Hackers could haunt global air traffic control: researcher

July 27 2012

An air traffic controller monitors flights while working in the Terminal Radar Approach Control center in 2011 in Denver, Colorado. Air traffic control software used around the world could be exploited by hackers to unleash squadrons of ghost planes to befuddle those entrusted to keep the skies safe, a security researcher said Thursday.

Air traffic control software used around the world could be exploited by hackers to unleash squadrons of ghost planes to befuddle those entrusted to keep the skies safe, a security researcher said Thursday.

Cyprus-based Andrei Costin demonstrated his findings at a Black Hat gathering of cyber defenders that ends Thursday in Las Vegas.

"This is for information only," Costin said as he outlined how someone with modest tech skills and about $2,000 worth of electronics could vex

air traffic controllers or even stalk celebrities traveling in private jets.

"Everything you do is at your own risk."

Costin's target was an ADS-B system in place for aircraft to communicate with one another and with air traffic control systems at airports.

The system, which has been rolled out internationally in recent years in a multi-billion dollar upgrade, was designed to better track aircraft so airport traffic can flow more efficiently.

A perilous flaw is that the system is not designed to verify who is actually sending a message, meaning that those with malicious intent can impersonate aircraft either as pranks or to cause mayhem, according to Costin.

"There is no provision to make sure a message is genuine," he said.

"It is basically an inviting opportunity for any attacker with medium technical knowledge."

Air traffic controllers faced with a signal from a fake airplane resort to cross-checking flight plans, putting relevant portions of air space off limits while they work.

"Imagine you inject a million planes; you don't have that many people to cross-check," Costin said. "You can do a human resource version of a denial of service attack on an airport."

Denial of service attacks commonly used by hackers involve overwhelming websites with so many simultaneous online requests that they crash or slow to the point of being useless.

Aviation agencies are adept at identifying and locating "rogue transmitters" on the ground, but not at countering signals from drones or other robotic aircraft becoming more common and available, according to the researcher.

Another danger in the new-generation air traffic control system, according to Costin, is that position, velocity and other information broadcast by aircraft isn't encrypted and can be snatched from the air.

"Basically, you can buy or build yourself a device to capture this information from airplanes," Costin said.

He listed potential abuses including paparazzi being able to track private jets carrying celebrities or other famous people.

Costin showed how a friend was able to identify a plane broadcasting the identification numbers of Air Force One, the military jet used by the US president, and plot it on a map on an iPad.

"It can be a very profitable business model for criminals to invest a small amount of money in radios, place them around the world" and then sell jet tracking services or information about flights, the independent researcher said.

"If it was Air Force One, why does Air Force One show itself?" Costin wondered aloud. "It is a very high profile target and you don't want everyone to know it is flying over your house."

There are websites with databases matching aircraft registration numbers with listed owners.