Satellite telecom vulnerable to hackers, researchers find

April 17 2014, by Rob Lever

Federal Aviation Administration System Command Center in Herndon, Virginia, on August 12, 2002

Security flaws in many satellite telecommunications systems leave them open to hackers, raising potential risks for aviation, shipping, military and other sectors, security researchers said Thursday.

A paper released by the security firm IOActive found "multiple high risk

vulnerabilities" in all the satellite systems studied.

"These vulnerabilities have the potential to allow a malicious actor to intercept, manipulate, or block communications, and in some cases, to remotely take control of the physical device," the report said.

Ruben Santamarta, author of the report, said he was concerned "because satellite communications are used in a variety of critical scenarios."

Santamarta told AFP that most ships and aircraft use satellite communications, and in some cases military communications use these commercial satellite systems.

If the systems are compromised, he said, "for military communications, a foreign government or agency can target these devices and they can track the location of units and soldiers."

For aircraft or ships, he said, an attacker "can spoof data" and either block or disrupt emergency communications.

Because of the nature of the systems using satellites, Santamarta said, "we expected better security."

Santamarta said he had no evidence of any disruption affecting Malaysia Airlines flight MH370, but noted that "it is technically possible" that its communications could have been tampered with.

The IOActive report studied communications over the Inmarsat and Iridium satellite networks. But Santamarta said the vulnerabilities were mainly in ground equipment which connects to the satellites.

"IOActive found that malicious actors could abuse all of the devices within the scope of this study," the report said.

"The vulnerabilities included what would appear to be back doors, hard-coded credentials, undocumented and/or insecure protocols, and weak encryption algorithms."

The company began its research in 2013, and in early 2014, a security warning was issued by the Computer Emergency Response Team, a group of researchers backed by the US Department of Homeland Security.

IOActive said however that most of the satellite telecom (SATCOM) vendors did not respond to the January alert to upgrade their systems despite the nature of the risks.

"If one of these affected devices can be compromised, the entire SATCOM infrastructure could be at risk," the report said.

"Ships, aircraft, military personnel, emergency services, media services, and industrial facilities (oil rigs, gas pipelines, water treatment plants, wind turbines, substations, etc.) could all be impacted by these vulnerabilities."

Santamarta added, "I hope this research is seen as a wake-up call for both the vendors and users of the current generation of SATCOM technology."