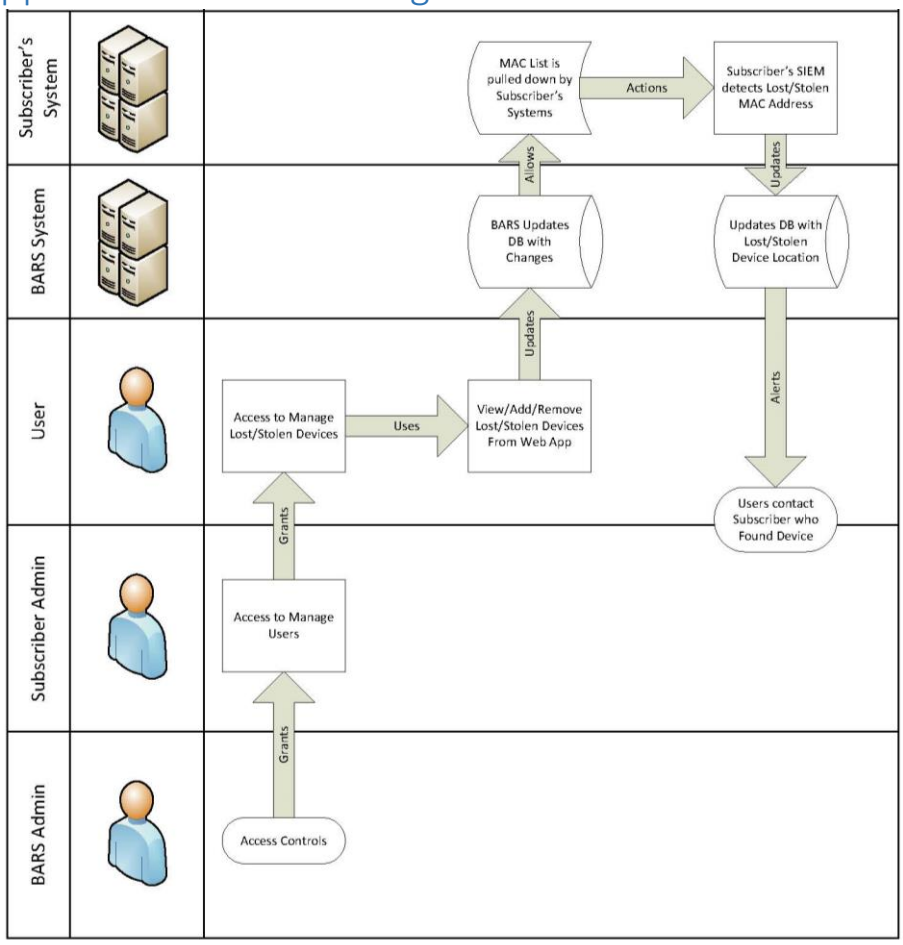

Figure 3: Use Case Diagram

Appendix C: Testing Reports

Item	Test Case	Input	Expected Output	Actual Output	Pass/Fail	Reason for Success/Failure	Date
1a.	1	Bob	Error	Error	Pass	It Works	4/6
1b.	1	L0v3B.Ar$	Success	Success	Pass	It Works	4/6
1c.	1	L0v3B.Ar$	Not Visible	Not Visible	Pass	It Works	4/6
1d.	1	CindyLoo	Error	Error	Pass	It Works	4/6
1e.	1	CindyLoo	Error	Error	Pass	It Works	4/6
1f.	1	Login	Menu	Menu	Pass	It Works	4/6
1g.	1	Modify	Deny	N/A	N/A	N/A	2/18
2	1	Add,Modify,Remove	Success	N/A	N/A	N/A	2/18
3	1	Add,Modify,Remove	Success	N/A	N/A	N/A	2/18
4	1	Install	Success	Success	Success	It Works	3/10
5	1	Connect	Success	Success	Success	It Works	3/10
6	1	Alert	Success	Success	Pass	It Works	3/10

Table 2: Testing Results

Appendix D: Gantt Chart

ID	Task Name
1	Submit Project Proposal
2	Weekly Team Meeting: Fall
29	Complete Functionality Requirements
22	Find Corporate Sponsors
23	Develop Process Flow
24	Determine Functionality Requirements
21	Secure 3 Committed Customers
25	Build Virtual Test Environment
20	Develop [B.A.R.S] Web Service
19	Build Virtual Servers
27	Migrate from Test to Production Environment
64	Enable and Enforce SSL on Web Server
65	Update Gantt Chart
35	Weekly Team Meeting: Spring
28	Secure Production Environment
66	Establish Desired UI, Begin Build
67	OS Vulnerability Scan, Fix
68	Progress on UI
69	Begin Test Plan/Report
70	Prepare for Deliverables Presentation

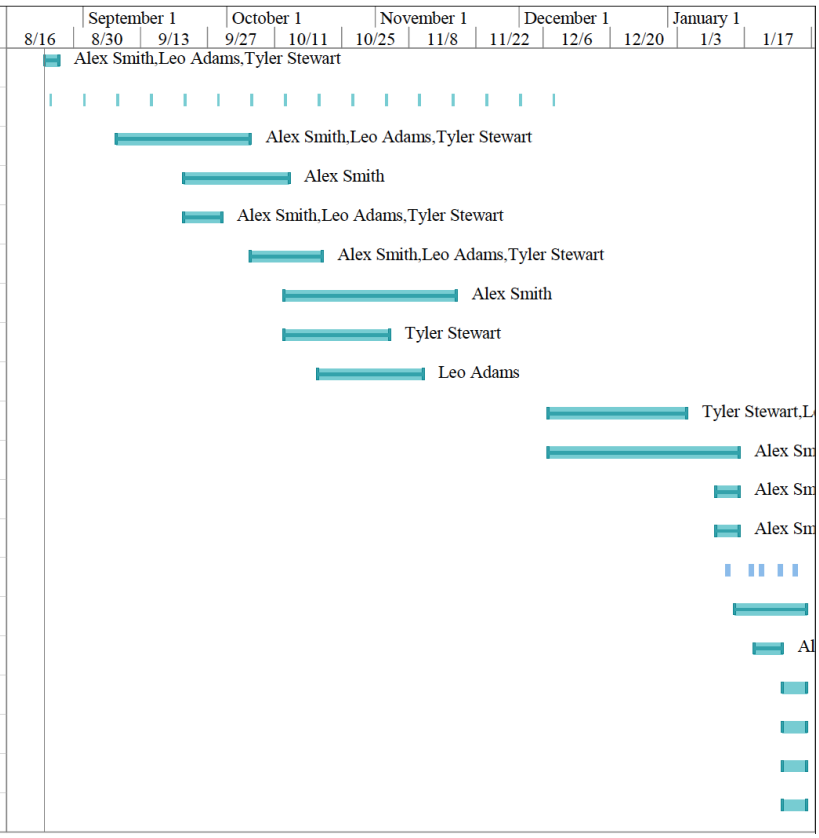

Table 3: Full Gantt Chart Part 1

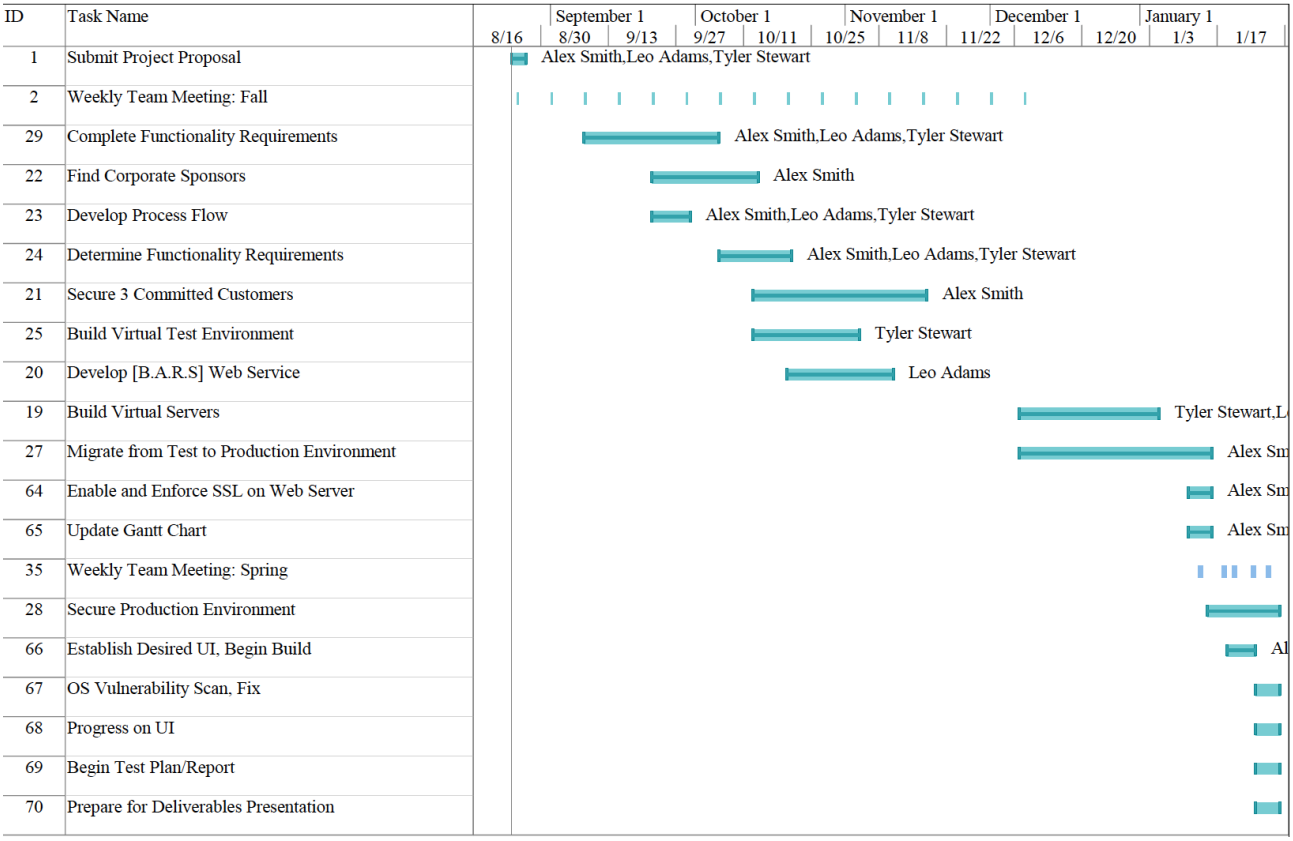

Table 4: Full Gantt Chart Part 2