Proof-of-concept: practical, flexible, affordable pentesting platform for ATM/avionics cybersecurity ('ATM-cybersec')

Executive summary

The world of air transportation is in active process of getting a huge overhaul. This includes development, implementation and roll-out of strategic and enormous modernization programmes such as SESAR (EU) and NextGen (USA). These programmes bring digitalization, interconnectivity and latest technologies to the many components of the Communication Navigation Surveillance (CNS), Air Traffic Management (ATM), Air Traffic Control (ATC), and pursue important benefits for next-generation aviation in terms of efficiency, safety, and environment. ICAO estimated that by 2027 about US$120 billion will be spent on the transformation of air transportation systems, and that stakeholders (including service providers, regulators, airspace users, manufacturers, researchers), will face increased levels of interaction as new, modernized ATM operations are implemented. At the same time, as security issues related to the transformation of the aviation system are coming into view, they will require a closer collaboration among experts in safety and security disciplines, and the security matters should be considered in the system changes that lie ahead.

Cybersecurity was a relatively minor issue in CNS/ATM/aviation, however this aspect is changing. At the same time, though the adoption of new technology is an ongoing activity in CNS/ATM/aviation fields, the current pace and extent of new information technologies is notably increasing the risk from cyber attacks, which is due to an increasing number of factors including ever increasing complexity and connectivity of the systems and growing technology stacks. Hence, cybersecurity is an issue because many ATM/aviation stakeholders rely on electronic systems for critical parts of their operations, including safety-critical functions. As SESAR/NextGen transformations are implemented, the CNS/ATM/ATC/avionics (sub-)systems become an overly complex combination of modern and legacy (and everything in-between) technologies combined in unexpected ways – connected to ethernet/internet links, communicating over several dozen frequencies/radio-links (1090 ModeS/ES, 978 UAT, 117-137 VDL2), using a similar amount of protocols and data-formats (ModeS, ADS-B ES, ADS-B UAT, TIS-B, ACARS, METAR) at various ISO/OSI-equivalent levels and processed by various types of devices (e.g., EFBs, cockpit/ATC displays). One of the practical approaches to assess/test cybersecurity levels (somehow "orthogonal" to the standard yet somewhat theoretical risk-management/risk-mitigation approach) is to actively (pen)test all the possible system instances/configurations with as many as possible pentesting inputs and scenarios. However, to the best of our knowledge there are no publicly available solutions/platforms/devices that would allow a great flexibility of (pen)testing for such a varied number of technologies/links/protocols, and importantly – provide all this at an affordable price for the final stakeholders and researchers.

This project aims at closing this gap by developing a proof-of-concept practical, flexible, affordable pentesting platform for ATM/avionics cybersecurity. For this purpose we have developed from scratch a novel and unique end-to-end early stage (TRL3-4) platform as well as a comprehensive hardware/software testbed. With these, we have performed several hundreds of experimental iterations and developed 4 novel attacks ("ADS-B-level DoS attack", "ADS-B coordinated attackers contradictory information injection") while implementing altogether more than 10 attacks. After pentesting more than 120 cumulative testbed configurations, we have discovered more than 40 vulnerabilities (e.g., Denial-of-Service, crashes, hangs) and a handful of logical and implementation bugs, all these posing imminent, realistic and dangerous cyber-physical threats to safe aviation/ATM/ATC. At the same time and using the same platform, we implemented and evaluated several defensive approaches (such as "RSS-Distance" model and "Doppler shift effect" model) for

detecting fake/spoofed ADS-B messages from attackers. We describe our methodologies and results in three distinct research manuscripts that undergo academic peer-review.

This project has received funding from the SESAR Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No 783287.