

Aviation Sector Must Confront Airport Cyber Risks

By **Laura Foggan, Brendan Mullan, Mark Meyer, Eileen Gleimer and Jeffrey Poston**
(November 7, 2019, 4:29 PM EST)

Cybersecurity is a real risk for the aviation sector generally. Cyber risks related to flight safety make the headlines. For instance, the U.S. Department of Homeland Security's announcement in 2017 that it hacked a Boeing 757 parked in Atlantic City, New Jersey, using radio frequency communications was front-page news.

2018 reports that researcher Ruben Santamarta successfully hacked into in-flight Wi-Fi networks also grabbed the headlines. More recently, a July 30 DHS alert warned that a device attached to a plane's controller area network could manipulate and provide false information regarding telemetry readings, compass and attitude data, altitude, airspeed and angle of attack.

Cybercriminals have also targeted airlines, stealing personal data and causing significant business interruptions. In 2018, in the largest reported airline data breach to date, a hacker accessed information pertaining to 9.4 million customers of Cathay Pacific Airways Ltd. In a separate incident, hackers gained access to individual Deutsche Lufthansa AG passenger accounts, and used frequent-flier miles to obtain vouchers and redeem rewards. Commentators also speculate that recent airline computer outages, which caused flights to be grounded across the United States, were caused by cyberattacks.

But less public attention has focused on how airports are susceptible to cyberattacks. There are, on average, 1,000 airport cyberattacks per month, a study by the European Aviation Security Agency found. Earlier this year, in April, Cleveland Hopkins International Airport suffered a ransomware attack that knocked out displays and disabled email. Airports present a large number of different cybersecurity issues, given the numerous systems and entities involved with airport operations.

Earlier this month, Pen Test Partners LLP published the results of an investigation identifying systems used at airports that are potentially at risk for a cyberattack. According to Pen Test, airports face a significant challenge to keep their systems secure, while still allowing interoperability for the large volume of entities that need access to the airport's systems, including, among others, passengers, crews, airline staff, security personnel, government agencies, fixed based operators, freight operators and meal service providers.



Laura
Foggan



Brendan
Mullan



Mark Meyer



Jeffrey
Poston

Pen Test identified 17 airport interfaces potentially exposed to a cyberattack, which we have grouped into the following categories: (1) the airport's Wi-Fi system; (2) crew and flight information; (3) airport building management; (4) passenger-assist systems; and (5) runway/taxiway/ramp. Each area is discussed below.

Airport Wi-Fi

An airport's Wi-Fi is linked to a number of issues identified by Pen Test in its review of cyber exposures. For instance, Pen Test noted that flight crews use an airport's Wi-Fi for legitimate aviation devices such as electronic flight bags.

Further, although briefing data is generally sent to an electronic flight bag, old-fashioned briefing rooms still play a key part in operations. For example, pilot briefing on information like load sheets, weather, routing and clearance is often done on a PC in the briefing room by pilots from different airlines. Thus, say Pen Test, "security controls can be a challenge to implement."

Other necessary airport operations also rely on the airport's Wi-Fi system. Gatelink, a data transfer system used to get information to and from the aircraft, is activated after the aircraft lands and uses an airport's Wi-Fi. Moreover, fuel delivery requests may also use the airport's network. For example, pilots can electronically request a fuel load, which, according to Pen Test, "is sent through an [application programming interface] to a tablet carried by the refueller, having been reviewed back at the airline's flight operations for weight and balance."

The risk to all these devices and many others connected to the Wi-Fi, as explained by Pen Test, is that "[s]poofing a network to try to attract some interesting kit or credentials is sometimes successful given the large number of devices connecting to them."

Crew Access Controls

Pen Test noted that the security of airline crew access control may be outdated. Airline crew access control must be interoperable, as it is not practicable, for example, to have access to one airport's crew area but not another.

According to the report, there is a "'legacy drag' as upgrading one system requires that all are upgraded at the same time ... so security controls often see a race to the bottom to ensure interoperability." Cloning — copying stolen card information to a new identification card — is therefore a real concern.

Airport Building Management and Physical Plant

Pen Test identified the building management system; heating, ventilation and air conditioning; concession spaces; ground power systems; airport security systems; and closed-circuit television as interfaces potentially susceptible to attack.

Pen Test stated that an airport's building management system, or BMS, is a susceptible area because it can control electronic doors and other systems, and may "have bypassable authentication and remote exploits." Similarly, an airport's HVAC system may be "controlled with a locally-managed BMS, though remote management by a specialist firm is very common."

It is possible that concession spaces may not be segregated, and may have access to other airport

systems, the report said. In addition, the control and billing systems for ground power are networked and are therefore exposed. More worryingly, Pen Test found that certain airside security functions, such as passport gates, were visible from the airport's corporate network; in fact, "[s]ecurity scanning/x-ray machines are also networked in many cases."

Finally, while there have been documented security issues with CCTV, Pen Test notes that "CCTV in some airports is amongst the finest in the world."

Passenger-Assist Systems

Pen Test identified agent computers and check-in kiosks, baggage systems and flight display systems as interfaces potentially susceptible to attack.

The computers used by airline agents to check in passengers are rented from the airport, and are often used by different airlines. Thus, they may raise user authentication issues. Further, the report says that interfaces to a baggage system, "although rarely directly exposed on an airport network," are sometimes exposed. Pen Test stated that "[r]eflashing or bricking a few critical controllers or tampering with a small amount of serial data can be enough to snarl up a baggage system and bring the airport to a halt."

The display systems that provide flight status and assigned gates may also have security issues. In fact, Pen Test stated that, with client permission, it successfully tampered with a client's flight display, and additionally noted that, fairly recently at Bristol Airport in the U.K., "a security incident, possibly ransomware, took out multiple systems including the flight displays."

Runway/Taxiway/Ramp

Pen Test identified airside vehicles, instrument landing systems, automated docking systems and robot tugs as interfaces potentially susceptible to attack.

Airside vehicles may use automatic dependent surveillance-broadcast, an unencrypted and unauthenticated protocol, that allows the vehicles to show up on ground radar. Pen Test explained that "[i]t wouldn't take much to broadcast a rogue ADS-B signal with [a software-defined radio] and place a phantom vehicle on a runway," which could cause chaos in low-visibility conditions.

Similarly, Pen Test explained, "it is not particularly difficult to spoof" an instrument landing system and "present a rogue signal that misdirects an aircraft." The spoofing would be obvious in good weather conditions, but might not be in poor visibility conditions. However, "Galileo [satellite navigation] can help as it is supposed to be more resilient to spoofing."

Pen Test also noted that automated docking systems, which employ infrared lasers to gauge the distance between the aircraft and the stop point, are becoming more common. Moreover, some airports have started using robotic tugs that use both Wi-Fi and custom radio frequency transmission over the 868 megahertz band, creating the potential for a tug to be remotely hijacked.

In sum, an airport is an extremely condensed, busy enterprise that poses numerous cyber risks. The Pen Test report suggests segregation of systems to alleviate some of the risks. But even when best practices are in place, it is evident that airport interfaces present many cyber exposures that must be taken into account by aviation industry members and their insurers.

Laura Foggan is a partner at Crowell & Moring LLP, and chair of the firm's insurance/reinsurance group.

Brendan Mullan is counsel in Crowell & Moring LLP's insurance/reinsurance group.

Mark Meyer is a partner at Crowell & Moring, and leads the firm's European insurance practice.

Eileen Gleimer is a partner at Crowell & Moring, and the chair of the firm's aviation group.

Jeffrey Poston is a partner at Crowell & Moring, and co-chair of the firm's privacy & cybersecurity group.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.