Cyber Security and System Safety in the Aviation Industry

Aviation remains a critical industry in the global economy. Important as a means of travel, tourism, and shipping, aviation is estimated to impact $2.2 trillion annually – or 3.5% of the global GDP.[i] Any interruption in service for the aviation sector could potentially be catastrophic on many levels. In addition to bringing personal travel to a halt, businesses would be unable to move their products, and the amount of revenue lost would be difficult to fathom.

At the same time, rapid development and expansion of technology has caused a new threat to emerge in the aviation industry. Currently, there exists a significant security threat: cyber security. Due to its influence on nearly every aspect of life and business, the aviation industry is a large target for cyber terrorists to organize an attack. Also, because of the ever-shifting nature of the technology itself, there are certain difficulties in defending such malicious attempts. Information theft is becoming increasingly prevalent as more people interact with cyberspace in-flight.

Image Via Flickr: trindade.joao

One of the greatest dangers facing the industry right now is the nebulous nature of the threat itself. There is no grounded way of determining when or where it will strike. As a result, there does not yet exist a unified, common and understood set of strategies for the defense against cyber terrorism. Fortunately, the industry is beginning to take notice of the emerging obstacles. As technology becomes more widespread and available, there will need to be a way to protect users from being exposed when they go online during their flight. Systems will need to be put into place to ensure that information remains safe. Collaborative research and design will be essential to creating a safe environment for air travelers.

Security of Personal Information

With today's technological advances, a passenger could conceivably connect online through in-flight networks and access personal information. The question is: How much of a risk does that pose for the passenger? If someone boards a plane and then decides to do online banking (or even check emails), is that information secure?

According to most studies, the answer is unfortunately no. This is because the network that passengers use is similar to a public network used in any place on the ground (think of a local coffee shop). These are often unsecured networks, and even if your session is secure, you can still be at risk. One of the major flaws in most users' security is caused when they don't apply the automatic service updates to their computers. These often come with security patches, which if not applied, leave a computer vulnerable to attacks. So even if you go through a secure network, a hacker can still access your information through the security hole in your computer.

Although major airlines such as Delta boast safe access through Gogo, there are still many risks involved with exposing personal information over a public network. However, industry leaders are already taking action to secure the networks and make online sessions safer for the average passenger. The International Air Travel Association (IATA) has unveiled a "three-pillar strategy, including work to understand, define and assess the threats and risk of cyber-attack, advocacy for appropriate regulation, and mechanisms for increased cooperation throughout the industry and with governments."[ii]

Flight Safety

The drive for security within cyber networks is not only for the benefit of passengers hoping to access online accounts. It is critical to ensure the safety of the flights themselves. Aviation is becoming increasingly dependent on new technology. Among the changes that have already or will soon affect the design of aircrafts:

- GPS replacing radar as the primary means of aircraft identification.
- Cockpit IT systems utilizing high-speed internet connections

While these changes represent significant advances in air travel, they also present serious security risks. Cockpit IT systems use wireless connections that are as

vulnerable as networks used by passengers. Information can easily be intercepted and manipulated.

Image Via Flickr

However, the GPS system creates even greater vulnerabilities. Several events – both designed and unintentional – have shown how susceptible GPS can be to interruption. In a 2012 demonstration to the FAA and Department of Homeland Security, researchers using only US$1,000 worth of equipment were able to successfully hijack a small drone, which relied on signals from open civilian GPS signals. Drones are notoriously prone to spoofing, as made evident in 2011, when Iran stated that it had captured a US drone by spoofing the GPS signals and fooling the drone into thinking it was landing at its home base.[iii]

As aviation and technology continue to converge, these are issues that must be addressed to ensure the safety and security of the industry.

Steps Being Taken

Although we are still in the early stages of designing effective solutions to these problems, there are already steps being taken to combat the dangers of cyber security. The American Institute of Aeronautics and Astronautics (AIAA) has made several recommendations for moving forward toward improved security measures, including: [iv]

- Increase cooperation and focus within the aviation community
- Leverage, extend and apply existing industry best practices, especially research and education efforts
- Build a roadmap by identifying near-, mid-, and long-term actions
- Establish a governmental and industry framework to coordinate national aviation cybersecurity strategies, policies, and plans

In general, AIAA stresses that we do not yet have a unified approach to the problem of cyber security. This is a relatively new topic in the history of aviation, so experts are only now beginning to come together to determine the best course of action.

The Federal Aviation Administration (FAA), meanwhile, has already rolled out its own system that promises to streamline and secure the aviation industry as it moves forward in the technological age. Called NextGen, these satellite-based and digital technologies have been designed to "provide air traffic controllers and pilots with the tools to proactively identify and mitigate issues associated with weather and other hazards. NextGen enables us to better meet our national security needs and ensure that travelers benefit from the highest levels of safety."[v]

While the technology does make the overall experience smoother and easier for both the pilot and the passenger, it comes at a cost. Experts have determined that NextGen comes with its own design flaws and vulnerabilities. Specifically, white-hat hackers have already produced ways to infiltrate aircrafts in-flight – one specialist injected fifty "ghost flights" into a plane's flight plans, simply by intercepting and spoofing satellite signals. "At a cost of billions of dollars and still early in its development," he remarked, "NextGen seems to have many of the same vulnerabilities as anything else."[vi]

The problem with any design is that the technology never remains static long enough. As soon as someone figures out how to solve one problem, the technology has already raced ahead and created several more. It is why the AIAA insists that we cannot continue chasing the problem – we must get ahead of the threat.

Looking Ahead

As the aviation industry becomes more inextricably intertwined with technological advances, security threats will increase. Physical attacks remain the largest potential risk in an aircraft, but cyber-attacks are quickly making up ground. Still, there are ways that industry leaders and even passengers can limit their risk without sacrificing the technology.

The best way to avoid security breaches is to avoid exposing yourself to those situations, experts say. Do not engage in online activities that can reveal personal or financial information to malicious users. For passengers, it is primarily a matter of awareness and education. Several organizations are working to help people

understand the dangers of in-flight networks, and a number of larger news sites have picked up this story as well. As passengers become more aware of these potential pitfalls, experts hope that they will use greater discretion when they board a flight.

As for securing the aircrafts themselves, this is still very much a work in progress. NextGen currently leads the way, although its vulnerabilities have already been exposed. Similar designs have appeared in the industry, but they all come with the same difficulties. Currently, there is a limitation to how secure you can make a network. As long as there is the slightest vulnerability, information thieves and cyber terrorists will be able to exploit it.

Schools and colleges are becoming increasingly involved, however, in an attempt to inspire a new generation of students to come up with the needed solutions. Embry-Riddle Aeronautical University in Daytona Beach has developed a cybersecurity engineering laboratory, which is designed "to meet instructional and research needs in the area of cyber security, offering a visualization infrastructure to apply visualization techniques to attack related data as well as to display information about ongoing attacks."[vii] The InfoSec Institute, a well-respected information security company, has also created its own aviation cybersecurity program, and specializes in hacking aviation systems so that they can attempt to patch vulnerabilities that they discover.

This will prove to be an ongoing issue for many years to come. Experts are still trying to understand the scope of the problem as technology becomes a much more complex tool. This represents a unique time in the history of aviation. It is a moment of incredible growth and innovation, but also an opportunity for new and extraordinary breakthroughs.

Maryruth Belsey Priebe

Maryruth can't help but seek out the keys to environmental sustainability - it's the fire that gets her leaping out of bed every day. With green writing interests that range from sustainable business practices to net-zero building designs, environmental health to cleantech, and green lifestyle choices to social entrepreneurism, Maryruth has been

exploring and writing about earth-matters and ethics for over a decade. You can learn more about Maryruth's work on JadeCreative.com.

Sources

[i] *The Connectivity Challenge: Protecting Critical Assets in a Networked World.* (2013, August). Retrieved from AIAA: https://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/AIAA-Cyber-Framework-Final.pdf

[ii] *IATA Fact Sheet: Cyber Security.* (2014, May). Retrieved from IATA: http://www.iata.org/pressroom/facts_figures/fact_sheets/Pages/cyber-security.aspx

[iii] Iasiello, E. (2013, August). *Getting Ahead of the Threat.* Retrieved from Aerospace America: http://www.aerospaceamerica.org/Documents/AerospaceAmerica-PDFs-2013/July-August-2013/Viewpoint-Getting-Ahead-AA-Jul-Aug2013.pdf

[iv] (The Connectivity Challenge: Protecting Critical Assets in a Networked World, 2013)

[v] *NextGen.* (2014, May). Retrieved from Federal Aviation Administration: http://www.faa.gov/nextgen/

[vi] *Cyber Threats against the Aviation Industry.* (2014, April). Retrieved from InfoSec Institute: http://resources.infosecinstitute.com/cyber-threats-aviation-industry/

[vii] *Cybersecurity Engineering Laboratory.* (2014). Retrieved from Embry-Riddle Aeronautical University: http://daytonabeach.erau.edu/about/labs/cybersecurity-engineering-lab/index.html