White Paper

Cybersecurity: A New Style of Risk for Aviation

April 2020

CCX Technologies Inc.
1525 Carling Ave. Suite 201
Ottawa, ON, K1Z 8R9 Canada

Cybersecurity: A Unique Problem for Aviation

Cybersecurity is a unique and growing concern for the aviation industry. It is increasingly clear that traditional approaches is leaving avionics equipment and aircraft networks open to vulnerabilities. A new approach is needed to ensure the security of aircraft equipment and data is improved.

The Traditional Approach to Cyber Security

Traditionally the aviation industry has used extensive analysis and testing to verify the integrity of products installed on aircraft. All the requirements of a device or system are verified during development and installation, using industry-defined procedures, guidelines, checklists, and best practices.

The level of scrutiny given to a specific product is dependent on its use. For example, equipment used for safety-critical functions is given more scrutiny than equipment used for cabin entertainment.

As a result, once a piece of equipment is installed, it is assumed to be correct. The update process for an installed piece of equipment typically requires a technician's intervention and physical access to the equipment, which can be inconvenient and costly. Inconvenient because it means aircraft down-time and costly because of the need to potentially remove the piece of equipment.

This traditional means of using data was the basis of defining a standard for network security, RTCA DO-326A. While a great starting point, this standard does not address the entire problem. Equipment cybersecurity is a unique new problem, and this traditional approach alone is not enough.

Static Analysis Isn't Enough

The traditional approach, where aircraft systems are isolated for analysis and tested as a single entity, does not recognize a fundamental change in the aircraft's network ecosystem. In the last two decades, these once separate systems have become increasingly interconnected.

This new interconnectedness has added an incredible amount of new utility. For example, it provides a means to perform data analytics to optimize aircraft operations and reduce operating costs. The more data that can be collected from these previously isolated networks, the more effective will be the pursuit of enhanced safety.

" In the last two decades, these once separate systems have become increasingly interconnected. "

When these interconnections are added, they are analyzed for network security impacts using traditional static analysis techniques, analyzing the implementation vs. known vulnerabilities as defined in RTCA DO-326A and other standards. Once again, this is a good starting point but since new vulnerabilities are constantly being discovered and exploited, it isn't enough.

For instance, before the discovery of the Spectre and Meltdown vulnerabilities[1] it was believed that two virtual machines running on the same processor could be completely isolated. This architecture could even have been used in Integrated Modular Avionics Systems to separate system software designed for different safety levels. We now know that this assumption is no longer valid. Systems

[1] https://meltdownattack.com/

analysed and found compliant using RTCA DO-326A before this discovery would have been approved. Those after this discovery could possibly require updates.

Even if a system is updated to include all known vulnerabilities there is no way of knowing the impact of undiscovered or undisclosed vulnerabilities. It is imperative that these networks are monitored to identify previously unknown and undetected nefarious activity. They must also be designed in a way that permits easy software and configuration updates so that access to equipment or features with newly discovered vulnerabilities can be blocked, and eventually patched to remove the vulnerabilities.

"It is imperative that these networks are monitored to identify previously unknown and undetected nefarious activity."

Unintended Interconnects

In addition to intended interconnects are unintended network interconnects that weren't anticipated when the systems were designed and installed. Hackers are persistent in discovering unintended interconnects. For instance, it is possible to record keystrokes on an air-gapped computer keyboard from a nearby Wi-Fi Access Point[2]. The deployment of Stuxnet demonstrated that it is possible to damage a physical system operating on an air-gapped network[3], and security researchers have shown that it is possible to use power-lines and pre-installed malware to bridge networks[4].

[2] https://threatpost.com/keystroke-recognition-uses-wi-fi-signals-to-snoop/120135

[3] https://en.wikipedia.org/wiki/Stuxnet

[4] https://www.secureworldexpo.com/industry-news/can-you-jump-air-gap

These are just a few of the exploits that CCX Technologies is aware of. With the resources of dedicated state-sponsored actors, new complex exploits are being developed daily, and are largely unaddressed by classic standard operating procedures.

A New Approach is Required

In the face of an ever-changing cybersecurity landscape a new approach is required to ensure the integrity of all networks on an aircraft. The persistent monitoring of all onboard networks and avionics data buses, including passenger entertainment networks, maintenance networks, and data-bus networks such as ARINC-429, and MIL-STD-1553 is a must.

The attacker only needs to be right once, with a new and novel approach. No existing TSO, STC, Cert. plan, air gapped or segregated networks can address unknown or newly discovered network vulnerabilities.

Understand more about avionics systems and cybersecurity.

Visit ccxtechnologies.com or call us:

+1 613 703 6161