Spoofing CAN data frames in small aircrafts

Rapid7, a cybersecurity company in Boston (USA), reported that engine readings, compass data, altitude, and other readings could be manipulated.

Limit physical access to CAN networks to authorized persons (Source: Adobe Stock)

The vulnerability disclosure report is the product of nearly two years of work. It focuses only on small aircraft because their systems are easier for researchers to acquire. Large aircraft frequently use more complex systems and must meet additional security requirements. The DHS (Department of Homeland Security) alert does not apply to older small planes with mechanical control systems. The security flaw is registered under ICS-Alert-19-211-01.

The CAN data link layer does not provide security measures at all. Security can be added by means of authentication on higher-layer protocols. Giving some non-authorized people physical access, of course, could lead to a security flaw. “Using doors with no locks,” said Holger Zeltwanger, CiA Managing Director, “requires some other protection mechanism.” In avionics, you need to bypass physical security controls. In many countries, laws mandate such limited access only for authorized staff.

The “Stinger” transceiver by NXP, could be used to protect the CAN network on the data link layer against man-in-the-middle attacks. But if someone has physical access to the CAN network, devices can be exchanged easily. To detect this, you need security measures on the higher-layer protocols.

The Rapid7 researchers observed the network traffic and sent falsified data content in CAN data frames from an injected node using the same CAN-IDs as the original devices. This spoofing attack was successful transmitted (e.g. manipulating the oil pressure). The false oil pressure was shown on the CAN-connected display. The “hackers” achieved the same with compass data – attitude and heading values.

hz