Aircraft Vulnerable to Cyber Attack

by Alex Dickinson via Kismo - The Courier Mail (QLD) *Sunday, Apr 3 2011, 8:47am*
international / mass media / other press

> *It's not news to hackers who, according to an unsubstantiated report, recently hacked into the systems of a military satellite -- an aircraft would be a simple matter by comparison.*

AIRCRAFT could be taken over by remote control and forced to crash with the use of newly invented computer software.

Cyber attacks are now viewed by experts as the second-biggest risk to aviation behind natural disasters.

Representatives from Qantas and Virgin Airlines were warned of the threat at the Asia-Pacific Aviation Security Conference in Hong Kong.

Australian cyber-security expert Ty Miller, from Pure Hacking, told the conference whole fleets of planes could be affected.

"The stereotypical Die Hard 2 airport attack, where aircraft controls can be taken over, is no longer just a movie script. It's an actual reality,'' Mr Miller said.

"Depending on what information was accessed . . . the control of the aircraft themselves could be compromised.

"You could deal with planes so that when they're in the air they all of a sudden start dumping all of their fuel, or force the planes to take a nose-dive. And it's not necessarily one plane it could be a whole fleet of planes.''

Mr Miller's firm engages in "ethical hacking'', which involves testing the security of a network by trying to crack its systems.

Posing as a rogue employee with general access to an airline's systems, Mr Miller was recently able to take over the airline's entire network within a day.

"That would give us full administrator access to the whole computer system and access to potentially sensitive documents and data,'' he said.

He cited the Stuxnet worm incident, where an unknown attacker last year used the software to sabotage one of Iran's uranium enrichment plants.

The Stuxnet attack overwhelmed the nuclear facility's internal network, causing it to go offline.

"The analysis of the Stuxnet attack (on Iran) showed that it would have required a team of five or ten people working for at least six months,'' Mr Miller said.

"It would have been extremely well funded, and the culprits would have had access to intelligence to conduct several multi-staged attacks on a number of different companies to perform industrial espionage.

"To compromise the avionics of an aircraft, hackers would have to have the same level of information and potentially need to hack into Boeing, the specific airline and the airport systems.''

A rogue employee was in fact more of a threat than terrorists, Mr Miller said.

http://tinyurl.com/3dnlzqq
