Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Prof. Laurent Vanbever
Networked Systems Group

Wireless Attack Evaluation in a Cyber Avionics Lab

Master thesis proposal (external thesis in collaboration with armasuisse)

A multitude of wireless technologies are used by air traffic communication systems during different flight phases. From a conceptual perspective, many of them are insecure as security was never part of their design and the evolution of wireless security in aviation did not keep up with the state of the art [1,2,3].

Recent contributions from academic and hacking communities have exploited this inherent vulnerability and demonstrated attacks on some of these technologies. However, all of these demonstrations have been conducted on a theoretical basis or in a lab setting with simulated hardware.

In this dissertation, your will use the newly established Avionics Lab at the Cyber-Defence Campus in Thun in order to conduct wireless attacks (e.g., spoofing, jamming) on real, certifiable aircraft avionics. Possible attack vectors include the GPS-System or the aircraft transponder and the Traffic Collision Avoidance System (TCAS). The goal is to evaluate the behaviour of the different subsystems under adverse conditions and to suggest possible countermeasures.

Beyond the wireless attack vectors, there is the possibility to test the software implementations security used in the avionics hardware, for example through modern fuzzing methods.

Requirements

- Knowledge of software-defined radio hard- and software (e.g., GNU Radio).
- Working understanding of radio frequency communication and physical-layer concepts.
- Programming knowledge in languages necessary, potentially also on a lower level (e.g., C)

References

[1] Experimental analysis of attacks on next generation air traffic communication.
Schäfer M, Lenders V, Martinovic I.
In International Conference on Applied Cryptography and Network Security 2013 Jun 25 (pp. 253-271). Springer, Berlin, Heidelberg.

[2] On perception and reality in wireless air traffic communication security.
Strohmeier, M., Schäfer, M., Pinheiro, R., Lenders, V. and Martinovic, I.
In IEEE transactions on Intelligent Transportation Systems, 18(6), 2017.

[3] Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices.
Costin, A. and Francillon, A., 2012. Black Hat USA, pp.1-12.

Contacts

- Dr. Vincent Lenders, vincent.lenders@armasuisse.ch
- Dr. Martin Strohmeier, martin.strohmeier@ar.admin.ch