May 2019

HACKING OUR NATION'S AIRPORTS

CYBER-KINETIC THREATS TO THE TECHNOLOGIES RUNNING AIRPORT OPERATIONS

Authored By:

Drew Spaniel, Lead Researcher, ICIT
Parham Eftekhari, Executive Director, ICIT

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

Hacking our Nation's Airports

Cyber-Kinetic Threats to the Technologies Running Airport Operations

May 2019

Contents

Introduction

As part of a nation’s critical infrastructure, airports are highly symbolic, integral to the economy, and directly or indirectly impact the lives of virtually every citizen. For these reasons, airports are high profile targets for malicious nation-state actors who seek high-profile attacks that will disrupt daily life, cause mass causalities and damage a country’s reputation [1].

Most of the 8 million people estimated to fly every day interact with the technologies running the “typical airport experience” - avionics software on planes, air traffic control systems, baggage handling systems, ticketing systems, security systems, etc. – without considering the resiliency and security of the software or equipment they interact with. However, as was recently seen with the Boeing 737 Max incident, if the technology running our airports is not responsibility developed, coded, and manufactured then the lives of hundreds of passengers and crew may be at risk {A5].

Today, we find ourselves at risk of attack from terrorists, criminals, and nation-state adversaries who may exploit vulnerabilities in the technologies running our airports, causing financial or physical harm. The European Aviation Safety Agency has reported over 1,000 cyber-attacks each month on aviation systems and suggested the number is most likely to increase with the advancing digitalization of passenger engagement [2]. Modern airports themselves are equally vulnerable to cyber attacks as they are dependent on technologies such as the Internet of things (IoT), cloud and integrated systems for efficient, uninterrupted management of the logistics required to run such a complex operation [1].

Unless the equipment, networks, and devices which make up an airport’s ecosystem were designed with cybersecurity and resiliency as a requirement, our national security is at jeopardy. Cyber attacks and software glitches can result in delays, loss of revenue, and safety risks to passengers and employees. It is critical for the airline community and stakeholders in capitol hill, federal and state agencies, and the private sector to understand these risks and prioritize improved technology development and layered security strategies to improve the resiliency of our nation’s airports and airline industry.

Transportation Attack Scenarios

On the surface, attacks on air travel infrastructure seem like the plot of a fictional Hollywood action thrillers. After all, ever since the attacks on September 11, 2001, airports have implemented layered security controls that prevent so much as a stray water bottle aboard, let alone a dangerous weapon. However, while the physical security procedures implemented have proven effective at mitigating kinetic threats, the same diligence has not been applied to securing the Information Technology (IT) and Operational Technology (OT) systems, networks, and equipment upon which airports depend.

Much of the OT infrastructure that supports airport operations remains vulnerable because its security is not as much a priority as passenger logistics and physical security. For the most part, these legacy systems and equipment were not developed with security-by-design as a priority throughout their development lifecycle. As a result, airport networks are vulnerable to disruptive and deadly cyber-kinetic attacks whose outcomes can range from irksome delays to catastrophic crashes. An illustrative, but undoubtedly not an exhaustive list of scenarios include:

Airport Cybersecurity Attack Scenarios
Attacks on electronic signage to disable signs or change content
Ransomware on airport, airline, or vendor systems
Baggage system disruptions or misconfiguration
Interruptions to HVAC, electrical, or other building functions
Parking system disruption
Credit or debit card data theft
Theft of sensitive emails or documents to blackmail or embarrass airport executives, personnel, or their families ("doxing")
Establishing a fake airport website to spread misinformation or gather personal information
Compromising access management systems and issuing physical credentials to a nefarious actor
Disruption of jetway or other ramp functions
Attacks to prevent access to airport networks
Disruption of airport systems via malware delivered via phishing emails
Attempts to access physical security systems
Watering hole attacks originating from airport public Wi-Fi
False flag attacks meant to distract authorities, disrupt operations, or cause mass panic
Destructive cyber-kinetic attacks on OT systems such as wiper malware that render systems permanently inoperable
Man-in-the-Middle attacks to propagate incorrect arrival, departure, and navigational data meant to cause air-traffic collisions
Cyber operations designed to allow dangerous individuals or items to bypass security safeguards
DDoS attacks leveraging or acting against Internet of Things enabled sensors and devices
Attacks to disrupt Automatic Dependent Surveillance-Broadcast (ADS–B) and other air traffic management systems
Tamper with airport self-serving customer systems
Accessing CCTV systems for surveillance

Threat Actors

Attribution is not the most crucial factor to defend airports, but it is important to have a high-level understanding of who would be interested in targeting airport IT-OT infrastructure in disruptive or destructive cyber attacks. Below, ICIT has included high-level profiles of common threat actor categories and their potential motivations for targeting airport networks.

State-Sponsored Advanced Persistent Threats (APTs)

The most serious and significant sources of attack are conducted by foreign military or intelligence-entities. These attackers are usually attempting to gain some military, political, or strategic advantage, and will attack the availability and integrity of systems to undermine the trust of the public or leaders. APTs usually target critical infrastructure facilities, military organizations, government agencies, or related public or private, non-governmental organizations to compromise and disrupt their operations or steal information.

Disruption of air travel at key airports could cause system-wide service disruptions or result in casualties, both of which would critically damage public trust and confidence in the entire National Airspace System [3]. In the past, BlackEnergy, Patchwork Elephant, APT 13, Anchor Panda, APT18, the Elderwood Platform, and the Helsing APT have targeted transportation sector systems.

Cyber-mercenaries

Attackers with this motivation are usually aligned with sophisticated organized cybercrime entities, or foreign governments that wish to steal or damage confidential or proprietary information from private and public companies. This type of attacker often seeks significant monetary gain, or social activist or corporate strategic goals. Airport planning, construction, budget, and public- or government-relations documents are examples of tempting targets for cyber-mercenaries that are intent on commercial espionage [4].

Hacktivist

A wide variety of individuals and groups engage in cyber attacks aimed at disrupting or disabling access to resources. They carry out their attacks for a range of reasons—from political protest and attempts at economic harm to simple amusement or to gain status within their peer group. These attacks are most often conducted by vandals, activists, or outsiders with an overarching agenda. They usually target networks or systems to deny user access, inflict damage, or steal or corrupt data. An example of this type of attack in the airport environment would be an attacker who attempts to prevent access to the airport website by flooding the site with more traffic than the site can handle (i.e., a distributed denial-of-service [DDoS] attack). Another example would be an attacker, seeking to expose perceived wrongdoing by airport management, who steals and publishes the contents of airport management email and executives' personal information on a site such as WikiLeaks or HackerForums. [4].

Cybercriminals

Cybercrime is perhaps one of the most rapidly growing areas of attack activity. These attacks are often less sophisticated than the other types of attacks discussed above, but over the last few years, cybercrime techniques and tools have improved and become much easier to obtain and use. These attackers usually target networks and systems directly for data they can steal and resell, such as customer identification, credit card, or banking information. Also, by using ransomware or destructive malware, actors can encrypt or destroy data, or threaten exposure of sensitive communications and information unless the victim pays a fee. Airport systems that handle credit card information parking services or baggage fees would be prime targets for these attackers [4].

Terrorists

Airplane crashes receive massive media attention and incite widespread fear in a population as the reliability and consistency in travel vectors is pivotal to a stable nation. Transportation hubs are defined by massive crowds of travelers rushing about in a shared and focused chaos. As a result, airports and other travel hubs are the ideal locations and default target of terrorist groups that either aim to harm many people or that design their machinations to allow them to remain anonymous and potentially escape the scene.

The vulnerabilities inherent in OT systems and associated IT networks could be exploited by terrorist organizations in a number of ways, from remotely fabricating a disruption that causes potential victims to aggregate in a desired location (e.g., a baggage claim) to dangerously affecting a subsystem that is vital to the safety of an incoming or departing aircraft.

Vulnerable Systems

The airport ecosystem and its underlying supply chain is a complex amalgamation of IT and OT systems. Virtually every one of its systems could jeopardize the safety of passengers if compromised by a creative cyber adversary. While studies exist that evaluate attackers' potential to hack in-flight airplanes, ICIT has focused this publication on highlighting the risk posed by under-secured OT support systems that are not likely to be prioritized in traditional security reviews.

Avionics Software

The recent crashes of two Boeing 737 Max commercial airliners -- Lion Air flight 620 in October and Ethiopian Air flight 302 in March – may have been the result of software errors in two subsystems; the angle of attack sensor -- a vane that measures the plane's angle in the air -- and the anti-stall system called MCAS [5].

Planes depend on millions of lines of code to operate safely. Poorly developed code, which is often the result of irresponsible development practices on the part of the airline or its suppliers, can result in errors or vulnerabilities that can be exploited by bad actors and result in catastrophic impacts.

Baggage Handling

Baggage-handling systems are designed to ensure that a person and their luggage arrive at the same destination at the same time. Disrupting baggage handling networks may seem trivial; however, they are some of the most accessible systems for attackers to compromise and offer some of the most diverse impacts. Baggage systems are among the most customer-facing OT system found in airports and are attractive targets because the adversary does not need to board a plane, or depending on the layout of the airport, even go through security to attack it. The attacker can compromise the systems by phishing an employee, injecting OT-specific malware onto the airport IT network, and then laterally navigating to the baggage handling system. Once the system is infected, the adversary could cause delays, disrupt operations, redirect luggage to other flights or airports, or prevent a bag from undergoing a secondary security screening.

From a national security perspective, this means adversaries can leverage this type of attack to smuggle illicit or dangerous substances on to a plane, steal sensitive personal items, or precision target the belongings of traveling intelligence personnel and steal their stowed electronic devices or other sensitive media [6]. In a complex attack scenario, a sophisticated adversary might redirect a piece of luggage, inject malware onto a stowed device, and then return the luggage to the queue so that an unsuspecting critical infrastructure operator remains unaware that their device is now infected with malware that could reveal operational details or further infect networks in secure facilities.

Aircraft Tugs

Aircraft tugs are vehicles that latch onto the wheel bar or axle of a plane and guide it into a gate to connect the jet bridge and other deplaning equipment. Modern tugs are wireless, and it is expected that the next-generation of tugs may be wireless, driverless, and IT connected. Tugs leverage sensors and calibration parameters such as weight and size of aircraft to determine operations such as the velocity to approach a gate. If an attacker injected malware onto tugs, they could back a large aircraft into the airport itself by forcing the system to use the parameters for a smaller and lighter aircraft instead. A more nuanced attack scenario might leverage the tug to damage the landing equipment of an airplane bound for a targeted destination [6].

De-icing Systems

Airplane de-icing relies on on-site OT devices that regulate and maintain the composition of critical de-icing chemicals prior to their application to the plane. Planes must be de-iced because at typical cruising altitudes (around 35,000 feet), temperatures dip as low as minus 60 degrees Fahrenheit and dangerous ice could form on the body of a plane. If those systems were attacked and the composition of the solution were altered, dangerous ice could build on the body of an aircraft.

In the right weather conditions, hacking de-icing systems could cause a crash without explosives, and the event may not even be recognized as an attack unless authorities were aware of the threat. Even a single millimeter of ice can dramatically affect the aerodynamics and maneuverability of a plane. [6]. Simply put, without the application of the correct de-icing mixture, the safety of a plane and its passengers and crew is in serious jeopardy.

Fuel Pumps

Planes are refueled at airports by either fuel trucks or hydrants that pump gas from storage tanks in the ground. These storage tanks, are connected via underground pipes that use OT systems to regulate the valves, controls, and equipment used to store, transfer, and dispense various types of jet fuel used by commercial aircraft. If an adversary compromises a network, they could laterally access the fuel farm systems and cause the wrong type or mixture of fuel to be pumped into a plane, thereby resulting in a wide range of issues from engine problems to a possible explosion [6].

Airport Smart Devices

Airport devices can be tampered with in a variety of unauthorized ways ranging from remote digital compromise to the injection of malware through physical media. Smart devices include IoT components, sensors, and other systems that bridge IT and OT networks. The unauthorized modification of smart devices could entail the manipulation of data at central reservation systems, administration IT systems, and an airport's stored sensor data. The threat of tampering also includes unauthorized modification of hardware or software with data deletion or corruption, which can affect the behavior of airport's self-serving systems like automatic check-in machines, passport control gates, and smart building management systems. As a result, attackers can potentially gain control over systems and result in physical safety breaches that severely impact an airport's security [4].

Third-Party Systems

In early April 2019, Several U.S. airlines including Southwest Airlines, American Airlines, Delta Air Lines, United Airlines, Alaska Airlines, and JetBlue experienced issues with their computing systems leading to flight cancellations and delays due to IT issues faced by the third-party contractor Aerodata which "offers aircraft performance data, weight, and balance data, and load planning services to the airline industry to support approximately 21,000 flights per day." According to a customer case study issued by VMware, AeroData’s “AeroData’s flight deck client-server application is the last application used by pilots before the aircraft entry door is closed prior to takeoff. As a result, just five minutes of system downtime can result in over 100 delayed flights and loss of revenue.”

Generally, an adversary can more easily compromise a third-party vendor network than that of a critical infrastructure organization. In cases such as AeroData, where one entity provides services to numerous airlines serving hundreds of flights per day, an attacker may be able to inflict significant impacts with minimal effort through targeted ransomware, wiper malware, or similar attacks [7].

Facial Recognition

JetBlue, Delta, and other major airlines are experimenting with implementing facial recognition as a means of expediting the boarding process. According to NBC news coverage, the information from the scan will only be used once and will be deleted out of the system within a few hours. Photos will then be securely transmitted to the Customs and Border Protection (CBP) database where they are cross-referenced against passport photos. Airlines do not have direct access to the photos, do not store them, and will be dependent on the determination of the remote CBP database. For the process outlined above to be secured, airports, airlines, and CBP must collaborate to verify the integrity of the data in storage, transmission, and processing so that the integrity of the received results can be assured. If systems are not properly secured, adversaries could conduct man-in-the-middle attacks to either falsely approve dangerous individuals for travel or falsely flag innocent individuals for detainment [8].

Mitigating Threats to Airport Technology

Airport security is a top concern for law enforcement, homeland security officials and passengers alike; however, it is critical that cybersecurity be prioritized as much as physical security in the defense of airports and other transportation hubs. Currently, it may be possible for adversaries of every level of sophistication to launch hybrid cyber-kinetic attacks against air travel IT and OT systems, the majority of which were not developed with layered security throughout their development lifecycle, and wreak havoc on a national and global scale.

Airports rely on a complex network of IT and OT systems that if compromised due to a lack of security-by-design or a lack of a layered security could pose significant risks to the safety of passengers and crew. Poorly designed or inadequately secured avionics software can cause a plane to crash from a software glitch or a malicious exploit. Baggage handling systems may be compromised to facilitate the theft of items or the smuggling of dangerous substances. Hacked aircraft tugs may prevent an incoming craft from decelerating properly. Attackers could alter the settings in exposed de-icing systems so that pilots lose control of planes at high altitudes. Explosions may be possible from cyber-kinetic attacks on fuel pump subsystems. Smart devices and sensors could leak sensitive data to cybercriminals and other adversaries. Third party systems may be compromised to laterally navigate malware onto airport networks or to disrupt operations at multiple airports simultaneously. Facial recognition systems could be subject to man-in-the-middle attacks that allow prohibited individuals to bypass security and enter the country. The scenarios seem endless.

Airport executives, policymakers, technology manufacturers and law enforcement need to understand the threat landscape surrounding airport technology and the risk that passengers are being exposed to by not properly securing IT and OT systems. Some of the measures that can be taken to improve airport cybersecurity include:

- Acquisition requirements for avionics software and OT systems should include guidance around minimum standards on security-by-design and layered security controls at each stage of development
- Legacy equipment should be replaced with secure modern alternatives.
- Comprehensive risk assessments and penetration tests should be conducted to help to identify vulnerabilities that adversaries could exploit to enter the network.
- Robust cybersecurity criteria for IT and OT systems connected to airport infrastructure should be developed by the regulatory and legislative community

Securing the technology that runs our nation's airports is a challenging problem that requires engagement with a complex supply chain. The risks of inaction, however, are too significant to not act with urgency to protect passengers and crew from current and future threats.

Sources

[1] V. Singhal, "Airport Cyber Attack Risks", *Cyberbit*, 2019. [Online]. Available: https://www.cyberbit.com/blog/ot-security/airport-cyber-attack/. [Accessed: 30- Apr- 2019].

[2] S. Gohil, "Airport Cybersecurity Risks Rise amid Rapid Digitalisation", *Computer Business Review*, 2018. [Online]. Available: https://www.cbronline.com/news/airport-cybersecurity-risks. [Accessed: 30- Apr- 2019].

[3] "Quick Guide for Airport Cybersecurity", *Sskies.org*, 2019. [Online]. Available: https://www.sskies.org/images/uploads/subpage/PARAS_0007.CybersecurityQuickGuide.FinalReport.pdf. [Accessed: 30- Apr- 2019].

[4] G. Lykou, A. Anagnostopoulou and D. Gritzalis, "Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls", *NCBI*, 2019. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6339064/. [Accessed: 30- Apr- 2019].

[5] D. Griffin, "Boeing whistleblowers report 737 Max problems to FAA", *Www-m.cnn.com*, 2019. [Online]. Available: https://www-m.cnn.com/2019/04/26/politics/faa-hotline-reports/index.html?r=https%3A%2F%2Fwww.google.com%2F. [Accessed: 30- Apr- 2019].

[6] E. Almer, "Airports & Operational Technology: 4 Attack Scenarios", *Dark Reading*, 2019. [Online]. Available: https://www.darkreading.com/vulnerabilities---threats/airports-and-operational-technology-4-attack-scenarios-/a/d-id/1334282. [Accessed: 30- Apr- 2019].

[7] S. Gatlan, "U.S. Airlines Cancel, Delay Flights Because of Aerodata Outage", *BleepingComputer*, 2019. [Online]. Available: https://www.bleepingcomputer.com/news/technology/us-airlines-cancel-delay-flights-because-of-aerodata-outage/. [Accessed: 30- Apr- 2019].

[8] J. Olabanji, "'Did I Consent?' JFK Traveler Unsettled by New Facial Tech", *NBC New York*, 2019. [Online]. Available: https://www.nbcnewyork.com/news/local/Facial-Recognition-Technology-at-Airports-Sparks-Privacy-Concerns-508974851.html. [Accessed: 30- Apr- 2019].