Source: Adobe Stock

CAN security case in small aircrafts

In July, the US Department of Homeland Security (CISA) has issued a security alert warning owners of small aircrafts about vulnerabilities that can be exploited to alter airplane telemetry.

The vulnerabilities reside in avionics (electronic equipment fitted in an aircraft), and more specifically inside a small aircraft's CAN network. The attacker needs to have physical access to the CAN network to inject false data, resulting in incorrect readings in avionic equipment reported CISA. This in mind, such an attack is not very likely, because the access to aircrafts is highly regulated and controlled in most countries. Rapid7 examined two small aircrafts, but not discovered the brand names.

Patrick Kiley from the Rapid7 cybersecurity company was one of the researchers, who investigated in CAN network integrity in avionics systems: “After performing a thorough investigation on two commercially available avionics systems, Rapid7 demonstrated that it was possible for a malicious individual to send false data to these systems, given some level of physical access to a small aircraft’s wiring.” Such an attacker could attach a device to an avionics CAN network in order to inject false measurements and communicate them to the pilot. These false measurements can include the following:

- incorrect engine telemetry readings
- incorrect compass and attitude data
- incorrect altitude, airspeed, and angle of attack (AoA) data

“In some cases, unauthenticated commands could also be injected into the CAN network to enable or disable autopilot or inject false measurements to manipulate the autopilot’s responses,” said Kiley. A pilot relying on these instrument readings would not be able to tell the difference between false data and legitimate readings, so this could result in an emergency landing or a catastrophic loss of control of an affected aircraft.

As mentioned, physical access to the CAN network was needed to perform the attack. The CAN data frames were injected by a USB dongle linked to the CAN networks. The frames from the avionics devices were recorded using a Linux operating system running the CAN-utils software. “The system was reverse engineered by sending individual recorded CAN frames back onto the avionics bus and observing what effects they had with the various nodes,” explained Kiley. This reversing technique is particularly effective in CAN explorations compared to other networking environments, since CAN network implementations are often susceptible to replay attacks. In addition, Rapid7 modified various CAN data frames to observe any interesting effects. ▷

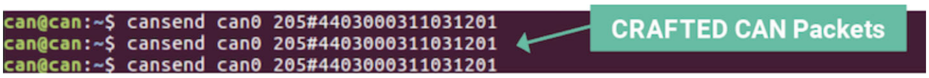

Figure 1: Crafted oil pressure CAN data frame (Source: Rapid7)

Findings in the first aircraft

The first examined avionic CAN network included the following devices:

- 10-inch glass panel combining the primary flight display (PFD) and the multi-function display (MFD)
- avionics concentrator
- engine Instrumentation controller
- electronic magnetometer (compass)
- attitude and heading reference system (AHRS)

Rapid7 researchers found out that CAN-ID 205_h contains the oil pressure, the oil temperature, and two cylinder head temperature values. “By sending crafted data frames using this CAN-ID, we were able to send false oil pressure, oil temperature, and cylinder head readings to the display,” said Kiley.

The compass uses the CAN-ID 241_h. The attitude and heading reference system (AHRS) transmits the CAN-IDs 281_h to 284_h with the AHRS acting as node 1. Nodes 2, 3, and 4 produce the CAN-IDs 291_h to 294_h, $2A1_h$ to $2A4_h$, and $2B1_h$ to $2B4_h$, respectively. The AHRS data frames were reverse engineered by spoofing messages from nonexistent AHRS units until the displayed aircraft attitude was changed, indicating an incorrect aircraft orientation.

The used higher-layer protocol does not provide any kind of built-in authentication mechanism. This is what makes the CAN communication easy to implement, but it also removes any assurance that the sending device was the actual originator of the provided data.

Finding in the second aircraft

The second examined avionic CAN network comprised the following devices:

- 10-inch combined PFD and MFD
- AHRS sensor
- electronic magnetometer (compass)
- autopilot servo
- engine Instrumentation controller
- flap/trim electronics controller

In this aircraft 29-bit CAN-IDs are used. The CAN-ID 10342200_h contains the oil pressure. By sending crafted data frames with this CAN-ID, Rapid7 engineers were able to send false oil pressure values to the display.

“We also identified that the CAN-IDs responsible for attitude and heading were part of a more complicated, non-standard CAN message format.

The electronic compass uses the CAN-IDs $10A8200_h$ and $10A82100_h$ to transmit the altitude and heading data. The data frame with the CAN-ID $10A8200_h$ acts as a header packet, with the third byte used to indicate the length of ▷

the message. “We reverse engineered the magnetic heading, time, and magnetic field strength fields by fairly standard protocol analysis techniques,” explained Kiley.

The payload of the AHRS data frames were also reverse engineered and turned out to be very similar to the messages described above. The AHRS sent 52- and 60-byte messages with CAN IDs 10242000_h to 10242200_h.

Rapid7 engineers were able to both replay messages as well as craft data frames that would then indicate on the PFD an incorrect altitude, attitude heading, or airspeed. This attack could then be combined with one against the autopilot system. It was identified that the autopilot could be engaged and disengaged (see Figure 6).

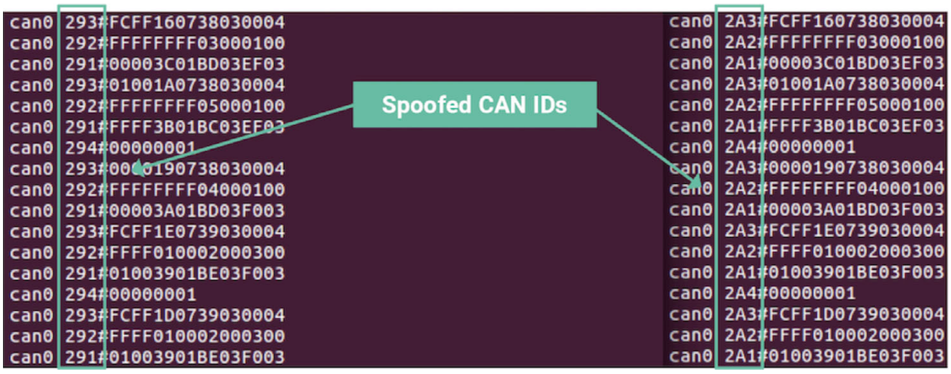

Figure 2: Spoofed CAN data frames from AHRS nodes 2 and 3 (Source: Rapid7)

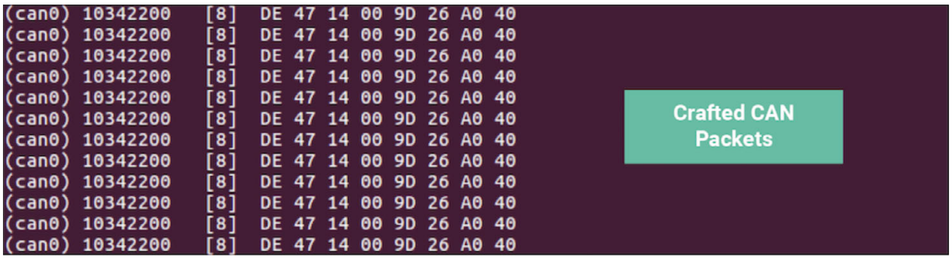

Figure 3: Crafted CAN data frames with false oil pressure values (Source: Rapid7)

An attack against the autopilot and attitude indicator could lead to an unusual attitude and potentially loss of control of the aircraft, given that forged CAN data frames can create disastrous scenarios very quickly.

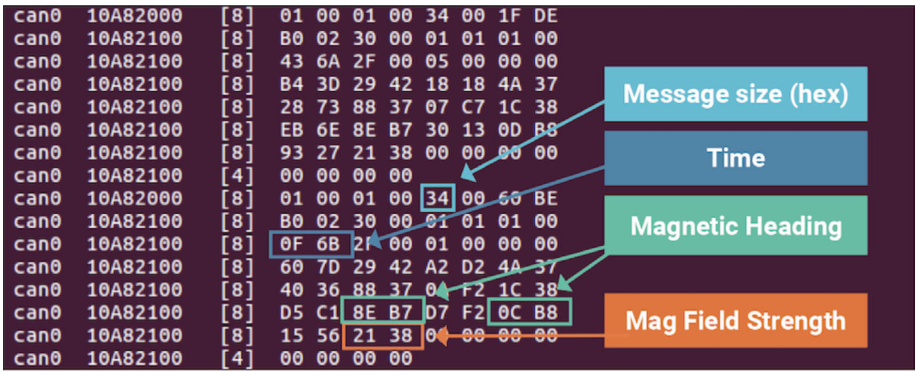

Figure 4: Example of the GMU 11 Magnetic Compass data frame (Source: Rapid7)

Conclusion and recommendations

In commercial and military aviation the physical access to aircrafts is limited and controlled. But still this is a single point of failure. In security engineering, it is well understood that relying on a single dimension of security for protection is precarious. In particular, in cybersecurity, it is generally frowned upon to rely on only securing the environment of the systems, rather than addressing vulnerability of the system itself.

“For example, while the most correct solution to a given database software vulnerability may be to apply a patch from a ▷

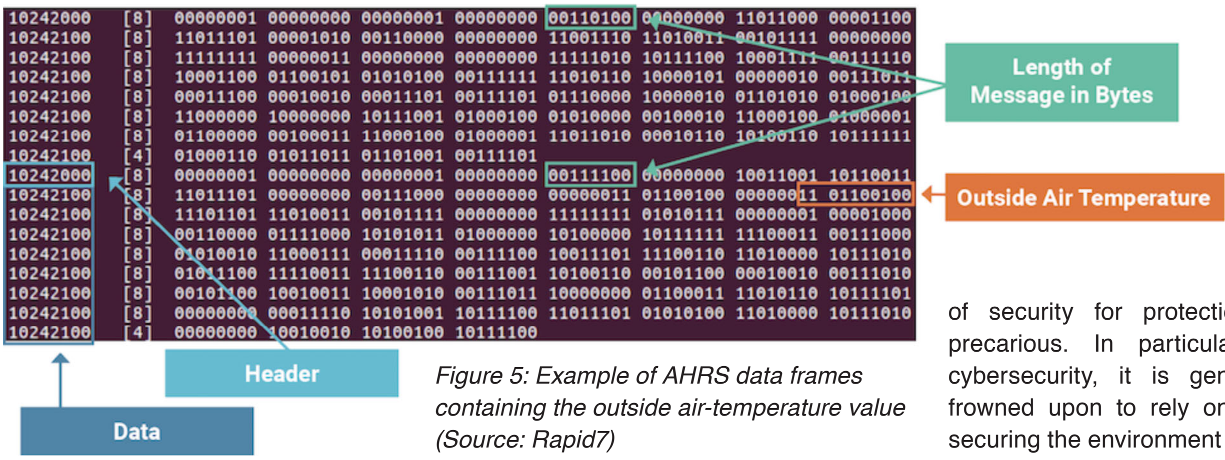

Figure 5: Example of AHRS data frames containing the outside air-temperature value (Source: Rapid7)

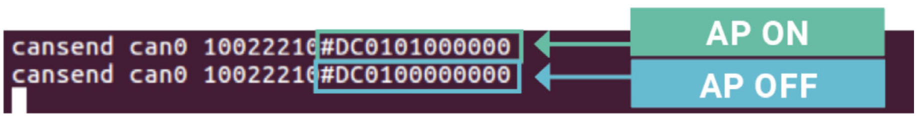

Figure 6: Autopilot data frames (Source: Rapid7)

vendor, a better solution would involve patching as well as limiting network access to that software through an operating system firewall and a local network firewall, and limiting physical on-keyboard access to authorized personnel. That way, if one of these systems happens to fail – a patch is skipped, a firewall rule is mistyped, or a physical door to a data center is left ajar – other defensive measures are in place to help prevent disaster," explained Kiley.

The CAN data link layer lacks modern network security design considerations, such as cryptographic assurances of data frame sources or authenticity. More critically, CAN-based networks often do not consider the threat model of an attacker with physical access to the shared wiring of the system. "While the physical security of airplanes is both well regulated and well tested, this reliance on physical controls may, in fact, be a leading cause as to why aviation CAN security has not matured at a pace similar to more traditional security or even automotive CAN security," said Kiley.

One solution to detect unauthorized access to the CAN network is the Stinger transceiver by NXP. However, the proposed solutions using CAN-specific filtering, whitelisting, and firewalling, do not appear to have gotten much traction in avionics networking, at least in the avionics systems favored by pilots of small aircraft, stated Patrick Kiley. He added: "This is due, in part, to the emphasis on physical security in aircraft; after all, even small, personal aircraft are rarely parked in unmonitored, open areas like open parking lots or public streets."

Small-aircrafts are also increasingly seeing similar enhancements with consumer technologies such as Bluetooth and Wi-Fi. These wireless interfaces are additional vulnerabilities. Rapid7 did not test this interface as a part of this research. "Given these realities, we offer two suggestions to reduce the risk of avionics CAN networks attacks based on false messages: Segment the CAN network from other networks and encourage secure designs for CAN network itself," explained Kiley.

"The open-ended nature of CAN should be seen as an invitation for security innovation. In particular, our research indicates that a message authentication protocol would strengthen defenses against attacks that leverage forged CAN messages," said Kiley. He proposed to use CAN FD with a payload of up to 64 byte: "Some of that extra space can now be used for security-critical features such as replay protection and cryptographic hashing. There is no reason to think that CAN could not enjoy a leveling-up of secure design if manufacturers, framers, regulators, and users demand it." ◀

hz