Building an Avionics Laboratory for Cybersecurity Testing

Martin Strohmeier
firstname.lastname@armasuisse.ch
Cyber-Defence Campus
armasuisse Science + Technology
Thun, Switzerland

Leeloo Granger
leeloo.granger@epfl.ch
EPFL
Lausanne, Switzerland

Giorgio Tresoldi
Vincent Lenders
firstname.lastname@armasuisse.ch
Cyber-Defence Campus
armasuisse Science + Technology
Thun, Switzerland

ABSTRACT

Aviation cybersecurity has received significant attention in the academic literature over the past decade, as software-defined radios have enabled practical wireless attacks on unauthenticated communication technologies. Typically, however, both attacks and countermeasures have only been examined in theoretical and simulated settings. Our Avionics Security Lab seeks to plug this gap by building a laboratory containing avionics built with certified, real-world aircraft hardware.

In this paper, we describe the Avionics Security Lab, our design goals and a first evaluation of the targeted threat vectors. We show that the first modules of the lab can successfully be used to realistically attack and analyze critical air traffic control and radar technologies such as ADS-B, TCAS and GPS. We further discuss the lessons that were learned in designing and assembling the lab. More modules with satellite telephony, CPDLC and electronic flightbags are currently being integrated and further extensions are planned. The Avionics Security Lab is open for use and collaboration with other researchers.

CCS CONCEPTS

• **Hardware → Analog, mixed-signal and radio frequency test**; • **Security and privacy → Systems security**; • **Computer systems organization → Embedded systems**.

KEYWORDS

aircraft, avionics, testbed, wireless security, aviation security

ACM Reference Format:
Martin Strohmeier, Leeloo Granger, Giorgio Tresoldi, and Vincent Lenders. 2022. Building an Avionics Laboratory for Cybersecurity Testing. In *Cyber Security Experimentation and Test Workshop (CSET 2022), August 8, 2022, Virtual, CA, USA.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3546096.3546101

1 INTRODUCTION

The safety and security of aircraft and the aviation ecosystem has fascinated people since the inception of flight. Due to the high profile of aviation and its status as critical infrastructure, any issues pertaining to safety are widely publicized. Consequently, even mere claims of being able to impact aircraft systems in flight, whether from on board [10] or from the ground [9] receive extensive attention and cost millions in verification and forensic assessment.

Apart from the hacker community, academic researchers have jumped on the task to examine the legacy information and communication systems used by aircraft and air traffic control. Using the available technical standards and software-defined radios, security testers were able to implement air traffic control communications and aviation datalinks in software, allowing them to send arbitrary messages and coming up with a vast array of creative attacks [3]. Recently, think tanks [2] and government entities [8] have also embraced the need to consider cybersecurity in the aviation sector while many practitioners are still divided on the matter [27].

However, while there has been extensive research on security issues in the wider aviation ecosystem, this has been done exclusively with simulated hardware and re-implemented targets. In our personal experience as security researchers in aviation, many skeptics — ranging from reviewers in the computer security community to safety engineers at aviation manufacturers — like to doubt the vast array of the existing research simply on these grounds. Claims that safety protocols, humans in the loop, redundancy, data fusion, or some proprietary black (box) magic successfully protect aircraft and air traffic control from cyberattacks are common place.

Why have these conflicting views not been consolidated over the past decade? Cybersecurity is certainly on the agenda, as working groups at most civil aviation institutions and novel initiatives such as the Aerospace Village[1] held regularly at DEFCON and RSA show. However, there are two main barriers to solving this issue. First, the aircraft industry (most manufacturers are also large defence contractors) is notoriously secretive and guarded against outsiders. It is well understood that tickets and aircraft are never sold on safety (or security) headlines [15], thus any potential negative publicity is to be avoided and working with independent security researchers is seen as too risky.

Second, it is naturally very difficult to get independent access to an actual aircraft, in particular for an extended time, within a relatively controlled environment, and without non-disclosure agreements. As buying a complete aircraft with modern avionics is too costly (compared to, say, a car or even a small satellite), renting would be preferred. However, in practice, nobody wants to provide an aircraft for penetration testing – it is difficult if not impossible to guarantee the restoration of flight integrity and thus full safety afterwards. While motivated and well-connected researchers have had the chance to spend some time figuring out how to work with scrapped airliners [17], this approach also has several drawbacks: research time onboard is limited, the hardware likely outdated, and

[1] https://aerospacevillage.org/

CSET 2022, August 8, 2022, Virtual, CA, USA

ACM ISBN 978-1-4503-9684-4/22/08…$15.00
https://doi.org/10.1145/3546096.3546101

the complexity of operating and monitoring a full commercial aircraft is significant. Similar reasoning, in addition to severely limited freedom of access and public engagement possibilities, applies to government programmes such as the US Department of Homeland Security's cyber testing of a Boeing 757 [33].

For all of these reasons, we decided to built a Avionics Security Lab, which enables independent research on real, certified avionics hardware and systems. We present it in this paper.

Contributions. With this paper, we make two main contributions:

- We design, build and present a novel integrated testbed for aviation security research. Our lab is built with real aircraft hardware and integrated by a professional certified avionics supplier and integration specialist. This ensures maximum reality of the setup without compromising on access.
- We evaluate the effectiveness of our design and integration by implementing several well-known attacks on aircraft communication technologies (ADS-B and GPS), which, until know where publicly shown only in simulated or emulated environments.

The remainder of this work is structured as follows. Section 2 discusses the related work in aviation security and related testbeds. Section 3 introduces the requirements and design goals of the Aviation Security Lab, before Section 4 presents the components and integration in detail. Section 5 provides a first evaluation of security testing with the lab. Section 6 discusses lessons learned and further extension plans, before Section 7 concludes.

2 RELATED WORK

We briefly discuss the vast amount of existing aviation security research, typically conducted on simulated hard- and software. Secondly, we discuss relevant existing approaches to (aviation) test laboratories.

2.1 Aviation Security Research

The field was kickstarted by several talks at hacker conferences on the then-novel Automatic Dependent Surveillance–Broadcast (ADS-B) protocol [3]. After initial denials of any problems by the aviation community, a growing body of work has analysed more than a dozen technologies used in a typical commercial aircraft flight throughout all flight phases. These technologies can broadly be divided into air traffic control communication (e.g., ADS-B or VHF), navigation aids (such as GNSS or the instrument landing system) and datalinks (e.g., ACARS, CPDLC or satellite links). From a computer security point of view, all these legacy systems are considered insecure as they do not offer authentication, (cryptographic) integrity or confidentiality.

Air traffic control systems such as ADS-B have shown to be insecure in the early 2010s by academics [3] and hackers [12]. Spoofing and other manipulation of ADS-B data in the cockpit or on controller's radar screens can be easily achieved with SDRs. Older analogue systems such as voice communication over VHF have similar issues, with regular interference reported [34].

Navigation aids, which provide positioning information for pilots, include Global Navigation Satellite Systems (GNSS) and various ground-based beaconing systems, including the instrument landing systems (ILS), which was the subject of recent risk analysis [19]. GPS/GNSS is the only non-aviation-specific technology considered in our work. Indeed, it is a well-known commodity in the wireless research community with countless attacks and countermeasures [30]. Still, the concrete impact of attacks on pilots and aircraft has not yet been analysed in practice.

Finally, there are several datalinks available on commercial aircraft, including Aircraft Communications Addressing and Reporting System (ACARS) and Controller–Pilot Data Link Communications. Both are known to be insecure and vulnerable [11, 21, 22] but not yet part of our Avionics Security Lab as they require additional hardware.

For a full overview of aviation security research, the reader is pointed towards several surveys covering the full breadth of aviation security research [26, 28].

2.2 Aircraft Laboratories

The closest related work to ours is the Triton testbed, introduced at CSET '19 [4]. It also features an ARINC 429 databus and real components. However, the main differences to our Avionics Security Lab are as follows: Instead of air traffic control technologies and navigation aids, Triton focuses on the datalink ACARS, which it offers through a physical CMU (Communication Management Unit) and FMC (flight management computer) with all other components simulated/virtualized. Consequently, the foreseen attack vectors of this testbed concentrate on ACARS and the physical data loader.

Beyond Triton, the US Air Force has provided an aircraft testbed for a hacking contests at DEFCON [32]. Specifically, participants were tasked to enter a F-15 fighter jet's Trusted Aircraft Information Download Station. As a military setup, this was naturally only accessible to pre-chosen and vetted participants.

In a further related attempt, the Federal Aviation Administration presented a "Cybersecurity Test and Evaluation Facility" at CSET '16 that sought to provide an adaptable cybersecurity research and development environment for internal training of FAA employees [13]. However, beyond the initial work, we found no evidence of further (public) use.

3 DESIGN GOALS

When we set out to construct the Avionics Security Lab, we settled on several main design goals: realism, independence, complete accessibility and physical wireless interfaces.

3.1 Certifiable Realism

The first and main goal is to use certified hardware. This means not buying avionics hardware off unknown online resellers and scrapyards. Instead, the hardware should be certified by the manufacturer (new or refurbished) for use in a real aircraft. As aviation standards describe clear interoperability and minimum operational requirements, the particular manufacturer is less important when examining avionics security.

3.2 Independence

While it may theoretically be possible to work with aircraft labs built at the different manufacturers (namely Boeing, Airbus, Bombardier,

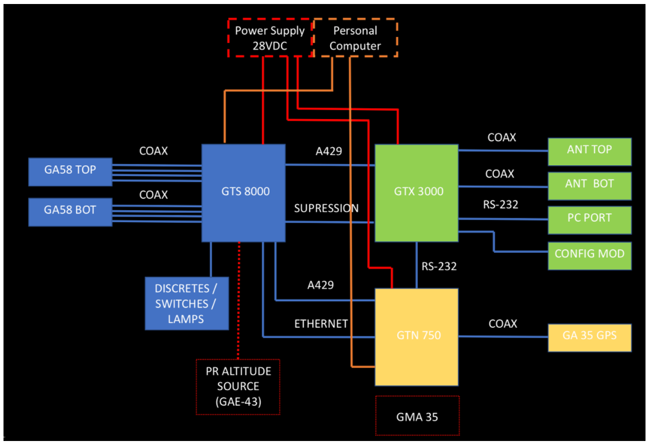

Figure 1: Logical overview of the Avionics Security Lab.

Embraer or Pilatus), this is typically only done under non-disclosure agreements and without the option to publish independently. By building our own lab, we are not subject to such business interests and restrictions. It helps that aviation is a heavily standardized industry, in particular concerning communication. This ensures compatibility across the world but also means that differences between manufacturers are less important when looking at testing the security of these standards.

3.3 Full Access

Related to the last point, there should be full access and control over the testbed. This means the hardware should be easily accessible via all interfaces and not physically locked away as in a full aircraft as it might be found on a scrapyard. Any simulated part should come with clear manuals and instructions how to manipulate them.

3.4 Wireless Interfaces

Finally, and key to realistic security research, was the requirement that the wireless interfaces found in an aircraft (i.e., the antennas) should not be emulated but physically available. Concretely, all five antennas for the transponder, the GNSS, and the collision avoidance system should be accessible. This enables the real-world evaluation of a whole host of SDR-based attacks from the security literature (e.g., [3]). The evaluation should in particular enable the analysis of physical-layer behaviour, which is crucial for example for TCAS (Traffic Collision Avoidance System), since it is inherently based on distance measurements using the round trip time.

4 THE AVIONICS SECURITY LAB

To build and integrate our requirements, we found a supplier certified by the European Union Aviation Safety Agency (EASA). We worked with them on the design and the requirements for several month until the successful deployment and acceptance test.

4.1 Logical Design

Figure 1 gives the logical overview of the Avionics Security Lab. The three main components, the Garmin GTS 8000, GTX 3000 and GTN 750 are connected via the ARINC 429 bus (plus redundant Ethernet and serial connections). The antennas are connected via coaxial cables: the GPS antenna to the GTN 750, the two transponder antennas to the GTX 3000 and the two antennas used for collision avoidance to the GTS 8000. The system is powered by a 28V DC power supply. To feed any necessary emulation data, the GTN 750 is connected to a personal computer using an Astronics UA2000 ARINC 429 to USB interface.

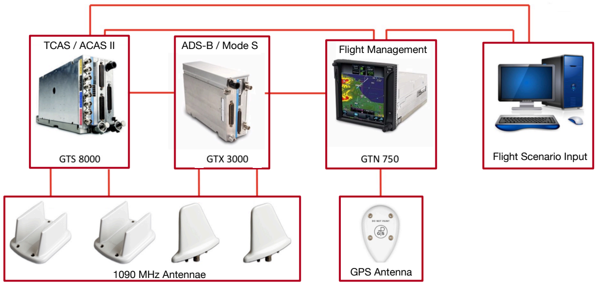

Figure 2: Components of the Avionics Security Lab.

4.2 Main Components

The four main components and their respective antennas are illustrated in Fig. 2. A picture of the final assembled rack can be seen in Fig. 3.

4.2.1 Flight Management System. The Garmin GTN 750 is a flight management system offering full navigation and communication capabilities for hundreds of aircraft makes and models.[2] It is typically installed in medium-sized aircraft and helicopters in order to put advanced navigation features in the cockpit, such as terrain mapping, flight planning, traffic target surveillance, weather, taxiway diagrams and others. Importantly, it interfaces with a wide range of other avionics hardware from different manufacturers offering a touch screen for easy configuration. With its GPS capabilities it also offers the option to fly an SBAS (Satellite Based Augmentation System) approach.

4.2.2 Aircraft Transponder. The Garmin GTX 3000 is a flight transponder, capable of Secondary Surveillance Radar and ADS-B Out.[3] In conjunction with the positional source from the GTN 750, it is a certified ADS-B solution for flying in instrument flight rules airspace. The transponder also serves as one input source for the TCAS collision avoidance system.

4.2.3 Collision Avoidance. The Garmin GTS 8000 is a collision avoidance device following the current TCAS II/ACAS II 7.1 standard.[4] Using the two antennas it interrogates nearby aircraft and displays their position based on the response. It interfaces with the display of the GTN 750, which issues any potential warnings. Notably, the GTS 8000 also uses ADS-B data from other nearby aircraft ("ADS-B In") via the GTX 3000 to further enhance the situational air display and issue traffic warnings. For a fully compliant TCAS

[2] Full specifications available at https://www.garmin.com/en-US/p/67886.
[3] Full specifications available at https://www.garmin.com/en-US/p/15012.
[4] Full specifications available at https://www.garmin.com/en-US/p/106233.

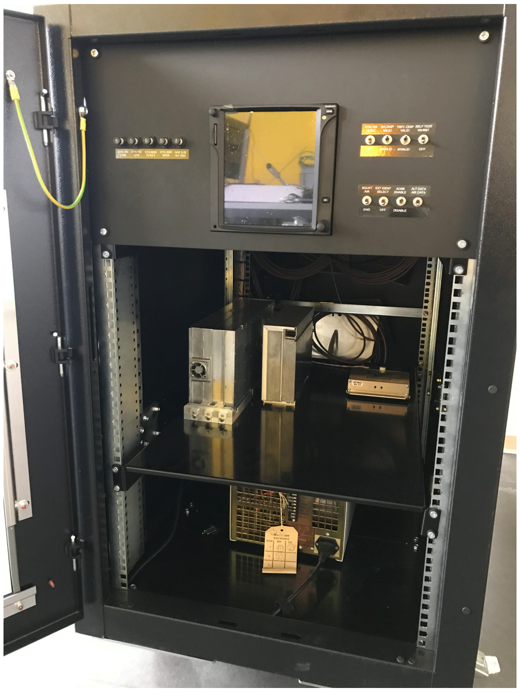

Figure 3: Picture of the Avionics Security Lab front.

system, there is a further requirement for a radio altimeter, which is naturally not sensible in a stationary laboratory setup. The data (i.e., the barometric altitude) that would normally come from this altimeter, must be fed to the system artificially.

4.2.4 CoPilot Software. As the example of the radio altimeter shows, not every component can realistically be installed in a laboratory setting. As some of these components are still required for proper functioning of the system, these must be emulated. This is taken care of by a separate laptop with the CoPilot software[5] installed, which sends the expected messages (e.g., from the altimeter) via a USB dongle onto the ARINC 429 bus. The main necessity is to set the radio altitude for a full functioning of the TCAS system.

4.3 Currently Supported Technologies

In the following, we describe the communication technologies currently supported by the Avionics Security Lab.

4.3.1 ARINC 429 Bus. Avionics buses such as ARINC 429 or its military equivalent MIL-STD-1553 have received significant attention over recent years due to their unauthenticated nature [5, 25]. If an adversary has access to the bus, they have free reign to send and receive all messages on the bus, impacting the attached devices which are crucial to the functioning of the aircraft. Crucially, until now, no public security evaluation of the physical ARINC 429 bus has been conducted, leaving open potential attack vectors on the attached devices.

There are a number of bus messages missing that are sent by endpoints which are not part of our lab (but would be in a full aircraft). The include, for example, the altimeter. In our lab, the ARINC 429 bus is fed all required data from a separate laptop running the CoPilot software using a USB-to-ARINC 429 dongle. This allows modification of all ARINC 429 messages within the normal parameters set by the CoPilot software and expected by the FMS.

4.3.2 SSR. Secondary Surveillance Radar (SSR) is a technology based on traditional identification, friend or foe (IFF) systems in the military domain. It is a legacy technology introduced in commercial aviation in the 1970s that is mandated in higher airspaces around the world. It is a cooperative technology, where the aircraft responds to interrogations from the ground. Through various transponder modes called Mode A, Mode C and Mode S, respectively, it provides target information on altitude and a globally unique identity, though no position. SSR uses digital messages with different frequencies and modulations for the interrogation (1030 MHz) and the reply (1090 MHz). Mode S is based on extensive, well-understood specification standards by the Radio Technical Commission for Aeronautic (RTCA) standard body and offers further message formats (e.g., aircraft intent or autopilot modes).

SSR is supported through the GTX 3000 with its two dedicated antennas.

4.3.3 ADS-B. ADS-B Out continually broadcasts ID, position and velocity as well as further information such as intent or urgency codes. These broadcasts happen twice a second in case of position and velocity, and once every 5 s for identification. The ADS-B mandate for larger aircraft has been postponed several times in various airspaces [29].

Our Avionics Lab supports the 1090ES (Extended Squitter) standard (but not the Universal Access Transceiver or UAT datalink). 1090ES is used by aircraft around the world and is based on legacy Mode S transponder technology on 1090 MHz and additional new RTCA standards.

As ADS-B uses the same underlying technology as SSR, it shares the same components, i.e., the GTX 3000 with its two connected antennas.

4.3.4 GNSS. Global Navigation Satellite Systems are crucial (if certainly not exclusive) to aircraft navigation and modern aviation. The insecurity of the the best known representative, the Global Positioning System (GPS), has been known publicly for over two decades. In the aviation context, broad GPS interference has been reported by pilots for years, making GPS the most attacked aircraft system as far as is publicly known. In hotspots such as the Eastern Mediterranean, the Baltics or the Black Sea, commercial pilots are acutely aware of GNSS spoofing and jamming, making it a crucial integrated technology in our Avionics Security Lab.

The GTN 750 is connected to a GPS antenna, which supports GPS but also SBAS such as the regional WAAS (USA), EGNOS (Europe), MSAS and QZSS (Japan), GAGAN (India) and others. As is typical, to get a (legitimate) positional fix, the GPS antenna needs to be positioned outside with a clear view of the sky.

4.3.5 TCAS. Traffic Alert and Collision Avoidance System (TCAS) II is an implementation of the Airborne Collision Avoidance System (ACAS) mandatory in Europe since 2015, having as purpose to reduce the risk of (near) mid-air collisions between aircraft. ACAS II gives traffic advisories (TA) and resolution advisories (RA) in

[5] https://www.astronics.com/avionics-test-simulation-software

vertical directions to the pilots. The former will only help the pilots visually, whereas the latter will actively recommend maneuvers. The system is independent from the navigation system and ATC and uses the transponder to interrogate Mode C and S transponders of nearby aircraft.

ACAS defines a protected volume of airspace in which an incoming aircraft will trigger RAs/TAs. This zone is defined through different thresholds depending on altitude, speed and heading of the aircraft with respect to the Closest Point of Approach (CPA) of an intruder [24].

TCAS is supported by the GTS8000, with two dedicated antennas, which also enable rough direction finding and round trip time measurements.

4.4 Supporting Lab Hardware

To augment the lab and make attacks fully operational, the Avionics Security Lab includes additional hardware for signal generation, control, and monitoring.

4.4.1 Software-defined Radios. SDRs are the backbone of much modern wireless security research, certainly in aviation. The low cost and ease of access have not only enabled independent security research, they have also significantly lowered the threshold for attacks on aviation infrastructure. Whereas a decade or two ago an attack on such systems would have fallen squarely into the realm of electronic warfare, now even hobbyist can download software to eavesdrop on or spoof aircraft messages. To conduct the attacks discussed in Section 5, among others, we have several Ettus USRP available in the lab (B210 and X300 models) for sending plus RTL-SDR dongles for easy reception and monitoring.

4.4.2 Labsat. Racelogic's LabSat[6] — being purpose-built and more specialized than a USRP — is much more automated and presents far more capabilities specifically for GNSS manipulation than an open-source SDR setup. The LabSat can transmit files or pre-configured "scenarios" that are on its SSD and simulate the signals of a range of GNSS satellite constellations (GPS, Galileo, GLONASS and others). Once a scenario is running, one can use its interface to check the approximate signal strength transmitted of each constellation, as well as vary the attenuation of the signal from -69dB up to +20dB. The LabSat being portable, one can easily mount it anywhere, without a need for an external power source or computer, making it very comfortable to use.

4.4.3 eConspicuity Devices. eConspicuity devices are small fully integrated transponder devices that are used by smaller aircraft. They can receive ADS-B data and in some countries such as the UK or Australia also transmit ADS-B Out data with reduced energy.

First, the Skyecho II by uAvionix[7] is a useful tool for monitoring the output of our lab transponder and the SDR attack setups. It receives ADS-B data and is also capable of transmitting it with up to 20 W. It has a GPS receiver and interfaces with a range of apps on phones or tablets. Its small footprint also makes it an excellent test and show device.

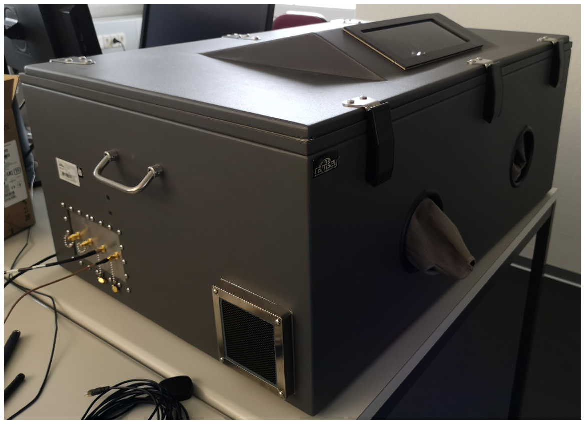

Figure 4: Picture of the outside Faraday cage with antenna connectors.

Secondly, we operate a PowerFLARM device for research on FLARM. FLARM (a portmanteau of "flight" and "alarm") is a system used by small aircraft such as gliders and drones to prevent potential aviation collision and to raise awareness of the pilot. The system obtains the aircraft's own position from an internal GPS (or potentially other GNSS) receiver, then calculates a projected flight path considering its speed, acceleration, track, turn radius, wind and other parameters.

Upon receiving other FLARM or also ADS-B messages, the FLARM system acts as a collision avoidance system similar to TCAS. It may issue alarms to alert the pilot or show the relative position if other aircraft are within detection range but there is no predicted collision.

4.4.4 Faraday Cages. To conduct our research safely and legally, we need to make sure no signals leak the perimeter of the laboratory. In order to do this, we have several customized Faraday cages of different size with the possibility to attach and loop through the different antennas. Fig. 4 illustrates one such setup. Where longer distance, physical layer analysis is needed, a larger anechoic chamber is planned.

5 EVALUATION: A FIRST LOOK

In order to evaluate that our setup works, we will now describe the setup and results of testing some classic wireless attacks on aviation technologies from the literature, namely the spoofing of the GPS and ADS-B subsystems via their respective antennas.

5.1 GPS Spoofing

First, we attempt to spoof the GPS subsystem, the main navigation aid for the GTX 3000. with professional Labsat signal simulator. The comparison of the two transmitters allows us to assess the difference between a more powerful adversary, and one with limited hardware capacities.

Finally, we test both static and dynamic GPS signals, i.e. whether our signal corresponds to a static geo-location or a moving object in space and time, causing the laboratory in effect believing to be flying.

[6] https://www.labsat.co.uk
[7] https://uavionix.store/general-aviation-ads-b-transceivers/skyecho-2

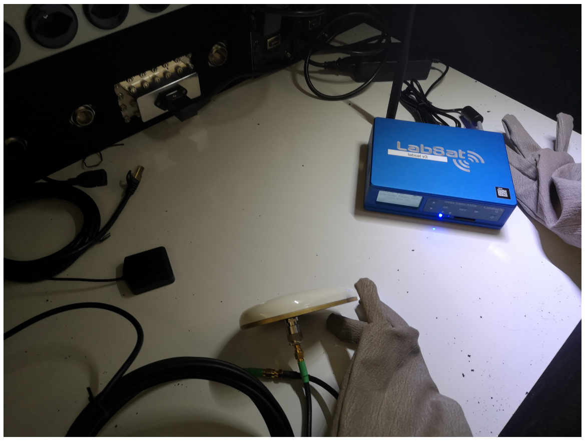

Figure 5: Setup for the GPS spoofing. The picture shows the inside of a custom-built Faraday cage with a Labsat signal generator, the aircraft's target GPS antenna (white) and a monitoring GPS antenna for the u-blox.

5.1.1 Setup. When transmitting signals, we always take precautions and use one of the Faraday cages. At the same time, we monitored that there was no signal leakage, i.e., the signal strength sent by the Labsat or the USRP was never strong enough to impact the outside world. We made sure that no damage could occur to any outside devices or receiver, as well as to GPS-dependent and/or Mode S capable vehicles.

To measure and monitor the received GNSS signals, we used a u-blox EVK-M8 GNSS evaluation kit. The u-blox helped us verify that we were indeed sending the signals that we wanted to sent and to monitor and ensure the safety of the experiments. The full setup is shown in Fig. 5.

The static scenario tested a variety of positions on different continents, e.g., in Boston or Sweden. The dynamic scenario was a straight scenario flying from Zurich to Geneva, both for the Labsat and the USRP with the open-source software *gps-sdr-sim* [7].

5.1.2 Experiences. After verifying the correct function by obtaining a lock from from the legitimate GPS constellation by putting the antenna outside, we moved to spoof the GPS location of the GTN750. In order to reduce debugging issues and get stable and flexible signals, we used the LabSat first. To start understanding what parameters were required for successful spoofing attempts, we first started the experiments with an isolated model, i.e. with no initial GPS lock and no outside signals.

At first, we were unsuccessful with this approach without any indication about the reason; the monitoring devices showed the correct GPS position. The Garmin GTN750 represented a sort of "black box" for our work. A discussion with the support services of Garmin verified that, in principle, the device implemented exactly the Minimum Operational Performance Specification (MOPS) for a GNSS receiver.

After several longer experiments, a lock on the spoofed signal was successful, however once the signal locked once, repeating a spoofing attack was not possible anymore. That is, once the GTN750 was turned on, it locked on any signal we were simulating whether in the future or in the past - but once the spoofing stopped, we were not able to spoof it again without a power cycle. This undefined behavior illustrates the need for trying out different parameters to figure out and estimate the feasibility of aircraft GPS spoofing in the real world.

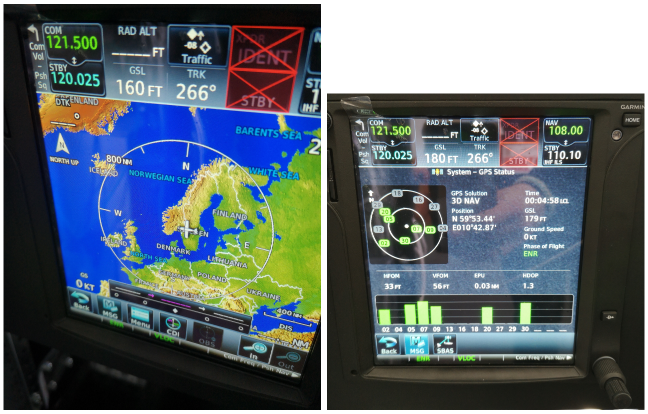

Figure 6: Static spoofing of the GPS position of the laboratory.

Finally, since the experiences were promising albeit not successful, we attempted scenarios of longer duration (37 minutes) to see if the receiver was actually trying to download the almanac data, which should take at least 12.5 minutes. This time, the experiment was very successful: After about 27 minutes, with spoofed signals of +5dB compared to the legitimate signals, it locked onto the spoofed signals as intended. Once this longer scenario was established, any further re-spoofing attempts were successful with both Labsat and USRP, giving in effect full and arbitrary control over the system.

5.1.3 Results. Fig. 6 shows the successful GPS spoofing experiments conducted on the GTN 750. On the left we see a static position in Sweden. On the right, we can see the GTN's GPS page. It shows the successfully acquired position and the individually spoofed satellites.

5.2 ADS-B Spoofing

In our second evaluation attempt, we aimed to spoof the inputs received by the transponder through its antennas. In a real-world situation, this would impact the situational awareness of the pilot, as "ghost" targets would appear on their cockpit traffic screen, which could have unpredictable consequences [23].

5.2.1 Setup. To have the best possible conditions to attack the traffic information on the GTN750, we firstly spoofed its receiving GPS antenna. The customized scenario comprised a flight in Switzerland at a geometric altitude of 9580 ft with a flight plan starting from Zurich and landing in Geneva, such that the GTN750 indicated the "En Route" status. The radio altitude was set to 8200 ft.

To send the spoofed ADS-B targets, we used custom-built transmission scripts from previous research (*withheld for anonymous review*) in conjunction with a USRP B210. To not make attacks too easy, such attack scripts are not publicly released but fundamentally trivial to convert from ADS-B receivers such as GNU Radio's

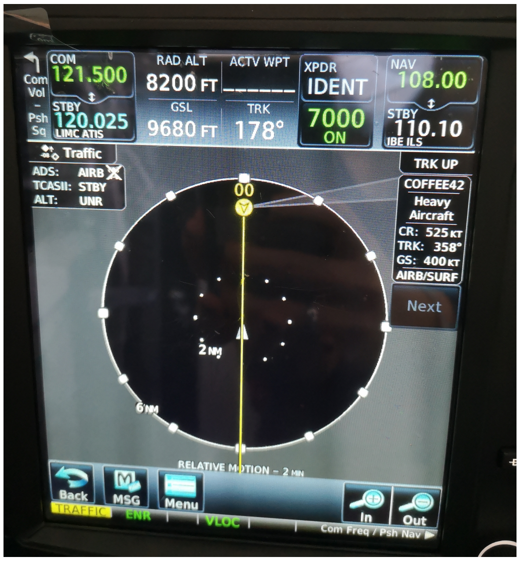

Figure 7: Successful spoofing of a ghost aircraft on collision course.

modes_rx.[8] Consequently, there are many independent developments shown by academic researchers and hackers in the literature.

5.2.2 *Experiences.* With the transponder activated, we further monitored the spoofed trajectory in real time with the use of the SkyEcho II device next to it. This indirect ADS-B spoofing happens as the spoofed GPS position is not only shown internally but also (if not for the Faraday cage) sent out to other aircraft and ground stations via ADS-B.

5.2.3 *Results.* We succeeded into making an intruder directly approaching the target on its trajectory. Once entering its surrounding airspace within a 3 NM range radius and 500ft in altitude, the GTN 3000 declared it as a Traffic Advisory (TA), as expected. This could be easily noticed because its icon went from a blue arrow to a yellow dot, signaling the threat and displaying the spoofed parameters on touching the target. This can be seen in Fig. 7. Being only ADS-B messages (no SSR/TCAS), no red alerts were triggered and it did not go to a Resolution Advisory - this attack is left for future work.

It is noteworthy that no changes where necessary to the original attack setup — confirming the validity of previous original research on ADS-B [3, 20].

6 DISCUSSION

After showing the effectiveness of our setup, we discuss the lessons learned and possible extensions. We want to note that while finding vulnerabilities in specific soft- and hardware implementations could also be of interest, we generally concentrate on class attacks, i.e. attacks on standards and protocols, which are independent of manufacturers and their implementations.

6.1 Lessons Learned

In building and testing the Avionics Security Lab, we learned several lessons, which may be helpful for similar endeavors. As far as we are aware, this project constituted a novel problem and was fully uncharted research ground. At least in the public domain, i.e. outside defense/aircraft manufacturers, this has not been attempted. As such, there were no references available for orientation; attempts at contacting several aircraft manufacturers for collaboration stalled.

(1) **Trade-Offs:** In building a laboratory, there are some natural trade-offs when trying to realistically reproduce the real world. In our experience, the main trade-offs are between realism, cost, and complexity, which all affect each other. Simulating more parts generally brings down cost and complexity at the cost of realism. We decided to focus on several specific goals, i.e. wireless access to certain systems, which was a favorable trade-off for us.

(2) **Provider:** We wanted to ideally work with a local provider, also to reduce cost and complexity in the buildup and integration phases. We examined the list of EASA-certified avionics companies in the region, contacted them, and were successful with only a single company. Most were unable or unwilling to work with us on the project as it was considered out of scope, or no engineering time was available (the ADS-B mandate meant that avionics integration specialists have been very busy over the past few years).

(3) **Manufacturer Attitudes:** Some aircraft and avionics manufacturers may seem to actively boycott testing, as there is a strict requirement to prove that one owns a real aircraft in order for someone to buy avionics hardware. Garmin was the only sympathetic avionics manufacturer. From a security point of view, we believe that this is a positive attitude (rather than security through obscurity) and we want to stress that we would view their products as potentially more secure because of this more open and collaborative. In the end, however, we believe the manufacturer of our lab hardware is largely irrelevant as most of the attacks proposed in the literature are standard-specific and implementation-agnostic. All manufacturers comply with the minimum operational performance standards (MOPS) and do not typically go beyond them because of reasons for cost, complexity and compatibility.

(4) **Extensibility:** We built the lab with a view towards future extensions in case it was a successful project (see next section). This meant looking carefully at the capabilities of the FMS and the other components such that they would not need to be exchanged later on, requiring additional planning and foresight.

6.2 Planned Extensions

We are in the process of planning and executing three further extensions to our Avionics Security Lab. These are all currently

[8] https://kb.ettus.com/Implementation_of_an_ADS-B/Mode-S_Receiver_in_GNU_Radio

being integrated and available for research and testing in the second half of 2022.

CPDLC:. Controller-Pilot Data Link Communication (CPDLC) is a novel datalink currently in the roll-out phase for commercial aircraft and required in more and more airspaces (e.g. in the Atlantic corridor). Like ACARS, it requires a CMU and a VHF antenna. To establish a realistic connection, an entry point to the CPDLC network and an endpoint to communicate with are also required. Despite its relative novelty, CPDLC is also unauthenticated and has been shown to offer several threat vectors for aircraft [11, 21].

Electronic Flightbag Support: Electronic flightbag (EFB) systems have been a recent focus of academic research [14, 16, 31]. EFBs are mobile cockpit information systems. Typically, this means that the pilot connects their (often personal) tablet to the aircraft avionics using Bluetooth or WiFi. This naturally opens new threat vectors, ranging from the tablet, its connection to the flight management system, to the software that the pilot might rely on [14, 31].

Satellite Telephony: Contrary to widespread belief, many satellite connections are in practice even less secure than direct aircraft-to-ground communication. Recent research has illustrated the widespread use of unencrypted satellite communication in the maritime and aviation domains [18]. Even where they are secured, the encryption might be weak [6]. As legacy systems will again be used for years and decades to come, this increases the possibilities for accessing satellite telephone calls by aircraft crew and passengers. In order to do such research in a legal and ethical way, a real aviation satellite phone setup using the Iridium satellite constellation is required. With this setup, we can conduct our own calls and data connections (including text messages and emails) and listen to them with available open source tools.

6.3 Scope

The potential scope of the (extended) Avionics Security Lab thus includes a number of wireless and wired attacks on several technologies. Radio frequency attacks will be possible on Mode S, ADS-B, TCAS, CPDLC, FLARM and the Iridium aircraft service. Consumer technologies for connecting EFBs, namely Bluetooth and WiFi, can also be examined. Wired attack vectors chiefly include the ARINC 429 bus. Both vectors can be used to examine the behavior of the soft- and hardware included in the various components of the lab, e.g. under cyber-physical system fuzzing [1]. Beyond this, it also serves as a demonstrator and teaching device to inform aviation experts on the reality of modern security threats.

7 CONCLUSION

We introduced our Avionics Security Lab, a research-oriented laboratory to conduct real-world security analysis otherwise not possible in practice. We discussed the design goals, focusing on free and open access (also) to wireless interfaces, and the lessons learned while assembling the lab. The final goal for the Avionics Security Lab is to support security testing of all onboard technologies. We provide early evidence of the effectiveness of our approach by showing successful attacks on the GPS and ADS-B interfaces of the Avionics Security Lab. With current and future extensions including additional critical aircraft technologies, scope and utility are being broadened further. We thus invite all researchers interested in this domain to bring their ideas for fruitful collaborations and maximize the utility of the lab. Any such inquiries are welcomed at cydcampus@armasuisse.ch.

ACKNOWLEDGMENTS

We are grateful for the support of Q.C.M. quality control management AG, who executed the Avionics Security Lab project with us. Concretely, we want to thank QCM's employees Christian Schusser, Santiago Llucià, Miroslav Šmid and Georg Riedler.

REFERENCES

[1] Yuqi Chen, Bohan Xuan, Christopher M Poskitt, Jun Sun, and Fan Zhang. 2020. Active fuzzing for testing and securing cyber-physical systems. In *Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis*. 14–26.

[2] Pete Cooper. 2017. *Aviation Cybersecurity: Finding Lift, Minimizing Drag.* Technical Report. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/aviation-cybersecurity-finding-lift-minimizing-drag)

[3] Andrei Costin and Aurelien Francillon. 2012. Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. In *BLACKHAT 2012, July 21-26, 2012, Las Vegas, NV, USA*, EURECOM (Ed.). Las Vegas.

[4] Sam Crow, Brown Farinholt, Brian Johannesmeyer, Karl Koscher, Stephen Checkoway, Stefan Savage, Aaron Schulman, Alex C Snoeren, and Kirill Levchenko. 2019. Triton: A {Software-Reconfigurable} Federated Avionics Testbed. In *12th USENIX Workshop on Cyber Security Experimentation and Test (CSET 19).*

[5] D De Santo, CS Malavenda, SP Romano, and C Vecchio. 2021. Exploiting the MIL-STD-1553 avionic data bus with an active cyber device. *Computers & Security* 100 (2021), 102097.

[6] Benedikt Driessen, Ralf Hund, Carsten Willems, Christof Paar, and Thorsten Holz. 2012. Don't trust satellite phones: A security analysis of two satphone standards. In *2012 IEEE Symposium on Security and Privacy*. IEEE, 128–142.

[7] Takuji Ebinuma. 2015. *Software-Defined GPS Signal Simulator.* https://github.com/osqzss/gps-sdr-sim.

[8] Tim Ellis, Michael Locasto, and David Balenson. 2020. Cyber State Requirements for Design and Validation of Trust in the Critical Transportation Infrastructure. In *International Conference on Critical Infrastructure Protection*. Springer, 69–83.

[9] Chris Gayomali. 2015. The hacker who claims he can crash your plane. Retrieved May 10, 2022 from https://theweek.com/articles/465612/hacker-who-claims-crash-plane

[10] Samuel Gibbs. 2015. Aviation experts dispute hacker's claim he seized control of airliner mid-flight. Retrieved May 10, 2022 from https://www.theguardian.com/technology/2015/may/19/hacker-chris-roberts-claim-seized-control-boeing-airliner-disputed-experts

[11] Andrei Gurtov, Tatiana Polishchuk, and Max Wernberg. 2018. Controller–pilot data link communication security. *Sensors* 18, 5 (2018), 1636.

[12] Brad Haines. 2012. Hacker + Airplanes = No good can come of this. Presented at DEFCON 20.

[13] David Ingegneri, Dominic Timoteo, Patrick Hyle, Fidel Parraga, and Alex Reyes. 2016. A Cybersecurity Test and Evaluation Facility for the Next Generation Air Transportation System (NextGen). In *9th Workshop on Cyber Security Experimentation and Test (CSET 16).*

[14] Syed Khandker, Hannu Turtiainen, Andrei Costin, and Timo Hämäläinen. 2022. 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. *IEEE Access* (2022).

[15] Jack Linshi. 2015. Why Airlines Don't Talk About Safety In Their Ads. Retrieved May 10, 2022 from https://time.com/3669161/airline-ads-safety/

[16] Devin Lundberg, Brown Farinholt, Edward Sullivan, Ryan Mast, Stephen Checkoway, Stefan Savage, Alex C Snoeren, and Kirill Levchenko. 2014. On the security of mobile cockpit information systems. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. 633–645.

[17] Ken Munro and Alex Lomas. 2020. *SDEF CON 28 Aerospace Village: 747-400 Walk through From a Hacker's Perspective.* https://www.youtube.com/watch?v=yq8wgJO-JXY.

[18] James Pavur, Daniel Moser, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2020. A tale of sea and sky on the security of maritime VSAT communications. In *2020 IEEE Symposium on Security and Privacy (S&P)*. IEEE, 1384–1400.

[19] Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir. 2019. Wireless attacks on aircraft instrument landing systems. In *28th USENIX Security Symposium (USENIX Security 19)*. 357–372.

[20] Matthias Schäfer, Vincent Lenders, and Ivan Martinovic. 2013. Experimental Analysis of Attacks on Next Generation Air Traffic Communication. In *Applied*

Cryptography and Network Security. 253–271.

[21] Joshua Smailes, Daniel Moser, Matthew Smith, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2021. You talkin'to me? Exploring Practical Attacks on Controller Pilot Data Link Communications. In *Proceedings of the 7th ACM on Cyber-Physical System Security Workshop*. 53–64.

[22] Matthew Smith, Daniel Moser, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2018. Undermining privacy in the aircraft communications addressing and reporting system (ACARS). *Proceedings on Privacy Enhancing Technologies* 2018, 3 (2018), 105–122.

[23] Matthew Smith, Martin Strohmeier, Jonathan Harman, Vincent Lenders, and Ivan Martinovic. 2020. A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems. In *27th Network and Distributed System Security Symposium*.

[24] Matthew Smith, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2020. Understanding Realistic Attacks on Airborne Collision Avoidance Systems. *arXiv preprint arXiv:2010.01034* (2020).

[25] Orly Stan, Yuval Elovici, Asaf Shabtai, Gaby Shugol, Raz Tikochinski, and Shachar Kur. 2017. Protecting military avionics platforms from attacks on mil-std-1553 communication bus. *arXiv preprint arXiv:1707.05032* (2017).

[26] Martin Strohmeier, Ivan Martinovic, and Vincent Lenders. 2020. Securing the Air–Ground Link in Aviation. *International Series in Operations Research & Management Science* (2020), 131–154.

[27] Martin Strohmeier, Anna K Niedbala, Matthias Schäfer, Vincent Lenders, and Ivan Martinovic. 2018. Surveying aviation professionals on the security of the air traffic control system. In *Security and Safety Interplay of Intelligent Software Systems*. Springer, 135–152.

[28] Martin Strohmeier, Matthias Schäfer, Rui Pinheiro, Vincent Lenders, and Ivan Martinovic. 2016. On perception and reality in wireless air traffic communication security. *IEEE transactions on intelligent transportation systems* 18, 6 (2016), 1338–1357.

[29] Junzi Sun, Xavier Olive, Martin Strohmeier, Matthias Schäfer, Ivan Martinovic, and Vincent Lenders. 2021. OpenSky Report 2021: Insights on ADS-B Mandate and Fleet Deployment in Times of Crisis. In *2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC)*. IEEE, 1–10.

[30] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. 2011. On the requirements for successful GPS spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security*. 75–86.

[31] Hannu Turtiainen, Andrei Costin, Syed Khandker, and Timo Hämäläinen. 2022. GDL90fuzz: Fuzzing-GDL-90 Data Interface Specification Within Aviation Software and Avionics Devices–A Cybersecurity Pentesting Perspective. *IEEE Access* 10 (2022), 21554–21562.

[32] Debra Werner. 2019. *Hackers as Allies*. Aerospace America. https://aerospaceamerica.aiaa.org/features/hackers-as-allies/.

[33] Frank Wolfe. 2020. Unclear What Happens After DHS Ends 757 Cyber Testing. Retrieved May 10, 2022 from https://www.aviationtoday.com/2020/03/31/department-homeland-security-ends-cyber-vulnerability-testing-boeing-757-200/

[34] Emma Younger. 2017. Melbourne Airport hoax caller Paul Sant pleads guilty to making fake flight calls, aborting Virgin landing. *ABC News* (Sept. 2017). http://www.abc.net.au/news/2017-09-05/melbourne-airport-hoax-caller-paul-sant-pleads-guilty/8873984