

The ever-evolving cyber threat to planes

17 June 2015, by Eric Randolph



Some professional hackers say airline computer systems are riddled with weaknesses that could allow someone to break in

Hackers and cyber-terrorists present an ever-evolving threat to airlines, with experts constantly testing for new vulnerabilities—including the fear that drones could be used to throw a plane off course.

Most agree hacking a plane would be a near-impossible feat, but some professional hackers have claimed airline computer systems are riddled with weaknesses that could allow someone to break in, perhaps even through the in-flight entertainment system.

US computer security expert Chris Roberts recently claimed to have hacked into a plane's controls through the entertainment console and to have issued a "climb" command.

But speaking at the Paris Air Show this week, Alain Robic of Deloitte Consulting, an expert on cybersecurity, said the claims were not credible.

Robic was working for Airbus in 2005 when a hacker showed them how he could penetrate the flight controls from a passenger seat while they

were designing the new A380.

"The bosses were shocked. It was a revolutionary moment. They re-engineered everything to separate the systems so it could never happen again," said Robic.

But there are plenty of other risks—and although they are unlikely, companies such as Airbus and Boeing take them very seriously.

David Stupples, a professor of electronic and radio systems at City University in London, who advises Airbus, said the latest threat he was exploring was whether a drone could be used to send radio signals to an aircraft and confuse its systems.

"If I could get a signal to the aircraft that caused it to become confused while it's on its final approach, could I cause an incident? My view is yes," said Stupples, adding that flying near to the plane could allow the drone to overpower signals from the ground.

Stopping this kind of activity means preventing drones from flying near airports—something that has only recently become possible with new forms of radar capable of spotting tiny aircraft.

The enemy within



Experts are looking at the potential risk drones pose to aircraft

Stupples said there was a greater threat of an employee with access to the computer data hubs uploading malware to an aircraft's systems.

"It could be a dissatisfied employee, or someone who has been bribed or who is doing it for a cause," he said.

Even this would be almost impossible, since airlines have highly complex, specially designed computing systems that only a handful of people know how to navigate.

"Between the probability of someone understanding what they're doing, the probability of getting the malware in and the probability of it acting like they want—the odds are pretty remote," said Stupples.

Even if all those factors came together perfectly, hackers would almost certainly not be able to take full control of the aircraft since pilots have manual overrides.

"But to crash, all you have to do is push the flight control systems into an unstable situation," said Stupples.

"I wouldn't say it's easy, but it's possible."

'Constantly probing'

While public concerns tend to focus on the terrorist risk, companies face a much more immediate and frequent threat from hackers trying to steal their commercial secrets.



Airlines face threats from hackers trying to steal their commercial secrets

Hacks can cost tens of millions of dollars to repair and could be used to extort money by planting threats.

As aviation goes increasingly digital, threats have adapted.

"A lot of data is now automatically uploaded to planes so they can remove the risk of human error as much as possible," said a pilot for a major airline, who was not allowed to give his name.

Many airlines now issue their pilots and cabin crew with iPads because they weigh less than piles of charts and passenger logs.

"The airlines are ultra-strict with us about the security of our iPads and everything else—much stricter than with passengers because they worry about coercion, that our family has been kidnapped or something," said the pilot.

Robic said it was time for the whole aeronautic industry to create a joint cybersecurity organisation to combine their efforts.

"There is a whole eco-system of staff that needs to be secured. There are a great many actors from development to maintenance, which exposes [airlines](#) to cyber risks," he said.

"What they're doing at the moment is not sufficient."

© 2015 AFP

APA citation: The ever-evolving cyber threat to planes (2015, June 17) retrieved 25 June 2019 from <https://phys.org/news/2015-06-ever-evolving-cyber-threat-planes.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.