



Boeing was concerned that the aircrafts' inflight entertainment system, which includes USB connections, could allow hackers to access a plane's computer. The Federal Aviation Administration granted Boeing permission to change its inflight systems five months ago.

"The integrated network configurations in the Boeing Model 777-200, -300, and -300ER series airplanes may enable increased connectivity with external network sources and will have more interconnected networks and systems, such as passenger entertainment and information services than previous airplane models," the U.S. Federal Register stated in a Nov. 2013 report. "This may enable the exploitation of network security vulnerabilities and increased risks potentially resulting in unsafe conditions for the airplanes and occupants."

Last year, a Spanish researcher showed it was possible to hack a plane using a mobile phone. According to WTOP, during a presentation in April 2013 at the Hack-In-The-Box security summit in Amsterdam, Hugo Teso allegedly proved that with an Android smartphone, a specific "attack code" and an Android app called PlaneSploit, he could hijack both a plane's system as well as the pilot's display.

The FAA quickly denied Teso's assertion that he could remotely commandeer a plane.

"The described technique cannot engage or control the aircraft's autopilot system using the FMS or prevent a pilot from overriding the autopilot," the FAA said in a statement following Teso's demonstration. "Therefore, a hacker cannot obtain 'full control of an aircraft' as the technology consultant has claimed."

