Airports & Operational Technology: 4 Attack Scenarios

Reference: Memo [190404-2] Date: 04/04/2019 - Version: 1.0
Keywords: Transportation, Aviation, Airports

Key Points

- Security in global aviation is increasingly dependent on vulnerabilities in information technology (IT) and operational technology (OT) systems.
- Airports are using several critical OT systems (e.g. baggage control, runway lights, air conditioning, and power).
- More than a hundred unique exploits have been spotted since the publication of proofs of concept and payload creation tools, after the disclosure.
- Four important risk vectors have been more specifically identified: Baggage Handling, Aircraft Tugs, De-icing Systems, Fuel Pumps.

Summary

A recent article relayed by the US Aviation Information Sharing & Analysis Centre (A-ISAC) is focusing on vulnerabilities across airport operational technology (OT) networks. Critical airport systems making use of OT include baggage control, runway lights, air conditioning, and power, and they're managed by means of network-connected digital controllers. According to the article, they are much less organised than conventional IT networks, are rarely monitored as closely, and are often left untouched for years. It's an emerging threat that has sparked the attention of dozens of airport Chief Information Security Officer(s). The article goes on and identify four important risk vectors.

- Threat 1: Baggage Handling. These systems are extremely attractive targets for an attack because they can be executed remotely; the attacker wouldn't even need to board the plane. All that's required is for a single person to fall for a simple phishing email and an attacker can introduce OT-specific malware into the airport network. This malware will find its way to the baggage handling system to execute the attack.
- Threat 2: Aircraft Tugs. Attackers could potentially hijack a tug's weight sensors and back a large jet into a gate at the velocity used for a small plane, causing it to crash through the wall of the airport.
- Threat 3: De-icing Systems. The liquid chemicals used for de-icing are stored at on-site facilities. These facilities use OT devices to regulate and maintain the composition of de-icing chemicals. If those systems were attacked and the composition of the solution altered, this could easily cause ice to form on the body of a plane. Tampering with the aerodynamics of a plane by hacking into de-icing systems is one way to cause it to crash without loading explosives onto it, which is likely why as obscure a risk vector as it is, de-icing systems are often one of the first OT systems airports monitor.
- Threat 4: Fuel Pumps. An attacker could, for example, hack into a fuel farm, causing the wrong type or mixture of fuel to be pumped into a plane, resulting in anything from engine problems to an explosion.

Comments

Security in global aviation is increasingly dependent on vulnerabilities in information technology (IT) and operational technology (OT) systems.

OT is usually defined hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices such as valves, pumps, etc.

Security reports published in aviation sector emphasis the increased IT/OT and Internet of Things (IoT) convergence in avionics, navigation, communications and passenger information systems, in-flight and ground services. The hyper-connectivity in aviation and aviation-related systems increases complexity in managing security risks.