CTC #2

2d Lt Marvin Newlin

CSCE 525

Lt Col Reith

10 Oct 18

As the aviation industry becomes a more digital and connected industry, cyber threats are increasing within this area. Three major threats within this industry are software vulnerabilities on aircraft, insecure communications, and lack of security in the associated aviation systems.

Aircraft today are controlled by computers as is to be expected in the world today. Additionally, flying can be a high-risk activity in the event that anything goes wrong. Given this, one would expect that the software that controls the airplanes that fly around the world everyday would be incredibly secure. However, this is not the case. In 2015, American Airlines experienced an incident in which an iPad experiencing some issues connecting to the aircraft cause the electronic devices that contain all of the planes logs and flight information to fail.2 In another incident, a passenger on board of a flight was able to access emails that belonged to a reporter on the plane who was working on the plane’s wireless internet.1 While these incidents may not seem as threatening as Stuxnet, when it comes to aircraft, everything is amplified because mishaps in the aviation industry can ripple out and cause economic and social effects.

Another threat that exists in the aviation industry is insecure communications. The Aircraft Communications Addressing and Reporting System (ACARS) is a digital system that aircraft use for air-ground communications. Surprisingly, this system that provides such pertinent information like flight plans and aircraft locations is largely unencrypted in most instances.1 Clearly, this threat could cause huge issues as it would be relatively straightforward to intercept these communications and put out a junk location or flight plan.

One other threat that is important in the aviation industry is the associated Air Traffic Control and airport software systems that make the industry operate. One example of this is when a virus was spread to some FAA computers in Alaska that controlled air traffic control systems, causing them to be shut down.1 In another case, a hack of the FAA’s computers resulted in the compromise of data from about 480,000 employees.1 Clearly, these are incredibly serious issues that have occurred in a minor context but could be amplified if attacks on a larger scale took place.

Notes

1. "Cyber Threats to the Aviation Industry." RealClearDefense. Accessed October 09, 2018. <https://www.realcleardefense.com/articles/2018/03/19/cyber_threats_to_the_aviation_industry_113216.html>.

2. CybeRisk. "Aviation Cyber Security | Threats Facing the Industry, Recommendations." CybeRisk. May 15, 2018. Accessed October 09, 2018. https://www.cyberisk.biz/aviation-cyber-security/.