Security expert said he accessed plane controls mid-flight (Update)

May 18 2015, byCarolyn Thompson

Boeing 737-700 jet airliner. Credit: Wikipedia/Arcturu

A security researcher told federal agents he was able to hack into aircraft computer systems mid-flight numerous times through the in-flight entertainment systems, and at one point he caused a plane he was on to

move sideways, according to an FBI agent's affidavit.

Although the claims are still being investigated, the airline involved, United, cast doubt on whether it was possible to control an airplane through the entertainment system, while other experts said such cyber threats should be taken seriously given that airplanes are increasingly connected to the Internet.

The researcher, Chris Roberts, was questioned upon his arrival at the Syracuse, New York, airport April 15. He had suggested on Twitter while on a United Airlines flight from Chicago that he could get the oxygen masks to deploy or interfere with the cockpit's alert systems, according to the court filing in support of a search warrant for Roberts' laptop and other electronics.

Roberts founded One World Labs, which tries to discover security risks before they are exploited. He had met previously, in February and March, with the FBI to discuss vulnerabilities with in-flight entertainment systems aboard certain aircraft, the affidavit said. During the meetings, Roberts claimed to have compromised the systems 15 to 20 times between 2011 and 2014, using a cable to connect his laptop to an electronics box located beneath passenger seats, the document said.

"He stated that he thereby caused one of the airplane engines to climb resulting in a lateral or sideways movement of the plane during one of these flights," the affidavit said.

Roberts declined to comment Monday when reached at his Denver, Colorado, office. In a statement issued through his attorney, he said his "only interest has been to improve aircraft safety."

"Given the current situation, I've been advised against saying more," said the statement provided by Nate Cardozo, a staff attorney with the San

Francisco-based Electronic Frontier Foundation.

A report by the U.S. Government Accountability Office last month said some commercial aircraft may be vulnerable to hacking over their onboard wireless networks.

"Modern aircraft are increasingly connected to the Internet. This interconnectedness can potentially provide unauthorized remote access to aircraft avionics systems," the report said.

The fact that passengers on flights with in-seat video monitors can shift between television and a map showing the plane's real-time location indicates a link between the flight control and passenger entertainment networks, said Steven Bellovin, a computer science professor at Columbia University. And airplanes that offer Wi-Fi are likely using the same data link used by pilots to communicate with the airline, he said.

"Now the question is, what is the form of isolation between the passenger network and everything else?" Bellovin said. "There is some kind of linkage but there are different ways to do this—really securely and not particularly securely, and I have no way of knowing which has actually been done here."

After stopping Roberts from continuing on from Syracuse to California following his FBI interview last month, the airline cited Roberts' "claims regarding manipulating aircraft systems."

"However, we are confident our flight control systems could not be accessed through techniques he described," spokesman Rahsaan Johnson told The Associated Press.

In a statement, a Boeing spokesman said in-flight entertainment systems on airliners are isolated from flight and navigation systems.

Pilots have more than one navigation system, spokesman Alder said. "No changes to the flight plans loaded into the airplane systems can take place without pilot review and approval," he said, declining to discuss specific design features for security reasons.

Tim Erlin, director of IT security and risk strategy at the cybersecurity firm Tripwire, said it's possible that systems are connected in some aircraft and not in others.

"There are many different types of aircraft in service, with varying levels of technology from different time periods," Erlin said via email. "If a system was installed well before these kinds of attacks and tools were conceived of, there would have been no reason not to connect them, and it might have been perceived as extra cost and complexity to keep them separate."