Charles Yang

Cybersecurity in Aviation

Cybersecurity in aircraft and the aviation industry is becoming more and more pertinent each year. Computers and networks are growing more sophisticated and interconnected all the time. The risk, however, is that the more interconnected and complex the systems, the more vulnerabilities have the potential to exist. One such vulnerability was demonstrated when cybersecurity researcher Chris Roberts (Sidragon) claimed to have hacked into and steered a commercial aircraft through the entertainment system at his seat[18]. He was investigated thoroughly by the FBI. While most doubt his claims as not possible, others are concerned the increased interconnectedness of avionics allows vulnerabilities like the one supposedly used by Roberts to exist[7]. In the same way some are concerned that self-driving cars have the potential to be hacked and controlled from afar, there exists a similar concern for the hacking of aircraft[17]. Currently, no cybersecurity laws regarding aircraft are in place yet. Thus, now is the time to discuss the possible methods for regulating cybersecurity in aviation before it becomes too late.

Flying is an integral part of our modern globalized economy. Everyday, over 100,000 flights carry over 8 million people around the world[11], indicating the extent to which people are increasingly reliant on air transport. When European airports were closed for merely one week in 2011 due to the eruption of Iceland's Eyjafjallajokull volcano, over 10 million people were stranded, airlines lost $1.7 billion in revenue, and the entire week cost the European economy $5 billion[8]. Solely a single isolated event miles away was able to adversely affect

millions of people and cost billions of dollars. When airports are shut down or flights are grounded, the costs can be staggering.

A well-executed cyberattack on an aircraft, airport, or any intermediate function could have similar costly effects, and this threat is compounded by the lack of relevant legislature. Many computer systems in the aviation industry were created and used without security as a priority. As an industry, aviation has not suffered many high-profile cybersecurity defeats, but it may be time for a wake up call. Industry leaders must pay attention now before standards become too relaxed. There are many cybersecurity risks regarding aircraft and some are extremely easy to take advantage of. A large cyberattack targeting known vulnerabilities could occur in the near future and damage the global economy and potentially threaten lives.

Many of the cybersecurity threats to aircraft target aircraft support systems such as air traffic controllers. In 2008, 800 cyber incident alerts of attacks were reported on FAA computer systems. When tested, 4,000 FAA computer systems were found to have vulnerabilities with 763 even being deemed high risk[2]. Vulnerable computers can allow malicious agents to inject their own code. A skillful malicious agent with access to an air traffic control terminal could cause remarkable damage limited only by their own imagination.

Apart from air traffic control the following computer systems related to aviation could all be potentially vulnerable to attack[4]:

- Reservation systems
- Access, departure and passport control systems
- Cargo handling and shipping
- Hazardous materials transportation

- Onboard computer and navigation systems

Arguably, the largest and most relevant security risk in aircraft is the result of new Federal Aviation Administration (FAA) policies. Current air traffic control protocols and technologies are outdated and struggle to remain efficient and safe as the number of flights worldwide continues to increase each year. The air traffic control system in place now is a remnant of the 1970s, when it was first introduced. Flight routes are carefully planned by air traffic control centers each day. Radar is used to measure an aircraft's position when in range, but this process has limitations. Human operators on the ground are required to communicate with pilots via voice channels to determine a plane's altitude and identity. Aircraft have little to no knowledge of other aircraft outside of radar information and the information fed to them by ground-based air traffic controllers[10].

As a way to improve upon the current system, the FAA has introduced a new air traffic control procedures and technology requirements called NextGen, which any aircraft flying in the US must be fully compliant to by 2020. The cornerstone of NextGen is a technology called Automatic Dependent Surveillance-Broadcast (ADS-B) which is already being equipped to many planes in the US. ADS-B accurately broadcasts an aircrafts exact location at all times while it is active. NextGen with ADS-B reduces costs, and saves fuel as well as time. Money is saved because the need to hire personnel to constantly communicate with aircraft is lessened. Additionally, human-error is reduced. Because more accurate location data is available, flights can be flown in tighter windows which saves airspace and time and increases efficiency. So what is the problem? What is wrong with reducing costs, time, errors and fuel usage and

increasing efficiency? ADS-B has serious security vulnerabilities, largely stemming from two major issues the data ADS-B transmits is both unencrypted and unauthenticated.

ADS-B's lack of encryption and authentication manifest in three main types of attack vulnerabilities: eavesdropping, injection, and jamming [5]. Before discussing the risks in further detail, it is useful to have more background information about ADS-B. ADS-B comes in two flavors, ADS-B Out and ADS-B In. ADS-B Out is the feature of ADS-B referred to in previous sections. Planes equipped with ADS-B Out broadcast their ID, position, and velocity among other things omnidirectionally nonstop. Planes equipped with ADS-B In can receive ADS-B messages sent from other aircraft. ADS-B In essentially allows for aircraft to aircraft communication and bypasses the need of a ground station. The FAA's NextGen plan requires all aircraft to have ADS-B Out by 2020 while ADS-B In is completely optional.

For each type of possible attack (apart from eavesdropping), the attack can be further subdivided based on the target: aircraft (ADS-B In) or ground station (ADS-B Out).
The first type of attack is:

1. **Eavesdropping.**

   ADS-B broadcasts are unencrypted and follow a publicly known protocol. Anyone can intercept and parse ADS-B transmissions to gain knowledge about aircraft. In fact, websites like planefinder.net already exist and populate their data by listening in to ADS-B broadcasts. Even aircraft that are not publicly broadcasting their flight information, but still using ADS-B for navigation routing purposes (Air Force One?) would still have their information intercepted[5]. While eavesdropping is not necessarily dangerous, it can provide an uncomfortable amount of intel about the location of our

aircraft to any potential nefarious agents. We feel the same unease we felt when we realized that Google tracks and records our locations at all times. That feeling of unease is compounded by the fact that all the information is publicly available and it extremely easy to eavesdrop. Anyone could buy a device for less than $100 and be able to receive ADS-B transmissions immediately.

The second type of attack is:

2. **Jamming.**

   Also known as flood denial, this can target either a ground station or an aircraft.

   a. **Ground Station Jamming.**

      This attack involves disrupting the 1090MHz frequency that all ADS-B signals propagate on. Simply being near a ground station and blocking the frequency would easily overpower legitimate ADS-B signals that originated from planes miles away[10]. Because a jamming device has to be relatively close to a target, jamming attacks usually occur in short durations (around 10 minutes) [5]. While a jamming attack is going on, there is virtually no way to stop it or work around it, apart from physically finding and destroying the jamming device. Jamming a control tower at a busy airport could cause all types of issues. While it unlikely a collision would occur, because planes are still equipped with radar to corroborate ADS-B signal data when possible, jamming could still prevent airplanes from landing, taking off, and other tasks that require communication with the ground station. A few delays can easily compound at a busy airport with

an end result of thousands of people being negatively affected or even put at risk. This attack is also very easy to execute due to the high availability of low-power jammers.

b. Aircraft Jamming

This attack similarly disrupts the 1090MHz frequency. An attacker, however, would have to be in close proximity to the target aircraft or have access to a high-power jammer, which is not readily available[10]. Jamming an aircraft's ADS-B In signal would simply have the effect of losing the benefits of ADS-B In. An aircraft could potentially still operate without issue using traditional radar and radio position detecting. The worst case scenario would be when the aircraft approaches an airport and needs to land or taxi, in which these operations could become more difficult[10]. Furthermore, not many aircraft are equipped with ADS-B In to begin with and many aircraft operate completely fine without it.

The third and potentially most dangerous type of attack is:

3. Injection.

An injection attack can target either a ground station or an aircraft equipped with ADS-B In. To perform an injection attack, an attacker broadcasts a false ADS-B signal to convince listeners a plane exists at the location broadcasted.

a. Ground Station Injection.

A ground station injection can pose various types of problems. A ground station that treats an injected ghost plane as real may change its routing, scheduling and

other communications based on the false data. An injection can also be more subtle. For example, a known flight path is injected or an existing flight is injected with slight variations. It can be very difficult to which signal is real and which is falsified[5]. An attacker could consistently inject the same false flight path to train the air traffic control system. Once air traffic control either believes the injection is a normal flight path or is trained to ignore it as a false signal, a nefarious agent could actually illegally fly on that path and be ignored[5]. Performing a successful ground station injection is not as simple as broadcasting an ADS-B signal. Despite the numerous other security flaws of ADS-B, the FAA argues that injection attacks are prevented by data validation and spoofed planes are filtered out[14]. However, some cybersecurity researchers disagree. Brad Haines (RenderMan) argues that the FAA uses multilateration to detect spoofed targets[]. Multilateration requires the use ground stations to detect signals and correlate data, but is not useful for preventing aircraft injection.

b. Aircraft Injection

As mentioned earlier, an air-to-air signal is much harder to prevent because there is no ground station with data to corroborate the signal. The FAA claims aircraft can use radar to complement ADS-B In to verify the signal; however, issues with the accuracy of radar arise frequently[5], as radar does not indicate another plane's altitude. Furthermore, radar frequently displays various landmarks such as mountains, which leads to questions regarding how a pilot could be able to distinguish between a radar anomaly for a falsified signal. If the

plane injected is on course for collision, the stakes are understandably extremely high. Furthermore, the FAA claimed ADS-B would replace radar in the future in its NextGen protocol.

Each attack type poses at least moderate to high risk to our privacy, as well as safety, regarding the use of aircraft. Each attack stems from the underlying lack of encryption and authentication. If the ADS-B messages were encrypted, it would be impossible to eavesdrop and glean meaningful information. It would also be harder to spoof messages that a receiver would find believable. With authentication, injection would be impossible. Jamming could still pose issues if it simply blocks the entire frequency, but if flood denial occurred by injecting many ghost planes, authentication could find the legitimate signals and avoid the attack. The current implementation of ADS-B only supports some data integrity in the form of a checksum. While some are working towards how to provide encryption for ADS-B to secure out skies, everyone agrees the task of creating a system that can manage and distribute keys for encryption is gargantuan if not unrealistic[16]. The FAA's Ron Jones stated, "Probably the most fundamental security issue with ADS-B is the core idea of broadcasting the identity and precise location of each aircraft. This would open the door for a terrorist to attack specific aircraft or aircraft of a specific airline or corporation. While some people have suggested some form of encryption might be applied, I do not see any way in which this could be effective without fully undermining the basic ADS-B concept and associated benefits." [14] As one can see, there is no good and obvious solution to the ADS-B vulnerabilities.

ADS-B is mandated in the in the USA by 2020. In Europe, it is required by 2015. It is already mandated in Canada. Already a huge portion of aircraft being used today have ADS-B Out. The entire UPS fleet is equipped with ADS-B Out, while half of it also has ADS-B In[10]. The FAA is looking into some solutions, but as long as it pushes the widespread use of ADS-B as it exists now, these threats will continue to exist. If our military aircraft are also equipped with ADS-B, using it could be a liability in war as well. For military use, mapping ADS-B over Mode 5 Level 2 (M5L2) can allow for an encrypted secure channel to relay the ADS-B signals[10]. Unfortunately, these techniques are not reasonable to use for civilian and commercial use.

Another technique employed by DARPA and their High-Assurance Cyber Military Systems project that can be used to prevent hacking of aircraft is software assurance. Using formal methods, the team at DARPA, strives to create unhackable code by finding proofs their code and new self-developed programming language, Ivory, are secure, among other things[13]. They successfully secured a helicopter drone from cyberattacks. This research, while still in its early stages, could some day secure all aircraft from cyberattacks.

Additionally, Senator Markey of Massachusetts has introduced the Cyber AIR act to congress in an attempt keep the legislation up to date with technology. The Cyber AIR act would create a cybersecurity standard for all aircraft operating in the US and notify and fix any cybersecurity vulnerabilities. With steps like this in the right direction, we can potentially secure our aircraft and the aviation industry from cyber threats before something truly damaging happens.

Works Cited

[1]Atherton, Kelsey D. "How DARPA Is Prepping For The Next Cyberwar." *Popular Science*. N.p., 11 Feb. 2016. Web. 16 Dec. 2016.

[2]Baldor, Lolita C. "Air traffic systems vulnerable to cyber attack." *NBCNews.com*. NBCUniversal News Group, 06 May 2009. Web. 16 Dec. 2016.

[3]Butts, Jonathan, Cindy Finke, and Robert Mills. "ADS-B encryption: confidentiality in the friendly skies." *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*. Tennessee, USA, Oak Ridge. New York: ACM, 2013. Web.

[4]"Cybersecurity in the Aviation Industry." *Florida Tech Blog*. Florida Tech, 2016. Web. 16 Dec. 2016.

[5]*DEFCON 20: Hacker + Airplanes = No Good Can Come Of This*. Perf. Brad Haines. DEFCON 20, n.d. Web. <https://www.youtube.com/watch?v=CXv1j3GbgLk>.

[6]Elias, Bart. *CRS Insights*. 18 June 2015. Protecting Civil Aviation from Cyberattacks.

[7]Harwell, Drew. "FBI probe of alleged plane hack sparks worries over flight safety." *The Washington Post*. WP Company, 18 May 2015. Web. 16 Dec. 2016.

[8]"How the 2010 ash cloud caused chaos: facts and figures." *The Telegraph*. Telegraph Media Group, 24 May 2011. Web. 16 Dec. 2016.

[9]Lynch, Kerry. "FAA Exploring Possible Privacy Protections for ADS-B." *Aviation International News*. The Convention News Company, 4 Aug. 2015. Web. 16 Dec. 2016. <http://www.ainonline.com/aviation-news/business-aviation/2015-08-04/faa-exploring-possible-privacy-protections-ads-b>.

[10]McCallie, Donald L. *Exploring Potential ADS-B Vulnerabilities in the FAA's Nextgen Air Transportation System*. Diss. Air U, 2011. N.p.: Air Force Institute of Technology (U.S.), 2011. Print.

[11]"New Year's Day 2014 marks 100 Years of Commercial Aviation." *IATA*. N.p., 31 Dec. 2013. Web. 16 Dec. 2016. <http://www.iata.org/pressroom/pr/Pages/2013-12-30-01.aspx>.

[12]Statler, Kent L. "Cybersecurity And The Commercial Aircraft - Delivering Leading-Edge Technology To Meet A Growing Threat." *Aviation Week Network*. Penton, n.d. Web. 16 Dec. 2016. <http://aviationweek.com/information-management-solutions/cybersecurity-and-commercial-aircraft-delivering-leading-edge-techn>.

[13]Sternstein, Aliya. "Pentagon on Path to Launch Hacker-Proof Boeing Drone by 2018." *Nextgov*. N.p., 11 Mar. 2015. Web. 16 Dec. 2016.

[14]Thurber, Matt. "ADS-B Is Insecure and Easily Spoofed, Say Hackers." *Aviation International News*. N.p., 3 Sept. 2012. Web. 16 Dec. 2016.

[15]Thurber, Matt. "Hackers, FAA Disagree Over ADS-B Vulnerability." *Aviation International News*. N.p., 21 Aug. 2012. Web. 16 Dec. 2016.

[16]Wesson, Kyle D., Todd E. Humphreys, and Brian L. Evans. "Can Cryptography Secure Next Generation Air Traffic Surveillance?" *IEEE SECURITY & PRIVACY* X.X (2014): n. pag. University of Texas Austin Radionavigation Laboratory. Web.

[17]Wolff, Josephine. "The Aviation Industry Is Starting to Grapple With Cybersecurity." *Slate Magazine*. N.p., 2016. Web. 16 Dec. 2016.

[18]Zetter, Kim. "Is It Possible for Passengers to Hack Commercial Aircraft?" *Wired*. Conde Nast, 26 May 15. Web. 16 Dec. 2016.