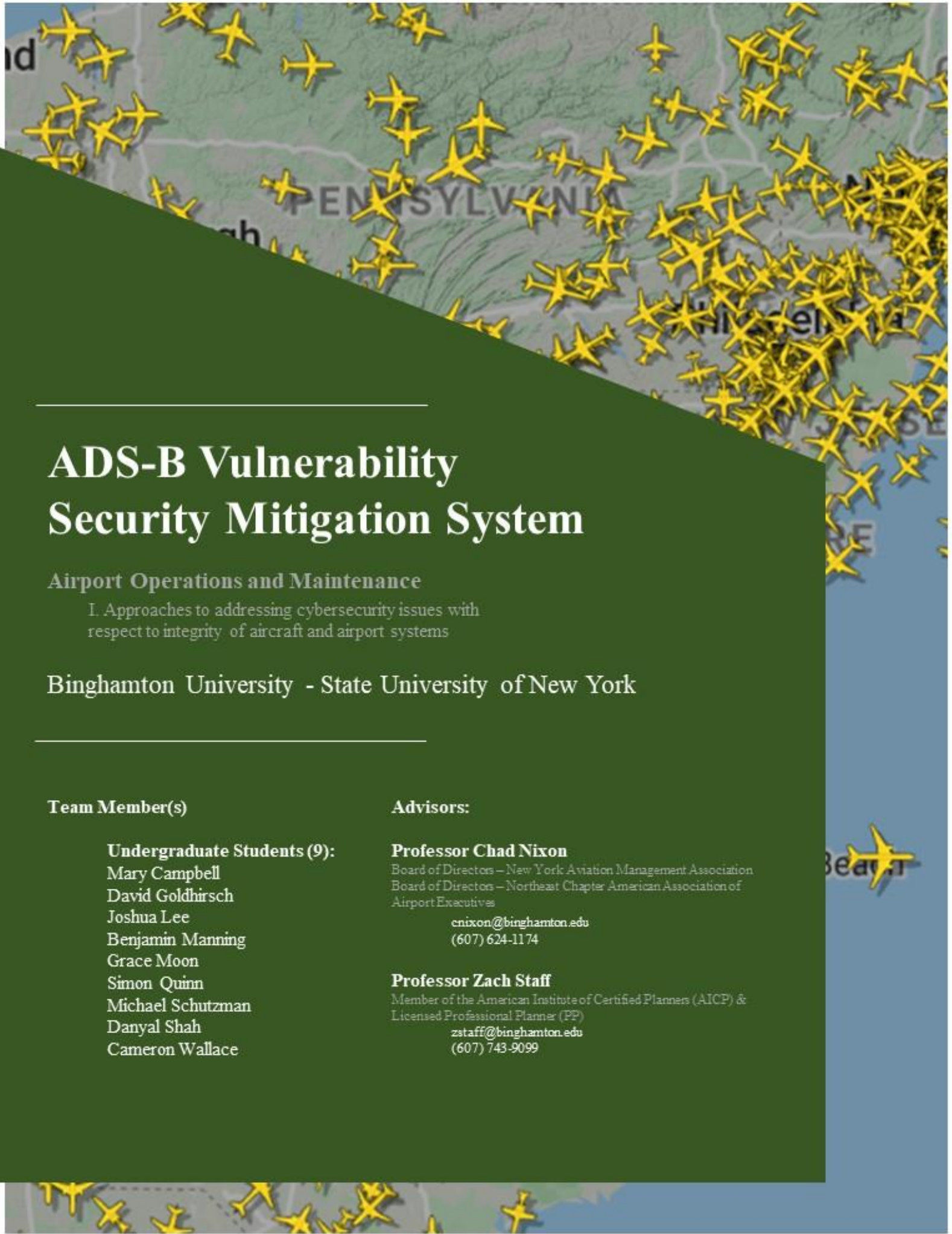

ADS-B Vulnerability Security Mitigation System

Airport Operations and Maintenance

I. Approaches to addressing cybersecurity issues with respect to integrity of aircraft and airport systems

Binghamton University - State University of New York

Team Member(s)

Undergraduate Students (9):
Mary Campbell
David Goldhirsch
Joshua Lee
Benjamin Manning
Grace Moon
Simon Quinn
Michael Schutzman
Danyal Shah
Cameron Wallace

Advisors:

Professor Chad Nixon
Board of Directors – New York Aviation Management Association
Board of Directors – Northeast Chapter American Association of Airport Executives
cnixon@binghamton.edu
(607) 624-1174

Professor Zach Staff
Member of the American Institute of Certified Planners (AICP) & Licensed Professional Planner (PP)
zstaff@binghamton.edu
(607) 743-9099

ADS-B Vulnerability Security Mitigation System

January 2020 - April 2020

Design Challenge Addressed: Airport Operations and Maintenance I. Approaches to addressing cybersecurity issues with respect to integrity of aircraft and airport systems.

Team Member(s)

Undergraduate Students (9):
Mary Campbell
David Goldhirsch
Joshua Lee
Benjamin Manning
Grace Moon
Simon Quinn
Michael Schutzman
Danyal Shah
Cameron Wallace

Advisors:
Prof. Chad Nixon
Prof. Zachary Staff

University: Binghamton University - State University of New York

Executive Summary

Automatic Dependent Surveillance-Broadcast (ADS-B) is a surveillance technology that allows aircraft to communicate with Air Traffic Control (ATC) Towers. This system, newly mandated in aircraft flying in Class A, B, C, and certain E airspace by the Federal Aviation Administration (FAA) as of January 1, 2020, augments the previously used radar technology. ADS-B allows for more reliable communication domestically; especially in areas with mountainous terrain, over the Gulf of Mexico, and more remote areas internationally. This system, while significantly improving air traffic communication and situational awareness, sends broadcasts that can be viewed by the general public and those who seek to do harm to the system. While no major security breaches have occurred to date, the accessibility of this information is a major cybersecurity vulnerability, as noted by cybersecurity experts.

Interception of ADS-B broadcasts could result in the insertion of false messages, deletion of valid messages, creation of spoof planes, or disruption of air traffic. Further intensifying the problem is the ease with which the public can obtain ADS-B transmitters and receivers, allowing anyone access to tamper with these broadcasts. As airports become increasingly more dependent upon technology, the potential for cybersecurity breaches has grown rapidly. More and more instances of similar events, such as the hacking of baby monitors, personal devices, and even driverless cars, foreshadow the possibility of cyber-attacks within aviation. With this increasing severity and reach of cyber-terrorism, ADS-B technology is more likely than ever to be hacked. Our recommendation is to mitigate cyber-threats by encrypting and adding an authentication code to ADS-B broadcasts to prevent malicious attacks. Encryption will provide a layer of security by eliminating the unrestricted access of these broadcasts by anyone with a receiver, while the authentication code will verify the sender to prevent spoofing attacks.

Table of Contents

Table of Tables

Table of Figures

1.) Problem Statement and Background

A. Communication between Aircraft and the ATC

The primary method for several decades of tracking and communicating with airplanes and other aircraft was a combination of radar and radio. However, with air travel and recreational flights increasing in volume, the industry has observed a greater influx in air traffic, which creates congestion and presses the limits of traditional radar, ATC, and aircraft communication. Radar has also historically been unreliable during bad weather conditions and in certain terrains, like mountains, gulfs, and some parts of the ocean [1] [2] [3]. As such, the FAA and the global aviation community mandated that ADS-B be used to augment the traditional system. ADS-B is a system of surveillance technology utilized between an aircraft and ATC as seen in Figure 1. ADS-B technology determines an aircraft's location via GPS satellites and broadcasts this information to the ATC as well as other planes with specific ADS-B hardware, enabling the aircraft to be tracked in real time. This technology also allows for nearly instantaneous broadcast updates on vital weather conditions, messages from pilots to ATC towers, and aircraft location [5] [6].

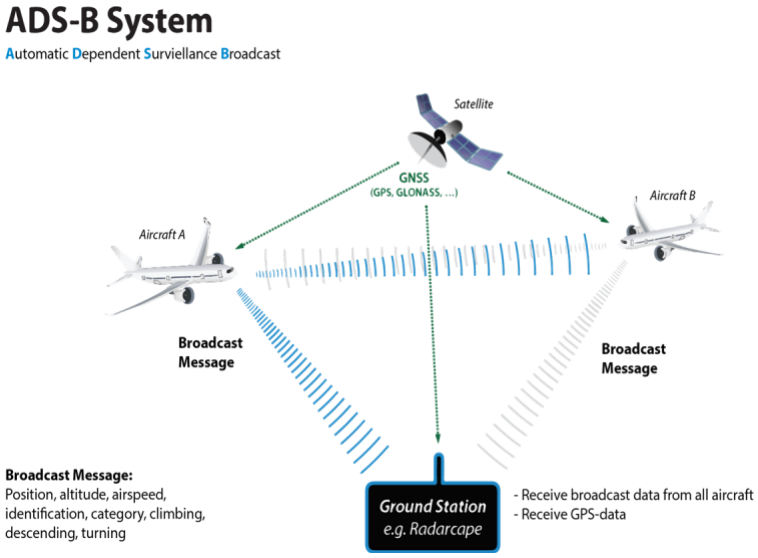

Figure 1. ADS-B Communication with Ground Control, other Aircraft, and Satellite [4]

The problem with this technology, however, is that these messages are being broadcast on an open, publicly accessible frequency without any cybersecurity measures in place. While

the structure of this broadcast system cannot drastically be changed to combat this issue, implementing encryption and an authentication system to render the messages being broadcast unintelligible to unauthorized parties may serve as a countermeasure. Encryption is the process of turning understandable data into incomprehensible code, thus scrambling a message so that only authorized parties with the corresponding 'key' can access the information (Figure 2). Encryption doesn't directly prevent interference from malicious parties but prevents them from reading crucial data when intercepted [1] [7] [8].

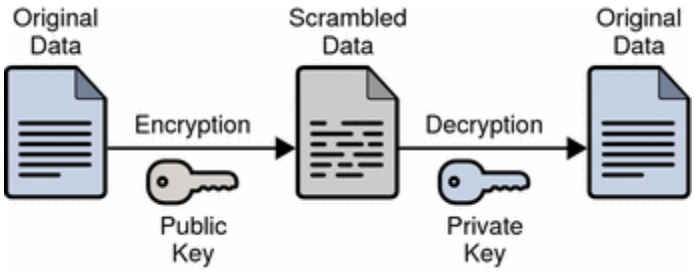

Figure 2. Basic Encryption Process of a Message [9]

This key can be used by the receiving party to then decrypt the data, thus keeping information safe during transit between users. Authentication codes allow the receiver to be certain that the message wasn't tampered with or injected from a spoof aircraft. However, this lack of security in ADS-B poses a serious security and safety risk. Any member of the general public could get the parts to build a receiver and transmitter without significant technical skills. With this equipment, a hacker could potentially inject fake messages which mimic other planes, thus veering an existing plane off course or, if many of these false messages are injected, shut off routes and cause havoc in ATC [10]. Hackers could feasibly intercept messages, create messages of their own, and delete or modify existing messages, confusing ATC and potentially putting the lives of passengers and pilots at risk. Also, unauthorized personnel having unobstructed access to information on exact locations, times, and messages from planes in the air could pose a massive security risk. From the perspective of an ATC tower, there would be no differentiation between

an authentic aircraft and a maliciously spoofed aircraft, leading to extensive air traffic disruptions. Along with security concerns, the financial losses of postponing and redirecting flights due to the presence of spoofed planes in the airspace would be substantial. Although the amount of accurate, efficient, and reliable information ADS-B technology provides is quite advantageous, its vulnerabilities in terms of cybersecurity are very alarming and call for serious and immediate action.

B. FAA Guidelines and Goals

Over the past couple of years, the aviation industry has been transitioning to the utilization of ADS-B as the primary method of aviation surveillance with traditional primary radar operating in the background. Several countries have already completed this transition. The United States followed suit as of 2020 with a FAA regulation mandating aircraft to equip ADS-B Out as of January 1. The FAA's 2010 performance target regarding cybersecurity from their *Portfolio of Goals* included the statement of their hope to have "zero cyber-security events that significantly disable or degrade FAA services." Their *Destination 2025* and FAA Portfolio of Goals outline a very similar performance matrix regarding cybersecurity as well [11] [12].

C. Intent of Project

There have been many expert discussions on how to better protect airlines and airplanes from cyber-attacks. With the long FAA certification process, the focus is often on the technology and not on the long-term manner in which threats could arise. Most of what is being done now regarding cybersecurity advances are just proposals, not concrete actions. One such idea is mandating the use of other surveillance systems, radar for instance, as verification systems. However, certain places, such as the Gulf of Mexico and the Hudson Bay, have ineffective radar signals which highlight these areas as primary targets for security breaches. Multilateration is an

additional practice which has been considered to combat the shortcomings of ADS-B; however, multilateration, while it can be used as an aircraft verification system, is not able to accurately determine altitude and is unable to prevent aircraft spoofing attacks [10]. From the perspective of ATC operators, there is no differentiation between spoofed aircraft and actual aircraft as seen in Figure 3. This could potentially lead to massive confusion.

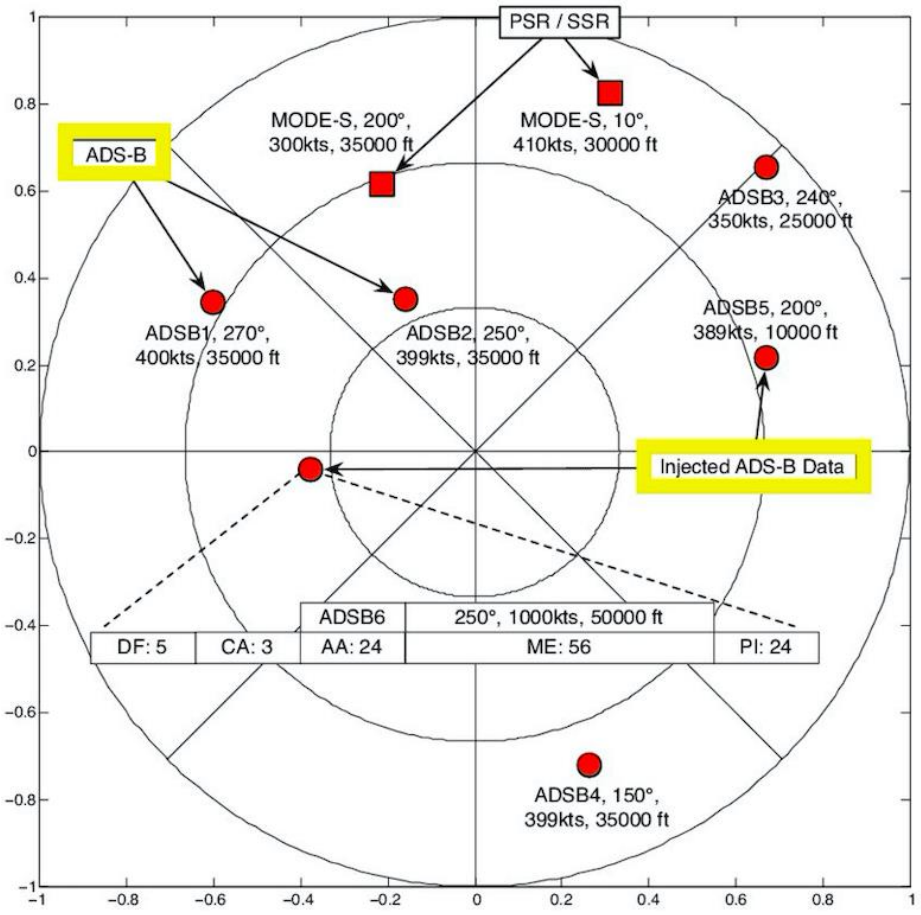

Figure 3. ATC Screen depicting how there is no differentiation between actual and spoofed aircraft in the perspective of ATC operators [9]

To call attention to the extent of ADS-B broadcast accessibility, the website flighttrader24.com provides real-time visualizations of thousands of airplanes. This includes information about flight course, status, and communications with airports. Clearly, the signals are free to be intercepted by everybody and anybody. As outlined before, this can lead to planes being hijacked, spoofed, directed off course, etc. Obviously, there is a massive threat to public

safety and endangerment of people's lives with the current system in place, and consequently, this proposal identifies a newer and safer mechanism for this system to better maintain aviation security and save the lives of passengers and personnel.

The proposal to ensure a more secure system of broadcasting ADS-B messages consists of encrypting the transmitted data and verifying the aircraft with an authentication code, thereby obstructing access to the general public and eliminating spoofing attacks. This will prevent hackers from overriding plane control systems, steering planes off course, tracking precise locations of flights, or overwhelming the ATC systems with fake messages.

2.) Airport Security and ADS-B Literature Review

A. Growing Cybersecurity Risks

As industries around the world are becoming increasingly dependent on computerized systems, cybersecurity is becoming a major concern for all. The Internet of Things (IoT) is a system of unsecured interconnected computing devices with the ability to efficiently transfer data over networks. Devices in the world of the IoT are at risk of various cyber-attacks due to the sheer volume of shared data and unprotected data transfers. With so many devices now within reach of hackers, there has been a steep increase in cyber-intrusions in many areas previously thought to be untouchable [13]. Even everyday objects can be a security concern as hackers have been capable of carrying out identity theft through smart refrigerators [14]. Similarly, baby monitors have proven to be vulnerable as multiple families reported their devices being taken over by hackers shouting through the speaker to wake up the baby [15]. Even more dangerous, however, is how this new vulnerability to hacking has affected vehicles. In 2016, two hackers were able to force a Jeep off the road, leading to the recall of 1.6 million vehicles [16]. In addition, physical methods like low-power lasers have been capable of meddling with smart car

computer systems. The amount of data accessible to hackers through smart vehicles will only continue to grow alongside the technology [17]. Concerns like these have impeded the adoption of smart vehicles, with one study revealing that over 70% of Americans are at least moderately concerned with smart car vulnerability to hackers [18]. Clearly, there is a major concern for the security of emerging technology and all industries should be prepared to deal with disruptive cyber-attacks and the increasing lethality of such attacks.

B. Cybersecurity in Aviation

One of the most affected industries in this new wave of cyber-warfare is aviation, especially as it transitions to a more technology-dependent state. Devices such as passenger check-in, traveler web services, and even communication systems installed in aircraft are just a handful of examples of smart devices in the IoT utilized by airports. Devices connected to an airport's network, such as the aforementioned, support vital functions of the interoperability between airports, ATC, and airport administration. However, the interconnectedness of the IoT highlights the potential threats that may arise within the aviation industry. The European Aviation Safety Agency reported over 1,000 cyber-attacks per month on aviation systems in 2019. In total, 22 areas vulnerable to cybersecurity attacks have been identified [19]. Personal data is highly vulnerable in airports; in London-Heathrow the Queen's location was able to be tracked due to the lack of secure and encrypted data. In Hong Kong, 9.4 million customers' personal data including their I.D. numbers and credit cards were stolen from an airport cybersecurity breach [20]. In a survey involving 200 of the busiest airports in the USA and Europe, nearly 85% used a digital platform for services and made use of the IoT to some extent and nearly 30% considered themselves a "smart airport" that fully utilizes and relies on IoT technology [21]. This increasing reliance on IoT technology has opened up a particularly

dangerous cybersecurity risk in computerized aerial vehicles. The use of unmanned aerial vehicles (UAVs) for inspection and maintenance can pose a serious threat; one such incident of a hacked UAV injured two and killed one [22].

In-flight operations are a major area of concern for cybersecurity breaches because the result of an attack could be catastrophic on a large scale. Gérard Duerrmeyer, chief information security officer at Norwegian Air Shuttle, said, "There will be a future where these systems are all online, and that will open the attack surface and the chance for exploitation" [21]. Researchers have recently discovered new means of hacking airplanes that haven't been addressed yet. One example involves a German researcher who created an android app that could redirect a plane, showing what little processing power is required to take over an airplane's flightpath [22]. Chris Roberts, a former security researcher, was able to issue a climb command and make a plane briefly change course [23]. With so many risks in both the airplane and the airport, cybersecurity is pivotal to the aviation industry moving forward.

In March 2019, the Boeing 737 Max planes were all grounded following the crash of two of these exact models, killing 346 people [24]. The cause of these crashes was attributed to a faulty sensor within the automated flight control system, forcing the plane into a continual descent. Boeing faced a massive economic setback with a record quarterly loss estimated to be 3.6 billion dollars, as shown in Figure 4 [24]. While this catastrophe was not attributed to a cybersecurity breach, such an attack is certainly not out of the question. Hackers could halt all air-traffic within an airport for days, cause the crashes of multiple aircraft, and overwhelm ATC leading to massive confusion. The nature of this inherent cybersecurity threat within ADS-B communication means that a breach could produce even more significant financial and human life losses than those experienced by Boeing, thus highlighting this issue as one requiring immediate and decisive action.

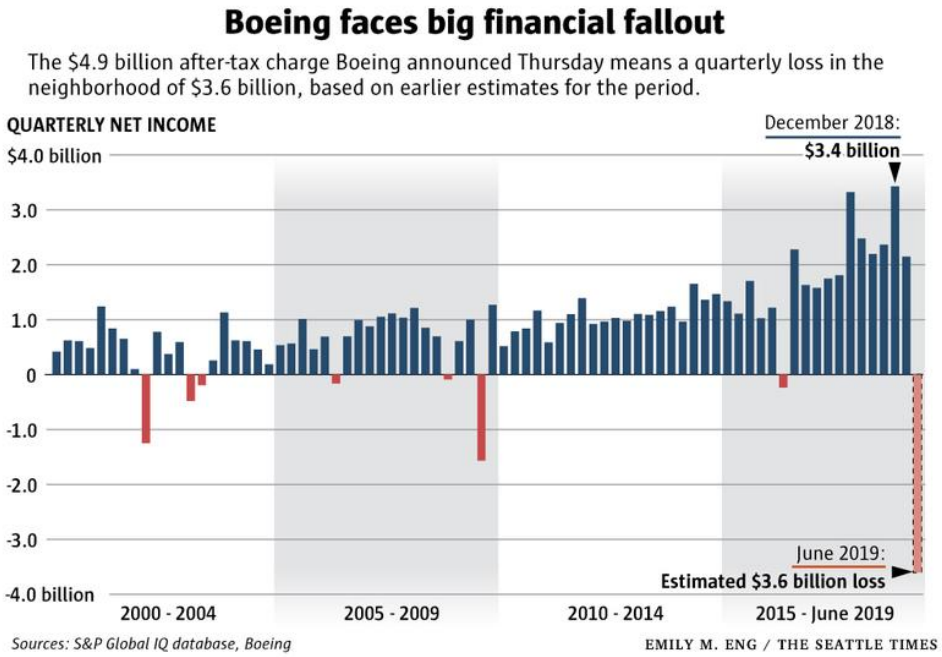

Figure 4. The financial loss of Boeing following the grounding of Boeing 737 Max Planes [24]

Many solutions have been proposed to decrease the vulnerability of these systems. One course of action experts recommend is government regulation. This would entail either setting mandatory cybersecurity requirements for IoT device manufacturers or direct monitoring of aviation industries by the government to ensure adequate cybersecurity is in place. Some have even proposed legalizing "hacking back," which would allow industries to beat hackers at their own game [25]. Another new development that could change the world of cybersecurity is quantum key encryption, which would allow for secure data transfer that is not vulnerable to hacking in the foreseeable future [26]. However, this technology is currently being researched and evaluated as it is not yet implemented in any major form of industry communication. Another effective solution that has arisen in industries that rely heavily on IoT and other devices is "cyber hygiene" education for workers, which has been useful in preventing vulnerabilities from opening up due to human error [27]. One additional proposition is the use of an intrusion

prevention system (IPS), which uses devices that are capable of detecting, blocking, and attacking botnets, a tool for hackers that uses the internet to attack IoT devices [28].

C. Automatic Dependent Surveillance-Broadcast

One of the most recent technological advances implemented at airports is the aircraft tracking system known as ADS-B. As a part of project NextGen, the FAA ordered the full augmentation of traditional radar with ADS-B by January 1st, 2020 [5] [6]. Radar gained prominence during WWII in the cockpit of military planes [2]. It has been used for determining the location of aircraft by sending radio waves through the air and reading the resulting interference from aircraft [29]. However, since the 1980s the number of vehicles in the sky has increased to the point where radar is ineffective. In addition, radar is heavily affected by weather, location and altitude. In a period of 19 years, 568 crashes occurred in Alaska because of difficulties associated with radar in remote areas [1] [2]. Radar is also interrogation based, meaning that pilots have to communicate altitude and speed to ATCs through radio communications [3]. As a result, the FAA searched for a more technologically advanced alternative. ADS-B improves upon radar as it is more accurate, covers more area, and updates every 0.5 seconds [7] [30] [31] [32]. In addition, ADS-B significantly reduces the cost of monitoring the airspace from $10-14 million with radar to $380,000 [33]. It has already been implemented in Australia, Canada, China, Sweden, and the UAE. As a result, in 2010 ADS-B was chosen by the FAA to become the primary method of geolocation [4]. The differences between these two methods of surveillance can be seen in Table 1.

Table 1: The Differences Between ADS-B and Radar Surveillance in Aviation

ADS-B	Radar
Coverage: reliable coverage everywhere	**Coverage:** unreliable in certain topography and weather conditions
Information: location of aircraft, weather, flight path, elevation, speed, and messages	**Information:** location of aircraft
Message Frequency: every 0.5 seconds	**Message Frequency:** ~12 seconds between message returns
Cost: $380,000	**Cost:** $10-14 million
Type of Aircraft: can be utilized by all aircraft with equal ability to transmit broadcasts	**Type of Aircraft:** smaller aircraft are less visible and reflective surfaces can distort readings

ADS-B technology is broken down into two types of equipment installed on aircraft, ADS-B Out and ADS-B In, with both modes working hand in hand [33]. ADS-B Out refers to an aircraft transmitting its location and other important information determined from satellites, while ADS-B In refers to an aircraft receiving informative broadcasts via ground network systems such as Traffic Information Services-Broadcast (TIS-B) and Flight Information Services-Broadcast (FIS-B) [34] [35]. Currently, ADS-B In transmitters are not mandated by the FAA to be installed in aircraft. ADS-B Out provides speed, location, and direction of planes. ADS-B communicates through a 1090 MHz Extended Squitter (1090ES) and Universal Access Transceiver (UAT) [36]. The 1090ES or the Mode S Squitter produces 112-bit messages; 56 of those bits are devoted to ADS-B geolocation [36]. When a location is transmitted, a message is sent to the receiver where it is decoded. In general, the system does not require any authentication, so the potential for hacking is high. In 2009, the US military discovered a militant group had video footage from an unencrypted US aircraft system. Using a $26 program called Skygrabber, the group was able to steal the information and discover military secrets [37].

Researchers have already proved that ADS-B signals can be tampered, jammed with false information, overwhelmed with fake aircraft, deleted, or eavesdropped by hackers [7] [10] [21] [31] [38] [39].

The current system most often utilized by airports for location authentication is multilateration. This technique uses multiple sensors to evaluate the location of aircraft based on the difference in time between the received signals of multiple aircraft [10]. The system is designed to identify possible spoofed aircraft, but it is expensive and requires around four times as many sensors as normal ADS-B transmissions. Multilateration also has multiple issues regarding transmission in mountainous areas, altitude calculations, and loss of portions of the transmissions over greater distances. Overall, this solution seems to only be sufficient in flat areas with airports in close proximity to one another [10]. Although ADS-B currently has inadequate cybersecurity safe-guarding measures, there are a few methods available to prevent hacking. Researchers have proposed a verification code called Message Authentication Code (MAC) to connect planes with the ATC, the use of radar to cross-check locations, and quantum computing to ensure secure data transfer [26] [33] [38] [40]. However, the main solution is to implement a means of encryption in addition to a MAC which provides authentication [1] [7] [8]. There are a variety of types of encryption, but when choosing one, the FAA must acknowledge the bit size of the encryption as the message is restricted in size due to hardware limitations. Highly complicated encryption systems may require a computer overhaul. Encryption seems to be the most effective protection for ADS-B in terms of cost, simplicity, and protection efficiency while the MAC provides aircraft authenticity.

3.) Problem Solving Approach

A. Initial Brainstorming Phase

The project began with our team looking over the ACRP competition guidelines and sections. Following this, we reviewed recent aviation issues to inspire potential topics to focus our research. Three major topic areas were considered after consultation with Professor Nixon, Professor Staff, and Professor William Ziegler, former instructor of the course and Director of the Binghamton University Scholars Program. These topics are listed below along with the reasons for rejection or adoption in Table 2.

Table 2. Topics Considered During Brainstorming Phase

Idea	Explanation	Reason for Rejection or Adoption
Polyfluoroalkyl substances (PFAS) contamination checklist	Airports could use a checklist of certain factors to determine the likeliness of groundwater contamination by a toxic chemical, Perfluorooctanoic acid.	This project was rejected. This idea has limited application, because it provides no solution for removing PFAS.
Piezoelectric energy for roadways	Utilize piezoelectric crystals embedded in the runways to create vibrational energy which could be used to heat and deice the runways.	This project was rejected because the idea of using piezoelectric crystals to harness alternative energy was in a past submission.
Cybersecurity for ADS-B	ADS-B transmissions can be secured using encryption, mitigating the threat of ADS-B-based cyber-attacks.	This project was adopted because of its importance for airports, the aviation industry, and the safety of its customers.

B. Research Conducted on ADS-B

After settling on cybersecurity issues relating to ADS-B as the basis for our project, we researched how hacking has affected other industries and technologies. Cybersecurity issues within other devices such as baby monitors, self-driving cars, smart refrigerators, and the IoT were investigated along with the response of the industries to these attacks. Cybersecurity breaches within airports, such as data theft, stolen passwords, and various other types of attacks were categorized by the weakness which allowed their exploitation. Once the scope of the problem concerning aviation was identified, similar broadcast-based messaging systems were researched in helicopters and ships to gain a better understanding of the applicability of this issue to ADS-B specifically. General research was conducted on how ADS-B functions, where/how ADS-B is implemented, system weaknesses, and the possible types of cyber-attacks that could occur within this system. The knowledge from this preliminary research allowed for the extension of our project to examine potential solutions to the previously discovered ADS-B system's inherent cybersecurity vulnerabilities. As seen in Figure 5, Professor Nixon is showing the team the complexity of flight patterns in the New York Metropolitan Area.

Figure 5. Professor Nixon explaining aircraft flight patterns at Morristown Airport and the New York Metropolitan Area

Additionally, it was necessary to review FAA requirements on cybersecurity and ADS-B. It should be noted that the FAA has required the use of ADS-B Out on all aircraft in 14 CFR

91.225 and 14 CFR 91.227. This is part of the FAA-led initiative referred to as NextGen, which will result in the modernization of U.S. airspace [41]. Furthermore, the FAA was instructed to address cybersecurity concerns in section 2111 of the FAA Extension, Safety, and Security Act in 2016 [42]. In response, the FAA and European Union Aviation Safety Agency (EASA) have created DO-326 and ED-202, respectively. These international standards must be complied with to receive the cybersecurity airworthiness certification [43]. Finally, as part of the FAA Strategic Plan, the FAA will seek to increase cybersecurity for airports and airplanes between 2019 and 2022 [43].

C. Solution and Assignments

Based on this research, the team developed a preliminary plan to secure ADS-B transmissions. The exploitable weaknesses of ADS-B are its accessibility to the public and lack of authentication. The best way to solve these problems is to encrypt ADS-B messages with a secure encryption key. Encrypted ADS-B transmissions are able to protect message content from the public eye and, with the addition of a MAC, allow for the authentication of messages. The implementation of an encryption system would be backwards compatible with existing ADS-B hardware, confirm that the information being transmitted from a plane is accurate, and prevent the majority of cyber-attacks. The encryption would be based on a symmetric key system (everyone has the same encryption and decryption key) to avoid complications that would arise from a more complicated asymmetric key system (contains both private and public keys). After researching the topic for several weeks, consulting with airport experts from Morristown Airport in Morristown, NJ, and consulting with a cybersecurity expert from Binghamton University, the team narrowed its focus to a specific type of encryption: the advanced encryption standard (AES). AES has been well tested and is widely used, thus serving as an excellent candidate for

ADS-B encryption. AES, however, does not function with the irregular 56-bit message size of ADS-B. To overcome this, the team proposed the use of FFX-A2, a mode of operation, which allows for the encryption of irregularly sized messages. An additional layer of security could be incorporated by implementing an authentication code system in addition to encryption, such as MAC. As an added benefit allowing ease of adoption, these proposed elements are digital and would require essentially no additional hardware or modifications besides those already in place for existing ADS-B installations. In addition, a possible key changing algorithm, decryption software, and an electronic key distribution system could be incorporated to increase security.

Once research was completed and a project proposal was decided on, the team was divided into five subgroups: the Project Leader (Mary), the Design Team (Danyal and Simon), the Engineering and Graphics Team (Michael and Grace), the Risk Assessment Team (David and Joshua), and the Strategies and Approach Team (Cameron and Benjamin). Each subgroup was given tasks to complete and to further report on. The Project Leader oversaw of all the subgroups, held team meetings, created the executive summary, and edited the final report. The Design Team was tasked with the technical aspects of the project and the projected impacts. The Engineering and Graphics Team was in charge of taking photos at different milestones during the project (such as when experts visited), general graphics in the report, the summary and conclusion, and the problem statement and background information. The Risk Assessment Team was responsible for writing the safety and risk assessment, creating several appendices (A, E, and F), and compiling the literature review for the entire project. Finally, the Strategies and Approach Team was responsible for interacting with airport experts, writing the problem solving approach, and for compiling appendices B and C. All of these tasks were assigned at the start of the Spring 2020 semester, and all of the parts were due 11 weeks into the semester or before.

It is worth noting how the team was impacted by COVID-19 and the measures taken by New York State to mitigate the outbreak. Starting on March 19th, most classes were moved online at Binghamton University. Most of the team went home, and subsequent classes, assignments, and discussions were performed online via Zoom and Discord. While the transition required the adjustment to remote communication, the team was still able to function and remain on schedule. The team can be seen having a Zoom meeting in Figure 6.

Figure 6. The team conducting a weekly meeting through Zoom

D. Consulting with Experts

In addition to the knowledge gained through online research, airport experts were contacted during the project and their advice enhanced our team's understanding of the project. First, we contacted Darren Large and Josh Moyer from Morristown Airport (MMU). These two experts confirmed that ADS-B has major security vulnerabilities, including false broadcast injections mimicking actual aircraft (spoofing attack), that decrease safety for pilots. This is especially the case where radar can't be used to crosscheck ADS-B signals. The experts considered a method of authentication to be the best method of securing ADS-B and agreed that encryption is a potential solution. Additionally, the experts pointed out that the ADS-B system can be very costly, especially for private pilots. We took the cost of ADS-B system modification into account by ensuring our design was backwards compatible so as to not put additional financial strain on private aircraft owners. Overall, Mr. Large and Mr. Moyer helped develop our understanding of the project, and we further developed our project keeping their suggestions in

mind. Additionally, the team learned how helpful real time expert feedback can be when determining how to implement a design.

We also contacted Scott Craver, the head of Binghamton University's Electrical and Computer Science department, to learn more about the technical aspects of encryption. Although Dr. Craver does not specialize in ADS-B message encryption, he has significant experience and research in information security. He explained some of the different types of encryption, such as block encryption and stream encryption, and how they could be relevant to our project. Stream encryption was of particular interest, since it encodes messages bit by bit instead of encoding an entire block (a message consisting of 32, 64, or 128 bits). This allows flexibility in the 'length' of the messages being sent. Block encryption, on the other hand, requires messages of fixed length. The strength of block encryption is its formulaic message size and algorithm. Dr. Craver also explained the weaknesses of both while offering ideas of how either type of encryption could be implemented in ADS-B. Finally, Dr. Craver briefly researched format preserving encryption, an approach that our team had found while researching, as a possible way to encrypt irregularly sized messages. Overall, Dr. Craver's expertise in the area of encryption was invaluable for our understanding of the technical aspects of the project. The team made necessary adjustments to the proposed solution based on the insight Dr. Craver provided, making the project more technically feasible.

In summary, we are seeking to address the inherent lack of security in ADS-B messages by implementing encryption and authentication in the transmissions, decodable by a symmetric key. The team's initial research into the shortcomings of airport cybersecurity gave us a clear indication that this was an area of opportunity for new ideas. After preliminary research, the scope of the project was confined to the ADS-B system. The proposed method of encryption alongside a MAC will provide a level of ADS-B security that currently does not exist. With the

help of the airport and encryption experts that were consulted, the finalized proposal should protect against hackers and decrease the inherent risks associated with using ADS-B.

4.) Safety and Risk Assessment

The FAA's main goal is to "provide the safest, most efficient aerospace system in the world." [45]. A major aspect of providing a safe environment is minimizing risk to and optimizing the protection of flights, communications, and equipment, which are all critical to the National Airspace System (NAS).

As a result, the FAA in the AC 150/5200-37 suggests the use of a safety matrix to identify hazards and to categorize them according to severity and likelihood as shown below in Figure 7 [46]. The matrix has three levels of risk: low, medium and high. Low is the target level

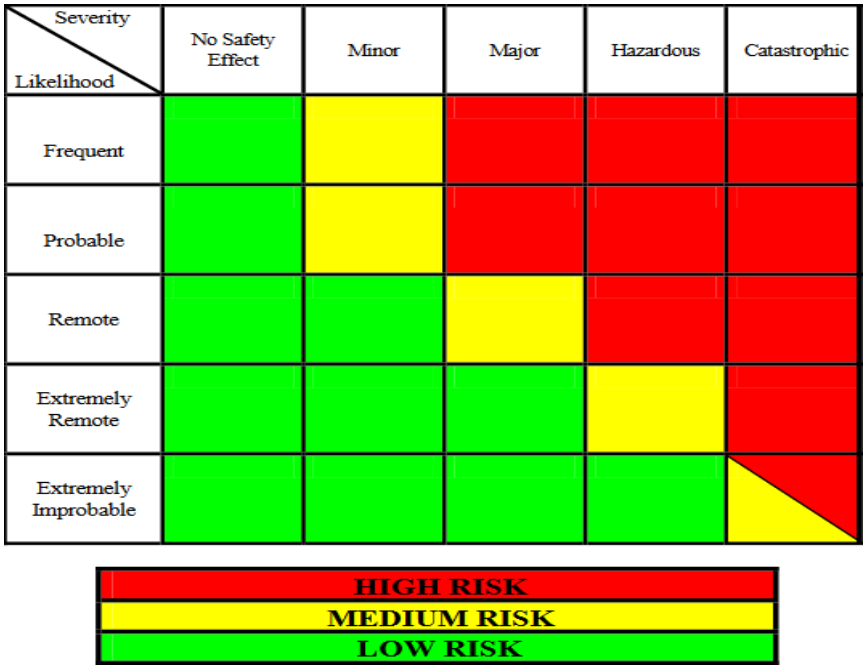

Figure 7. The FAA's Sample Safety Matrix [46]

of risk; no countermeasures need to be taken. Medium risk is acceptable, but there should be monitoring and a potential solution in the future. High risk requires immediate attention due to the fact it may lead to damage of the equipment, disruption to air traffic, or even loss of life [46].

In the case of ADS-B encryption, there are few risks considering the implementation of encryption is itself a form of risk mitigation. For example, this change would be largely unaffected by inclement weather. However, there are some downsides to this system that can pose potential safety risks. The most prevalent risks to be examined in this report include ADS-B data lost in transmission, slower transmission speeds, and encryption malfunction. Due to the nature of ADS-B keys, a certain percentage of the message is lost upon transmission. This information loss generally increases with transmission distance, creating a significant issue at longer ranges as displayed in Figure 8 [10]. However, since ADS-B is updated almost

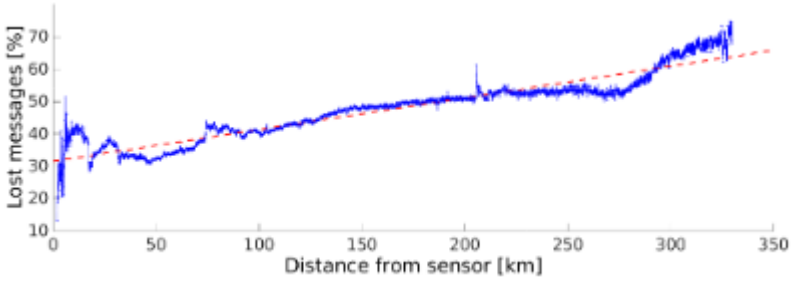

Figure 8. ADS-B bit loss as a function of transmission distance [10]

instantaneously, this issue can often be remedied by filling in missing information with subsequent messages [6]. It should also be noted that the addition of encryption to the ADS-B key may exacerbate this issue as there will be less space for significant information and parts of the encrypted key may be lost. It is possible that this could lead to incorrect identification, location, and evaluation of airplane situations if the information is not found in later transmissions. This is compounded over greater distances, just as it is currently, as more of the encrypted message will likely be lost and it is unknown as to how many future transmissions will be needed to relay the missing information.

Despite such a large percentage of the key being lost at long distances, the development of an actual problem is quite remote due to the rapid transmission updates of one message every 0.5 seconds. This problem is one that already exists and may worsen slightly but is already

considered manageable. In this situation, one of the worst problems that can occur as a result of missing information is a particular aircraft requiring additional ATC attention. This is not a direct issue with the air traffic system itself, therefore it warrants a minor threat classification. Altogether, the risk level for this issue would be classified as medium and can likely be mitigated by increasing the coverage of ADS-B receivers.

The addition of some form of encryption will slow the transmission of ADS-B messages. Before encryption, messages are required to be transmitted every 0.5 seconds [6]. One form of encryption called Identity Based Encryption takes 1.833 seconds for each communication link [17]. This would significantly decrease the efficiency of ADS-B, but this is still approximately a five-times improvement over radar which is transmitted every 5 to 10 seconds [16]. Additionally, another form of encryption called Stage Identity Based Encryption can relay messages at 0.204 seconds [17]. Although there are several means of encryption, the team suggests the use of AES FFX-A2. However, there are no exact numbers on what the delay is for this form of encryption. Before advancing a particular encryption for implementation, the delay must be known to see if it falls within FAA guidelines.

As with all software, there is the possibility of a malfunction. According to the SMS Safety Manual, “When a system includes software and/or hardware… Systematic design processes are an integral part of detecting and eliminating design errors.” [45]. For the implementation of encryption, there should be an overarching process that slowly introduces the new system. The system should have multiple experiments with one or two planes that adopt this security measure. After many successful trials, the system should be used within a low air traffic region, and slowly other regions should experiment with the new system. In the phase of multiple years, it can be gradually be adopted into FAA regulations. With the use of long-standing encryption protocols, the safety and confidence of the system is greatly increased.

Table 3. A Safety Matrix of Encryption in ADS-B Messages

Hazards	Severity	Likelihood	Risk Level	Solution
Data loss	Minor	Remote	Medium	Fill in missing data with following messages
Slower speeds	Minimal	Frequent	Low	Accept the risk
Encryption malfunction	Major	Extremely Remote	Medium	Have programmers troubleshoot the issue
Weather	None	None	None	None

Without the implementation of encryption or some form of authentication for ADS-B, the risk of catastrophic loss is significantly higher. In the absence of authentication, hackers could create a number of spoof planes, jam signals, hide planes, or even modify in-flight information to cause disruptions in air traffic [7]. According to Darren Large, the Director of Morristown Airport, if two spoof planes were fabricated on each side of a runway, the entire runway could be disabled until the areas were cleared. Disruptions in air traffic could lead to massive delays, which in a high traffic area such as JFK would cost millions. In addition, spoof planes on route would force pilots to take alternate routes. If only one spoof plane was introduced, a pilot may not be significantly affected. However, a coordinated attack that targeted many planes at once in a limited visibility environment may lead to a pilot taking immediate evasive action causing an aircraft or multiple aircraft crashes. In the worst-case scenario, without cybersecurity, hacking ADS-B is a high-level risk with the potential for catastrophic results including crashes and disruption of hundreds of flights. However, when ADS-B with encryption and authentication is rolled out, the risk drops substantially.

5.) Technical Aspects Addressed

A. Introduction

Airport security is at a crucial turning point with the rising technological dependence of airports, necessitating new measures to counteract an increase in hacking instances. In utilizing the current FAA-mandated ADS-B system, airports are placing thousands of aircraft at risk for malicious cybersecurity intrusions by not encrypting or providing authentication of these broadcasts. The proposed solution of encrypting ADS-B using AES with the FFX-A2 mode of operation, a type of format-preserving encryption, will provide airports with much needed security to protect against cyber-attacks. Authentication of aircraft can be accomplished by using a MAC in addition to AES FFX-A2. Encryption and authentication prevent hackers from reading the messages or injecting fake messages, thus securing information about flight patterns, aircraft position, and ensuring sender authenticity.

B. Proposed Solution

When choosing the best form of encryption, different parameters must be taken into consideration since many different methods of encryption exist. The first parameter analyzed was the type of key used to decrypt the encrypted information. There are two options: an asymmetric key, which assigns a different key for each user, and a symmetric key, which uses a key that is identical for encrypting and decrypting all information [8]. A symmetric key was selected because asymmetric encryption requires too many iterations of the same message to be sent and received with different keys, and the cost and coordination required would necessitate a massively more complicated system. With symmetric keys however, only one key is needed to both encrypt and decrypt the information.

The second parameter analyzed was the way the information would be encrypted, known as ciphers. There are two types of ciphers for symmetric encryption: block and stream [8]. A block cipher encrypts a block, or chunk, of text, while a stream cipher encrypts one character at a time. A block cipher is currently the best choice of the two because block ciphers are much more widely researched and implemented, particularly in the case of AES when it was developed by the U.S. National Institute of Standards and Technology (NIST) in 2001 [47]. Another complication of a stream cipher is that it encrypts character by character, meaning that the starting and stopping points within the algorithm would have to be recorded in order to successfully decrypt the broadcast messages. Block ciphers, by utilizing the same algorithm for each transmission, are much simpler to decode with the one shared symmetric key. Without access to this key, however, decrypting messages would be exceedingly challenging for external parties.

Information takes up space, or bits. Depending on the size of the information, the number of bits it occupies varies. Standard block ciphers encrypt in blocks of 32, 64, or 128 bits; however, ADS-B stores the information of aircraft location in 56 bits as seen in Figure 9.

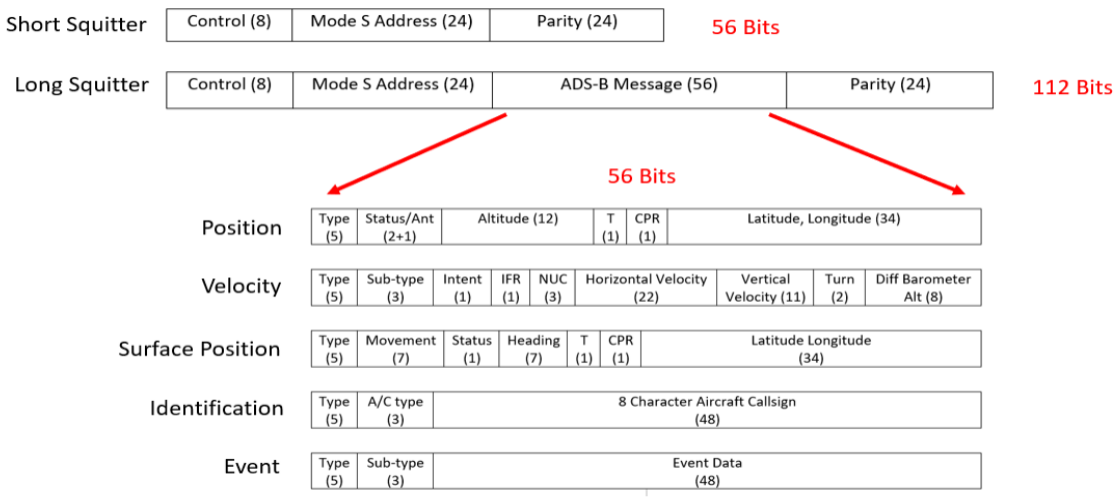

Figure 9. The composition of an ADS-B message, including the 56-bit size of data

This bit size doesn't conform within the block required by AES. Since ADS-B is incapable of adding or subtracting bits from the message, a different mode of operation must be used to accommodate this bit size. A solution to this issue is the use of format-preserving encryption (FPE) within AES, which creates an encrypted message that is the same bit size as the original despite it having a non-conforming bit size [8]. One form of FPE known as format-preserving, Feistel-based encryption (FFX), is a mode of operation for the well-known AES system that changes the block cipher program slightly to allow for abnormal block sizes. FFX enables the operation of AES encryption by changing the 56-bit size so it fits into the necessary block size. The specific form of FFX best fit for ADS-B would be FFX-A2, which is specifically designed for blocks of 8 to 128 bits, which the 56-bit data component fits into perfectly as seen in Figure 10 below [48].

Parameter	Value	Comment
Radix	2	Alphabet is 0, 1
Lengths	[minlen = 8 ...maxlen = 128]	Permissible message length
Keys	$\{0,1\}^{128}$	128-bit AES key
Tweaks	$BYTE^{\leq M}$ $M = 2^{64} - 1$	Tweaks are arbitrary byte strings
Addition	0	Character-wise addition (XOR)
Method	2	Alternating feistel
split(n)	$\lfloor \frac{n}{2} \rfloor$	Maximally balanced feistel
rnds(n)	12 if $32 \leq n \leq 128$	From entropy-based heuristic
F	AES CBC-MAC	Defined in Figure 4

Figure 10. The structure of FFX-A2's parameters [48]

In addition, incorporating encryption into ADS-B transmission wouldn't require hardware modifications, only a software update [49]. This will significantly decrease the cost of implementation, making the option of encryption more attractive than current, and less trustworthy, security options available.

C. Addition of MAC

While encryption is able to prevent the unwanted eavesdropping of aircraft communications, it does not provide true authentication of aircraft. If a hacker were to inject an arbitrary message into the ATC controls, the fake message could be identified due to the fact it wouldn't conform to the encryption algorithm. However, if thousands upon thousands of these arbitrary messages were sent, the massive increase in processing all these messages could jam the system. In a case such as this, identifying the actual sender of the message is essential. A MAC is a type of function capable of verifying the original sender of the message [48]. MAC operates by generating a short summary, or tag, for every message. This unique tag can both be generated and verified by use of a secure key between the two parties. In the case of ADS-B, implementing a MAC in addition to the AES FFX-A2 encryption would allow aircraft transmissions to both be protected from viewing or tampering, and verified as authentic messages coming from actual aircraft. A particular type of MAC that can be used in conjunction with the AES FFX-A2 encryption is a key-hashed message authentication code (HMAC). It uses a hash algorithm (Figure 11), as a means of authentication.

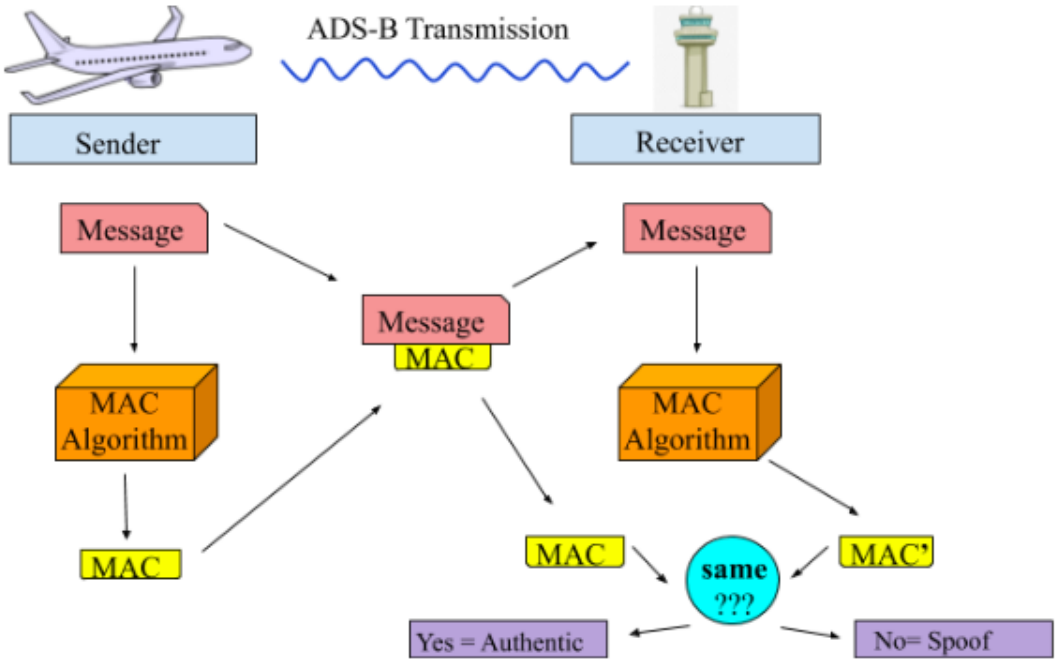

Figure 11. Schematic of how Message Authentication Codes (MAC) operate

With HMAC, the ADS-B out system on aircraft will send the ATC tower the 56-bit message with a proceeding hash key. If this hash key 'tag' on the message matches the ATC generated hash key 'tag' of the received message, then the authenticity of the aircraft is verified. As a result, spoof planes can easily be identified. MAC allows security from spoofing attacks and the aforementioned jamming attacks. By maintaining the content, confidentiality, and sender verification of ADS-B transmissions, AES FFX-A2 alongside a MAC function, such as HMAC, provides the most cybersecurity.

6.) Interaction with Airport Operators

On March 5, 2020, industry professionals Darren Large and Josh Moyer of MMU met with the team via a conference call to discuss the project's logistics and provide feedback. Darren Large is currently the Director of Facilities and Operations. Josh Moyer is the Airport Operation Coordinator at MMU in Morristown, NJ. Mr. Moyer was able to provide insightful information regarding the function and implementation of ADS-B due to his role in overseeing the installation of ADS-B servers on their own aircraft and the integration of the ADS-B system at MMU. Additionally, Mr. Large highlighted the potential consequences of hacked ADS-B signals concerning airport operations, characterizing them as "catastrophic results" especially in metropolitan air zones such as the one MMU occupies.

Through the phone call with two experts from MMU, Mr. Darren Large, director of facilities and operations, and Mr. Josh Moyer, operations coordinator, the reality and severity of this threat had been confirmed. Mr. Large and Mr. Moyer emphasized that there is no authentication of a signal, which means that there is nothing on the receiving end to validate that a described aircraft exists. Following our initial question and answer, Mr. Large recommended we include a risk assessment of ADS-B vulnerability to further strengthen the team's claims.

Moyer also encouraged the group to watch a YouTube clip, "DEFCON 20 Hacker + airplanes = no good can come from this" from DEFCON, one of the largest hacking conventions in the world. The clip is a hacker's perspective of the vulnerabilities within the ADS-B system and the feasibility of hacking the broadcasts. The team can be seen during the call with Mr. Large and Mr. Moyer in Figure 12.

Figure 12. The team calling experts from Morristown Airport

Aside from the latter two suggestions, both professionals confirmed a lot of the group's prior research on ADS-B, as well as supported the group's claim for immediate action taken towards cybersecurity involving ADS-B. In the same manner, the two professionals acknowledged the timeliness and relevance of the project design following the FAA's recent legislation requiring ADS-B Out in all planes starting January 1st, 2020.

7.) Projected Impacts

A. Portfolio of Goals

Every year, the FAA releases a portfolio of its goals and strategies moving into the future. In recent years, cybersecurity issues have become a growing concern. The FAA aims to maintain an extremely high level of security for all of the airports in the National Airspace System and aircraft operating therein. The administration is conscious of the growing interconnectedness of the aviation system and believes it is important to identify and address all potential cybersecurity risks [50]. The exploitation of ADS-B technology is a relatively new concern with undetermined consequences; however, it is a concern that has growing interest. Although the FAA has not officially addressed potential issues with ADS-B regarding cybersecurity in its recent portfolio of goals, the administration has acknowledged a plethora of

other general cybersecurity risks and aims to make airports and aircraft more secure by all means moving forward. Encrypting ADS-B using AES via the FFX-A2 mode of operation with a MAC authentication system is a proactive, viable option for significantly increasing security.

B. Process of Implementation

Like many other issues in the world of aviation, the first main step in addressing ADS-B cybersecurity vulnerabilities requires the FAA to pass regulations. Until the FAA releases an official mandate, implementing AES to properly encrypt ADS-B technology will be a virtually unachievable task. The FAA should look to mandate the use of AES FFX-A2 alongside a MAC, such as HMAC, to secure ADS-B transmissions by January 2021. Due to the significant and urgent nature of leaving ADS-B unencrypted and insecure, the proposed date for such regulation is a necessary goal. This is especially true since it will be roughly a full year after the mandate made by the FAA that required all aircraft within the Class A, B, C, and most within Class E airspace to be equipped with ADS-B as of January 1, 2020.

The physical implementation of AES in the current ADS-B technology within aircraft is achievable, which makes it an ideal type of encryption and a consummate solution overall. If the AES encryption algorithm were to be put into practice, its software would operate on the internal processor of ADS-B. Therefore, it would not be necessary to look for changes in the hardware or ADS-B itself, leading to a smooth, cost-effective implementation. Implementing an encryption system on the roughly 220,000 civil aircraft in the United States would take time to complete; however, encrypting ADS-B technology with AES FFX-A2 encryption and a MAC verification code is a necessary operation that would provide proper, long term cybersecurity [51].

C. Cost-benefit analysis

The cost and associated benefit of implementing AES via the FFX-A2 mode of operation with a MAC authentication system are important factors in determining whether ADS-B should be encrypted. Without encryption or authentication, airports and the aviation system are vulnerable to a variety of cyber-attacks that could cause aircraft to crash, endangering human lives. Although it is morbid to consider the potential hazards of an attack through ADS-B, it is necessary to consider the loss of human life. According to the FAA, the average human's life is worth 9.6 million dollars [52]. The most common aircraft in use today is the Boeing 737, which seats anywhere from 85 to 215 passengers. If a Boeing 737 was to be seated at full capacity and crashed as the result of a cyber-attack, it could cost anywhere from 816 million to roughly 2.06 billion dollars, based upon the FAA assigned dollars to the loss of life. On top of this, when adding the cost of a Boeing 737 - approximately 82 million dollars - a single crash could cost roughly 900 million dollars and catastrophic loss of life. This is the cost of an incident that could occur at any time without encryption on ADS-B. Further, in the event of an ADS-B attack, it is highly likely that the event would involve multiple aircraft.

Determining the cost to implement FFX-A2 is the next step. Once again, there are currently about 220,000 registered airplanes in the United States and the labor costs of this proposal must be determined [51]. It would take approximately one hour to install a software update on one aircraft [53]. Determining how much a software engineer would be paid is tough to pinpoint precisely, however, at the very most, it would cost $75 per hour [54]. Across all registered airplanes in the US, the labor costs of implementing AES FFX-A2 and a MAC would be approximately $16.5 million. Bids for the exact amount of the cost for purchasing an encryption key and the appropriate software are highly variable and dependent on the exact system one is looking for. Police Departments in Erie County, Pennsylvania implemented the

encryption of their radio communication systems as the security vulnerability of allowing the public to listen in to law enforcement officers' communications was recognized. Erie County's Next Generation Public Safety Radio System budget, including the encryption of radio transmissions within 10 local police departments, cost $26.5 million dollars [55]. The cost of labor compounded with the rough cost estimate from Erie County's Next Generation Public Radio System places the cost of implementation at roughly $43 million dollars. While this price may seem daunting at first glance, the cost of just one airplane crash due to a cyber-attack would be exponentially more expensive as shown in Figure 13.

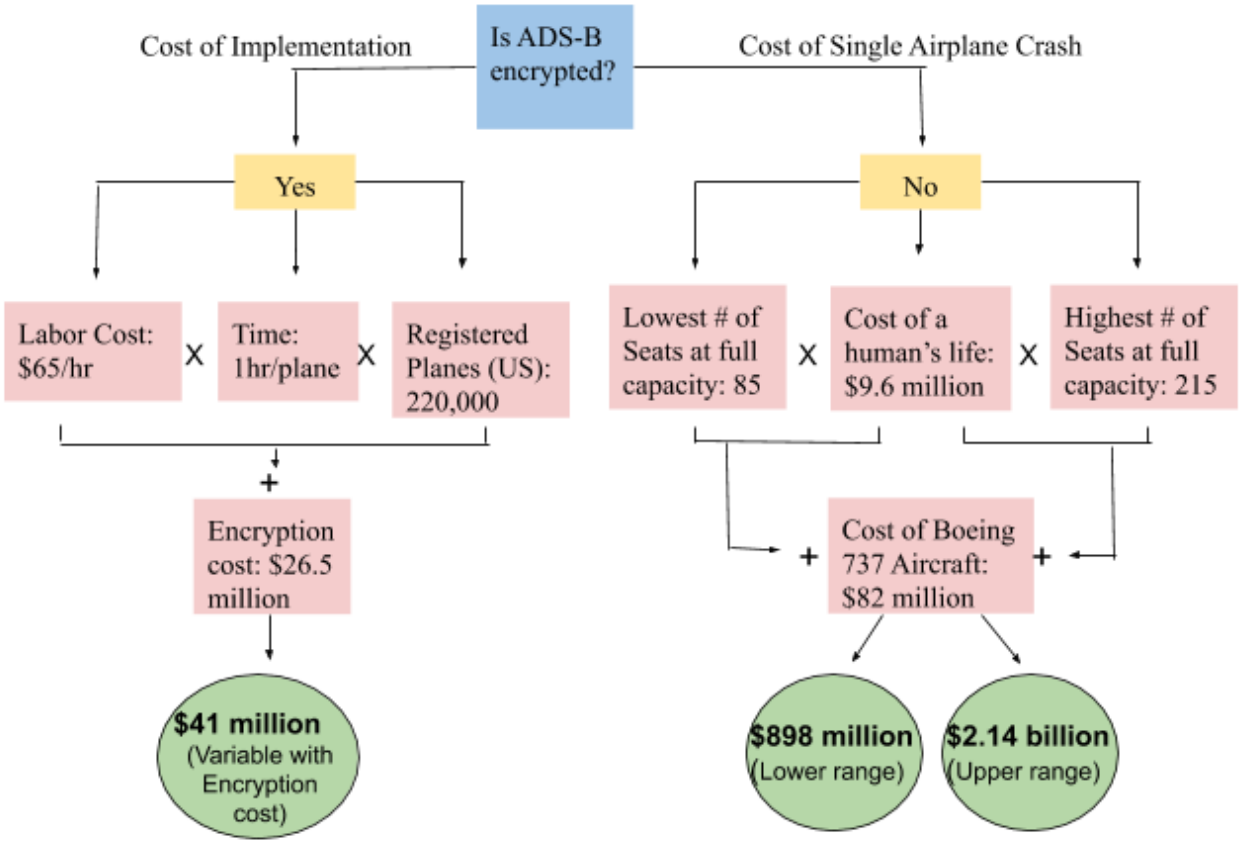

Figure 13. Cost analysis of implemented encryption in ADS-B broadcasts versus the lack of encryption leading to an airplane crash

8.) Summary/Conclusion

Alongside the massive technological advancements in recent years, hacking tactics have progressed rapidly and are constantly evolving, often more quickly than the ability of companies to keep up. The aviation industry, which has typically been concerned about traditional threats, has become increasingly aware of cybersecurity threats; the FAA outlined a plan in their 2010 performance target from their *Portfolio of Goals* to have "zero cyber-security events that significantly disable or degrade FAA services" [11]. The heightened use of aircraft broadcasting technology in aviation has brought about better communication with aircraft and a greater ability to track in-flight aircraft. However, the implementation of new technology has also made more information available to the public, creating novel risks. With the availability of instantaneous information about aircraft locations, destinations, and flight patterns on public domains, hackers have an unprecedented ability to launch cyberattacks. Even one incident involving a cybersecurity breach could result in the disruption of flight patterns or the collision of aircraft with serious loss of life, disruption in service, and financial ramifications. Everyday communications such as emails and text messages are protected by encryption while ADS-B transmissions remain vulnerable to attack. The lack of encryption within the ADS-B system allows these messages to be received, tampered with, deleted, or even generated by anyone, anywhere.

The approach to combat this inherent vulnerability stemmed from research on other technologies that had been hacked, such as household appliances and transportation systems. Based on the flaws in these systems, the biggest problems with ADS-B seemed to be the lack of authentication and the unrestricted accessibility to the general public. Encryption and authentication systems, such as MAC, seemed to be both the logical and practical response to these major issues. The team contacted several industry experts who provided valuable insight

into how pilots are affected by the use of ADS-B signals and how encryption might be implemented in ADS-B. This interaction also revealed how easily someone could conduct a cyber-attack and how catastrophic such an attack would be. Figure 14 depicts the team compiling the final proposal.

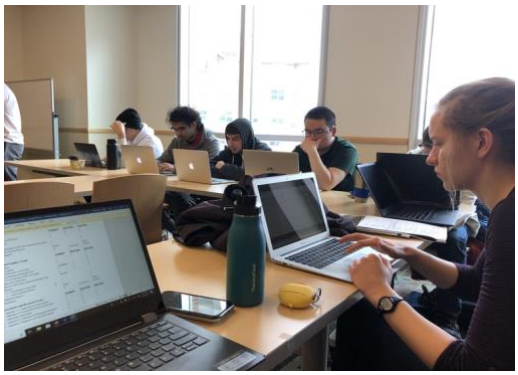

Figure 14. Team working together to finalize ideas

This report proposes encryption and authentication of ADS-B transmissions, since the existing techniques are currently inadequate to secure these broadcasts. Multilateration is currently the most widely used method to determine aircraft location from ground-based signals. However, multilateration does not determine the height of planes accurately, and the ADS-B messages are still openly available to the public. The continued use of radar to cross-check ADS-B has been proposed as a potential solution; radar, however, does not work reliably over large bodies of water or mountainous terrain. This would make aircraft in those areas the primary targets for attacks. The lack of viable alternatives led us to propose encryption and a MAC system as a solution to secure ADS-B messages. This type of encryption must operate with a symmetric key to limit the complexity of assigning a unique key to each aircraft. A block cipher, specifically AES, was chosen for its extensive presence in literature. Due to the non-conforming bit size of ADS-B messages, a mode of operation which could adapt the messages to fit within the block cipher was also necessary. With these parameters in mind, the AES FFX-A2 encryption was chosen to secure ADS-B transmissions from cybersecurity breaches with a MAC, such as HMAC, in addition to provide authentication of aircraft.

This proposal aims to highlight the threat the cybersecurity liability poses for the FAA, aviation community, and the general public. The FAA and aviation community are in desperate

need of long-term solutions for aviation cybersecurity. If security vulnerabilities such as those found within the current ADS-B system are not mitigated with proactive measures, the aviation community may soon face disaster. The security of aviation is of utmost importance and accordingly, it is crucial to implement the necessary technology to combat potential future cyber-attacks.

The solution described within this proposal is realistic, relevant, and timely. It is our desire to raise awareness and present a viable solution to this important concern in the aviation industry.

Table of Acronyms

ADS-B: Automatic dependent surveillance-broadcast
AES: Advanced Encryption Standard
ATC: Air Traffic Control
DO-326: "Airworthiness Security Process Specification" (USA)
EASA: European Union Aviation Safety Agency
ED-202: "Airworthiness Security Process Specification" (Europe)
FAA: Federal Aviation Administration
FFX: Feistel-based format preserving encryption Mode of Operation for FPE
FIS-B: Flight Information Services
FPE: Format preserving encryption
HMAC: Hash Based Method Authentication Code
MAC: Message Authentication Code
MMU: Morristown Municipal Airports
NIST: National Institute of Standards and Technology
PFAS: Polyfluoroalkyl substances
TIS-B: Traffic Information Service - Broadcast
UAV: Unmanned Aerial Vehicle

Appendix A

Students:

Mary Campbell
mcampbe6@binghamton.edu

David Goldhirsch
dgoldhi1@binghamton.edu

Josh Lee
jlee691@binghamton.edu

Benjamin Manning
bmannin2@binghamton.edu

Grace Moon
gmoon2@binghamton.edu

Simon Quinn
squinn5@binghamton.edu

Michael Schutzman
mschutz2@binghamton.edu

Danyal Shah
dshah33@binghamton.edu

Cameron Wallace
cwallac5@binghamton.edu

University Advisors:

Chad Nixon
Adjunct Professor—Binghamton University Scholars Program
Binghamton University
State University of New York
Binghamton, NY 13902-6000
cnixon@binghamton.edu
(607) 624-1174

Zachary Staff
Adjunct Professor—Binghamton University Scholars Program
Binghamton University
State University of New York
Binghamton, NY 13902-6000
zstaff@binghamton.edu
(607) 743-9099

Non-University Partners:

Joshua Moyer, C.M.
Airport Operations Coordinator
DM AIRPORTS, LTD. Operators of MMU
8 Airport Road, Morristown, NJ 07960
www.mmuair.com | 973-538-6400

Darren S. Large, A.A.E.
Director, Facilities & Operations
DM AIRPORTS, LTD. Operators of MMU
8 Airport Road, Morristown, NJ 07960
www.mmuair.com | 973-538-6400

Appendix B. Description of Binghamton University

Binghamton University, as seen in Figure 15, is a public research university located in Broome County, New York, with campuses in Vestal, Binghamton, and Johnson City. Binghamton was founded in 1946 under the jurisdiction of Syracuse University in order to educate local World War II veterans. Binghamton University became a member of the State University of New York (SUNY) system in 1950, following its separation from Syracuse University [56]. Since the university's chartering, it has grown to offer over 130 academic programs and six prestigious colleges: College of Community and Public Affairs, Decker School of Nursing, Harpur College of Arts and Sciences, School of Management, School of Pharmacy and Pharmaceutical Sciences, and Thomas J. Watson School of Engineering and Applied Science [57] [58]. The 930-acre campus is home to 14,021 undergraduate students and 3,747 graduate students, along with over 50 Emeritus distinguished professors, and over 30 SUNY distinguished faculty [59] [60]. This past year, Binghamton University added its first Nobel Laureate winner to its accolades.

Figure 15. Binghamton University Peace Quad Pictured in Spring 2019

Binghamton University continues to be one of the most prestigious schools in the Northeast as *Business First, 2019* ranks Binghamton as the #1 Top Public College in N.Y., and the 2020 rankings from *U.S. News & World Report* has Binghamton as #31 Top Public Schools

in the Nation. A multitude of academic programs offered at Binghamton University are world renowned, including fourteen undergraduate programs, and seventeen of the Graduate School's programs as they make *U.S. News and World Report*'s "Best Graduate Schools 2020" list [61].

Appendix C. Description of Non-University Partners

a) Morristown Airport

Morristown Airport (MMU) is a public airport located in and owned by Morristown, New Jersey. MMU is located 27 miles west of New York City and is classified as a general aviation reliever airport for the New Jersey and New York City areas [62]. As a general aviation reliever airport, MMU mainly handles privately chartered flights into and out of the airport. On average, MMU conducts 72,702 flights annually and 199 flights daily [63]. Additionally, MMU has 81 single engine aircraft, 17 multi-engine aircraft, 78 jet aircraft, and seven helicopters on the field [64]. Regional Sky is the only commercial airline that services MMU [65]. The current manager of the airport is Scott McMahon [64].

Appendix E: Evaluation of Educational Experience

Students:

1. Did the Airport Cooperative Research Program (ACRP) Design Competition provide a meaningful learning experience for you? Why or why not?

The ACRP Design Competition has provided us with an extremely meaningful learning experience by providing the opportunity to develop teamwork skills, problem-solving skills, and research skills while expanding our knowledge of aviation and cybersecurity. It also gave us important experience working to compile and generate our own reports on a new design that addresses real-world issues. This project also showed the value of hard work, collaboration, and communication as we learned how to work in a team, meet deadlines, and hone our writing and oral presentation skills. The freedom of chasing down answers to radical questions was a particularly interesting learning experience as it was outside our comfort zones and new to most of us.

2. What challenges did you and/or your team encounter in undertaking the Competition? How did you overcome them?

Initial setbacks in choosing topics were overcome through delegation of research, planning, and group brainstorming. After overcoming this issue, we found that our consensus resulted in a topic that held even more potential than our original ideas. Reading complicated research articles was also a challenge as we had many questions, even after reading numerous journal articles. Communication with industry professionals was helpful in answering these

questions, allowing us to solidify our understanding and plan of action. In order to deal with the standard difficulties that come with working as a team, we held weekly team meetings outside of class and broke into sub-teams with specific responsibilities outlined.

3. Describe the process you or your team used for developing your hypothesis.

First, our team reviewed the ACRP competition prompts to find areas of interest in the aviation industry. We then researched solutions for those prompts, and cybersecurity was decided on as a research topic. When researching airport cybersecurity, it was quickly made apparent that the ADS-B poses a major cybersecurity risk. After researching this topic, we came to the conclusion that the two biggest problems with ADS-B were its lack of authentication and easy accessibility to the general public. After analyzing the steep costs of implementing a new communication system, we focused on protecting the current ADS-B system from cyber-attacks. Encryption and MAC seemed to be both the most logical and practical response to this issue.

4. Was participation by industry in the project appropriate, meaningful and useful? Why or why not?

Yes, our phone call with cybersecurity and ADS-B professionals within the industry helped us tremendously refine our topic and answer many crucial questions that we had. These industry professionals helped make it clear that the topic of ADS-B and cybersecurity is extremely important to the aviation industry. The actual feasibility of changing the ADS-B system to involve encryption was also reaffirmed by professional input.

5. What did you learn? Did this project help you with skills and knowledge you need to be successful for entry in the workforce or to pursue further study? Why or why not?

The ACRP Design Competition has helped us learn many useful skills in teamwork and planning that have improved our abilities to operate in a team setting. Coordination, communication, and delegation are particularly useful tools for the future. This project has also shown us the significance of ADS-B technology and why cybersecurity in airports is such a significant issue, especially moving into the near future. In this group project, we have been able to exercise our oral presentation, time management, and networking skills which will greatly contribute to our success in the workforce.

ii. Faculty Response

1. **Describe the value of the educational experience for your student(s) participating in this Competition submission.**

Experiential learning is a critical element in the overall academic experience. One of the goals of Binghamton University is to increase this type of learning and this competition advances that goal. While lecturing and laboratory time have great value, they are limited in their ability to allow students a real-world experience on a project team. The ACRP Design Competition provides the opportunity for students to take an idea, their idea, all the way from the brainstorming stage to a well-researched concept that has real potential for implementation. Creating their own solutions that do not currently exist for challenges facing an industry such as aviation allows the students to take true ownership in the educational experience.

Over the course of the design competition, a team of diverse students had to not only develop a sound proposal but also gain trust in each other by working in teams. Individually and collectively they had to deliver on milestones each week to ensure that the proposal stayed on track for meeting the submission deadline. This is a life skill that cannot be easily taught in class and the ACRP Design Competition provides this critical educational opportunity.

2. **Was the learning experience appropriate to the course level or context in which the competition was undertaken?**

Two groups of ten (10) students each were involved in this design competition. These students were mostly Freshmen and were not accustomed to working in a team setting. This opportunity required a high level of effective communication, management of schedule and assets in the form of smaller teams working on individual project components. Having small groups that had to report back to Project Leaders provided an additional layer of accountability at the student level. Although this was new ground for most of the students, it pushed them to improve their communication and time management skills. This is a key element of the learning experience and one that will help the students as they complete their education and move into a career. Overall the experience was appropriate and effective.

3. **What challenges did the students face and overcome?**

The students had several challenges to overcome during the development of their proposal for the competition. Creating a design proposal from scratch is something that they

have never undertaken before. They are similarly not familiar with working and depending upon all team members to make the project a success. This presented an additional challenge to the proposal development. Lastly, the competition and all of the world was affected by the COVID-19 pandemic. This occurred in the middle of the course and competition further challenging the ability of the students to complete the project and engage with industry experts.

Regarding the development of the proposal from scratch; the team was able to overcome this challenge through near flawless teamwork and well-organized project leaders. The project leaders set the tempo and checked in frequently with the team to organize assignments and make sure that the groups involved in the proposal were working cohesively.

The competition deadline, while challenging, was achieved through disciplined delegation of duties through the entire project team. The entire class was well aware that if any of the students or the teams did not perform at the highest level that the entire team would suffer. This created a camaraderie amongst the team that was evident during weekly check-ins where team members provided me assessments or 'grades' of how the other team members were performing within the group. All students reported very good or excellent participation.

4. **Would you use this Competition as an educational vehicle in the future? Why or why not?**

We would highly recommend this competition to future students and faculty. We have presented this competition at various Binghamton University events as an example of how to engage students in 'real world' learning. As previously mentioned, this particular competition gives students a very different experience than they gain from typical courses and classroom

activities. The significant collaborative effort that is required to develop a winning proposal is something that cannot be easily taught. This competition provides for an educational experience on communication, time management, team building and original writing that will serve the students well as they enter the workforce. We are confident that you will see Binghamton University participating in the competition again.

5. **Are there changes to the Competition that you would suggest for future years?**

New topics and categories have been added to the competition over the last couple of years. This is important to keep the competition interesting and relevant. The continued addition of new areas of focus would be my primary recommendation for future years. ACRP may also want to consider a research and development pipeline tied to winning proposals. Not all of the ideas are easily adopted; however certain proposals should be advanced to at least the prototype level and possibly beyond. Ultimately the competition serves as an important introduction to innovation in the aviation industry but could be more with additional federal funding and visibility to potential private investors. Overall, the competition is extremely well run and represents the type of educational opportunity that is critically needed in academia.

Appendix F: References List

[1] S.A, Busyairah, W.Y. Ochieng, W. Schuster, A. Mamjudar, T.K. Chiew, Eds. "A Safety Assessment Framework for the Automatic Dependent Surveillance Broadcast (ADS-B) System," *Safety Science,* vol. 78, pp. 91-100, Oct. 2015. [Online] Available: https://www.sciencedirect.com/science/article/pii/S0925753515001034. [Accessed: 20-Feb-2020].

[2] "What is Different in ADS-B (Out) Compared to Radar Technology," *BOCA Blog*. [Online]. Available: https://bocamx.com/blog/What-is-Different-in-ADS-B-(Out)-Compared-to-Radar-Technology. [Accessed: 22-Feb-2020].

[3] M. Strohmeier, V. Lenders, and I. Martinovic, "On the Security of the Automatic Dependent Surveillance-Broadcast Protocol," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1066–1087, 2015.

[4] "What is ADS-B, Which Requirements?," *Jetvision*, 05-Jan-2017. [Online]. Available: https://shop.jetvision.de/Blog/What-is-ADS-B-What-Requirements. [Accessed: 04-Apr-2020].

[5] "Automatic Dependent Surveillance-Broadcast (ADS-B)," FAA seal, 12-Mar-2019. [Online]. Available: https://www.faa.gov/nextgen/programs/adsb/. [Accessed: 19-Feb-2020].

[6] "eCFR - Code of Federal Regulations," *Electronic Code of Federal Regulations (eCFR)*. [Online]. Available: https://www.ecfr.gov/cgi-bin/text-idx?SID=d52bd1cac72f136bfeb34d99232035f3&mc=true&node=se14.2.91_1227&rgn=div8. [Accessed: 12-Feb-2020].

[7] E. Hableel, J. Baek, Y. Byon and D. S. Wong, "How to protect ADS-B: Confidentiality framework for future air traffic communication," *2015 IEEE Conference on Computer Communications Workshops* (INFOCOM WKSHPS), Hong Kong, 2015, pp. 155-160. [Online] Available: https://ieeexplore.ieee.org/abstract/document/7179377. [Accessed: 22-Feb-2020].

[8] C. Finke, J. Butts, and R. Mills, "ADS-B encryption: confidentiality in the friendly skies," *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop* [Online]. Available: https://dl.acm.org/doi/10.1145/2459976.2459986. [Accessed: 14-Feb-2020].

[9] M. Dubey and Y. Yadav, “Comparative Analysis of RSA and Modified RSA Cryptography,” *i-manager's Journal on Computer Science*, vol. 3, pp. 23–28, Dec. 2015. [Online]. Available: https://imanagerpublications.com/home/articleHtml/4830/21#ref27. [Accessed: 4-Mar-2020].

[10] M. Strohmeier, V. Lenders, and I. Martinovic, *“*Lightweight Location Verification in Air Traffic Surveillance Networks*,” Proceedings of the 1st ACM Workshop on Cyber-Physical System Security - CPSS 15,* Apr. 2015. [Online] Available: https://www.cs.ox.ac.uk/files/7230/cpss_strohmeier.pdf. [Accessed: 12-Feb-2020].

[11] “Portfolio of Goals.” *FAA*, Available: www.faa.gov/about/plans_reports/media/fy10%20portfolio%20of%20goals.pdf.

[12] *Destination 2025*. [Online]. Available: https://www.faa.gov/about/plans_reports/media/destination2025.pdf. [Accessed: 07-Apr-2020].

[13] R. H. Weber and E. Studer, “Cybersecurity in the Internet of Things: Legal aspects,” *Computer Law & Security Review*, vol. 32, no. 5, pp. 715–728, Aug. 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0267364916301169. [Accessed: 23-Feb-2020].

[14] E. Holm, “The Role of the Refrigerator in Identity Crime?,” *International Journal of Cyber-Security and Digital Forensics*, vol. 5, no. 1, pp. 1–9, Jan. 2016. [Online]. Available: https://pdfs.semanticscholar.org/39a3/6847e4fb024a37f27e739004f409053b80ef.pdf. [Accessed: 16-Feb-2020].

[15] K. Albrecht and L. Mcintyre, “Privacy Nightmare: When Baby Monitors Go Bad [Opinion],” *IEEE Technology and Society Magazine*, vol. 34, no. 3, pp. 14–19, 2015. [Online]. Available: https://ieeexplore.ieee.org/document/7270426. [Accessed: 13-Feb-2020].

[16] H. Tuttle, “Hacking cars: when considering the risks of cutting-edge automotive technology, the first thing that usually comes to mind is autonomous vehicles. But focusing too much on self-driving technology risks ignoring a critical reality: Today's cars and trucks are already connected to the internet, and like any other internet-connected device, they can be hacked,” *Shibboleth Authentication Request*, 2017. [Online]. Available: https://go-gale-

com.proxy.binghamton.edu/ps/i.do?id=GALE|A481160884&v=2.1&u=bingul&it=r&p=AONE&sw=w. [Accessed: 14-Feb-2020].

[17] C. Lee, "Grabbing the Wheel Early: Moving Forward on Cybersecurity and Privacy Protections for Driverless Cars," *Federal Communications Law Journal*, vol. 69, no. 1, pp. 25–52, 2017. [Online]. Available: http://www.fclj.org/wp-content/uploads/2017/04/69.1.2-Chasel-Lee.pdf. [Accessed: 19-Feb-2020].

[18] K. Kaur and G. Rampersad, "Trust in driverless cars: Investigating key factors influencing the adoption of driverless cars," *Journal of Engineering and Technology Management*, vol. 48, pp. 87–96, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0923474817304253. [Accessed: 14-Feb-2020].

[19] D. Spaniel and P. Eftekhari, "Hacking our Nation's Airports: Cyber-Kinetic Threats to the Technologies Running Airport Operations," *Institute for Critical Infrastructure Technology*, 2019. [Online]. Available: https://icitech.org/wp-content/uploads/2019/05/ICIT-Brief-Hacking-Our-Nations-Airports-1.pdf. [Accessed: 19-Feb-2020].

[20] V. Saraogi, "Five times airports were involved in cyberattacks and data breaches," *Airport Technology*, 30-Jan-2020. [Online]. Available: https://www.airport-technology.com/features/five-times-airports-were-involved-in-cyberattacks-and-data-breaches/. [Accessed: 14-Feb-2020].

[21] G. Lykou, A. Anagnostopoulou, D. Gritzalis, "Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Control," *Sensors*, vol. 19, no. 1, pp. 1-19, Jan. 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/1/19/htm. [Accessed: 19-Feb-2020].

[22] C. G. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*, pp. 194–199, 2017. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8088163. [Accessed: 19-Feb-2020].

[23] K. Zetter, "Feds Say That Banned Researcher Commandeered a Plane," *Wired*, 15-Jan-2018. [Online]. Available: https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/. [Accessed: 13-Feb-2020].

[24] D. Gates, “Boeing faces largest quarterly loss in its history after a $4.9 billion financial hit due to 737 MAX grounding,” *The Seattle Times*, 18-Jul-2019. [Online]. Available: https://www.seattletimes.com/business/boeing-aerospace/boeing-announces-a-4-9-billion-accounting-charge-due-to-737-max-grounding/. Available: https://www.seattletimes.com/business/boeing-aerospace/boeing-announces-a-4-9-billion-accounting-charge-due-to-737-max-grounding/
[Accessed: 07-Apr-2020].

[25] S. S. Beale and P. Berris, “Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses,” *Digitization and the Law*, pp. 21–40, 2018. [Online]. Available: https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/dltr16&id=158&men_tab=srchresults. [Accessed: 20-Feb-2020].

[26] D. Hayford, “The Future of Security: Zeroing In On Un-Hackable Data With Quantum Key Distribution,” *Wired*, Sep. 2019. [Online]. Available: https://www.wired.com/insights/2014/09/quantum-key-distribution/. [Accessed: 14-Feb-2020].

[27] J. A. Oravec, "Emerging “cyber hygiene” practices for the Internet of Things (IoT): Professional issues in consulting clients and educating users on IoT privacy and security," *2017 IEEE International Professional Communication Conference* (ProComm), Madison, WI, 2017, pp. 1-5. [Online]. Available: https://ieeexplore-ieee-org.proxy.binghamton.edu/document/8013965. [Accessed: 14-Feb-2020].

[28] S. Stanković and D. Simić, “Defense Strategies Against Modern Botnets,” *International Journal of Computer Science and Information Security*, vol. 2, no. 1, pp. 1–7, Jun. 2009. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/0906/0906.3768.pdf. [Accessed: 14-Feb-2020].

[29] “How Radar Works,” *How Radar Works*. [Online]. Available: http://www.bom.gov.au/australia/radar/about/what_is_radar.shtml. [Accessed: 21-Feb-2020].

[30] M. Strohmeier, M. Schafer, V. Lenders, I. Martinovic, “Realities and challenges of nextgen air traffic management: the case of ADS-B,” *IEEE Communications Magazine*, vol. 52, no. 5, pp. 111-118, May 2014. Accessed on 18-Feb-2020. [Online] Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6815901. [Accessed: 18-Feb-2020].

[31] Z. Zhigang, D. Yajing, Y. Jun, “Transmission of Meteorological Information to a Cockpit and Application of ADS-B,” *Meteorological & Environmental Research*, vol. 7, no. 1, pp. 19-29. [Online] Available: https://eds.b.ebscohost.com/abstract?site=eds&scope=site&jrnl=21523940&AN=114968416&h=HTRJttbhA7s6CmTDCA3fcy3Skck6arr7JfgvxXVWdLLYpcehirMQiM3Vt8%2blCmfLFWWkL7XXFkFyeMVuHTIeeA%3d%3d&crl=c&resultLocal=ErrCrlNoResults&resultNs=Ehost&crlhashurl=login.aspx%3fdirect%3dtrue%26profile%3dehost%26scope%3dsite%26authtype%3dcrawler%26jrnl%3d21523940%26AN%3d114968416. [Accessed: 20-Feb-2020].

[32] M. Strohmeier, D. Moser, M. Schafer, V. Lenders, I. Martinovic, “On the Applicability of Satellite-Based Air Traffic Control Communication for Security,” *IEEE Communications Magazine*, vol. 57, no. 9, pp. 79-85, Sep. 2019. [Online] Available: https://ieeexplore.ieee.org/document/8847232. [Accessed: 20-Feb-2020].

[33] T. Kacem, D. Wijesekera, P. Costa, J. Carvalho, M. Monteiro, and A. Barreto, “Key distribution mechanism in secure ADS-B networks,” *2015 Integrated Communication, Navigation and Surveillance Conference (ICNS)*, 2015. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7121252. [Accessed: 21-Feb-2020].

[34] U. Šolar, “Security of ADS-B system in heavy multipath propagation environments,” *Electrotechnical Review / Elektrotehniški Vestnik,* vol. 82, no. 5, pp. 297-301, Nov. 2015 Accessed on 20-Feb-2020. [Online] Available: https://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=5&sid=8760504a-97b1-421-8a31-2f09360602ff%40sessionmgr1. [Accessed: 20-Feb-2020].

[35] “How ADS-B works,” *Airservices RSS*, 18-Sep-2015. [Online]. Available: http://www.airservicesaustralia.com/projects/ads-b/how-ads-b-works/. [Accessed: 14-Feb-2020].

[36] “ADS-B and other means of surveillance implementation status,” 15-Mar-2018. [Online]. Available: https://ec.europa.eu/transport/sites/transport/files/20180515-sesar-ads-b-report.pdf. [Accessed: 17-Feb-2020].

[37] S. Gorman, Y. J. Dreazen, and A. Cole, “Insurgents Hack U.S. Drones,” *The Wall Street Journal*, 18-Dec-2009. [Online]. Available: https://www.wsj.com/articles/SB126102247889095011. [Accessed: 12-Mar-2020]

[38] “Few Answers for ADS-B Security Concerns | Business Aviation News: Aviation International News,” [Online]. Available: https://www.ainonline.com/aviation-

news/business-aviation/2018-02-14/few-answers-ads-b-security-concerns. [Accessed: 14-Feb-2020].

[39] D. Cummings, “ADS-B and Cybersecurity: Lessons from the Maritime Domain,” [Online]. Available: https://www.psware.com/ads-b-and-cybersecurity/. [Accessed: 17-Feb-2020].

[40] T. Kacem, A. Barreto, D. Wijesekera, and P. Costa, “ADS-Bsec: A novel framework to secure ADS-B,” ICT Express, vol. 3, no. 4, pp. 160–163, 2017. [Online]. Available: https://www-sciencedirect-com.proxy.binghamton.edu/science/article/pii/S2405959517302783. [Accessed: 14-Feb-2020].

[41] “Modernization of U.S. Airspace.” [Online]. Available: https://www.faa.gov/nextgen/.
[Accessed: 09-Mar-2020].

[42] “FAA Has Made Progress but Additional Actions Remain To Implement Congressionally
Mandated Cyber Initiatives.,” p. 23.

[43] “DO -326A and ED-202A : An Introduction to the New and Mandatory Aviation Cyber-Security Essentials.” [Online]. Available: https://www.sae.org/learn/content/c1949/. [Accessed: 09-Mar-2020].

[44] “FAA Strategic Plan, FY2019-2022,” p. 42.

[45] FAA, "Safety Management System Manual April 2019", 2019. [Online]. Available: https://www.faa.gov/air_traffic/publications/media/ATO-SMS-Manual.pdf

[46] FAA, "AC 150/5200-37", FAA, 2007. [Online]. Available: https://www.faa.gov/documentLibrary/media/advisory_circular/150-5200-37/150_5200_37.pdf.

[47] “Announcing the ADVANCED ENCRYPTION STANDARD (AES)". *Federal Information Processing Standards Publication 197*. United States National Institute of Standards and Technology (NIST), November 26, 2001.

[48] C. Finke, J. Butts, R. Mills, and M. Grimaila, “Enhancing the security of aircraft surveillance in the next generation air traffic control system,” *International Journal of*

Critical Infrastructure Protection, vol. 6, no. 1, pp. 3-11, Feb. 2013. [Online] Available: https://www-sciencedirect-com.proxy.binghamton.edu/science/article/pii/S1874548213000048 [Accessed: 21-Feb-2020]

[49] R.J. Reisman, "Air Traffic Management Blockchain Infrastructure for Security, Authentication, and Privacy," *AIAA SciTech Forum 2019*. [Online] Available: https://www.aviationsystemsdivision.arc.nasa.gov/publications/2019/SciTech2019_Reisman.pdf [Accessed: 20-Feb-2020].

[50] "FY 2019-2022 FAA Strategic Plan" *Federal Aviation Administration,* 2019 [Online] Available: https://www.faa.gov/about/plans_reports/media/FAA_Strategic_Plan_Final_FY2019-2022.pdf [Accessed: 14-Mar-2020]

[51] "State of General Aviation" *Aircraft Owners and Pilots Association (AOPA),* 2019 [Online] Available: http://download.aopa.org/hr/Report_on_General_Aviation_Trends.pdf [Accessed 30-Mar-2019]

[52] "Treatment of the Values of Life and Injury in Economic Analysis" *Federal Aviation Administration,* September, 2016 [Online] Available: https://www.faa.gov/regulations_policies/policy_guidance/benefit_cost/media/econ-value-section-2-tx-values.pdf [Accessed: 28-Mar-2020]

[53] R. Verger, "Jet engines get planes in the sky, but software keeps them safe" 14-Mar-2019 [Online] Available: https://www.popsci.com/boeing-software-update/ [Accessed: 4-Apr-2020]

[54] "How Much Do Software Engineer Jobs Pay per Hour?" *ZipRecruiter,* 28-Mar-2020 [Online] Available: https://www.ziprecruiter.com/Salaries/How-Much-Does-a-Software-Engineer-Make-an-Hour [Accessed: 4-Apr-2020]

[55] M. Rink, "Erie County police to encrypt radio communications," *GoErie.com*, 25-Feb-2019. [Online]. Available: https://www.goerie.com/news/20190225/erie-county-police-to-encrypt-radio-communications. Available: https://www.goerie.com/new/20190225/erie-county-police-to-encrypt-radio-communciations [Accessed: 07-Apr-2020].

[56] "About Us: Our Story," *Binghamton University: State University of New York* [Online]. Available: https://www.binghamton.edu/about/our-story.html

[57] “Undergraduate Admissions: Academics - Programs,” *Binghamton University: State University of New York* [Online]. Available: https://www.binghamton.edu/admissions/academics/programs.html

[58] “Undergraduate Admissions: Academics - Schools,” *Binghamton University: State University of New York* [Online]. Available: https://www.binghamton.edu/admissions/academics/schools.html

[59] “Binghamton University, SUNY - Student Life,” *U.S. News and World Report* [Online]. Available: https://www.usnews.com/best-colleges/suny-binghamton-2836/student-life

[60] “Office of the Provost: Faculty Resources - Distinguished Faculty,” *Binghamton University: State University of New York* [Online]. Available: https://www.binghamton.edu/academics/provost/faculty-resources/distinguished.html

[61] R. Yarosh, “Binghamton Continues To Rise In National College Rankings,” *Binghamton University News,* Sept. 2019. Available: https://www.binghamton.edu/news/story/1975/binghamton-continues-to-rise-in-national-college-rankings

[62] “MMU | Morristown Airport New Jersey | General Aviation Airport.” [Online]. Available: https://www.mmuair.com/#. [Accessed: 09-Mar-2020].

[63] “Morristown, NJ Airport (MMU) - Private Jet Charters.” [Online]. Available: https://www.luxuryaircraftsolutions.com/morristown-nj-airport-mmu/. [Accessed: 09-Mar-2020].

[64] “MMU - Morristown Municipal Airport | SkyVector.” [Online]. Available: https://skyvector.com/airport/MMU/Morristown-Municipal-Airport. [Accessed: 09-Mar-2020].

[65] “Morristown (MMU) - Flight Status, Maps & more - KAYAK.” [Online]. Available: https://www.kayak.com/Morristown-Morristown-Airport.MMU.ap.html#airlines. [Accessed: 09-Mar-2020].