THE WALL STREET JOURNAL.

http://www.wsj.com/articles/faa-officials-discuss-standards-to-neutralize-cyberattacks-1466081595

TECH

FAA Officials Discuss Standards to Neutralize Cyberattacks

Experts seek to create safeguards able to track and isolate hostile intrusions

An airplane flying between the air-traffic control tower and the Washington Monument at Washington's Ronald Reagan National Airport in 2015. Regulators and industry officials are increasingly focused on devising standards to ensure that cyberattacks against aviation are detected and neutralized. *PHOTO: ASSOCIATED PRESS*

By **ANDY PASZTOR**

Updated June 16, 2016 7:10 p.m. ET

WASHINGTON—Even as U.S. and European regulators jointly pursue ways to fend off cyberattacks against aviation, they are increasingly focused on devising standards to ensure that any successful hackers will be detected and neutralized.

Those twin goals are being widely discussed at an international safety conference here this week, while new details emerge about proposed safeguards being developed by a Federal Aviation Administration-created panel of government and industry officials.

These experts envision that future aircraft systems will be designed with the assumption that some hacking efforts eventually are likely to succeed. But the long-term solution, they said, is to create robust safeguards able to identify, track and isolate

RELATED

- Panel Reaches Preliminary Agreement on Airliner Cybersecurity Standards (http://www.wsj.com/articles/panel-reaches-preliminary-agreement-on-airliner-cybersecurity-standards-1465848030)
- U.S., European Aviation Authorities at Odds Over Cybersecurity (http://www.wsj.com/articles/u-s-european-aviation-authorities-at-odds-over-cybersecurity-1450816124)
- Airline Trade Group Warns About Cybersecurity Threats (http://www.wsj.com/articles/airline-trade-group-warns-about-cybersecurity-threats-1436444810)
- (http://www.wsj.com/articles/airline-trade-group-warns-about-cybersecurity-threats-1436444810) U.S. Panel Aims to Shield Planes From Cyberattack (http://www.wsj.com/articles/u-s-panel-aims-to-shield-planes-from-cyberattack-1435537440)

hostile intrusions while maintaining the integrity of critical safety functions.

The recommendations are scheduled to be delivered to the FAA in August.

As airliners, business jets and even small private aircraft become more connected to various ground and satellite systems, cybersecurity is "a huge issue we need to think about," FAA chief Michael Huerta told the conference earlier this week.

Afterward, Mr. Huerta said in a brief interview that "as you rely on broader networks" to swap data, "you have to build many layers" of protection. But at the same time "you have to assume at some point, someone is going to break through" that safety net, he added, and then the most important factor will become "how do you isolate it, how do you track it?"

By drafting a range of cybersecurity protections for operators spanning different types of aircraft, industry and government experts are "actually telling them there is likely to be a hack" at some point, according to Jens Hennig, co-chairman of the international advisory committee set up by the FAA.

At this point, experts agree there hasn't been a single verified incident in which a commercial airliner's flight controls, engine controls or other key safety systems have been hacked.

Since roughly 2005, the FAA has issued about 3,000 emergency airworthiness directives mandating immediate fixes to commercial jets. However, Peter Skaves, the agency's chief scientific and technical adviser on cyber issues, told the conference "we've never written one on information security."

Nevertheless, cybersecurity concerns are increasingly shaping the industry's work on advanced navigation computers, automated maintenance-messaging systems and air-

traffic control upgrades.

For starters, regulators and industry leaders expect to dissect cybersecurity incidents as though they were traditional accidents, according to Luc Tytgat, head of strategy and safety management at the European Aviation Safety Agency. “There is always a need to reconstruct” them, he said during the conference. EASA hopes to have a comprehensive cybersecurity plan in place by the end of 2018.

The European agency expects, among other things, to vet continuing air-traffic control modernization projects and existing maintenance-messaging systems for cyber vulnerabilities, according to Mr. Tytgat. Such efforts, he said, underscore that “this is a message of caution” because threats can come from any segment of aviation operations.

EASA also worries progress may be impeded by “reluctance of the operators” to share details about hacking “experiences that may have been painful” and could damage corporate reputations, according to Mr. Tytgat.

In the U.S., the FAA is sponsoring an array of research, partly seeking to reassure itself that ever more sophisticated cabin entertainment systems installed on jetliners don’t pose hazards for safety systems.

Agency officials “really want to make sure” there is a firewall separating the two domains and “a connection path can never happen” to allow data to flow between them, according to Mr. Skaves. On older jetliners, such migration is physically impossible but that isn’t the case with newer models.

John Craig, Boeing Co.’s chief engineer for network systems, told attendees the Chicago plane maker started carefully assessing potential cyberthreats to its aircraft as far back as the mid-1990s—beginning with software upgrades to the Boeing 777 at remote locations. “We’re trying to leverage” established safety practices to control cyberthreats, Mr. Craig said, by “trying to parallel some procedures and practices” that have successfully driven down accident rates.

But big challenges remain to protect safety applications . “The whole industry is continuing to refine what we’re doing to monitor” cyberthreats, according to Mr. Huerta.

Write to Andy Pasztor at andy.pasztor@wsj.com

What To Read Next...