Paper Title: On the (In)Security of 1090ES and UAT978 Mobile Cockpit Information Systems—An Attacker Perspective on the Availability of ADS-B Safety- and Mission-Critical Systems
Authors: Syed Khandker, Hannu Turtiainen, Andrei Costin, Timo Hamalainen
Reviewer: Pedro Oliveira (PO)
Paper Link: https://ieeexplore.ieee.org/document/9749067/

Contributions:

What are the major issues addressed in this publication?

- FAA intends to make air traffic control/navigation purely digital by using Automatic dependent surveillance-broadcast (ADS-B) systems. Such systems can be connected to smartphone-based mobile cockpit information systems (MCIS) in order to display traffic information. The main issue is that such systems are vulnerable to cyberattacks: they do not offer any authentication nor encryption guarantees, allowing attackers to read and change the communication as well as send messages on behalf of others.
- While there is several work that studies the security of ADS-B systems, there is no much research focused in the security of MCIS systems, which is the main focus of this paper.

What are the main contributions (as stated by the authors)?

- Study security of 6 MCIS systems and 21 EFB applications.
- DoS attack and Fuzzing on UAT978 and 1090ES devices with different EFB applications.

Strengths:

- Good description of state of art: PSR with SSR (Mode A/C/S) that motivate the introduction of ADS-B. Also description of previous security work in regards to ADS-B: message injection, spoofing, attacks based on SDR (software-defined radio), big data, link jamming, ….
- Small description of UAT978/1090ES (used for different flying altitudes)
- Good variety of systems and apps tested.
- Attack was performed on a variety of apps and devices (different smartphone/OS). 9 out of 24 tested configurations were affected by the DoS attack – they suffered a crash or became clogged or unresponsive. The other apps that were not affected, dropped a significant number of legitimate messages.
- Authors propose mitigations by referencing previous work: ADS-Bsec, collaborative attack detection, DNN-based spoofing detector, wireless witnessing,

Weaknesses:

- On page 3 it is referred that “EFB applications hosted on smartphones or tablets are connected to the transceiver device via WiFi”… There is no comment regarding the security implications of this type of connectivity. By being a more ubiquitous type of connectivity couldn't this be more easily exploited by attackers?

- From the 21 distinct applications, different types of tests were performed on a different subset of applications. No explanation of why the same tests weren't performed on all apps.

Points of interest:

- SDR tools used to perform tests: HackRF, BladeRF, PlutoSDR.
- EFB Applications openly available via Android and iOS App stores.
- Fuzz software: AFL (American Fuzzy Lop)