Research and Development of an Unmanned Aerial Vehicle to Automate Monitoring of Wireless Access Points

Kenneth L. Bernstein

Follow this and additional works at: http://digitalcommons.apus.edu/theses
Part of the Computer Security Commons, and the Science and Technology Studies Commons

Recommended Citation
APUS Library Capstone Submission Form

This capstone has been approved for submission to and review and publication by the APUS Library.

<table>
<thead>
<tr>
<th>Student Name [Last, First, MI]</th>
<th>Bernstein Kenneth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course Number [e.g. INTL699]</td>
<td>ITCC698 Paper Date [See Title pg.] 05/2015</td>
</tr>
<tr>
<td>Professor Name [Last, First]</td>
<td>Dr. Watson-Stone, Novadean</td>
</tr>
<tr>
<td>Program Name *</td>
<td>See list Master of Science in Information Technology</td>
</tr>
<tr>
<td>Keywords [250 character max.]</td>
<td>wireless, wireless access, wireless security, automation, UAV, 802</td>
</tr>
<tr>
<td>Passed with Distinction * Y or N</td>
<td>Y</td>
</tr>
<tr>
<td>Security Sensitive Information * Y or N</td>
<td>N</td>
</tr>
<tr>
<td>IRB Review Required * Y or N</td>
<td>N</td>
</tr>
<tr>
<td>Turnitin Check * Y or N</td>
<td>Y</td>
</tr>
</tbody>
</table>

* Required

If YES, include IRB documents in submission attachments.

All capstone papers must be checked via Turnitin.

Capstone Approval Document

The thesis/capstone for the master's degree submitted by the student listed (above) under this title *

RESEARCH AND DEVELOPMENT OF AN UNMANNED AERIAL VEHICLE TO AUTOMATE MONITORING OF WIRELESS ACCESS POINTS

has been read by the undersigned. It is hereby recommended for acceptance by the faculty with credit to the amount of 3 semester hours.

<table>
<thead>
<tr>
<th>Program Representatives</th>
<th>Signatures</th>
<th>Date (mm/dd/yyyy)</th>
</tr>
</thead>
</table>
| Signed, 1st Reader * capstone professor | Novadean Watson-Stone | Digitally signed by Novadean Watson-Stone
DN: cn=Novadean Watson-Stone
ou=American Public University System
o=APUS, email=hwatson@apus.edu, c=US
Date: 2015.07.07 11:18:23-04'00' |
| Signed, 2nd Reader (if required by program) | Novadean Watson-Stone | Digitally signed by Novadean Watson-Stone
DN: cn=Novadean Watson-Stone
ou=American Public University System
o=APUS, email=hwatson@apus.edu, c=US
Date: 2015.07.07 11:18:23-04'00' |
| Recommendation accepted on behalf of the program director * | Novadean Watson-Stone | Digitally signed by Novadean Watson-Stone
DN: cn=Novadean Watson-Stone
ou=American Public University System
o=APUS, email=hwatson@apus.edu, c=US
Date: 2015.07.07 11:18:23-04'00' |
| Approved by academic dean * | Dan Benjamin | Digitally signed by Dan Benjamin
DN: cn=Dan Benjamin
ou=American Public University System
o=APUS, email=dbenjamin@apus.edu, c=US
Date: 2015.07.08 11:57:09 -04'00' |

* Required
RESEARCH AND DEVELOPMENT OF AN UNMANNED AERIAL VEHICLE TO
AUTOMATE MONITORING OF WIRELESS ACCESS POINTS

A Master Thesis

Submitted to the Faculty

of

American Military University

by

Kenneth L. Bernstein

In Partial Fulfillment of the
Requirements for the Degree

of

Master of Science

June 2015

American Military University

Charles Town, WV
DEDICATION

I dedicate this to my family and friends, who have given me their support, encouragement, understanding, and most importantly, their undying love. Without them, this would not have been possible.
ACKNOWLEDGEMENTS

I wish to thank the faculty and staff of American Military University for their facility during the writing of this thesis and over the course of this degree. Their assistance has been much appreciated. My graduate advisor, Dr. Novadean Watson-Stone, has been of particular support during the writing of this thesis, providing guidance through an otherwise formidable process. Her encouragement and belief that I could succeed has ultimately led me to this point.
ABSTRACT OF THE THESIS

RESEARCH AND DEVELOPMENT OF AN UNMANNED AERIAL VEHICLE TO AUTOMATE MONITORING OF WIRELESS ACCESS POINTS

by

Kenneth Lawrence Bernstein

American Military University, June 2015

Charles Town, West Virginia

Dr. Novadean Watson-Stone, Thesis Professor

The proliferation of wireless access to privileged networks in the enterprise introduces a potentially large attack surface and a unique set of security concerns. Using wireless technologies, attacks against the network are based on proximity rather than physical access. Currently, the monitoring of an organization’s wireless access points, including security auditing, is performed by IT security professionals in a time-consuming process, if performed at all. This project addresses the need for an efficient system to monitor a campus’ wireless landscape by developing an autonomous unmanned aerial vehicle containing wireless monitoring components. This vehicle will be constructed using commercial off-the-shelf hardware and software, and will be capable of automatically traversing a preset course while monitoring and logging data from all 802.11 wireless access points within range, including malicious access points. Ultimately, this unmanned aerial vehicle was constructed and tested successfully, but sustained damage during testing, placing the project in an out-of-scope condition for both time and financial resources. Therefore, this project can be considered a partial success.

Keywords: wireless, wireless access, wireless security, automation, UAV, 802.11
TABLE OF CONTENTS

COPYRIGHT PAGE

DEDICATION

ACKNOWLEDGMENTS

ABSTRACT OF THE THESIS

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER

I. INTRODUCTION

Significance of Project

Description of Project

Project Schedule

II. LITERATURE REVIEW

Description of Project Consistency with Course of Study

Wireless Communications Overview: History and Modalities

Development of 802.11 Standards

The Physics of Electromagnetic Radiation
Development of Wireless Security

Wired Equivalent Privacy

Wi-Fi Protected Access

Wi-Fi Protected Access 2

WPA-2 Enterprise

WPA2-Personal

Wireless Attack Methods

Passive Attacks

Sniffing

Active Attacks

Denial of Service (DoS)

Application Layer Exploits

EAP Attacks

Data Packet Injection

Evil DNS Server

Rogue Access Point (Rogue AP)

ARP Spoofing

UAV as Research and Development Platform
Technological Automation

Historical Responses to Technological Automation

Effect of Technological Automation on Workplace Dynamics

Legal and Ethical Questions

Public Response to the Use of Drones

Legality of the Use of UAVs

Section 333 Exemption

Special Airworthiness Certificate (SAC)

Ethical Use and Misuse of Security Tools

Objectives Achieved Through Completion of Project

OBJ1

OBJ2

OBJ3

OBJ4

OBJ5

OBJ6

Future Objectives to Consider

Conclusion
III. FINDINGS LOG/JOURNAL

Project Journal

Week 1
Week 2
Week 3
Week 4
Week 5
Week 6
Week 7
Week 8
Week 9
Week 10
Week 11
Week 12
Week 13
Week 14
Week 15
Week 16
AUTOMATED UAV WAP MONITORING

Week 17 ................................................................................................................................

Week 18 ................................................................................................................................

Week 19 ................................................................................................................................

Project Experience vs. Theoretical Knowledge ................................................................

Limitations and Biases ........................................................................................................

Limitations ..............................................................................................................................

Biases ................................................................................................................................

IV. THE PROJECT ....................................................................................................................

Outcomes ................................................................................................................................

Recommendations for Further Research ..............................................................................

Collision Avoidance System (CAS) ........................................................................................

Real-Time Telemetry ............................................................................................................... 

Crash Cage ..............................................................................................................................

Real-Time Video ......................................................................................................................

Post-Mortem ...........................................................................................................................

Schedule ................................................................................................................................

Budget ...................................................................................................................................

Satisfaction ..............................................................................................................................
Scope ............................................................................................................................................................

Negotiating Skills ...........................................................................................................................................

Staffing ...........................................................................................................................................................

Skills and Training .........................................................................................................................................

Project Planning and Reporting ....................................................................................................................

Development Approach ................................................................................................................................

Contractors, Consultants, and Vendors ........................................................................................................

General Issues ..............................................................................................................................................

Lessons Learned............................................................................................................................................

V. LIST OF REFERENCES .................................................................................................................................

VI. APPENDICES................................................................................................................................................

Appendix A: List of Acronyms ........................................................................................................................

Appendix B: Initial/Final Requirements .......................................................................................................... 

Appendix C: Cost Breakdown ..........................................................................................................................

Appendix D: Project Media ............................................................................................................................... 

Appendix E: Sponsor Endorsement ..................................................................................................................
LIST OF TABLES

TABLE

1. 802.11 Standards .................................................................................................................................

2. Project Schedule ....................................................................................................................................

3. Commonly Used Non-802.11 Wireless Communication Protocols ......................................................

4. Comparison of 802.11 Amendments .....................................................................................................

5. Weaknesses Associated with WEP .........................................................................................................

6. Possible Attacks Against WPA2-Enterprise ........................................................................................

7. Wireless Attack Methods and Project Detectability .............................................................................

8. Definition of Automation .....................................................................................................................


10. Project Objectives ...............................................................................................................................
LIST OF FIGURES

FIGURE

1. Growth of Mobile vs. Total Internet Traffic

2. Illustrative Graph of Total Signal Strength vs. Distance from Emitter

3. Amazon Prime Air Drone
Introduction

Wireless Local Area Network (WLAN) communication allows the use of Electromagnetic (EM) radiation as a communication medium between radio-enabled devices and a wired network. The first use of EM waves for internetwork communication took place at the University of Hawaii in 1971. Dubbed ALOHANET, this wireless communication scheme used packet radio communication between seven campuses across four islands (Seymour & Shaheen, 2011). In 1985, the Federal Communications Commission (FCC) authorized the public use of the Industrial, Scientific, and Medical (ISM) frequency bands at 900 MHz, 2.4 GHz, and 5.8 GHz allowing commercial development of WLAN technology (Seymour & Shaheen, 2011). Wireless LAN technology is becoming the preferred method of network access in the home, and with the rapid adoption of Bring Your Own Device (BYOD) policies, wireless access is becoming increasingly popular in the workplace (Somalwar & Nguyen, 2014).

Significance of Project

One of the primary security considerations of WLAN access is that it can be considered a “touchless” system, meaning no physical interaction with a network is required by a user wishing to access it. Therefore, it is not necessary for an attacker to have physical contact with a privileged network in order to attempt unauthorized access. Instead, the attacker can set up wireless equipment anywhere within transmission range of the Wireless Access Point (WAP). Table 1 lists several commonly used 802.11 WLAN standards, and describes aspects of each, including transmission distances. A WAP emits Radio Frequency (RF) waves outward to a maximum effective distance as defined by the specific standard being used. Depending on the particular 802.11 standard used as well as the physical placement of the WAP, there is a possibility the wireless signal can be acquired from outside the building, eliminating the need for
an attacker to perform physical infiltration. This presents an attack surface which is extremely attractive to an attacker as it represents both an increase in the total attack surface, and a significant decrease in physical risk associated with malicious activities. It is this wireless attack surface which will be researched, and which the project associated with this thesis seeks to mitigate. By doing so, the overall security of the network will be increased.

**Table 1**

*802.11 Standards (Harwood, 2009).*

<table>
<thead>
<tr>
<th>IEEE Standard</th>
<th>Frequency (GHz)</th>
<th>Speed (Mb/s)</th>
<th>Topology</th>
<th>Transmission Range (Indoors)</th>
<th>Access Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11</td>
<td>2.4</td>
<td>1-2</td>
<td>Ad hoc/Infrastructure</td>
<td>20 ft.</td>
<td>CSMA/CA</td>
</tr>
<tr>
<td>802.11a</td>
<td>5</td>
<td>54</td>
<td>Ad hoc/Infrastructure</td>
<td>25-75 ft.</td>
<td>CSMA/CA</td>
</tr>
<tr>
<td>802.11b</td>
<td>2.4</td>
<td>11</td>
<td>Ad hoc/Infrastructure</td>
<td>150 ft.</td>
<td>CSMA/CA</td>
</tr>
<tr>
<td>802.11g</td>
<td>2.4</td>
<td>54</td>
<td>Ad hoc/Infrastructure</td>
<td>150 ft.</td>
<td>CSMA/CA</td>
</tr>
<tr>
<td>802.11n</td>
<td>2.4/5</td>
<td>300</td>
<td>Ad hoc/Infrastructure</td>
<td>175+ ft.</td>
<td>CSMA/CA</td>
</tr>
</tbody>
</table>

**Description of Project**

This project is concerned with automating the discovery, inventory, baselining, and auditing of WAPs. For the Information Security (IS) professional, these tasks comprise part of Risk Assessment (RA) and management duties. Discovery of all devices and data associated with the network is one of the first steps of a formal RA, and is of such importance that no protection scheme can be devised or implemented until all assets are known and documented (Schou &
Shoemaker, 2007). This process is also known as baselining the network, as it represents a complete picture of the network to be defended at the outset of the process.

The second difficulty this project addresses is that of auditing WAPs; noting their locations, SSIDs, signal strengths, etc., in order to confirm that no equipment is failing, has failed, has been moved to a new location, or that new, unauthorized equipment has been put in place. The placement of unauthorized equipment in an enterprise environment could be an indicator of a Rogue AP or an Evil Twin/Evil Server, both of which are common wireless attack methods in which an attacker places their personal WAP within range of the physical network with the intention of harvesting user credentials and/or sensitive information traversing the network (Cache, Wright & Liu, 2010). This project is especially suited for the detection of these Rogue Access Points and “Evil” servers, and can also detect a number of ongoing, active attacks.

Given both the necessity of initial discovery/baselining and ongoing auditing of wireless networks, it would seem prudent to develop a method which would automate these tasks. This project attempts to do so, and involves the adaptation of an Unmanned Aerial Vehicle (UAV), specifically, a multi-engine craft capable of hovering, commonly known as a Quadcopter, and designated as a personal or hobby craft. This type of UAV was chosen for the following reasons:

- **Cost:** Because this type of UAV is marketed to individuals as a hobby or non-commercial craft, the overall cost of flying and maintaining crafts of this type is relatively low.
- **Maintenance and Repair:** As stated above, this type of craft is targeted toward the hobbyist. Therefore, maintenance, replacement, and repair is relatively straightforward using Commercial Off-the-Shelf (COTS) hardware and software.
• Ease of Use: Hobby UAVs are easy to use, containing hardware guidance boards which keep the craft stable in flight. Due to their use as a hobby craft, the mechanics of flight are well-known and easy to learn.

• Customizability: As part of a hobby market, a great number of options exist for customization, decreasing the necessity for custom designed and built solutions.

While presenting many advantages, the use of UAVs also carries with it some disadvantages, which include:

• Future Federal Aviation Administration (FAA) Regulations: The FAA is currently evaluating the use of Unmanned Aerial Systems (UASs), which includes the type of hobby craft to be used in this project. Although exemptions exist in the Special Rule for Model Aircraft, the FAA is currently enacting regulation for the future use of this type of craft. For commercial use, FAA approval is required, either through obtaining a Special Airworthiness Certificate in either the experimental or restricted categories, or by an exemption through Section 333 (Federal Aviation Administration, 2015a).

• Weather Factors: The use of any flying craft depends on relatively calm weather conditions, specifically, the amount of steady and gusting wind. Under high wind conditions, the stability and overall airworthiness of UAVs is questionable.

• Interference with UAV: Although not specifically limited to hobby UAVs, the use of any unmanned, autonomous drone carries with it the risk of individuals interfering, damaging, or otherwise obstructing the performance of its duties, either accidentally, or with malicious intent.
Project Schedule

Because this project involves three components – hardware, software, and documentation – and since the timeline is fixed and relatively short at sixteen weeks total, it is imperative that a schedule be established. The following schedule, shown in Table 2, has been produced so that it is realistic, attainable, and should contain enough redundancies that unforeseen events will have a minimal impact on the project outcome.

Table 2

*Project Schedule.*

<table>
<thead>
<tr>
<th>Week Number</th>
<th>Objective</th>
<th>Tasks to Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Identify project requirements and appropriateness</td>
<td>Determine feasibility of project&lt;br&gt;Compile requirements of project&lt;br&gt;Determine scope of project&lt;br&gt;Make adjustments to project based on above results&lt;br&gt;Purchase/use laboratory notebook for project archives</td>
</tr>
<tr>
<td>2</td>
<td>Increase knowledge of project</td>
<td>Begin theoretical and background research&lt;br&gt;Begin practical research on UAV platform&lt;br&gt;Begin preliminary literature review</td>
</tr>
<tr>
<td>3</td>
<td>Determine specific hardware platform</td>
<td>Continue both theoretical and practical research&lt;br&gt;Determine UAV platform based on requirements&lt;br&gt;If appropriate UAV platform unavailable, research alternatives</td>
</tr>
<tr>
<td>4</td>
<td>Evaluate project and propose changes if required</td>
<td>Evaluate appropriateness of design&lt;br&gt;Make changes to project based on this evaluation</td>
</tr>
<tr>
<td>5</td>
<td>Increase knowledge and incorporate changes if required</td>
<td>Continue research&lt;br&gt;Produce high-level project designs&lt;br&gt;If changes made to project, incorporate into project plan</td>
</tr>
</tbody>
</table>
### Table 2 – continued

<table>
<thead>
<tr>
<th></th>
<th>Begin writing documentation and order project hardware</th>
<th>Write project thesis introduction Order appropriate UAV and/or components</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Design project research</td>
<td>Determine areas/types of research and acceptance criteria Determine bug bars and quality gates Write project thesis research design document</td>
</tr>
<tr>
<td>8</td>
<td>Finish preliminary research and literature review</td>
<td>Continue theoretical and practical research Finish writing project thesis literature review Begin UAV platform construction, if required Begin writing draft project thesis document</td>
</tr>
<tr>
<td>9</td>
<td>Hardware testing and software design</td>
<td>Test UAV platform for airworthiness Determine requirements for collision avoidance system Determine project software requirements</td>
</tr>
<tr>
<td>10</td>
<td>Software development</td>
<td>Begin authoring software based on project requirements</td>
</tr>
<tr>
<td>11</td>
<td>Software development and change assessment</td>
<td>Continue software development Assess requirements and changes made to project Incorporate changes to project as required</td>
</tr>
<tr>
<td>12</td>
<td>Software testing/project thesis draft</td>
<td>Continue software development Begin integration testing as appropriate Finish writing first draft of project thesis</td>
</tr>
<tr>
<td>13</td>
<td>Hardware/software integration and testing</td>
<td>Continue to integrate hardware and software Continue integration testing of UAV</td>
</tr>
<tr>
<td>14</td>
<td>Finish integration testing and perform final testing</td>
<td>Finish integration testing Begin functional testing Begin writing final project thesis</td>
</tr>
<tr>
<td>15</td>
<td>Finish project and submit final project thesis</td>
<td>Finish functional testing Finish and submit final project thesis</td>
</tr>
<tr>
<td>16</td>
<td>Project wrap-up</td>
<td>Examine lessons learned Archive documentation Post project multimedia presentation</td>
</tr>
</tbody>
</table>
Literature Review

Description of Project Consistency with Course of Study

Because this project addresses the issue of automating the important albeit repetitive tasks of WAP discovery, baselining, inventory, auditing, and threat control, this review of the current literature will examine:

- The explosive growth of wireless communication technologies and security protocols
- The advantages of automating the aforementioned tasks
- The use of UAV drones as an effective platform to perform these tasks.

As a result, this literature review will conclusively demonstrate the consistency of this project with the graduate course of study in Information Technology with a specialization in Information Assurance and Security.

Wireless Communications Overview: History and Modalities

Wireless communication amongst computing devices has become a ubiquitous presence in the Information Technology (IT) landscape. Since the implementation of the first packet-based radio communication network at the University of Hawaii in 1971, the research and development of wireless technology has undergone exponential growth (Seymour & Shaheen, 2011). Currently, there exist many different technologies and protocols for such communication, with research being conducted on the use of the millimeter wave band at 60 GHz with data transfer rates exceeding 1 Gb/s, the development of so-called “smart” antennas, schemas for the coexistence of data and television transmissions, and the development of Smart Utility Networks (Sherif & Maeda, 2011). Standards and descriptions for currently used non-802.11 wireless protocols are given in Table 3.
In 1985, the FCC made available the Industrial, Scientific, and Medical (ISM) frequency bands at 900 MHz, 2.4 GHz, and 5.8 GHz for commercial development of wireless communication (Seymour & Shaheen, 2011). These frequencies were viewed with ambivalence
by developers at the time. Researchers were attracted to the open development environment these frequency bands provided, as FCC licensure was no longer required for their use. However, interference from other users in these bands was notably significant and reduced the performance of early systems in terms of both performance and coverage (Seymour & Shaheen, 2011).

**Development of 802.11 standards.** WLAN communication protocols and technologies were developed as a direct subset of the IEEE 802 standard, which describes wired LANs and Metropolitan Area Networks (MANs). Arguably, the most well-known 802 protocol is IEEE 802.3; Ethernet (Wicks & Kemerling, 2004). In 1997, the 802.11 working group released the first WLAN standard, and two task groups, TFa for 802.11a and TFb for 802.11b, were formed to develop specific wireless communication standards. By 1999, the two amendments, 802.11a and 802.11b were completed. 802.11b utilized the 2.4 GHz band with a maximum data rate of 11 Mb/s, while 802.11a utilized the 5 GHz band with a maximum data transfer rate of 54 Mb/s (Wicks & Kemerling, 2004). Each of these protocols had individual strengths and weaknesses. 802.11a had much greater data transfer rates, but the cost of implementing 5 GHz radio transmissions at the time made efficient use of this frequency band impossible (Kim & Lee, 2015). Conversely, 802.11b enjoyed the relatively inexpensive 2.4 GHz band, but data transfer rates greater than 11 Mb/s were ultimately desired. Ultimately, the goal at the time was to achieve data transfer rates of at least 54 Mb/s using the 2.4 GHz band, and the newly formed 802.11g task force (TFg) decided to use the physical (PHY) and media access control (MAC) specifications from 802.11a (Kim & Lee, 2015). Table 4 compares the different 802.11 amendments.

In 2003, the 802.11g amendment was released. It used a combination of modulation methods to achieve the required data transfer rates using the 2.4 GHz band. However, Internet
data and multimedia usage continued to grow, and a new task force was charged with achieving wireless data rates of up to 100 Mb/s in a new amendment to be known as 802.11n. The 802.11n standard was released in 2009, and achieved High Throughput (HT) by using Multiple-Input Multiple-Output (MIMO) methods such as Spatial Division Multiplexing (SDM), Space Time-Block Coding (STBC), and Transmit Beamforming (TxBF) (Kim & Lee, 2015).

In 2013, the 802 working group released the 802.11ac amendment, which achieved Very High Throughput (VHT) by adding novel MIMO methods such as Downlink Multi-User MIMO (DL MU-MIMO), which achieved throughput rates of greater than 1 Gb/s (Kim & Lee, 2015). Currently, research is being conducted in many different 802.11a* standards, as can be seen in Table 4.

As is demonstrated by the partial list of wireless communication modalities presented in Table 4, the use of wireless communication between computing devices is both increasing and diversifying. This growth represents not only an increase in the number of different protocols available for communication, but its importance to network communications overall. This synergistically coupled growth of wireless devices is displayed in Figure 1. In 2013, there were 5 billion wirelessly connected devices worldwide (Baldemair, et al., 2013), which represents 0.71 wireless devices per human on Earth. It is this ever increasing importance and dependence on wireless communication that will be leveraged by this project, thus demonstrating its significance to the field of network security and communications as a whole.
## Table 4

*Comparison of 802.11 Amendments.*

<table>
<thead>
<tr>
<th>Name</th>
<th>Approved</th>
<th>Title</th>
<th>Maximum Data Rate</th>
<th>Modulation</th>
<th>Frequencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11</td>
<td>1997</td>
<td>IEEE Standard for Wireless LAN Media Access Control MAC and Physical Layer PHY Specifications</td>
<td>1 – 2 Mb/s</td>
<td>FHSS, DSSS, IR</td>
<td>2.4 GHz</td>
</tr>
<tr>
<td>802.11a</td>
<td>1999</td>
<td>Higher Speed PHY Extension in the 5 GHz Band</td>
<td>54 Mb/s</td>
<td>OFDM</td>
<td>5 GHz</td>
</tr>
<tr>
<td>802.11b</td>
<td>1999</td>
<td>Higher Speed PHY Extension in the 2.4 GHz Band</td>
<td>11 Mb/s</td>
<td>DSSS</td>
<td>2.4 GHz</td>
</tr>
<tr>
<td>802.11g</td>
<td>2003</td>
<td>Further Higher Data Rate Extension in the 2.4 GHz Band</td>
<td>54 Mb/s</td>
<td>DSSS, OFDM</td>
<td>2.4 GHz</td>
</tr>
<tr>
<td>802.11n</td>
<td>2009</td>
<td>High Throughput</td>
<td>100 Mb/s</td>
<td>OFDM</td>
<td>2.4/5 GHz</td>
</tr>
<tr>
<td>802.11ac</td>
<td>2013</td>
<td>Very High Throughput</td>
<td>&gt; 1Gb/s</td>
<td>OFDM</td>
<td>5 GHz</td>
</tr>
<tr>
<td>802.11ad</td>
<td>2012</td>
<td>Very High Throughput 60 GHz</td>
<td>&gt; 6 Gb/s</td>
<td>Low Power OFDM</td>
<td>60 GHz</td>
</tr>
<tr>
<td>802.11ah</td>
<td>2016 (est.)</td>
<td>Sub 1 GHz</td>
<td>40 Mb/s</td>
<td>OFDM</td>
<td>900 MHz</td>
</tr>
<tr>
<td>802.11aj</td>
<td>2016 (est.)</td>
<td>China Millimeter Wave</td>
<td>&gt; 10 Gb/s</td>
<td>OFDM</td>
<td>45/60 GHz</td>
</tr>
<tr>
<td>802.11ax</td>
<td>2019 (est.)</td>
<td>High Efficiency WLAN</td>
<td>14 Gb/s</td>
<td>MIMO-OFDM</td>
<td>2.4/5 GHz</td>
</tr>
<tr>
<td>802.11ay</td>
<td>2017 (est.)</td>
<td>Next Generation 60 GHz</td>
<td>100 Gb/s</td>
<td>OFDM</td>
<td>60 GHz</td>
</tr>
</tbody>
</table>
The physics of electromagnetic radiation. Since wireless communication utilizes an EM field as a substrate, it is important to consider two critical factors regarding EM fields. The first consideration is that of effective communication distance. EM radiation decays according to the distance from the radiating source, in this case, the antenna. This distance can be subdivided into three zones, or regions, each of which has a different associated rate of field decay. These three zones are referred to as (from nearest the emitter to farthest) the reactive near field, the radiative near field (Fresnel region), and the far field. In the reactive near field region, the electrostatic field term becomes most significant, causing the EM field to decay as the cube of the distance between the antenna and receiver ($1/r^3$). In the radiative near field region, the EM
field decays as the square of the distance ($1/r^2$), and in the far field, the rate of decay can be viewed as linear ($1/r$) (Brewster, 2009). The relative proportions of these three regions and a graphical representation of EM decay are illustrated in Figure 2, which is presented for illustrative purposes. Note that both the reactive near field and far field regions display asymptotic behavior, while the Fresnel region is dominant. In practical use, the reactive near field and far field are not considered. In the case of the reactive near field, the distances are located so close to the emitter (antenna) that they do not represent any practical use for wireless communication (Brewster, 2009). The far field is not considered because the strength of the signal has decayed enough that it cannot effectively be detected by modern wireless receivers. Therefore, in practical terms, the rate of EM decay over distance is considered to be $1/r^2$, and the power density in Watts per meters squared (W/m$^2$) of the EM field created by the emitter can be represented $S = \frac{P_{tx}}{4\pi d^2}$ where $S$ is the power density, $P_{tx}$ is the transmission power level, and $d$ is the distance from the emitter (Holt & Huang, 2010). Because the effective radiated power also decays as the square of the distance, this represents a limiting factor in terms of communication distance.
The second consideration when using EM radiation for wireless communication is that the signal is available to anyone within range who has the proper equipment to capture and demodulate it. It is this fact that makes wireless communication an attractive vector for attack. Concerns over the confidentiality and integrity of wireless messages sent and received between a wireless client and the associated WAP has been a primary concern and area of research and development from the onset of its use (Kim & Lee, 2015), and the implementation of encryption methods was seen as the solution to securing these communications.

**Development of wireless security.** The necessity for security associated with the use of 802.11 communication has been recognized from the onset of its initial implementations. The rapid development and improvements made with each iteration of security methods demonstrates its overall importance within the 802.11 standard.
Wired equivalent privacy. The initial security model developed for wireless communication was released with the original IEEE 802.11 standard in 1999. Known as Wired Equivalent Privacy (WEP), it was meant to provide protection of confidentiality and integrity of wireless communications, as well as access control to the network. WEP accomplished this through the use of an RC4 stream cipher using a 40-bit WEP key, combined with a 24-bit random number known as an Initialization Vector (IV) (Wong, 2003). The sender of the message XORs the stream cipher with the plaintext data, creating an encrypted data stream. This ciphertext is formed into a standardized packet and transmitted to the receiver, which uses the stored WEP key to decode the message. WEP was released prior to the finalization of the full wireless security standard described in IEEE 802.11i, and as an interim protocol, was not subjected to peer scrutiny prior to release (DeBeasi, 2004; Wong, 2003). WEP was later found to have several serious security vulnerabilities associated with its use. These vulnerabilities are enumerated and described in Table 5.

Table 5
Weaknesses Associated with WEP
**Wi-Fi protected access.** In 2003, after WEP received a significant amount of peer review and was found to be unsuitable for security purposes, the Wi-Fi Alliance released an interim protocol known as Wi-Fi Protected Access (WPA), a partial implementation of the 802.11i standard, which provided updated security protocols for wireless communication. WPA utilized a subset of the 802.11i standard solely concerned with addressing and mitigating the weaknesses present in WEP (Rumali & Chaudhari, 2011). In order to overcome the security flaws present in WEP, WPA provided three new protocols; 802.1X Extensible Authentication Protocol (EAP), Temporal Key Integrity Protocol (TKIP), and the Michael Message Integrity Check (MMIC) (Seymour & Shaheen, 2011; Wong, 2003). As a subset of 802.11i, WPA only implemented those changes necessary to overcome the weaknesses in WEP, and as such, did not implement features such as Secure IBSS (ad-hoc mode), secure fast handoff (VoIP), or advanced encryption protocols (Rumali & Chaudhari, 2011).

**Wi-Fi protected access 2.** An updated IEEE 802.11i security protocol suite was released with the ratification of the IEEE 802.11i standard in 2004. Known as WPA2, it utilized the full implementation of the 802.11i standard, and offered security improvements over WPA. The

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEP Key Recovery</td>
<td>WEP uses the same key for transmission, and the IV space is limited to the range 0-16,777,215 (Wong, 2003). Therefore, the IVs are reused, and an attacker can collect enough of these IVs to crack the WEP key.</td>
</tr>
<tr>
<td>Unauthorized Decryption</td>
<td>Having recovered the WEP key, an attacker can freely decrypt and read transmitted messages, as well as modify messages in transit.</td>
</tr>
<tr>
<td>Poor Key management</td>
<td>There is no mechanism in place to renew compromised WEP keys (such as in the case of termination of an employee), The new key must be entered into the WAP manually. Although this does not present a difficulty in a home or SOHO environment, in the enterprise, this task can be seen as nearly impossible (Wong, 2003).</td>
</tr>
<tr>
<td>Lack of Access Point Authentication</td>
<td>WEP only provides a method for Network Interface Cards (NICs) to authenticate WAPs, and no method for the AP to authenticate the NIC. Therefore, an attacker could possibly reroute data flow through an unauthorized path (Wong, 2003).</td>
</tr>
</tbody>
</table>
encryption standard used in WPA2 was the Advanced Encryption Standard (AES), a strong encryption method supporting 128-bit, 192-bit, and 256-bit keys. The use of AES offered greater security than RC-4/TKIP used in WPA (Rumhali & Chaudhari, 2011). WPA2 introduced two modes of operation; Personal and Enterprise.

**WPA2-enterprise.** WPA2-Enterprise is a managed security service using EAP protocol with a separate authentication server, thus separating the message privacy and integrity functions from user authentication. This separation creates a security schema which is extremely scalable and therefore attractive to the enterprise (Sakib, Jaigirdar, Munim & Akter, 2011).

Authentication occurs using the 802.1X authentication standard. The three actors during the authentication process are the client joining the network (supplicant), The WAP (authenticator), and the server which makes authentication decisions (RADIUS). While WPA2 is a complete implementation of 802.11i, there have been a number of potential security weaknesses identified with its use. There are four operational phases associated with the authentication process;

1. Security policy agreement
2. 802.1X authentication
3. Key derivation and distribution/Master key (MK) distribution by RADIUS
4. RSNA data confidentiality and integrity.

Because data confidentiality and integrity are not defined until the fourth step, steps one through three are non-secured, leading to the possibility of compromise of the supplicant or authenticator (Sakib, Jaigirdar, Munim & Akter, 2011). The possible attack methods against WPA2-Enterprise are presented in Table 6. Because WPA2-Enterprise contains the potential security weaknesses enumerated in Table 6, the importance of securing wireless communication in the enterprise is markedly elevated.
WPA2-personal. WPA2-Personal offers many of the same improvements over WPA as does WPA2-Enterprise, but does not utilize an authentication server. Instead, it relies solely on the client and WAP generating a 256-bit PSK from a plaintext pass phrase, or string. Since user authentication is not separated from message integrity and privacy, WPA2-Personal does not offer the scalability of WPA2-Enterprise, and is most suited for personal home use or SOHO settings (Sakib, Jaigirdar, Munim & Akter, 2011).

<table>
<thead>
<tr>
<th>Actor Affected</th>
<th>Operation Compromised</th>
<th>Description of Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplicant</td>
<td>Security policy agreement</td>
<td>Rogue AP can collect and extract security policy information.</td>
</tr>
<tr>
<td>Supplicant</td>
<td>802.1X authentication</td>
<td>PSK can be sniffed since it is transmitted in plaintext.</td>
</tr>
<tr>
<td>Supplicant</td>
<td>Key derivation and distribution</td>
<td>PTK, GTK, KEK, and KCK can be sniffed because they are transmitted in plaintext.</td>
</tr>
<tr>
<td>Authenticator</td>
<td>Security policy agreement</td>
<td>Attacker can compromise WAP by sending security policies that have a 1 in 100 chance of matching those of the authentication system.</td>
</tr>
<tr>
<td>Authenticator</td>
<td>802.1X authentication</td>
<td>WAP can be forced to send authentication request to RADIUS server by the attacker using a dictionary attack to send identity or PSK and by spoofing MAC.</td>
</tr>
</tbody>
</table>

Wireless Attack Methods
Preventing attacks against WAPs was one of the main motivations behind this project, and a description of possible attack methods will both illuminate the necessity for vigilance in monitoring the location and status of WAPs as well as provide a register of attack methods specifically suited to be detected by the autonomous UAV. Note that with any type of wireless attack, the attacking computer needs to be within range of the wireless signal. Table 7 lists these attack methods and presents a determination of applicability of these methods to this project.

**Passive attacks.** Passive attacks require no direct interaction with the target network and consist solely of network traffic monitoring. This type of attack does not insert any data or commands into the target network.

**Sniffing.** Wireless sniffing refers to the act of placing a computer within range of a WAP and monitoring traffic without transmitting any data to the WAP. With the proliferation of small single board computers (SBCs) such as Raspberry Pi and Arduino, concealment of the computing device would be straightforward. Software tools available for passive sniffing include airodump-ng and Ferret/Hamster for stealing HTTP cookies (Cache, Wright & Liu, 2010).

**Active attacks.** Active attacks require the attacker to send data or command packets into the network, or to directly interact with the target network in some way. This classification of attack is diametrically opposed to passive attack methods, as it requires a dynamic interaction between the attacking client and the target.

**Denial of service (DoS).** DoS attacks involve an attacking computer sending a large amount of requests to a target WAP in order to overwhelm the WAP with useless demands, thus making it difficult, if not impossible, for normal users to utilize the WAP. In an enterprise setting, the most common form of DoS attack is a deauthorization attack, whereby the attacker
sends deauthorization packets (deauth) to the WAP, immediately ending all user sessions (Cache, Wright & Liu, 2010). Software available for this type of attack includes aireplay-ng, Kismet, and Void11. DoS attacks against enterprise targets can be part of a coordinated attack, such as setting up a rogue Access Point (AP) (Low, 2005).

**Application layer exploits.** In a typical attack, the attacker will often pursue weaknesses in applications. According to 2013 data from the National Vulnerability Database (2015), Internet Explorer, Oracle Java, Mozilla Firefox, and Adobe Flash Player were among the top twelve applications for the total number of vulnerabilities present. The software “tool of choice” for application layer exploits amongst attackers is metasploit (Cache, Wright & Liu, 2010).

**EAP attacks.** Extensible Authentication Protocol (EAP) is available in many vendor-specific or vendor-agnostic types. Core EAP types include EAP-MD5 and EAP-TLS. Microsoft developed PEAP, and Cisco has developed LEAP and EAP-FAST. Specific attack tools have been developed for many types of EAP, including asleap for LEAP, eapmd5pass for EAP-MD5, and FreeRADIUS-WPE for PEAP and EAP-TLS. All EAP implementations are vulnerable to compromise of the confidentiality of authentication credentials (Cache, Wright & Liu, 2010).

**Data packet injection.** This attack involves directly sending specifically crafted packets toward a client on the network, which appear as if they have originated from the WAP itself. This can be a simpler alternative to getting a network client to browse the attacker’s network (Cache, Wright & Liu, 2010). Software available to automate this process include AirPWN, airtun-ng, and IPPON.

**Evil DNS server.** This attack is able to send the target’s DNS traffic to a server which is under the control of the attacker. In this way, the target can be redirected to any malicious site
the attacker wishes, or in conjunction with Cross Site Request Forgery (CSRF), a router’s web interface can be exploited. There are no automated tools for this purpose, so an attacker would have to manually set up a DHCP server, known as a Rogue DHCP Server (Cache, Wright & Liu, 2010). Once the DHCP server is running, Metasploit’s browser_autopwn plugin can be used to set up the Evil DNS server.

**Rogue access point (Rogue AP).** A rogue AP is an access point set up and controlled by an attacker which will lure users onto the AP by dynamically setting the SSID of the rogue AP according to user’s Probe Request packets. These packets list the APs the user wishes to connect to, and contains desired setup data such as SSID, encryption type, and authorization type. The attacker then customizes the rogue AP to satisfy these requirements. This process (with the exception of setting up the DHCP server) can be automated using Metasploit with KARMA plugins, commonly known as Karmetasploit (Cache, Wright & Liu, 2010).

**ARP spoofing.** In this attack, the attacker sends spoofed (false) Address Resolution Protocol (ARP) messages in order to bind the attacker’s MAC address with the target’s IP address in order to redirect traffic from the host to the attacker. Popular targets for ARP spoofing are the default gateway. Ettercap is a popular software tool that automates this process.

As is demonstrated by the information in Table 7, this project will be most effective against an attacker’s use of Rogue or Evil servers against the target network. Other attack methods can only be detected during the active phase of an attack, when radio signals are being transmitted by the attacking client.

**Table 7**

<table>
<thead>
<tr>
<th>Attack Method</th>
<th>Description</th>
<th>Affects</th>
<th>Possibility</th>
<th>Comments</th>
</tr>
</thead>
</table>

*Wireless Attack Methods and Project Detectability*
| **Sniffing** | Passively monitoring wireless communication. | Confidentiality | None | Can only detect active EM signals. |
| **Denial of Service** | Sending large amount of requests to WAP, overwhelming its ability to respond to other users. | Availability | High | Always detects an active attack. |
| **Application Layer Exploits** | Leveraging vulnerabilities present in software applications. | Integrity, Availability | Low | Can only pinpoint transmitter location (if active). |
| **EAP Attacks** | Using specific attacks against EAP to bypass authentication. | Confidentiality, Integrity | Medium | Can only detect active attack. |

Table 7 – continued

| **Data Packet Injection** | Sending specifically crafted packets to client on network. | Confidentiality, Integrity | Medium | Can only detect active attack |
| **Evil DNS Server** | Controlling target DNS traffic for redirection or router control. | Confidentiality, Integrity | Very High | Will always detect. |
| **Rogue Access Point** | Lures network users to an AP controlled by the attacker. | Confidentiality | Very High | Will always detect. |
| **ARP Spoofing** | Send false ARP messages to redirect traffic to attacker. | Confidentiality | Medium | Detects active attack. |

**UAV as Research and Development Platform**

Drones have enjoyed a recent upsurge in popularity, not only by hobbyists, but as possible commercial work platforms as evidenced by the 1,384 current legislative items (as of April 28, 2015) surrounding FAA exemptions for the use of such drones (Regulations.gov,
2015). The use of these drones for commercial purposes requires filing an exemption with the Federal Aviation Administration (FAA), as described in the Legal section of this document. As of April 28, 2015, there have been 244 such exemptions approved by the FAA (Federal Aviation Administration, 2015b). Purposes for commercial drones as filed with the FAA include such tasks as precision aerial surveying, aerial photography for motion pictures and television, mapping and survey applications, hydroelectric system asset inspection, and delivery of packages (Federal Aviation Administration, 2015b).

Figure 3. Amazon Prime Air drone (Amazon.com, 2015).

In light of this increase in popularity of commercial drone development and the probable benefits to efficiency and reproducibility derived from the implementation of a UAV platform, the use of such a drone for this project is therefore established.

**Technological Automation**

Since the necessity for monitoring wireless communications and WAPs has been demonstrated, it is now necessary to determine the effectiveness of, efficiency of, and human response to automating this task. Table 8 gives the definition of automation.
Table 8

Definition of Automation

1. The technique of making an apparatus, a process, or a system operate automatically.
2. The state of being operated automatically.
3. Automatically controlled operation of an apparatus, process, or system by mechanical or electronic devices that take the place of human labor.

As will be demonstrated in this section, one of the primary concerns of automation and its implementation is described by the third definition of automation and the replacement of human labor in the workplace. The term technological automation is used in order to differentiate this type of automation from automation methods using strictly mechanical means. This section will address these concerns as well as demonstrate the efficiency and effectiveness implementing an automated solution.

**Historical responses to technological automation.** In 1922, James Joyce addressed the problem of technological advancement and the increasing use of automation and the effect on workers in his book, Ulysses, when he wrote (1922, chap. II, para. 402), “Couldn't they invent something automatic so that the wheel itself much handier? Well but that fellow would lose his job then? Well but then another fellow would get a job making the new invention?”

In his 1930 essay entitled, Economic Possibilities for our Grandchildren, The British economist John Maynard Keynes wrote of “technological unemployment,” and the loss of human labor in the workplace, but continues on to write (as cited in Pecchi & Piga, 2008, pg. 21), “All this means in the long run that mankind is solving its economic problem. I would
predict that the standard of life in progressive countries one hundred years hence will be between four and eight times as high as it is today.”

During the 1960’s, the United States government, under the direction of President Lyndon B. Johnson, formed a panel to study the impact of technology on the American economy. The report recognized the rapid decrease in the amount of time taken to develop technological innovations, as well as the public’s overall resistance to change and fears of a future where, “the notion of gainful employment is obsolete (U.S. Department of Health, Education, and Welfare, 1966).” The report recognized the public’s ambivalence regarding automation; the recognition that technology and automation have made modern life easier, simultaneously coupled with the fear of joblessness and economic ruin.

This ambivalence carried through to the 1980’s with the advent of affordable computers and the promise of the “paperless office.” However, it was recognized that technology and automation alone were not a panacea, and that firms must adapt to this new paradigm (Rio & Cardinali, 1993). Due in part to the rapid proliferation of computing devices that began in the 1980’s and 1990’s, there was a shift in employment statistics as employees began moving into the nascent technology field, either working directly with technology, or in a supportive role. According to the U.S. Bureau of Labor Statistics, computer and data processing was the fastest growing industry during the time period 1979-1989, with 492,600 new jobs for an increase of 181.9% (Plunkert, 1990). This trend continued during the time period from 1989-1999, and although the computer and data processing field fell to the number two position, there were 1,094,500 new jobs for an overall increase of 148.6% (Hatch & Clinton, 2000).

**Effect of technological automation on workplace dynamics.** As was described in the previous section, a shift in the workforce began in the 1980’s toward computing and data
processing in response to the use of technology to automate office tasks, coupled with a drop in technology costs that was both rapid and significant. The question remains, how has the implementation of technological automation affected the workplace?

One study which examined this question surveyed workers who were present before and after the implementation of technological automation. By limiting the survey to this group, an accurate representation of tasks performed before and after the implementation of automation was obtained. The results of the survey found the implementation of technological automation resulted in significant gains (in descending order of significance) to leadership, strategy, people, partnership and resources, processes, customer results, people results, society results, and key performance results (Yaghoubi & Sargazi, 2014).

Overall, the study of automation in the workplace has yielded mixed and sometimes contradictory results, and it has been suggested this is due to examining automation from a holistic viewpoint, rather than investigating the effects of automation by function or type (Wright & Kaber, 2005). Results of implementing technological automation can differ quite markedly, depending on the function that is automated, e.g., information acquisition vs. information analysis. It was found that the function which had been automated affected workplace dynamics differently. Introducing automation of an information acquisition function resulted in decreased communication bottlenecks, while the introduction of automation of information analysis functions led to increases in the coordination of team members and teamwork skills (Wright & Kaber, 2005). Similar studies have demonstrated enhanced performance coupled with a decreased workload with the implementation of information acquisition automation (Clamann, Wright & Kaber, 2002). An analysis of studies regarding information acquisition vs. information
analysis automation shows that the implementation of information acquisition automation is best suited for psychomotor, as opposed to cognitive functions (Wright & Kaber, 2005).

Since the manual recording of WAP signal data is a psychomotor task, the current literature supports the use of technological automation, and promises benefits to team communication and performance, with a parallel decrease in overall workload. Therefore, this project is an appropriate choice for the application of technological automation.

Legal and Ethical Questions

Public response to the use of drones. At the current time, the American public holds an overwhelmingly negative view of the expansion of the use of drones for non-military purposes. Concerns from the public, especially concerns regarding privacy, have been steadily increasing. A recent study showed that 63% of Americans believe it would be problematic if, “personal and commercial drones are given permission to fly through most U.S. airspace (Smith, 2014).” This finding mirrors an abundance of accounts in the media relating stories of alleged privacy violations involving drones. As the cost of drone technology drops and the ability to fit these drones with high-definition cameras or other monitoring devices increases, complaints about privacy have also increased (Bennett, 2014). One of the main complaints regarding drones is their ability to hover for sustained periods of time, leading to a new phenomenon known as, “persistent aerial surveillance (The Economist, 2015)” The ability of drones to engage in persistent surveillance could increase with the development of what is being called a, “perching drone,” which will have the ability to power down its motors and grasp onto objects using
articulated feet, leaving the drone sufficient power to conduct extended surveillance (Ackerman, 2014).

**Legality of the use of UAVs.** At the current time, commercial use of UAVs is undergoing a regulatory shift. The FAA’s involvement in the regulation of non-military drones has been slowly but steadily increasing since 2012, and its involvement in drone regulation is expected to grow in the future (Bennett, 2014). In 2013, the FAA released a document outlining its plans and timeline for drone regulation. This document was mandated by the FAA Modernization and Reform Act of 2012, Public Law 112-95 (Federal Aviation Administration, 2013), and presents a five-year projection on the steps necessary for complete regulation of civilian drones. The FAA will accomplish this in three phases; accommodation, integration, and evolution. Currently, the FAA is issuing certificates for drone use via one of two avenues; section 333 exemption and special airworthiness certificate.

**Section 333 exemption.** This certification is used for commercial drone development and operation in environments which can be considered controlled and low-risk (Federal Aviation Administration, 2013).

**Special airworthiness certificate (SAC).** This certification relates to the research and manufacture of drones, and the application must include descriptions of design, construction, and manufacture of the drone (Federal Aviation Administration, 2013).

Given both the current public climate toward drone use, and the nascent, fluctuating nature of regulation, the use of a UAV drone to perform the operations against WAPs in this project carries with it a certain amount of risk. However, since these devices are to be used within the confines of an enterprise campus, and will not be introduced into public airspace, it is
the belief of this author that the use of a UAV drone for this purpose is justified through the use of a section 333 exemption.

**Ethical use and misuse of security tools.** With any discussion regarding the research, development, and deployment of a new network security tool, a discussion of the ethics underlying its use is warranted. Security assessment tools are developed to assist the IT security professional by automating/semi-automating common security tasks. It is assumed that in the vast majority of cases, these tools are operated ethically by such professionals. However, when such a tool is released, it is released to everyone, not just the IT security professional, which means the very tools meant to secure networks are also available to be used as an attack vector by malicious hackers. Tools that fall into this category are numerous and it is beyond the scope of this document to list or describe all of them. Table 9 lists several security tools which are popular with security professionals and malicious hackers alike. Websites, such as http://insecure.org/, https://www.defcon.org/html/links/dc-tools.html, and http://en.softonic.com/s/hacking-tools contain links to download these tools.

One industry response to the malicious use of security assessment tools is to increase the purchase price past the point at which a malicious hacker is willing to pay. However, many paid security applications offer trial software and/or community (free) versions. Even if the price of a particular tool or suite of tools is beyond the financial limit of a malicious hacker, many “cracked” versions of these applications are available. For example, the vulnerability assessment and penetration testing tool Core Impact is licensed for $30,000 per year (Stephenson, 2009), but is available as a cracked version via torrent (http://kickass.to/core-impact-pro-7-2-t5412458.html). It is therefore understood the development of a security tool will attract those wishing to use it for malicious purposes, and is incumbent upon the security professional to use
such tools ethically. This project is a physical device and not a security software application, and it is assumed the appeal to malicious hackers would be minimal, as it is more labor-intensive but much less expensive to simply discover WAPs manually.

Table 9
Common Network Security Tools

<table>
<thead>
<tr>
<th>Name</th>
<th>Type of Tool</th>
<th>Developer</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireshark</td>
<td>Sniffer</td>
<td>Wireshark Foundation</td>
<td>Free</td>
</tr>
<tr>
<td>Metasploit</td>
<td>Exploit Framework</td>
<td>Rapid7</td>
<td>Free/Paid</td>
</tr>
</tbody>
</table>

Table 9 – continued

<table>
<thead>
<tr>
<th>Name</th>
<th>Type of Tool</th>
<th>Developer</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nessus</td>
<td>Vulnerability Scanner</td>
<td>Tenable Network Security</td>
<td>Free/Paid</td>
</tr>
<tr>
<td>Aircrack</td>
<td>Password and Wireless Auditor</td>
<td>Aircrack-ng</td>
<td>Free</td>
</tr>
<tr>
<td>Tcpdump</td>
<td>Sniffer</td>
<td>Tcpdump/LibPcap</td>
<td>Free</td>
</tr>
<tr>
<td>Burp Suite</td>
<td>Web Scanner</td>
<td>Portswigger Web Security</td>
<td>Free</td>
</tr>
</tbody>
</table>

Objectives Achieved Through Completion of Project

Upon successful completion of the project, several objectives (OBJs) will be achieved. These objectives are based on both the initial and revised requirements as set forth in the project schedule as well as the determination of the scope of the project. These objectives are enumerated in Table 10, and described in this section.

Table 10
**Project Objectives**

<table>
<thead>
<tr>
<th>Number</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBJ1</td>
<td>Determine a need for the platform being researched</td>
</tr>
<tr>
<td>OBJ2</td>
<td>Use open source and/or COTS hardware/software</td>
</tr>
<tr>
<td>OBJ3</td>
<td>Research and develop UAV platform</td>
</tr>
<tr>
<td>OBJ4</td>
<td>Project platform must fly autonomously</td>
</tr>
<tr>
<td>OBJ5</td>
<td>Determine effectiveness of UAV drone platform</td>
</tr>
<tr>
<td>OBJ6</td>
<td>Determine efficiency of UAV drone platform</td>
</tr>
</tbody>
</table>

**OBJ1.** Prior to initiating the project, a determination must be made as to the need for such a device. The fact that no such device/platform currently exists does not alone imply that it is either necessary or desirable. This objective will be met indirectly, with the use of thorough research into the current literature. Since there is no direct literature regarding this topic, all facets surrounding the development and use of this UAV project will be considered for both necessity and if possible, desirability.

**OBJ2.** Reduce development and implementation costs by using open source and/or COTS hardware/software. This approach not only keeps development and implementation costs down, but also decreases cost of repairs, both in terms of money as well as time. Since open source/COTS components are usually well tested, research and development time will be markedly reduced. The use of this type of software/hardware also encourages modularity and reusability of components.

**OBJ3.** Global objective to develop a UAV drone which will automate discovery, inventory, baselining, and auditing of wireless infrastructure, specifically, Wireless Access Points. Currently, this is done manually (if at all), and it is believed that reliably automating this...
task will save resources for an organization as well as provide a new and novel method for performing these measurements.

**OBJ4.** One of the key objectives for this project is the ability of the UAV drone to fly without the need of a human pilot. While it would be an easier development process to simply incorporate an SBC onto an existing drone and have a human pilot controlling the flight, this method would not offer an organization as substantial a savings of resources, since resources would need to be spent on the pilot performing his/her duties, as well as the learning curve associated with drone flight mechanics.

**OBJ5.** Effectiveness of the UAV drone platform would be measured using three distinct metrics. First is the ability of the UAV drone to perform and log measurements of data from WAPs, including data such as SSID, security protocols, and signal strength. Second is the question of reliability, and the ability of the UAV drone to gather the above information from WAPs in a consistent fashion. The third consideration is that of reproducibility, and comparisons could be made to collected data not only from previous flights, but against data gathered by human action.

**OBJ6.** Efficiency of the UAV drone regards the ability of the platform to perform the task of detecting WAP information in such a fashion that it saves resources over alternative methods of performing the same task. These resource savings would be represented as decreased time and/or capital expenditures.

**Future objectives to consider.** Although the following objectives are not addressed by this thesis, they are important enough to bear consideration during future development, past the scope of this thesis. Of primary concern is the inability of this system to detect malicious clients
which are not actively broadcasting. Future research should be directed at methods of forcing such clients to identify themselves, possibly in response to pinging, probing, or an, as yet, unidentified method. Secondly, is the development and addition of a Collision Avoidance System (CAS), what the FAA refers to as Airborne Sense and Avoid (ABSAA) systems (Federal Aviation Administration, 2013). This system would be based on a 6-axis ultrasonic transducer array, and would increase the overall safety associated with the use of the drone. This drone is one component of a complete, integrated, and automated Wi-Fi security assessment tool project, and the two proposed components (the drone and a long-range, automated wireless hacking tool) will be integrated to work in tandem in the future, past the scope of this project.

Conclusion

This literature review has demonstrated in a conclusive manner the appropriateness of using a UAV drone to perform the task of WAP discovery, inventory, baselining, and auditing. Radio waves are a form of electromagnetic radiation, and as such are perfectly suited for remote detection. Various open-source or free-of-charge tools exist to perform this function, and the computer required for the operation of this wireless signal scanner is available in a small, lightweight, and relatively inexpensive Linux platform. The choice of a UAV drone for this project allows efficiency, team support, and reproducibility to be built in to an organization’s wireless auditing program. This project will be most effective in locating Rogue APs or Evil Servers, and other attacks can also be detected, if they are active. Although drones are currently unpopular with the public, the FAA is allowing companies to apply for, and granting exemptions and airworthiness certificates for the use of commercial drone technologies. The choice of using a UAV drone to detect wireless access points/signals has been shown to be an appropriate and efficient tool for this function.
Findings Log/Journal

This project was attempted with a sixteen-week completion window, and all requirements and deliverables will be part of the project, but are out of scope with the project timeline. In addition, any requirements and/or deliverables that are considered enhancements to this project will also be discussed.

Project Journal

The project journal closely approximates the schedule as detailed in Table 2. This section will describe the actual vs. the projected timeline, as well as provide discussions for any problems encountered, especially those which impacted the projected timeline.

Week 1. Online research was conducted to determine whether this project was not only feasible, but could be accomplished within the given sixteen-week timeframe. As a result of this research, a determination was made that this project was not only feasible, but could be accomplished within the timeframe given strict adherence to the project requirements and scope.

As part of the feasibility study, a cost estimate was performed. It was found that the cost to purchase a pre-assembled UAV drone was prohibitive, as any appropriate drone was priced in the $1,000+ range. The three factors that determined the appropriateness of a UAV drone platform were flight time, lift capability, and the ability to integrate an automated flight system. Further research was conducted into purchasing a UAV frame and all necessary components, then assembling the platform from COTS hardware and software. This approach was found to fit well within the financial scope of the project, and a determination was made to continue.

Having established the feasibility of the project, a list of project requirements was authored. These requirements were separated into three categories; necessary, time-permitting, and future consideration. The inclusion of the time-permitting category allowed a certain degree...
of flexibility, and the ability to adjust the final requirements and deliverables based on the project experience vs. theoretical reasoning. The initial and final requirements document for this project is presented an Appendix B.

**Week 2.** Began research on UAV component parts and general drone theory and construction techniques.

**Week 3.** Began research into components required to construct drone according to requirements. Conducted research based on criteria of highest quality parts for the lowest price. Discovered hobbyking.com, with every necessary component being available, although not always at the lowest price.

**Week 4.** Began planning which components to use in drone construction. Designing a semi-custom airframe required considerations into motor power, blade type, battery type, and overall power consumption. Began researching SBCs.

**Week 5.** Determined overall design for craft, incorporating changes made during requirements assessment phase. Decided on BeagleBone Black for SBC due to high processing power with a quad-core ARM processor, as well as low power consumption.

**Week 6.** Began ordering components for quadcopter from hobbyking.com, amazon.com, and ebay.com. Realized that components for construction would cost over $500.00, and detailed multiple purchases over time to fit project budget.

**Week 7:** Began planning construction of drone. Waiting for components to arrive via delivery/mail. Probable difficulty was noted with hobbyking.com, as the company is located in the U.K., and although there are Hobbyking warehouses in the U.S., the supply of components in these warehouses is limited.
**Week 8.** First round of components arrived. Began construction of frame, and calculated position of additional electronics/equipment. It was determined that a CAS was not possible to design, test, and construct in the given timeframe. Moved this requirement to the “Future” category.

**Week 9.** Although the project schedule stated to test airworthiness of UAV this week, due to staggered ordering of components, was unable to perform this test. Continued ordering components for UAV, and integrating them as they arrived/as appropriate.

**Week 10.** Began exploration of SBC operating environment and interfaces. Changed OS on SBC to Debian from Angstrom Linux due to familiarity with Debian Linux and the knowledge that Debian would perform all necessary computing functions. Encountered difficulties with SBC interface. Would not display on computer monitor due to resolution conflicts. Researched how to force change SBC resolution. It was determined that if the SBC could not display properly, the project would ultimately fail.

**Week 11.** Difficulties with SBC continued, most likely due to unfamiliarity with the product. Research was performed, and expectations changed regarding usage and programming of SBC. Took three attempts to change OS to Debian Linux on SBC. Attempted to overcome display resolution problems and communicate with board via Secure Shell (SSH) with varying success. Recognized project was approximately 2 – 3 weeks behind proposed schedule due to unforeseen challenges with both UAV design/construction and SBC use.

**Week 12.** Construction of basic UAV airframe complete. Moving on to calibrating the airframe prior to first flight test; stability while hovering. Calibration is carried out with the transmitter and receiver for the UAV, and performed using a series of tones generated by the
FCB. There was no visual feedback. Took several hours to learn the meanings of the different tones, and began attempting calibration. Initial flight tests were extremely unsuccessful, with extreme instability noted.

Specifically, the FCB was causing a motor condition known as “cogging” where the FCB was overcompensating, causing the engines to “sputter” while standing still, instead of the desired condition of remaining powered down until flight. Several phone calls were made to both diagnose and fix this condition, but the advice received was that the ESCs were probably bad, and needed to be replaced. Due to financial and supply chain problems, it was decided to try to rectify the cogging situation. Began researching online various tutorials on calibration.

Continued attempts at communication with SBC.

**Week 13.** Video resolution difficulties with SBC were overcome, and the unit displays properly. Began integrating Wi-Fi module into SBC, but was having difficulty with the SBC recognizing and mounting the Wi-Fi adapter. Began online research on adding this adapter. Broke 5 propeller blades, and was necessary to order eight new blades. Began integrating autopilot system.

**Week 14.** Continued efforts on incorporating Wi-Fi adapter into SBC with limited success. Continued online research into this process. Downloaded Windows and android app for autopilot system. Flashed autopilot with new firmware. New propeller blades arrived and installed. Continued calibrating and testing UAV airframe for airworthiness.

**Week 15.** Successfully integrated and mounted Wi-Fi adapter on SBC. It was necessary to compile the Wi-Fi driver from source code. Installed and configured Kismet on SBC for measuring and logging Wi-Fi data.
Week 16. UAV has still not passed preliminary hover tests, and it was recognized that the project would fail given a sixteen-week timeline. A one-month academic extension was applied for and received.

Week 17. SBC mounted onto airframe, and autopilot fully integrated. Flashed latest firmware onto autopilot.

Week 18. UAV marginally passed hover test with some instability noted. It was noted that the autopilot now had complete control of the UAV in flight, and would need to be recalibrated from flight involving only FCB. Continued calibration of UAV components under autopilot control to increase stability.

Week 19. UAV fully calibrated, and full test of UAV with wireless signal measurement performed. During the terminal stages of the test, the operator mistakenly identified instability in the craft and took manual control of landing. Due to lack of manual flying experience, the UAV suffered a crash in which two of the motor mounts were bent and the landing gear broken. Neither time nor resources were available to repair the UAV, and an out-of-scope condition was reached. It was noted that due to the flawless performance of the UAV prior to manual takeover, the autopilot would probably have performed an adequate landing. Thus, Proof of Concept (POC) was obtained, and the project was judged a partial success.

Project Experience vs. Theoretical Knowledge

The experience of constructing and testing this project was markedly different from the expectations held at the onset. Although difficulties are always expected and one attempts to compensate for them, the difficulties encountered during the course of this project far exceeded expectations. Factors for this included unfamiliarity with both UAV design, construction and
usage as well as unfamiliarity with the use of the SBC. Other difficulties encountered included the inability to order all components at the outset of the project, and conflicts with personal vs. professional life.

It was during the 13th week of the project the realization that completing the project within the 16-week timeframe was in jeopardy. There was an abundance of theoretical knowledge available on UAV construction/calibration and SBC usage. However, the practical knowledge was quite different, as this researcher has had no experience with either prior to the initiation of the project. A one-month academic extension was obtained in order to counter these difficulties.

**Limitations and Biases**

**Limitations.** Several of the limiting factors involved with this creative project have been previously discussed, including financial and knowledge-based limitations. However, can a lack of knowledge be considered a limitation? It is this author’s opinion that a lack of knowledge in the field in which one writes a thesis and/or develops a creative project is a prerequisite and not a limitation. The overall objective of a graduate degree is (in this author’s opinion) to be able to conduct independent research in a field where the researcher may have some, but not necessarily in-depth knowledge. Given that definition, lack of knowledge is not a limitation.

The largest limitation identified during the course of this creative project/thesis was that of time. A 16-week timeframe does not allow for an ambitious project, and even an insignificant project will have unforeseen difficulties which will invariably arise and cause delays to some degree. Prior to beginning this project, this researcher should have had a more appropriate idea of the possible difficulties that would arise. On the surface, building a quadcopter drone does not
appear to be overly ambitious. However, the number and magnitude of difficulties encountered during the course of this project demonstrate the severity of the imposed time limitation which was intensified by the lack of specific knowledge.

**Biases.** As human beings, we cannot escape bias, we can only attempt to minimize its impact. However, this project presented information and challenges which were easily quantifiable, creating an environment of relative objectivity. Therefore, this researcher believes the existence of any potential or real bias will have a minimal overall impact on the project.
The Project

Outcomes

Many challenges were faced during the research and development of this project, both foreseen and unforeseen at its initiation. These difficulties will be enumerated and discussed in the following section on project post-mortem.

Overall, this project can be considered a partial success, due to the ability of the drone to fly autonomously and measure wireless signal data. However, it can also be considered a partial failure, although not one of concept or design. The failures suffered by this project were primary (e.g., out-of-scope for time requiring an extension), secondary (e.g., lack of knowledge/experience), or tertiary (e.g., supply chain). This researcher continues to believe that the idea of using a small, automated drone perform the task of WAP auditing is sound, and this belief is supported by both the review of literature as well as the partially successful test flight. The fault, if any is to be assigned, lies solely with this researcher and the choice of a project which, ultimately, was not appropriate for a 16-week period given the amount of previous experience with drone construction and SBCs.

At the time of this writing, the drone is damaged from the crash suffered during testing. Two of the four motor mounts are bent, and cannot be straightened without introducing an unknown amount of metal fatigue, and therefore need to be replaced. The landing gear was also damaged in the crash and need to be replaced. However, an out-of-scope condition now exists for both time and financial resources, and these damaged components cannot be replaced prior to the project deadline. It is the intention of this researcher to continue development of this project past the terminal deadline, in hopes of attaining a complete and perfect success.
Recommendations for Further Research

There are several additional subsystems which could have been implemented into this project if the timeline had been longer and the budget larger. These subsystems are left as further research into future enhancements and include the following:

Collision avoidance system (CAS). Although the flight plan for this UAV is preset, taking into account obstacles in the flight path, it does not take unexpected events into consideration (e.g., people walking through the flight path). Therefore, it is necessary to add a system for dynamically adjusting the path of travel according to current conditions. A 6-axis ultrasonic CAS would provide complete coverage from unexpected obstacles, and would afford increased safety to both the UAV and its surroundings.

Real-time telemetry. COTS telemetry units are available for UAVs of this type, and allow streaming of flight data to a ground station. This would allow the operator to view the progress of the UAV in its flight path in real time. Currently, the UAV flies the path in a “fire and forget” manner, and gives the operator no indication of its location, attitude, altitude, heading, etc.

Crash cage. Due to the damage sustained during testing, it is highly recommended that a cage be constructed which completely surrounds the entire unit, and will protect it from damage should a crash occur.

Real-time video. Although not required to perform its duties, the inclusion of a real-time video camera would provide the operator an instantaneous view of any areas of interest or concern during flight.
Post-Mortem

According to Moss (2008), the project post-mortem contains within it several main goals and should be conducted among the following topics – schedule, budget, satisfaction, scope, negotiating skills, staffing, skills and training, project planning and reporting, development approach, contractors/consultants/vendors, and general issues. This section will perform the project post-mortem and will address these topics.

**Schedule.** In retrospect, the schedule for this project was a bit ambitious. Originally, the deliverables for this project included an ultrasonic CAS. It was determined midway through the development process that this deliverable was unattainable in the timeframe provided. Resources in the form of time and capital were lost during the preliminary design of this subsystem. The primary reason for overreaching on the project schedule was researcher inexperience with the various systems to be utilized in the course of the project. It is recommended for future projects to determine schedule according to intimate knowledge of the systems being developed as well as the inclusion of a percentage of the total time to mitigate difficulties and/or challenges that may arise.

**Budget.** Early in the project, it was noted that appropriate, pre-manufactured, or RTF drones were priced at approximately $1000, and due to budgetary concerns, it was decided to construct a semi-custom drone using COTS components. The final financial expenditure on this project as given in Appendix C was $607.04, which was still slightly over the preliminary budget of $500. Again, researcher inexperience with projects of this type was determined to be the causative factor. For future projects, it is recommended that the budget contain some overhead in order to cover unexpected costs. Also, during the budget planning process, input is required from researchers knowledgeable about the subject.
Satisfaction. This topic deals with customer satisfaction and as the project was not intended for customer release, is not applicable in this case.

Scope. The scope of the project was identified as being slightly ambitious and overreaching, and changed several times during the course of the project. This was borne by the researcher planning a project with inadequate knowledge of the processes involved as well as unfamiliarity with all possible complications that could arise during the course of the project. For future projects, it is recommended that the scope be determined by researchers who are familiar with the project systems and subsystems.

Negotiating skills. This topic deals with negotiations between the project team and the customer, and is not applicable for this project.

Staffing. This was a major concern and cause of difficulty during the course of this project. The project was composed of a staff of one, the primary researcher. As such, there was a significant amount of ancillary or supportive work which was inappropriate for the researcher to perform. These types of tasks included shopping for and buying components and interacting with customer service. Also, it was noted that during a single-person project, the processes of brainstorming and creative problem-solving were hindered, thus affecting both time and scope of the project. For future projects it should be noted that multi-person teams are more efficient, as they eliminate many of the bottlenecks which existed during the course of this project.

Skills and training. This topic was identified as one of the primary difficulties during the course of the project. The primary researcher began the project with an unfamiliarity of the major components of the project. To wit, drone construction and the use of SBCs. Perhaps one of these knowledge deficiencies could have been mitigated in the given timeframe, but as was
demonstrated, multiple knowledge deficiencies add a near exponential hurdle to overcome. The assignment of a researcher to a system or subsystem they are not familiar with carries a steep learning curve which reduces the overall effectiveness of that researcher and metastasizes to the project as a whole. For future projects, staff selection should be a key issue. Choosing staff who are intimately familiar with the subject matter will help ensure scope stability as well as having an effect on overall project success.

**Project planning and reporting.** This was another identified difficulty. Aside from issues of lack of knowledge and inadequate and variable scope, the fact that project development and reporting had to occur simultaneously instead of sequentially added to the global project overhead. The scope of the project should have included time for the preparation of this document, and because the timeframe was fixed at 16 weeks, there was no possibility of time scope creep. During the course of this project, the primary researcher found necessary project processes falling farther behind as difficulties were encountered. For future projects, it is recommended that the project schedule and time scope be determined with both adequate knowledge of the subject and allows for the sequential operation of project development and reporting.

**Development approach.** The development approach for this project was as sound as possible. From the onset of the project, it was determined that development should be both iterative and incremental, composed of the following repeated steps for each system or subsystem:

1. Research.
2. Develop.
The processes involved with the project were laid out in a schedule which at the time seemed both adequate and accomplishable. The systems and subsystem processes were scheduled in the following order:

1. Airframe construction.
2. Addition of basic flight components.
3. Calibration.
5. Integration of autopilot.
6. Autopilot flight testing.
7. Integration of SBC.
8. Final flight testing.

For future projects, it is suggested that, if time permits, the processes of development and reporting should be separated and executed in a sequential manner, or assigned to separate individuals. An iterative and incremental approach as used during the course of this project would be an appropriate choice, given mitigation of other difficulties encountered.

**Contractors, consultants, and vendors.** During the course of the project, several vendors were used in order to obtain the UAV components. The primary vendor was Hobby King, where most, if not all, components necessary for the completion of the project were located and reasonably priced. The difficulty encountered was that Hobby King is based in the United Kingdom, and the bulk of their inventory is located in European warehouses. There are two warehouses located in the U.S. (East and West), however, the inventory at these locations is relatively limited. This, coupled with financial challenges, added an unwanted time delay to the project. The choice of Hobby King as a vendor would have been appropriate given more time to
allow for overseas deliveries. For future projects, the proximity and shipping times of vendors should be considered, and this consideration is reciprocal, meaning consideration of proximity should increase as the available timeframe for the project decreases.

**General issues.** There were no team-related, business communication, or customer issues present during the course of this project, as research and development was performed by an individual. The ideal of a project post-mortem is to identify present difficulties in order to increase the chance of future project successes (Moss, 2008). To that end, the lessons learned during this project as well as suggestions for future projects will be presented here.

**Lessons learned.** The following list represents lessons learned during difficulties encountered during the course of this project. It is as exhaustive as possible in order to enhance the possibility of future project successes, and is presented in what is believed to be the order of descending criticality.

1. Lack of researcher knowledge. This negatively impacted the overall time required to complete the project, and resulted in time scope creep, and overall is believed to be the primary cause of the project partial failure.
2. Lack of inclusion for difficulties encountered in project. The scope of this project was determined without knowledge of every possible difficulty which could be encountered. This led to an extremely large amount of time scope creep, and when coupled with lack of knowledge, led to the failure conditions as noted previously.
3. Lack of inclusion of time and financial resource limitations in project scope. This difficulty resulted in a project scope with very little room for error. Coupled with the researcher’s relative lack of knowledge, this caused the project to become steadily and
increasingly unmanageable and behind schedule. Future projects should include time for such limitations.

4. Lack of recognition of reporting time. Because this project included a large reporting component, adequate time should have been allowed for both the performance of the development and reporting processes. Development and reporting by an individual should optimally be performed sequentially.

5. Financial base. The initiation of a project should carry with it adequate resources available for its completion. This was not the case in this project, and all available financial resources were spent during the initial round of component purchases.

6. Proximity and shipping time of vendors. Vendors who directly supply necessary components should have a relatively short period of time between ordering and delivery. During the course of this project, this difficulty played a relatively minor yet significant role in that component failure and replacement was not accounted for.

7. Lack of support. It was noted during the course of this project that certain research and development functions, such as brainstorming, creative solutions, and problems involving the resolution of lack of knowledge were hindered by this project consisting of a single researcher. Single researcher projects should be avoided unless the researcher is very knowledgeable about the subject or the scope is exceedingly simple.
References


Regulations.gov. (2015). *1,384 results for “section 333 FAA”*. Retrieved from http://www.regulations.gov/#!searchResults;rpp=25;po=0;s=%2522section%252B333%252BFAA%2522;fp=true;ns=true


http://dx.doi.org/10.6007/UARBSS/v4-i8/1105
## Appendix A

List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSAA</td>
<td>Airborne Sense and Avoidance</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>APUS</td>
<td>American Public University</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device</td>
</tr>
<tr>
<td>CAN</td>
<td>Controller Area Network</td>
</tr>
<tr>
<td>CAS</td>
<td>Collision Avoidance</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial Off-the-Shelf</td>
</tr>
<tr>
<td>CSMA/CA</td>
<td>Carrier Sense Multiple Access/Collision Avoidance</td>
</tr>
<tr>
<td>CSRF</td>
<td>Cross Site Request Phantom</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DL MU-MIMO</td>
<td>Downlink Multiuser Multiple-Input Multiple-Output</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EM</td>
<td>Electromagnetic</td>
</tr>
<tr>
<td>FAA</td>
<td>Federal Aviation Administration</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>HT</td>
<td>High Throughput</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IS</td>
<td>Information Systems</td>
</tr>
<tr>
<td>ISM</td>
<td>Industrial, Scientific, and Medical</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>IV</td>
<td>Initialization</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MAN</td>
<td>Metropolitan Area Network</td>
</tr>
<tr>
<td>MIMO</td>
<td>Multiple-Input Multiple-Output</td>
</tr>
<tr>
<td>MK</td>
<td>Mascheknecht</td>
</tr>
<tr>
<td>MMIC</td>
<td>Michaelson Message Integrity Code</td>
</tr>
<tr>
<td>PHY</td>
<td>Physical</td>
</tr>
<tr>
<td>POC</td>
<td>Proof of Concept</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-Shared Key</td>
</tr>
<tr>
<td>RA</td>
<td>Remote Access Dial-In User</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Radio Frequency Access Dial-In</td>
</tr>
<tr>
<td>RF</td>
<td>Ready</td>
</tr>
<tr>
<td>SBC</td>
<td>Single Board Computer</td>
</tr>
<tr>
<td>SDM</td>
<td>Spatial Division Multiplex</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>STBC</td>
<td>Space Time-Block Code</td>
</tr>
<tr>
<td>TFa</td>
<td>Task Function A</td>
</tr>
<tr>
<td>TFb</td>
<td>Task Function B</td>
</tr>
<tr>
<td>TFg</td>
<td>Task Function G</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>TxBF</td>
<td>Transmit Beamforming</td>
</tr>
<tr>
<td>UAS</td>
<td>Unmanned Aircraft</td>
</tr>
<tr>
<td>UAV</td>
<td>Unmanned Aerial Vehicle</td>
</tr>
<tr>
<td>VHT</td>
<td>Very High Throughput</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless Access Point</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy</td>
</tr>
<tr>
<td>WPA</td>
<td>Wi-Fi Protected Access</td>
</tr>
<tr>
<td>WPA2</td>
<td>Wi-Fi Protected Access Version 2</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WMAN</td>
<td>Wireless Metropolitan Area Network</td>
</tr>
<tr>
<td>WPAN</td>
<td>Wireless Personal Area Network</td>
</tr>
<tr>
<td>XOR</td>
<td>Exclusion OR</td>
</tr>
</tbody>
</table>
## Appendix B

### Initial/Final Requirements

<table>
<thead>
<tr>
<th>Requirement Number</th>
<th>Description</th>
<th>Initial Applicability</th>
<th>Final Applicability</th>
<th>Requirement Met</th>
</tr>
</thead>
<tbody>
<tr>
<td>R01</td>
<td>UAV platform must be able to lift all required flight components</td>
<td>Necessary</td>
<td>Necessary</td>
<td>(4/26/2015)</td>
</tr>
<tr>
<td>R02</td>
<td>UAV platform must be able to lift SBC, wireless components, and SBC battery</td>
<td>Necessary</td>
<td>Necessary</td>
<td>(5/4/2015)</td>
</tr>
<tr>
<td>R03</td>
<td>UAV will be purchased Ready to Fly</td>
<td>If Possible</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>R04</td>
<td>UAV and SBC components will be COTS</td>
<td>Necessary</td>
<td>Necessary</td>
<td>(5/1/2015)</td>
</tr>
<tr>
<td>R05</td>
<td>UAV will be capable of automated flight</td>
<td>Necessary</td>
<td>Necessary</td>
<td>No</td>
</tr>
<tr>
<td>R06</td>
<td>SBC will be capable of running wireless sniffing software</td>
<td>Necessary</td>
<td>Necessary</td>
<td>No</td>
</tr>
<tr>
<td>R07</td>
<td>SBC will run Linux</td>
<td>Necessary</td>
<td>Necessary</td>
<td>(5/7/2015)</td>
</tr>
<tr>
<td>R08</td>
<td>UAV will be fitted with ultrasonic Collision Avoidance System</td>
<td>Necessary</td>
<td>Future</td>
<td>No</td>
</tr>
<tr>
<td>R09</td>
<td>UAV will be capable of 20+ minutes of flight</td>
<td>Necessary</td>
<td>Necessary</td>
<td>(3/26/2015) (Theoretical)</td>
</tr>
<tr>
<td>R10</td>
<td>UAV will work in conjunction with automated WAP auditing tool</td>
<td>Future</td>
<td>Future</td>
<td>No</td>
</tr>
<tr>
<td>R11</td>
<td>UAV will require minimal interaction with operator to set up for flight</td>
<td>Necessary</td>
<td>Necessary</td>
<td>No</td>
</tr>
<tr>
<td>R12</td>
<td>UAV will require no operator interaction in the performance of duties</td>
<td>Necessary</td>
<td>Necessary</td>
<td>No</td>
</tr>
</tbody>
</table>
## Appendix C

### Cost Breakdown

<table>
<thead>
<tr>
<th>Date</th>
<th>Part</th>
<th>From</th>
<th>Unit Cost (dollars)</th>
<th>Total Cost (dollars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/20/2015</td>
<td>BeagleBone Black SBC</td>
<td>Amazon</td>
<td>83.49</td>
<td>83.49</td>
</tr>
<tr>
<td>03/05/2015</td>
<td>GPS and Compass Module</td>
<td>eBay</td>
<td>15.39</td>
<td>15.39</td>
</tr>
<tr>
<td></td>
<td>Autopilot Mega Control Board</td>
<td>eBay</td>
<td>38.69</td>
<td>38.69</td>
</tr>
<tr>
<td>03/08/2015</td>
<td>5600 mAh External Battery Charger</td>
<td>Amazon</td>
<td>23.64</td>
<td>23.64</td>
</tr>
<tr>
<td></td>
<td>USB Wi-Fi Adapter</td>
<td>Amazon</td>
<td>13.95</td>
<td>13.95</td>
</tr>
<tr>
<td>03/12/2015</td>
<td>AX-2810Q-750KV Brushless Quadcopter Motor x 4</td>
<td>Hobbyking</td>
<td>19.50</td>
<td>78.00</td>
</tr>
<tr>
<td></td>
<td>Turnigy H.A.L. Quadcopter Frame</td>
<td>Hobbyking</td>
<td>36.56</td>
<td>36.56</td>
</tr>
<tr>
<td></td>
<td>30A Brushless Speed Controller x 4</td>
<td>Hobbyking</td>
<td>11.67</td>
<td>46.68</td>
</tr>
<tr>
<td></td>
<td>Multirotor Control Board</td>
<td>Hobbyking</td>
<td>17.99</td>
<td>17.99</td>
</tr>
<tr>
<td></td>
<td>Quadcopter Power Distribution Board</td>
<td>Hobbyking</td>
<td>3.99</td>
<td>3.99</td>
</tr>
<tr>
<td></td>
<td>Carbon Fiber Propeller Blades x 4</td>
<td>Hobbyking</td>
<td>7.89</td>
<td>31.56</td>
</tr>
<tr>
<td></td>
<td>Battery Mount Plate</td>
<td>Hobbyking</td>
<td>3.21</td>
<td>3.21</td>
</tr>
<tr>
<td></td>
<td>6000 mAh LiPo Battery</td>
<td>Hobbyking</td>
<td>52.75</td>
<td>52.75</td>
</tr>
<tr>
<td></td>
<td>Battery Strap</td>
<td>Hobbyking</td>
<td>1.75</td>
<td>1.75</td>
</tr>
<tr>
<td>04/03/2015</td>
<td>3.5mm Gold Bullet Connector</td>
<td>Amazon</td>
<td>8.99</td>
<td>8.99</td>
</tr>
<tr>
<td></td>
<td>4-Port USB Mini-Hub</td>
<td>Amazon</td>
<td>7.51</td>
<td>7.51</td>
</tr>
<tr>
<td>04/04/2015</td>
<td>HDMI to Micro HDMI Cable</td>
<td>Amazon</td>
<td>11.27</td>
<td>11.27</td>
</tr>
<tr>
<td>04/09/2015</td>
<td>LiPo Voltage Checker/Warning Buzzer</td>
<td>Amazon</td>
<td>5.99</td>
<td>5.99</td>
</tr>
<tr>
<td></td>
<td>FCB Power Module</td>
<td>Amazon</td>
<td>10.99</td>
<td>10.99</td>
</tr>
<tr>
<td></td>
<td>iMAX B6 LiPo Charger/Discharger</td>
<td>Amazon</td>
<td>34.99</td>
<td>34.99</td>
</tr>
<tr>
<td></td>
<td>Helping Hands Magnifier</td>
<td>Amazon</td>
<td>5.50</td>
<td>5.50</td>
</tr>
<tr>
<td>04/10/2015</td>
<td>6 Channel Tx/Rx</td>
<td>Hobbyking</td>
<td>29.99</td>
<td>29.99</td>
</tr>
<tr>
<td></td>
<td>HXT to XT60 Battery Adapter</td>
<td>Hobbyking</td>
<td>3.20</td>
<td>3.20</td>
</tr>
<tr>
<td>04/14/2015</td>
<td>AC Adapter</td>
<td>Amazon</td>
<td>8.63</td>
<td>8.63</td>
</tr>
<tr>
<td>05/05/2015</td>
<td>Rechargable AA Batteries</td>
<td>Amazon</td>
<td>17.03</td>
<td>17.03</td>
</tr>
<tr>
<td>05/08/2015</td>
<td>Replacement Propellers x 2</td>
<td>Amazon</td>
<td>15.90</td>
<td>15.90</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td></td>
<td>607.04</td>
<td></td>
</tr>
</tbody>
</table>
Appendix D

Project Media
Appendix E

Sponsor Endorsement

American Military University:

I met with Ken Bernstein to receive an overview, demonstration and detailed explanation of his project.

This work definitely addresses an area of significant concern for any business or institution with a campus. Even more than ever this last couple years; the advent of very cheap and highly portable computing technologies and wireless access has greatly exacerbated the already difficult problems of operating safe and secure networks.

Ken’s approach, that of combining appropriate commercial off the shelf (COTS) technologies, to develop a tool that aids the burden of maintaining the safety and security of networks is commendable in its segmentation of a solution. The recognition that aerial platform technology has reached the point that it can be treated as a commodity (including guidance and routing software) is an important step.

Combining the aerial platform with open source radio detection and analysis is novel and clever. Having a platform that can easily perform repeatable (and repeated) aerial patrols, likewise. Here is where part of the strength of the system really is, in having longitudinal data on the radio environment of a campus.

Ken showed excellent grasp of each of the technologies brought together in this project and good reasoning in the selection of each component from the available alternatives. I think that this project is a useful and important step forward and its use of COTS technologies greatly increases the probability of eventual contribution to productization.

June 20, 2015

Steven Friedrich
co-founder, Layered Logic, Inc.
School of Science, Technology, Engineering, and Math

MS in Information Technology

The thesis for the master’s degree submitted by

Kenneth L. Bernstein

under the title

Research and Development of an Unmanned Aerial Vehicle to Automate Monitoring of Wireless Access Points

has been read by the undersigned. It is hereby recommended for acceptance by the faculty with credit to the amount of 3 semester hours.

(Signed, first reader) (Date) June 30, 2015

(Signed, second reader, if required) (Date)

Recommend for approval on behalf of the program

(Signed) (Date)

Recommendation accepted on behalf of the program director

(Signed) (Date)

Approved by academic dean

Date
I, Kenneth L. Bernstein, owner of the copyright to the work known as Research and Development of an Unmanned Aerial Vehicle to Automate Monitoring of Wireless Access Points hereby authorize APUS to use the following material as part of his/her thesis to be submitted to American Public University System.

Line Numbers or Other Identification

Signature

KL Bernstein
This capstone has been approved by Dr. Novadean Watson-Stone for submission, review, and publication by the Online Library.

Author’s Name: Kenneth L. Bernstein

Title: Research and Development of an Unmanned Aerial Vehicle to Automate Monitoring of Wireless Access Points

Professor: Dr. Novadean Watson-Stone

Second reader, if required: N/A

Program: Master’s of Science in Information Technology with a concentration in Information Assurance and Security

Pass with Distinction: [YES] [NO]

Keywords/Descriptive Terms: wireless security, 802.11, wireless access point, automation, UAV, drone

Contains Security-Sensitive Information [ ]