Sign In | Register

CSO

PRIVACY AND SECURITY FANATIC
By Ms. Smith, CSO
NOV 12, 2017 10:33 AM PT

About
Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

TODAY'S TOP STORIES

Homeland Security team remotely hacked a Boeing 757

A Department of Homeland Security official admitted that a team of experts remotely hacked a Boeing 757 parked at an airport.

During a keynote address on Nov. 8 at the 2017 CyberSat Summit, a Department of Homeland Security (DHS) official admitted that he and his team of experts remotely hacked into a Boeing 757.

This hack was not conducted in a laboratory, but on a 757 parked at the airport in Atlantic City, N.J. And the actual hack occurred over a year ago. We are only now hearing about it thanks to a keynote delivered by Robert Hickey, aviation program manager within the Cyber Security Division of the DHS Science and Technology (S&T) Directorate.

[Read also Elon Musk's top cybersecurity concern: Preventing a fleet-wide hack of Teslas. | Get the latest from CSO by signing up for our newsletters.]

"We got the airplane on Sept. 19, 2016. Two days later, I was successful in accomplishing a remote, non-cooperative, penetration," Hickey said in an article in Avionics Today. "[That] means I didn't have anybody touching the airplane; I didn't have an insider threat. I stood off using typical stuff that could get through security, and we were able to establish a presence on the systems of the aircraft."

While the details of the hack are classified, Hickey admitted that his team of industry experts and academics pulled it off by accessing the 757's "radio frequency communications."

Commercial airliner vulnerabilities a concern for years

We've been hearing about how commercial airliners could be hacked for years.

You might remember when a governmental watchdog admitted that the interconnectedness of modern commercial airliners could "potentially provide unauthorized remote access to aircraft avionics systems." The concern was that a hacker could go through the Wi-Fi passenger network to hijack a plane while it was in flight.

And in a 2015 report by the U.S. Government Accountability Office (pdf), the agency warned, "Internet connectivity in the cabin should be considered a direct link between the aircraft and the outside world, which includes potential malicious actors."

At the time, U.S. Rep. Peter DeFazio (D-Ore.) said, the "FAA must focus on aircraft certification standards that would prevent a terrorist with a laptop in the cabin or on the ground from taking control of an airplane through the passenger Wi-Fi system."

The same year, security researcher Chris Roberts ended up in hot water with the feds after tweeting about hacking the United Airlines plane he was traveling on. The FBI claimed Roberts said he took control of the navigation.

A Hack In The Box presentation by Hugo Teso in 2013 suggested that thanks to the lack of authentication features in the protocol Aircraft Communications Addressing and Report System (ACARS), an airliner could be controlled via an Android app. Flight management software companies, as well as the FAA, disputed Teso's claims.

All of that means that airline pilots have heard of those vulnerabilities before, too. Yet at a technical meeting in March 2017, several shocked airline pilot captains from American Airlines and Delta were briefed on the 2016 Boeing 757 hack. Hickey said, "All seven of them broke their jaw hitting the table when they said, 'You guys have known about this for years and haven't bothered to let us know because we depend on this stuff to be absolutely the bible.'"

As CBS News pointed out, Boeing stopped producing 757s in 2004, but that aircraft is still used by major airlines, such as American, Delta and United. President Trump has a 757, and Vice President Pence also uses one. In fact, Avionics Today claimed 90 percent of commercial planes in the sky are legacy aircraft that were not designed with security in mind.

Boeing told CBS that it firmly believes the test "did not identify any cyber vulnerabilities in the 757, or any other Boeing aircraft."

Furthermore, an unnamed official briefed on the test told CBS the results of the hack on an older aircraft was good information to have, adding, “but I’m not afraid to fly.”

Next read this:

- *How to prevent data loss with Windows Information Protection*
- *6 new and noteworthy security features in Windows 10 Fall Creators Update*
- *How AI can help you stay ahead of cybersecurity threats*
- *Preparing for GDPR compliance: Where you need to be now and how to get there*
- *Shadow cloud apps pose unseen risks*

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

Follow

New! Download the State of Cybercrime 2017 report

You Might Like

Ads by Revcontent

Vancouver Casino Accidentally

Iconic 'Pretty Woman' Scene Has One

Strange Link Between Eggs and Diabetes

Remember Fabio? Try Not to Gasp when

Canada: People Are Cancelling Their Netflix

The Tribune PensAndPatron HealthHackTips MommyThing My Finance Today

They Installed This "Stealth" Camera and
Tech4you

The Unusual Link Between Coconut Oil and
Memory Repair

You Won't Believe What She Caught
Tech4-you

Best Security Hidden Camera: Find out What's
Tech4you

Start Your Home Woodworking
WoodProfits.com

Copyright © 2017 IDG Communications, Inc.