Getting Ahead of the Threat: Aviation and Cyber Security

Emilio Iasiello, Private Sector

Available at: http://works.bepress.com/emilio_iasiello/8/
Since May 1962, when the first U.S. airline was hijacked to Cuba, to the catastrophic events of September 11, 2001, the individual—whether terrorist, ideologue, or criminal—has been the biggest threat to airline operations and passenger safety. Motivated by 9/11’s unprecedented fallout, the aviation industry committed itself to revamping its security apparatus, collaborating with government, industry, and labor to enhance its ability to identify and mitigate the physical threat to aviation.

Many significant accomplishments have resulted from this effort, including the creation of the Transportation Security Administration to oversee U.S. public transportation; establishment of DOT Rapid Response Teams, charged with developing recommendations to improve security; and the development of a common aviation industry strategy to address onboard criminal and terrorist acts.

However, while the aviation industry continues to refine physical security practices, it still has not addressed the potential cyber threats against its information infrastructure and the ‘fragilities’ that can be exploited therein. Part of the reason may be rooted in a few anecdotal instances of hackers successfully compromising airline information assets.

Nevertheless, the absence of evidence does not equate to an absence of threat. In its 2003 National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, the government classified the transportation sector as of vital economic importance and the aviation industry in particular as a key symbol of U.S. technological and industrial achievement. As a result, the industry should be compelled to develop a comprehensive strategy to shore up its cyber security posture through policies, standards, and an international regulatory framework to position itself ahead of the threat rather than reacting to it.

**NETWORK VULNERABILITIES**

Successful civil aviation operations rely on a highly networked and interconnected environment that includes voice and data communications traversing the aircraft, the air traffic management system, and any ground or satellite stations feeding data through this cycle. These innovations promise to revolutionize our aviation experience with state of the art equipment to facilitate...
processes, increase flight safety, improve communications, and streamline operations. However, the more networked an enterprise, the greater the opportunities to exploit any inherent weaknesses. Aircraft-to-ground, aircraft-to-aircraft, and in-aircraft access points can all be exploited.

- By 2020, ADS-B (Automatic Dependent Surveillance Broadcast) will be a compulsory requirement on the majority of aircraft, as part of the U.S. Next Generation Air Transportation System (NextGEN) initiative, as well as Europe's SESAR project, according to Airport Technology, an online resource for the aviation industry. ADS-B is a surveillance technology that will be replacing radar as the primary means of tracking aircraft. As a data infrastructure, ADS-B will provide traffic and weather information, offering better communication between the aircraft and air traffic control.

As these efforts are implemented worldwide, there are concerns regarding the security of the system and the information traversing its infrastructure. To date, the ADS-B system remains unprotected and vulnerable to cyber attack. Communications between aircraft and air traffic controllers remain unencrypted and unsecured, potentially granting hostile actors a vector from which to cause disturbances in air transportation.

The FAA asserts that ADS-B signals will be confirmed by radar, while automatically weeding out ‘fake’ signals using a process called multilateration to determine the origin of every ADS-B signal. While such redundancies should help foster safe operations, the FAA does not offer any specifics on how this would work, citing sensitivity considerations.

Multilateration employs a number of ground stations that implement a method known as Time Difference of Arrival to accurately locate aircraft. However, multilateration is not exempt from potential tampering. Nodes are susceptible to attacks by malicious actors seeking to manipulate data or the nodes themselves, for example, reporting false position and distance information or modifying measured positions and distances of wireless nodes.

In addition, several aspects of NextGEN place the new system in its current form at risk to cyber-based attacks. It is unknown how the FAA’s security action plan would respond should any of its devices and solutions be exploited.

- COTS. NextGEN will use information services that have implemented COTS hardware and software technology. While popular and accessible, COTS technology presents significant security challenges for its operators, due to the difficulty in verifying the security of COTS products. These systems regularly are used without ownership of, knowledge of, or access to source and application code. That same code is of-
In 2011, Iran stated that it had captured a U.S. drone by spoofing the GPS signals it received, fooling the drone into thinking it was landing at its home base.

Ten developed overseas, with little documentation, minimal configuration management, or both. And as COTS use expands, identified weaknesses can be exploited to attack all the users of that same system. In addition, COTS software is generic and does not typically address instance-specific features of an enterprise’s unique operating environment. Also, hidden functions can be embedded into COTS technology as developers and operators tend not to test for things they do not know about.

• GPS. NextGEN will replace radar with GPS as the primary means of aircraft identification. Several incidents have demonstrated that GPS has been subject to intentional and unintentional targeting and disruption by both state and nonstate actors. For example, in a 2012 demonstration to FAA and Dept. of Homeland Security representatives, researchers using only $1,000 worth of equipment hijacked a small drone, highlighting the exposure of unencrypted GPS signals. In the U.S., nonmilitary drones rely on signals from open civilian GPS, which make them prone to spoofing.

In 2011, Iran stated that it had captured a U.S. drone by spoofing the GPS signals it received, fooling the drone into thinking it was landing at its home base. By jamming the remote control communications, the drone is forced into autopilot, thereby being susceptible to receiving spoofed coordinates. Earlier, in 2009, Newark Liberty International Airport experienced sporadic outages of the GPS Ground-based Augmentation System used for precision approach landing. The ground station 300 ft away experienced signal interference every day at about the same time. The FAA discovered the cause of the outage was a GPS jammer being used by a truckdriver to avoid being tracked by his employer.

• Cockpit IT systems. New generation aircraft include advanced cockpit IT systems that use generic Internet Protocol. These cockpit systems are integrated with ground networks through high-speed communication links on the ground (over wireless technologies) and in flight (over broadband satellite networks). Wireless access points are notoriously very weak, often unsecured, and susceptible to signal interception and manipulations. COTS technologies are also used to support these systems.

• Satellites/ground stations. Aircraft relying on satellites for communications provide another avenue of access to malicious actors. By gaining access to a satellite or its ground station, an attacker can deny or degrade, as well as forge or otherwise alter, the satellite’s transmission.

AVIATION HACKING INCIDENTS

Physical attacks continue to be the biggest threat facing aviation. However, unconventional threats such as hacking have surfaced in recent years that endanger aviation facilities and operations. Technology used in the aviation transportation system infrastructure is not immune to cyber threats, and the networks that support critical airport information assets are susceptible to both virtual and physical threats. The 21st century has ushered in a vast cyber threat landscape, bolstering the need to ensure the confidentiality, integrity, and availability of information and information systems as passenger numbers and flights increase globally.

Recent incidents demonstrate an escalating interest from actors targeting aviation. In 2011, radio hackers broke into frequencies used by British air traffic controllers and gave false instructions to pilots or broadcast fake distress calls. In 1998, three similar incidents were reported; in 2010, 18 were reported, and halfway through 2011, 20 were noted. In 2011, the Australia-based Internet security company Pure Hacking performed a penetration test on an airline network. With one hack, the tester escalated privileges that resulted in the complete compromise of an airline network. This included capturing credit cards, plans, communications, and databases.

In 2009, the FAA admitted that the nation’s air traffic control systems were vulnerable to cyber attack, following 2008 incidents when hackers accessed personnel records and network servers.

THREAT ACTOR LANDSCAPE

The threat actor landscape is vast, composed of groups and individuals with the intent to target critical infrastructures to meet tactical and strategic objectives. While capabilities may hinder some of these actors, resources are becoming more available and at an increasingly reduced cost.

Simply put, the window of opportunity is an expanding aperture. Aviation relies on the public trust for its success; hostile actors can undermine this trust through cyber attacks meant to deny, degrade, disrupt, or
destroy aviation’s information systems or the information itself, and publicizing their actions. In this regard, the target of the attack is not the system so much as the public’s confidence in the integrity of networks and systems. The players may range from attention seekers to hostile nations.

• Hackers/hacktivists. These groups represent the largest segment of the hostile online underground, ranging from individuals to large groups with varying levels of sophistication. Typically, those inclined to attempt to compromise the aviation industry most likely are seeking a challenge and/or notoriety rather than actually trying to impact airline operations. Also, white-hat hackers such as security consultants may try to compromise aviation in order to reveal vulnerabilities in an attempt to raise awareness for security purposes.

Hacktivists, however, would seek to target aviation if doing so supported their political/ideological beliefs. In 2011, the TSA reported that unidentified hackers, allegedly from overseas, launched cyber attacks against a railroad company, disrupting rail signaling and traffic in the northwestern U.S. for two days.

• Terrorists. Aviation remains a prime target for terrorists and terrorist organizations that are seeking a visible, damaging impact on a significant public infrastructure. Though this group has largely used the Internet for communications, planning, recruitment, and propaganda, there has been limited evidence of terrorists or terrorist sympathizers actually conducting cyber attacks.

In March 2012, Assessing Cyber Threats to Canadian Infrastructure, a paper prepared for the Canadian Security Intelligence Service, noted that “passenger flights, cargo flights, and airport facilities have all been subject to terror attacks as part of al-Qaeda’s economic jihad against the West.” In addition, laptops taken from al-Qaeda operatives have held information related to programming data and software sites for SCADA (supervisory control and data acquisition) systems, power, and water company sites, indicating a growing interest in critical infrastructure as a possible target.

• Nation states. Typically, hostile cyber activity has targeted the aviation industry (primarily companies involved in the manufacturing process) in order to steal sensitive and proprietary information, rather than against airports, airport/aircraft communications, or aircraft in flight.

Although aviation may be a tactical objective for terrorists, it would serve more often as a strategic target for a nation state. Any type of network mapping or reconnaissance directed against airports, aircraft, or air traffic communications would support a strategic objective that could be leveraged should nation state relations deteriorate and military conflict become evident.

Is the hacking threat against aviation real? Absolutely. As a key critical infrastructure and an essential link to commerce and passenger transportation, the global aviation industry will remain a target for adversaries seeking to make a statement or cause substantial loss to life and financial bearing. Like many emerging threats, cyber attacks still loom in the periphery, bordering on the ‘not yet realized,’ and are seen more as a stylized fiction than an actual possibility.

...the target of the attack is not the system so much as the public’s confidence in the integrity of networks and systems.

However, the U.S. has borne witness that all it takes is one incident to transform possibility into reality. The consequences of not foreseeing such an event cost the aviation industry considerably. According to the International Air Transportation Association, U.S. airline revenues dropped from $130.2 billion to $107 billion in 2002. Losses of $19.6 billion were reported in 2001-2002, and between December 2002 and October 2005, United, Delta, Northwest, and US Airways had filed for Chapter 11 bankruptcy reorganization.

The aviation industry is being given another opportunity to prepare for a threat that as yet has not severely impacted its operations. Terrorists—a visible threat—caused people to avoid air travel after September 11. Gradually, confidence returned as more stringent security was implemented, but not before grievous loss of life as well as serious financial losses were incurred. Fast forward to today, as aircraft become more technologically advanced. If proper security considerations are not enacted, vulnerabilities can and will be exploited.

The one constant in the cyber world is that all modern and advanced technologies have either been hacked or are looking to be hacked by the bad guys. The key to being secure in this environment is being ahead of the threats, not reacting to them after they’ve already commenced.