The Current Situation and Potential Future of Aviation Security in the United States of America

By Daniel Baigel

1. Abstract

Nobody likes to think of airplanes as being potentially vulnerable to cyber attacks. Unfortunately, according to a report conducted by the United States Government Accountability Office (GAO), the Federal Aviation Administration (FAA) is vulnerable in some key areas to potential cyber attacks. The FAA is currently in the process of switching to a more interconnected IP-networked system for their Air Traffic Control systems and their airplanes, called NextGen, and this change will bring about more security risks than before. This paper will outline where the security vulnerabilities are in the systems, and how the FAA can better protect itself and its planes from attacks.

2. Introduction

The Internet today is busier than ever. Every modern device can connect to the web, and you can find almost anything on it. The web is a complex system of connections, making finding bugs and vulnerabilities easier for the average attacker. As devices become more interconnected, we put ourselves more at risk for cyber attacks. Attackers can now gain access to things like phones, wearable devices, drones, and even light bulbs. So why should airplanes be any different? Millions of people travel around the world by airplane everyday, and each plane can carry hundreds of people at a time to a desired location. The airplane companies' reputations are on the line every time a trip is made because a plane crash could destroy a companies' reputation (think Malaysia Airlines) as well as kill hundreds of innocent people. Leaving a plane vulnerable to an attacker potentially allows that person to gain access to the cockpit controls and cause serious situations. That attacker can roll out a series of attacks ranging from causing the oxygen masks to fall down in order to cause a panic on board, or even command the plane to change course. It goes without saying that making sure airplanes are secure should be a top priority for both the airplane industry and the government.

One man in the industry today has become famous online for claiming to hack into a plane while onboard and issue the CLB or climb command, causing the plane to move in a lateral movement (Foster). This man's name is Chris Roberts, and after tweeting about the potential for enacting such a hack while sitting on a plane, he was escorted off of the plane and questioned by the FBI. Here is the exact tweet

that got him arrested on April 15th 2015: “Find myself on a 737/800, lets see Box-IFE-ICE-SATCOM, ? Shall we start playing with EICAS messages? "PASS OXYGEN ON" Anyone? :)”. The airline took this tweet as a threat, rather than a tweet to raise awareness like Chris Roberts claimed it was, and contacted the FBI on landing. Chris Roberts owns a company called One World Labs (OWL), which is a security intelligence and threat detection firm. Essentially they are a cyber security consulting company that gets hired by other companies to go through all their code and detect risks before they are exploited. Their services include security code review, incident response and forensics, security consulting, and assessment and penetration testing (OWL Cybersecurity). Chris Roberts started his career in vehicles in general (trains and cars) and in the past few years has shifted his focus to airplanes.

Chris Roberts gives talks all over the world about aviation security, and he claims that planes are potentially vulnerable through standard IP networking techniques. In fact, according to a report conducted by the U.S. Government Accountability Office, “the [Federal Aviation Administration] has taken steps to protect its ATC systems from cyber-based threats. However, significant security-control weaknesses remain that threaten the agency’s ability to ensure the sage and uninterrupted operation of the national airspace system” (FAA, 13).

3. To The Community

Aviation security is important to the public community because thousands of flights occur every single day, in almost every single country around in the world. In fact, over 100,000 flights occur every single day worldwide. If each flight only carried 50 people, that would mean 5 million people fly on an airplane every single day. That is a lot of people. People fly for various reasons: for work, for vacation, or to visit family or friends. Regardless of the reason, it is of utmost importance that these flights run smoothly and are secure. If a passenger, remote attacker, or terrorist intentionally or unintentionally breaks down the airplane's security and causes enough damage to crash the plane, not only will many innocent lives be lost, but also people will stop trusting airplanes as a means of travel. Airline industries will go bankrupt, and it will make traveling much more difficult for any type of traveler.

Not only is it important to discuss this issue because it is a concern for the public's safety, but also it is important to inform the public that security vulnerabilities exist, even in unexpected places. Planes are supposed to be places of extreme safety; guns, knives, and even containers of liquid over 3.4 ounces aren't allowed on board a standard flight according to the Transportation Security Administration. However, it is impossible to screen for a person's ability to hack into an airplane. If airplanes are vulnerable to attacks from passengers in the cabin, then all these preventive safety measures the TSA take, much like the state of cyber security today, are as good as useless.

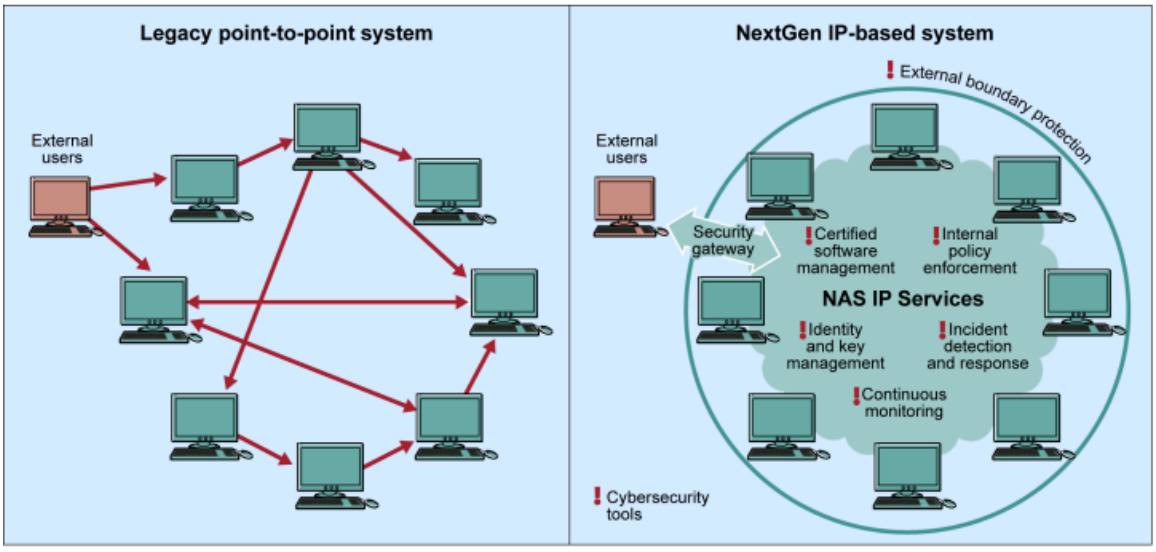
4. Vulnerabilities

In order to determine how to defend against potential aviation attacks, it is first important to understand where the airplane industry is vulnerable, and how attackers might go about exploiting those vulnerabilities. The Federal Aviation Administration (FAA) oversees all aspects of aviation in the United States of America, and is responsible for developing air traffic control (ATC) systems for both civil and military aircrafts (http://www.faa.gov/). In 2004, the FAA started a modernization effort called the Next Generation Air Transportation System (NextGen), to modernize the way that aircraft flight control systems (controllers) and pilots communicate and navigate. This modernization included increasing the digital communication between the controllers and pilots, which means using an Internet Protocol based network to communicate. The plan also called for transforming the old ground-based ATC system into one that uses satellite-based navigation and other advanced technology (FAA, 4). The U.S. Government Accountability Office (GAO) decided to conduct an in depth risk assessment of how the NextGen program was working in September 2013, and the report was published recently in March 2015.

The report states, "[the modernization] will also employ digital and Internet-based computer-networking technologies, exposing the air traffic control (ATC) system to new cyber security risks" (FAA, 6). The current system mixes the older and more modern (IP networked) systems together. As shown in figure 1 below, the older system consists of hardwired information systems that share information only within their limited wired configurations. The modern systems however, consist of

information systems networked together with IP technology (FAA, 12). These older systems are much harder to access remotely because they don't use the Internet to connect from the FAA to other entities. However, because these systems have limited connectivity, they are not protected with cyber security controls and thus are easy to breach.

This was not a massively severe issue because even if one system was breached, an attacker could not access other systems due to the limited connectivity. The issue now however, is that the newer system involves interoperating and high connectivity across all systems to communicate with the FAA. As the GAO report bluntly puts it, "if one of the systems connected to the IP network is compromised, damage could spread to other systems across the network, drastically increasing the risk" (FAA, 13). The issue of having a hybrid system is that now the original legacy systems are connected to modern IP network system. Since the legacy systems are not difficult to breach, now when an attacker gains access to one system, that attacker is free to gain access to other systems due to the increased interconnected system. The following figure demonstrates the differences between the older and newer ATC systems as explained above.



Source: GAO. | GAO-15-370

Figure 1 : Legacy ATC Systems Compared to NextGen IP-Networked Systems

So how can an attacker actually attack an IP network? If an ATC system uses an IP network, then that ATC system can be attacked just like any other computer. Common attacks against IP networks include IP Address spoofing, DDoS attacks, and Man–in-the-Middle attacks. Any of these attacks on an ATC system could cause serious damage, and since the systems are now all interconnected due to the NextGen program, attackers can potentially gain access to multiple systems.

Not only are ATC systems vulnerable, but also according to the GAO report, "modern aircrafts are also increasingly connected to the Internet, which also uses IP networking technology and can potentially provide an attacker with remote access to aircraft information systems" (FAA, 19). If these systems were to be breached remotely, attackers could then gain access into other areas of the plane's network. The worst-case scenario would be an attacker gaining "the ability to access the avionics systems, monitor and possibly influence the control interfaces and other critical flight environments typically found on the private plane subnet" (Homeland

Security News). Chris Roberts adds that an attacker breaching the system would give him or her the ability to intercept and possibly modify the packets of data being sent form the controls to the actuators using readily available software.

5. Defenses

It is important to know what kind of attacks can be done, so that the FAA can understand how to defend against them. Right now the hybrid system of combined aviation operations is called the enterprise. The FAA is developing a defense mechanism called the enterprise approach. Theoretically, the way that it would work would be to think of each IP-networked system as a subsystem of the larger enterprise-wide system. Subsystems can still interoperate as planned, while an enterprise-wide set of shared cyber security controls called “common controls” and a monitoring program protect and increase the resiliency of the subsystems (FAA, 14). Using common controls will help increase security because in the case where a new security flaw or threat is discovered, instead of having to fix the vulnerability in each individual system, the FAA can protect all the interoperating systems by fixing just the common controls.

Another great tool for detecting security breaches and threats is building a holistic threat model. A holistic threat model would include real-time monitoring of the enterprise system, detection of potential attackers probing for vulnerabilities, and other monitoring activities such as incident detection. According to the report conducted by the GAO, the FAA has not created such a model due to lack of funds

and time (FAA, 17). This is a huge issue, and could cause the FAA to miss important risks while overprotecting against less severe risks. Furthermore, only 9 of the current 39 IP connected ATC systems provide activity reports, which increase the chances that a risk or attack goes undetected (FAA, 18). However, the FAA does plan on implementing activity reports in all 39 systems within the next three years.

6. Conclusion

Although the FAA has taken steps to create more secure systems throughout all their departments, "significant security control weaknesses remain, threatening the agency's ability to ensure the safe and uninterrupted operation of the national airspace system" (Homeland Security News). IP networks in in-flight entertainment systems, cockpit communications, or the NextGen ATC system leave flights open to attacks. There are a lot of steps that the FAA can still take to increase the security of their planes and ATC systems. It is unbelievable to think that something so large like an airplane can be just as vulnerable as an average computer. The problem is that an airplane carries hundreds of people and a small security flaw could lead to an awful situation, costing millions of dollars and potentially hundreds of lives. Thus, even though increasing cyber security within the FAA will cost a lot of time and money, it is imperative to do because otherwise countless lives are in danger.

Works Cited

OWL Cybersecurity. Web. 2 Dec. 2015. <https://oneworldlabs.com/services>.

"FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen." United States Government Accountability Office, 1 Apr. 2015. Web. 1 Dec. 2015.

"Federal Aviation Administration." *Federal Aviation Administration*. Web. 30 Nov. 2015. <http://www.faa.gov/>.

Foster, Peter. "Hacker 'made Plane Climb' after Taking Control through In-flight Entertainment System. *"The Telegraph*. Telegraph Media Group, 17 May 2015. Web. 4 Dec. 2015.

"In-flight Plane Control Systems Vulnerable to Remote Hacking." *Aviation Security, Cyber Threats. Business | Homeland Security News Wire*. Homeland Security News Wire, 26 Mar. 2015. Web. 1 Dec. 2015.

Rundle, Michael. "In-flight Wi-Fi Is a 'direct Link' to Hackers, Warns US Report (Wired UK)." *Wired UK*. 15 Apr. 2015. Web. 14 Dec. 2015.