the Availability Digest

www.availabilitydigest.com
@availabilitydig

Can An Airliner Be Hacked?

May 2015

Joining the Internet of Things (IoT) is airliner avionics. The flight controls of major jets are controlled by complex computers that connect to major flight systems by an Intranet-like Ethernet bus using IP addresses. In many airliners, the passenger in-flight entertainment systems (IFEs) are also connected by an Intranet; and in some cases these networks are not segregated. Rather, they are separated by firewalls.

Could a hacker access a plane's flight controls via the IFE system while sitting in his seat? Manufacturers, airlines, and experts say no. Chris Roberts says yes and claims that he has done it.

The Airline Hacking Achievements of Chris Roberts

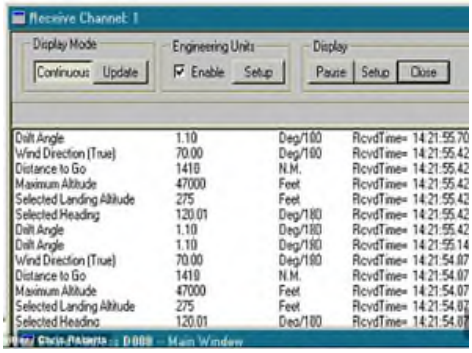
Chris Roberts is the founder of One World Labs, a security intelligence firm that identifies risks before they are exploited. About six years ago he became interested in the issue of airline hacking via the IFE system.

With a research colleague, he obtained publicly available flight manuals and wiring diagrams for various commercial passenger jets. The diagrams showed how, on some planes, the IFE systems were connected to the passenger satellite phone network and were in turn connected to the planes' cabin control systems and the planes' avionics systems.

Roberts built a test lab to explore what he could do with an airliner's networks and found successful ways to hack into the avionics systems from the IFE systems. He spoke to several airplane manufacturers with little success, and gave a presentation on his findings at the BSides security conference in Las Vegas. Based on his work, Roberts has been issuing warnings about vulnerabilities in IFE systems for six years.

Last February, the FBI requested a meeting with him. The meeting was followed up by another in March. Roberts said he had identified vulnerabilities with IFE systems on Boeing 737-800, 737-900, 757-200, and Airbus-320 aircraft. Roberts disclosed that he had sniffed data traffic over the avionics networks on more than a dozen flights after connecting his laptop to the IFEs. He gained access to the IFEs via a Seat Electronics Box (SEB) located underneath each row of seats. He was able to pry the cover of the SEB located under his seat and connect his laptop to it with an Ethernet cable.

He claimed that he had compromised systems about fifteen to twenty times from 2011 through 2014 and was able to sniff cockpit data. In a previous tweet, he had posted pictures containing details of aircraft data. He was furnishing this information because he would like to see the vulnerabilities fixed.



However, he claimed to the FBI that he had hacked the avionics network only in simulation in his laboratory.

One Joke Too Many

On a United Airlines flight from Denver to Chicago on April 15, 2015, frustrated after years of trying to get Boeing and Airbus to heed his warnings about security issues with their passenger communications systems, Roberts got into trouble when he jokingly tweeted that he could deploy the cabin's oxygen mask system:

> "Find myself on a 737/800, let's see Box-IFE-ICE-SATCOM? Shall we start playing with EICAS messages? "PASS OXYGEN ON" anyone?"

(ICE is Inflight Communications Equipment, SATCOM is Satellite Communications, EICAS is Engine Indication Crew Alerting System).

Roberts was on his way to speak at a major security conference about vulnerabilities in modern transportation systems. In Chicago, he boarded a connecting flight to Syracuse, New York.

However, an employee with United's Cyber Security Intelligence Department became aware of the tweet and contacted the FBI. He told them that Roberts was on a connecting flight to Syracuse. At Syracuse, Roberts was escorted off the plane by two FBI agents and two police officers. His computer and iPad were seized and he was interviewed by the FBI for several hours before being released.

He was scheduled to board another United flight to his destination, but United barred him from any further flights. He finally was able to take an alternate flight.

The FBI Takes Action

The FBI tracked the plane in which Roberts was flying from Denver to Chicago and found that the cover of the SEB under his seat had been pried loose. However, Roberts claimed that the SEB damage was due to people shoving bags under their seats.

Roberts referenced research he had done years ago on vulnerabilities that would allow an attacker to access cabin controls and deploy a plane's oxygen masks. During the interception interview, Roberts showed FBI wiring schematics of multiple airplane models that were publicly available

Contrary to Robert's earlier statements, the search warrant issued by the FBI for the confiscation of his computers claims that his computers contain evidence that Roberts had commandeered the network of an inflight airplane using default user names and passwords. Having gained access to the network, the FBI claims that Roberts had overwritten code on the airplane's Thrust Management Computer to successfully issue a climb command. This caused one engine to increase power and thrust the airliner into a lateral movement. Roberts denies this, claiming that the FBI took this information out of context. (Note: This allegation has not been proven in a court of law. Roberts has yet to be charged with any crime.)

Following the interview, Roberts tweeted:

> "Over the last 5 years, my only interest has been to improve aircraft security."

The Government Weighs In

Following the FBI interview with Roberts, the TSA and FBI issued a bulletin to airlines to be on the lookout for passengers showing signs they may be trying to hack into an airplane's Wi-Fi or IFE system. It warned of security threats facing modern aircraft that might allow a hacker to take control of the airplane.

According to a U.S. Government Accountability Office report, which interestingly was issued the day before Roberts' joking tweet:

> "Modern aircraft are increasingly connected to the Internet. This interconnectedness can potentially provide unauthorized remote access to aircraft avionics systems. As part of the aircraft certification process, FAA's Office of Safety currently certifies new interconnected systems through rules for specific aircraft and has started reviewing rules for certifying the cybersecurity of all new aircraft systems."

A Boeing spokeswoman said that her company did indeed design a solution to address the FAA concerns. She wouldn't go into detail about how Boeing was tackling the problem but said Boeing was employing a combination of solutions that involved some physical air-gapping of the networks as well as software firewalls. "There are places where the networks are not touching, and there are places where they are," she said.

Opinions of Other Experts

According to other security experts, the situation is muddled. There have been cases where networks have not been properly segmented, leaving open vulnerabilities. Other law enforcement sources have said there is no evidence a hacker could gain control of an airliner's avionics network.

According to Bruce Schneier, a computer security specialist, Boeing 787 and Airbus A350 and A380 airliners have a single network that is used both by pilots to fly the plane and passengers for their Wi-Fi connections. The avionics and passenger systems are connected thorough a firewall that blocks malicious traffic between the two. However, there are no known vulnerabilities in these systems.

Bug Bounty Programs

Many companies have now initiated "bug bounty programs" in which they will pay hackers who report security bugs to them. Barracuda offers $50 to $3,133 for a disclosure. Cash bounty programs have been implemented by Google, Microsoft, and Facebook. Google will pay $500 to $50,000 depending upon the severity of the vulnerability. Facebook has paid out over $3 million in rewards since 2011. Adobe has a bug bounty program, but doesn't pay cash. Instead, it rewards points that enhance the submitters' HackerOne reputation score.

Bug bounty programs have become so common that a website has sprung up to support them. Dubbed Bugcrowd, the website provides bug bounty and penetration services. It currently has 220 active bounties, 33,150 security vulnerability submissions, and 14,300 researchers participating in its crowdsourced security program.

Some researchers feel that bug bounty programs only serve to encourage hackers. Supporters claim that these programs help incentivize people to report security vulnerabilities in a responsible manner.

United Airline's Bug Bounty Program

United Airlines is now offering the first bug bounty program in the airline industry. In order to be eligible for the bounty, submitters must:

be the first to submit a bug.
be a Mileage Plus member.
not reside in a country on the United States sanction list.
must not be an employee or family member of any Star Alliance member airline.
must not be the author of the vulnerable code.

Summary

Is Chris Roberts a hero, an irresponsible hacker, or a hoax? Only time will tell. But the story he brings to the table is compelling and one that speaks volumes to the security future of the Internet of Things.

Acknowledgement

Material for this article was taken from the following sources:

FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen, *U.S. Government Accountability Office*; April 14, 2015.
Feds Say That Banned Researcher Commandeered a Plane, *Wired*; April 15, 2015.
FBI Search Warrant; April 15, 2015.
Alleged airplane hack creates more questions than answers, *TechTarget*; April 18, 2015.
Security expert banned from ALL United flights after boasting he knew how to hack into aircraft controls and bring the plane down, *Daily Mail*; April 19, 2015.
Despite benefits, skepticism surrounds bug bounty programs, *TechTarget*; April 28, 2015.
Adobe's new twist on bug bounty programs: No cash for bug hunters, *TechTarget*; May 6, 2015.
Hacker told FBI he made plane fly sideways after cracking entertainment system, *APTN*; May 15, 2015.
FBI Investigating Claim Computer Expert Hacked Plane In-flight, *ABC News*; May 17, 2015.
Security researcher 'hijacked plan in-flight': questions and (some) answers, *Graham Cluley*; May 17, 2015.
FBI Claims Banned Researcher Admitted Hacking Plane Controls … But Is Someone Lying?, *Forbes*; May 18, 2015.
New scrutiny on bug bounties: Is there strength in numbers, *TechTarget*.
United Airlines bug bounty program, *United Airlines Web Site*.
Hacking Airplanes, *Schneier on Security*.