Note on the security of computer networks airline
Vulnerabilities of “connected planes

Several articles have recently raised the issue of computer security of commercial flights by evoking the "connected aircraft, hackers target" or "Wi-Fi on planes, an open door for hackers? "Or" Can you hack the computer of an Airbus or a Boeing? ". The feared scenario consists in a takeover of operational aircraft software that would intentionally cause a crash

Based on a vulnerability found in an embedded system software (FMS, "flight management system"), through the system of ACARS air-ground data exchanges, the scenario would result in influencing the level settings flight of the aircraft.

Airbus and Honeywell in other linked aircraft manufacturers, including Boeing, have conducted intensive work to assess the credibility of hackers claims about this vulnerability. The European Aviation Safety Agency for its part had formally asked Airbus to report its findings on the matter.

The European Aviation Safety Agency has alerted the aircraft manufacturers and suppliers and asked for an analysis of the potential vulnerabilities of the FMS and other embedded systems connected to the ACARS and the possible impact on flight safety if such a scenario is produced. She also informed the authorities FAA (USA), ANAC (Brazil) and TCCA (Canada).

Following this work, no vulnerabilities of embedded systems, which would allow such a scenario, is yet proven.

For its part, the DGAC has examined the possible consequences, if any, such vulnerability on operations and flight safety.

1. Analysis of the threat

- After analysis, it appears that the described vulnerability only affects software present in the simulation of FMS, and not in software of embedded equipment.
- Embedded systems connected to the ACARS have been identified and analysed the impact on security in the event that an attack of this type would be launched. Following the first test results, There is confidence about the robustness of its planes with respect to the identified threat.
- Moreover, even if the sending "pirates" frames to ACARS is complicated because of the stack of protocol layers ; but repeatedly sending fake messages via ACARS ACARS, a pirate transmitter could lead the FMS to declare failure.

2. Effects on Flight Safety

Assumption of the loss of FMS

- The loss of FMS in a single plane would have a moderate impact on safety because it is manageable by the crew with the help of air traffic control, means of conventional navigation still available in this case. However an impact study should be conducted to study the consequence of such a failure simultaneously affecting several approaching aircraft.

Wrong assumption of loading data into an FMS

Loading into the FMS of incorrect data, especially a false flight plan, would also have a very limited impact, the crew or air traffic control being able to detect it before any impact on flight safety.

Taking control of the FMS could introduce inappropriate and independent aircraft shares in the will of the driver. These actions would therefore alter the uncomfortably path with instructions from air traffic control or programming the flight plan.

In controlled airspace where the traffic flow is under the constant supervision of air traffic controllers (monitoring being provided by a radar display system) which establish a sound dialogue with each aircraft pilot via radio VHF, any improper maneuverer is detected quickly, especially in the most critical phases of flight, as the approaches, and verbal instructions are given to the driver to remedy the situation. Instructions can even be sent to surrounding devices to avoid a hazard.

In addition, a number of systems available to the control will automatically detect these deviations (radar processing system, areas of surveillance, reconciliation detection system with the relief) thus providing valuable assistance to the controller. This malicious takeover will be quickly counteracted by close cooperation between the controller and the pilot. He could then take control of his plane.

To be more specific, or the takeover led to a slow drift, and then that's probably the pilot control cooperation that will lead to the detection and takeover. The drift is slow, the risk is manageable. Either drift is fast, or then most likely the driver will realize as quickly and unplug the FMS, to take conduct of the flight.

In uncontrolled airspace, the pilot monitors more carefully its trajectory and has elements beyond FMS providing precisely its position in space. This is most often areas, at least in Europe, close to an aerodrome to which or from which the operations will therefore request a separate manual control of FMS. So in this situation the driver keep the hand.

The inclusion of any threat scenario other than taking control of an aircraft by the FMS considered here require a new analysis to assess the risks for air traffic and flight safety.

3. Conclusion

The analyses and tests conducted do not conclude to a risk that could impact directly the safety of flights in the short term given the present safety nets elsewhere (pilots, air traffic control). In particular, there is no identified possibility of taking control of the plane from the ground.

However, hacking attempts could potentially lead to the loss of the FMS flight. The potential impact in terms of safety should be evaluated more carefully if several aircraft were affected simultaneously in the same space.