Towards a Unified Cybersecurity Testing Lab for Satellite, Aerospace, Avionics, Maritime, Drone (SAAMD) technologies and communications

Andrei Costin, Hannu Turtiainen, Syed Khandker, Timo Hämäläinen
Faculty of Information Technology
University of Jyväskylä
Finland
{ancostin,turthzu,syibkhan,timoh}@jyu.fi

***Abstract*—Aviation, maritime, and aerospace traffic control, radar, communication, and software technologies received increasing attention in the research literature over the past decade, as software-defined radios have enabled practical wireless attacks on communication links previously thought to be unreachable by unskilled or low-budget attackers. Moreover, recently it became apparent that both offensive and defensive cybersecurity has become a strategically differentiating factor for such technologies on the war fields (e.g., Ukraine), affecting both civilian and military missions regardless of their involvement. However, attacks and countermeasures are usually studied in simulated settings, thus introducing the lack of realism or non-systematic and highly customized practical setups, thus introducing high costs, overheads, and less reproducibility. Our *"Unified Cybersecurity Testing Lab"* seeks to close this gap by building a laboratory that can provide a systematic, affordable, highly-flexible, and extensible setup.**

In this paper, we introduce and motivate our *"Unified Cybersecurity Testing Lab for Satellite, Aerospace, Avionics, Maritime, Drone (SAAMD)"* technologies and communications, as well as some peer-reviewed results and evaluation of the targeted threat vectors. We show via referenced peer-reviewed works that the current modules of the lab were successfully used to realistically attack and analyze air-traffic control, radar, communication, and software technologies such as ADS-B, AIS, ACARS, EFB, EPIRB and COSPAS-SARSAT. We are currently developing and integrating support for additional technologies (e.g., CCSDS, FLARM), and we plan future extensions on our own as well as in collaboration with research and industry. Our *"Unified Cybersecurity Testing Lab"* is open for use, experimentation, and collaboration with other researchers, contributors and interested parties.

I. Introduction

Aviation, maritime, and aerospace traffic control, radar, communication, and software technologies received increasing attention in the research literature over the past decade, as software-defined radios have enabled practical wireless attacks on communication links previously thought to be unreachable by unskilled or low-budget attackers. Critical protocols and implementations in these domains have been demonstrated to be either insecure or exploitable under various attacks – EPIRB and CCSDS (Section IV-A and *our other SpaceSec23 submission on "COSPAS-SARSAT/EPIRB"*), ADS-B [1], [2], AIS [3], [4], ACARS [5], GDL90 [6]. Moreover, recently it became apparent that both offensive and defensive cybersecurity has become a strategically differentiating factor for such technologies on the war fields (e.g., Ukraine), affecting both civilian and military missions regardless of their involvement. However, attacks and countermeasures are usually studied in simulated settings, thus introducing the lack of realism or non-systematic and highly customized practical setups, thus introducing high costs, overheads, and less reproducibility.

At the same time, satellite, space and aerospace is strongly interconnected with aviation, maritime and Search-and-Rescue (SAR) domains, e.g., satellites processing aviation (ACARS, ADS-B) and maritime (AIS) data arriving over various communication links. Given this tight interconnect of technologies, the "additive complexity" may give rise to additional attacks such as Cross-Channel (XC) as both theorized and demonstrated by [6], [7], and somewhat equivalent of Cross-Channel Scripting (XCS) for IoT and web domains [8].

Our *"Unified Cybersecurity Testing Lab"* seeks to close this gap by building a laboratory (with its associated extensible programmatic platform and testbed devices) that can provide a systematic, affordable, highly-flexible, and extensible setup. Consequently, our unified lab approach allows to experiment with and test the scenarios that would be otherwise hard or impossible to test in labs dedicated solely to specific domains, e.g., avionics-only, maritime-only, space-only.

A. Contributions

In this paper, we introduce and detail a *"Unified Cybersecurity Testing Lab for Satellite, Aerospace, Avionics, Maritime, Drone (SAAMD)"* technologies and communications, as well as some peer-reviewed results and evaluation of the targeted threat vectors. We show via referenced peer-reviewed works that the first modules of the lab were successfully used to realistically attack and analyze traffic control, radar, communication, and software technologies related to satellites, space, aerospace, avionics, and maritime systems (e.g., EPIRB, CCSDS, ADS-B, AIS, ACARS). We are currently developing and integrating support for additional technology (e.g., drones

Workshop on Security of Space and Satellite Systems (SpaceSec) 2023
27 February 2023, San Diego, CA, USA
ISBN 1-891562-89-4
https://dx.doi.org/10.14722/spacesec.2023.239280
www.ndss-symposium.org

– FLARM, RemoteID), and we plan future extensions and improvements to our lab (e.g., GPS attacks/controls, more sophisticated environment control). With this, we aim to convince that a unified lab (with strong focus on space and satellite technologies) is not only beneficial but many times necessary in order to test complex scenarios as well as to be prepared for the leading role of space/satellites in years to come.

B. Organization

The rest of this paper is organized as follows. We discuss related studies in Section II. We describe our lab and pentesting platform in Section III. Then, in Section IV, we describe different attacking scenarios, their impact on ADS-B, ACARS, and AIS receivers, and analysis of the results. Finally, we conclude this paper with Section V.

II. Related Work

Although avionics and maritime communication has been the subject of profound research [1]–[3], [6], [9]–[24], the focus has been mainly on a specific attack or in theory. Recently Strohmeier et al. [25] researched building an avionics laboratory for cybersecurity testing. Their approach was testbed with "certifiable realism," meaning that the equipment must be capable of in-plane use. They also maintain that the testbed should be device manufacturer agnostic and in-laboratory contained. They utilized Garmin GTN 759 flight management system, Garmin GTX 3000 aircraft transponder, and Garmin GTS 8000 TCAS collision avoidance systems in their laboratory with some auxiliary equipment such as software-defined radios and Faraday cages. Currently, they support ARINC 429 avionics communication bus, secondary surveillance radar (SSR), Automatic Dependent Surveillance-Broadcast (ADS-B), Global Navigation Satellite Systems (GNSS), Airborne Collision Avoidance System (ACAS), and Traffic Alert and Collision Avoidance System (TCAS) technologies. The authors' initial tests of their testbed were successful, and the results were promising. For further research, the authors provided some guidance in their work. They concluded that constructing environment "realism" in a laboratory setting has trade-offs in complexity and cost, affecting the laboratory's expandability and future-proofing. They also received pushback from avionics manufacturers for collaboration and acquiring the equipment. In conclusion, Strohmeier et al. [25] built a highly-capable and effective laboratory setup for trustworthy avionics cybersecurity testing.

Avionics laboratories can also be particular for thoroughly testing specific equipment. For example, they required a sophisticated testing suite when South Korea's defense department rolled out their new utility helicopter with a new kind of Mission Equipment Package (MEP) integrated mission control system. Kim et al. [26] conducted a requirement assessment and designed a system integration laboratory to verify the MEP's capabilities and functionality before accepting the technology for active duty. Viana Sanchez and Taylor [27] introduced a Reference Architecture System Testbed for Avionics (RASTA). Their goal was to define an architecture for a laboratory that could combine, at the time, the latest agreements of avionics communication as well as the requirements for end-to-end spacecraft communication. Dey et al. [28] investigated drone security vulnerabilities. Their testbed contained two drones (DJI Phantom 4 Pro and Parrot Bebop 2), a LabSat GPS simulator, and two mobile phones for hosting the drone-controlling application. By performing several attacks, such as deauthentication, GPS spoofing, unauthorized file access, and others, they concluded that the vulnerabilities in drones could lead to invasions of privacy, concerns with aircraft safety, and even personal injury.

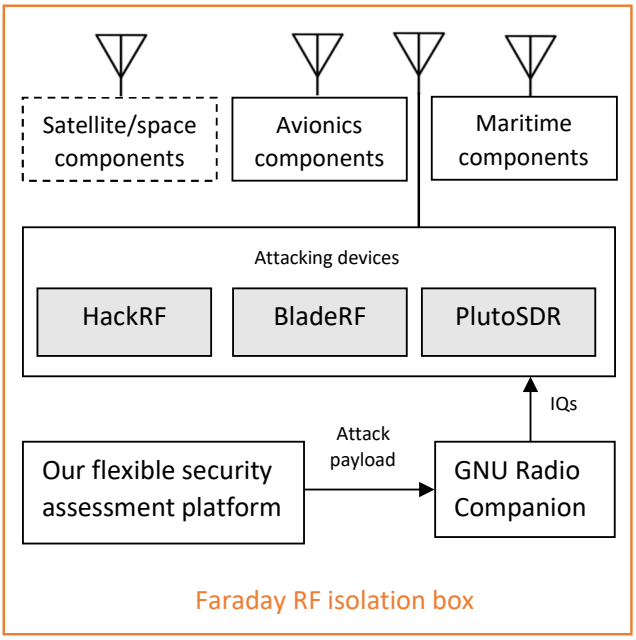

Figure 1. Diagram of our lab testing approach.

Our work relates closest to the recent work of Strohmeier et al. [25]. Even though our labs have inherent fundamental similarities in their designs, goals, and protocols, there are also several unique differentiating features. First, our lab and platform already cover aerospace (EPIRB, CCSDS) and maritime (AIS), in addition to the focused aviation/avionics (ADS-S, ACARS) field. Second, our lab, platform, and tests crucially focus on the attacker's perspective (e.g., attack vectors, successful exploitation, new attack techniques) with subsequent defensive improvements to the affected systems, even though testing the adherence to functional specifications and cybersecurity standards is also within the scope and capabilities of our lab. Last but not least, our lab aims is fitted to research offensive and defensive cybersecurity in highly complex end-to-end scenarios. One example is researching the effect of ADS-B/AIS attacks when ADS-B/AIS is attacked directly via an interface on aircraft/ships or via interfaces on satellites supporting these links. Another example is researching the effect of attacks when the attacker pivots across protocols (e.g., ADS-B to CCSDS and vice-versa) or across devices (e.g., ADS-B transponder of aircraft to satellite RF boards vice-versa). However, another example is researching the effect of common IT vulnerabilities (e.g., log4j) in cases when vulnerable components are used in aviation, maritime, aerospace infrastructure, and devices [7].

III. Our Testing Lab

The main goal of our investigation was to keep the testing scenario close to the realistic one. Therefore, we used transmission-capable SDRs to generate real-like but fake or non-standard signals, e.g., for ADS-B, AIS, and ACARS. We then tested different avionics, aerospace, maritime and satellite devices over the wireless interface. The reasoning the tests on the devices as well is due to the fact that researchers have shown that IoT and specialized embedded devices are generally highly vulnerable [29], [30]. Figure 1 shows the design of our lab. We developed a flexible and extensible security assessment platform that, at present, can create ADS-B 1090ES, UAT978, and AIS payload according to the protocol specifications and attack/test specifications. We used a signal processing software called GNU radio companion (GRC) to generate IQs of the RF signal of the payload. Then the IQs were sunk into the transmission-capable SDRs to create ADS-B and AIS RF signals. Even though one type of SDR is enough for the test, we tested three to check the attacking devices' availability. The list of different hardware and software in our laboratory is as follows.

A. Software

An RF testing laboratory requires much software to be functional. Our laboratory already employs an extensive software suite, and we are constantly adding more. In Table I, we disclose the software we currently use at the time of writing.

TABLE I. List of different software

Platform	Software name	Functionality
Aviation	Dump1090	Decoding and displaying 1090ES data
	Dump978	Decoding and displaying UAT978 data
	RTL1090	Decoding and displaying 1090ES data
	PlanePlotter	Displaying 1090ES data
	Micro ADS-B	Displaying 1090ES data
	QGround Control	Displaying 1090ES data
	Mission Planner	Displaying 1090ES data
	Garmin Pilot	Displaying 1090ES and UAT978 data
	ForeFlight	Displaying 1090ES and UAT978 data
	Airmate	Displaying 1090ES and UAT978 data
	AvPlan	Displaying 1090ES and UAT978 data
	Easy VFR4	Displaying 1090ES and UAT978 data
	FlyQ	Displaying 1090ES and UAT978 data
	Stratus Insight	Displaying 1090ES and UAT978 data
	OZRunways	Displaying 1090ES and UAT978 data
	Horizon	Displaying 1090ES data
	SkyDemon	Displaying 1090ES and UAT978 data
	ADL Connect	Displaying 1090ES data
Maritime	OpenCPN	Displaying AIS data
	iRegatta	Displaying AIS data
	Ships	Displaying AIS data
	Boating	Displaying AIS data
	iBoating	Displaying AIS data
	Boat Beacon	Displaying AIS data
	AF track	Displaying AIS data
	RTL AIS driver	Decoding AIS data
	AIS Share	Sharing AIS data
	ShipPlotter	Decoding and displaying AIS data
	AISmon	Decoding and sharing AIS signal
Others	SDR Sharp	Receiving RF signal
	GNU Radio Companion	Generating IQs
	Our Pentesting Platform	Generating offensive/non-standard payloads

B. Avionics components

We tested 11 ADS-B receivers, and some had transmitting capability too. They all support ADS-B 1090ES, four support dual ADS-B mode, and four support UAT978. Table II shows our laboratory's avionics components.

TABLE II. List of Avionics components in our laboratory

Device name	Functionality
uAvionix Skyecho2	1090ES and UAT978 receiver. 1090ES transmitter
uAvionix echoUAT	1090ES and UAT978 receiver. UAT978 transmitter
ForeFlight Sentry	1090ES and UAT978 receiver
Garmin GDL 52	1090ES and UAT978 receiver
Aerobits TR-1W	1090ES receiver and transmitter
ADL 180	1090ES receiver
Helios Avionics SensorBox	1090ES receiver
Plane Gadget Radar (PGR)	1090ES receiver
Aerobits EVAL-TT-SF1	1090ES receiver
PX4	1090ES receiver
Cube Orange	1090ES receiver

Figure 2 shows the avionics component of our laboratory.

Figure 2. Aviation/avionics components

C. Maritime components

We tested a commercial transponder, a professional AIS receiver, and many RTL SDR-based mobile AIS setups in our laboratory. Table III shows the list.

TABLE III. List of maritime components in our laboratory

Device name	Functionality
Matsutec HP-33A	Stand alone AIS transponder
Quark-elec QK-A027	AIS receiver
McMurdo G8	COSPAS-SARSAT AIS/EPIRB transmitter
RTL-SDR	RF front-end for AIS mobile applications

Figure 3 shows the maritime component of our laboratory.

D. Satellite and aerospace components

At the time of this writing, we already have in our lab a space device (Theia Space ESAT), COSPAS-SARSAT devices, and an aerospace drone device (DJI MATRICE 300 RTK), as depicted in Figures 4 5. A fast preliminary implementation already allowed us to discover some Denial-of-Service vulnerabilities on the satellite device that effectively disables RF/COMM communication board and requires a hard reboot.

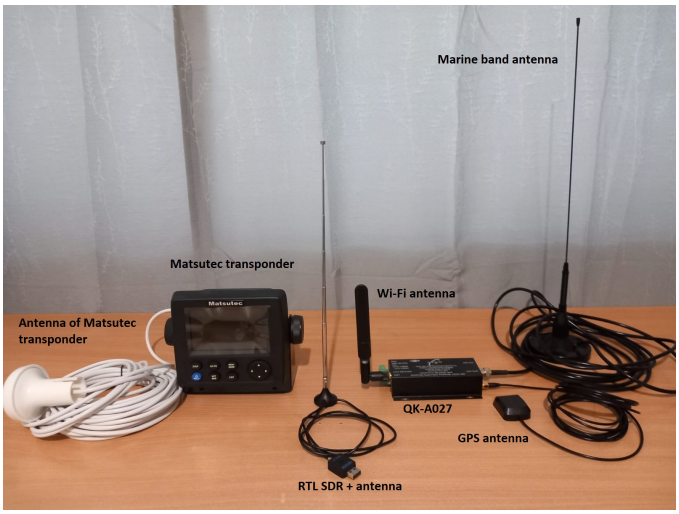

Figure 3. Maritime components

Thanks to our lab and platform, we discovered this is a problematic scenario for satellites, as availability is a top priority in the field. Immediate future work is to research, develop, and integrate into our pentesting platform additional and complete support for software and protocols for these devices and subsequently thoroughly evaluate their cybersecurity posture when facing both existing attacks [1], [4], [6], [23], [31] and perhaps novel ones.

TABLE IV. LIST OF SATELLITE, SPACE, AEROSPACE DEVICES

Device name	Functionality
Theia Space ESAT	a) CCSDS receiver; b) "System security" payloads/boards
DJI Matrice 300 RTK	a) ADS-B, FLARM, RemoteID; b) Remote-carrying of "attacking devices" III-E
McMurdo G8	COSPAS-SARSAT EPIRB 406 transmitter

Figure 4. Satellite/aerospace and drone components – Theia Space ESAT and DJI MATRICE 300 RTK

E. Attacking devices

We used three types of SDRs to transmit the attack/test signals. All of them supported sending of ADS-B signals. HackRF and BladeRF support AIS transmission, but the Pluto SDR's operating frequency is out of the AIS frequency range. Table V shows the list of the attacking devices.

Figure 5. Satellite/aerospace technology – a COSPAS-SARSAT EPIRB McMurdo G8 [32]

TABLE V. LIST OF ATTACKING DEVICES

Device name	Functionality
HackRF	Generating ADS-B, AIS, EPIRB signals using Python/GRC
BladeRF	Generating ADS-B, AIS, EPIRB signals using Python/GRC
Pluto SDR	Generating ADS-B, EPIRB signals using Python/GRC

Figure 6 shows the attacking and auxiliary devices of our laboratory.

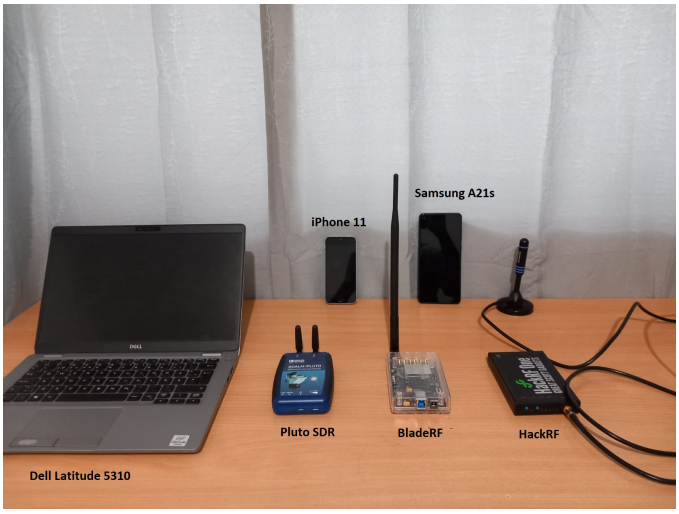

Figure 6. Attacking SDRs of our laboratory with auxiliary devices

F. Environment control components

During the development and testing of such labs and platforms, best practices are advised:

- Whenever possible or applicable, configure the transmitters (e.g., HackRF) and receivers (e.g., RTL-SDR)

to use the ISM-band, meaning that the transmission and reception of the signal waves were done on the central carrier frequency of 433.800 MHz. For example, in the authors' geography (Finland), the 432–438 MHz ISM-band is allocated for transceivers exempt from licensing [33], and it is a good practice to familiarize with the local/national regulations.

- Whenever possible or applicable, set the lowest transmit power to limit unintended interference in the unlicensed ISM band.
- In addition, use a certified "faraday cage" — specifically a Disklabs Faraday Bag — featuring a double layer military-grade RF faraday shielding, which is also commonly used for well-contained wireless and RF testing and forensics (Figure 7).
- Moreover, use a certified radio power density meter — specifically a TriField Model TF2 EMF Meter — to double-check and ensure that the signals do not escape the faraday cage/lab premises (Figure 7).

All these precaution measures are complementary and ensure a well-controlled environment, which is also in line with commonly accepted practices.

Figure 7. Environment control components – Disklabs Faraday Lab Box LB2 (leak protection), and Trifield EMF Meter Model TF2 (leak detection)

G. Summary and comparison with related work

In Table VI, we present a comparison of the main related work and our present paper, and below, we introduce the meaning of symbols used in Table VI.

- ◔: Some of these apply to system/setup: demonstrated minor early-stage results; implementation is very early-stage; qualifies for low Technical Readiness Levels (TRL).
- ◑: Some of these apply to system/setup: demonstrated some limited results; implementation is partial or does not cover all use-cases; qualifies for medium Technical Readiness Levels (TRL).
- ●: Any (or generally all) of these apply to system/setup: generally covers all mentioned use-cases; has extensible and/or close-to-complete implementation; demonstrated extensive results; qualifies for high Technical Readiness Levels (TRL).

IV. Results

We formulated and tested many existing and novel attacks on ADS-B and AIS with the mentioned setup. Because our setup supports encoding raw data, besides different attacks, we also sampled some technical limitations of the receivers, such as error handling capability. All the experiments have been conducted within a controlled lab environment, running at minimal power and shortest duration possible. We briefly describe the test result below.

A. Experiments on satellite systems

We conducted the following tests on the satellite and COSPAS-SARSAT EPIRB system: noitemsep

- Replaying
- Spoofing
- Fuzzing
- Denial-of-service (DoS)

On the COSPAS-SARSAT EPIRB implementations, while we were unable to achieve DoS or crashes (as only very basic EpirbPlotter software was available as the target receiver at this point), we have successfully achieved replaying, spoofing, and fuzzing [35]. In Figures 8 9 10, we show successful EPIRB spoofing attacks, wehere we can accurately control virtually any field of the EPIRB messages.

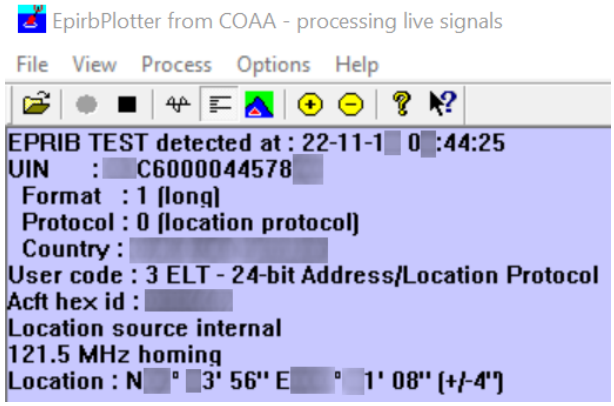

Figure 8. Our *spoofed* EPIRB-ELT signal (contains ICAO24 aircraft ID) well received by EpirbPlotter.

On the Theia Space ESAT, all attacks above were implemented successfully on the satellite's CCSDS implementation. Moreover, thanks to fuzzing, we discovered specific packets and CCSDS sequences that consistently trigger a quasi-permanent DoS, i.e., the device requires a hard reset in order for the communication with the device to be possible again.

One main challenge limiting the number of attacks tested is the highly-limited access to the COSPAS-SARSAT systems (including software and devices) which itself is due to either high costs or restricted access (related to the sensitive nature of such systems). As immediate future work, we aim to establish national and international contact points with COSPAS-SARSAT centers to bootstrap cybersecurity readiness testing and exercises involving presented and future/novel attacks.

TABLE VI. SUMMARY COMPARISON WITH RELATED STATE OF THE ART "LAB SETUP" WORKS.

Paper	Satellite + Space + Aerospace	Aviation	Maritime	Drones	GPS	RF shielding	Open to researchers
Strohmeier et al. [25]	◑ (SATCOM)	● (ADS-B, TCAS, CPDLC, extensible)	NO	◔ (FLARM)	◑	◑	YES
Predescu et al. [34]	NO	◑ (ARINC 429, ARINC 664)	NO	NO	NO	NO	N/A
Dey et al. [28]	NO	NO	NO	◑	◔	NO	N/A
Our current paper	● (CCSDS, COSPAS-SARSAT, EPIRB, extensible + cross-channel (XC))	● (ADS-B, EFB, ACARS, EPIRB-ELT, extensible + cross-channel (XC))	● (AIS, EPIRB-MMSI, extensible + cross-channel (XC))	◔ (RemoteID, FLARM)	NO	◔	YES

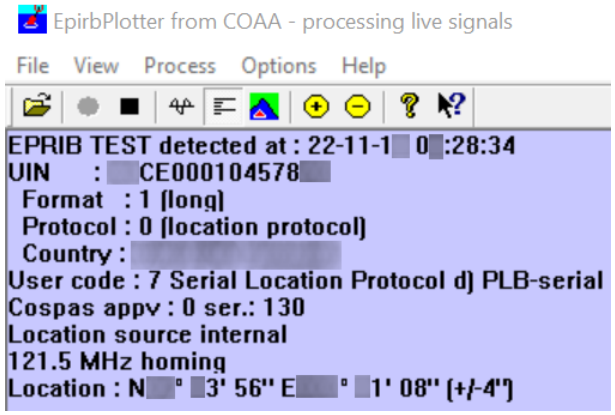

Figure 9. Our *spoofed* EPIRB-PLB signal well received by EpirbPlotter.

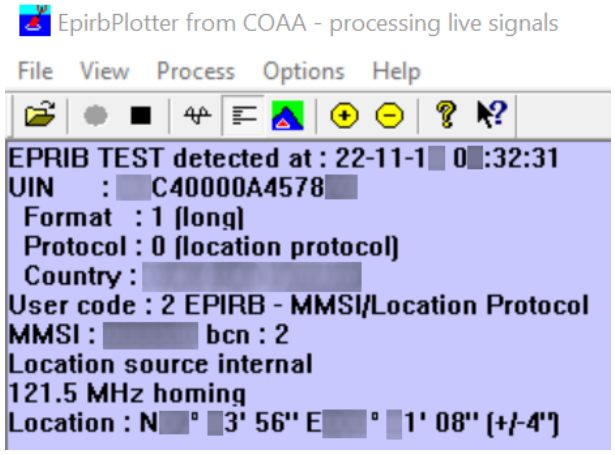

Figure 10. Our *spoofed* EPIRB-MMSI AIS signal (contains MMSI ship ID) well received by EpirbPlotter.

B. Experiments on avionics system

We have successfully tested the following attacks on the ADS-B system: noitemsep

- Aircraft reconnaissance
- Spoofing
- Flooding
- Jamming
- False emergency signal
- Aircraft disappearance
- Trajectory Modification
- Logically invalid data encoding
- Fuzzing avionics protocol (GDL-90)
- Denial-of-Service (DoS)
- Attacks on ADS-B CRC error handling
- Highly-Coordinated attackers attack

We implemented and tested these 12 cyberattacks on ADS-B, of which five attacks were presented or implemented for the first time. Six portable mobile cockpit information system (MCIS) devices combined with 21 EFBs, resulting in 44 ADS-B 1090ES and 24 UAT978 configurations, were tested for the DoS attack, which affected approximately 63% and 37% of 1090ES and UAT978 setups, respectively [23], [31]. Moreover, the GDL 90 fuzzing experiment shows a worrying and critical lack of security in several electronic flight bag (EFB) applications. Out of 16 tested configurations, nine (56%) were impacted (crash, hang, and abnormal behavior) [6].

C. Experiments on maritime system

We conducted the following tests on the AIS system: noitemsep

- Spoofing
- Fake alert "Man OverBoard" (MOB)
- Fake alert "Vessel Collision"
- Jamming
- Overwhelming alerts
- Visual navigation disruption
- Logically invalid data encoding
- Denial-of-Service (DoS)
- Highly-Coordinated attackers attack
- Error handling test
- AIS preamble test

We implemented and tested 11 different tests/attacks on 19 AIS setups. The results showed that approximately 89% of

the setups were affected by DoS attacks. We also identified an implementation/specification flaw related to the AIS preamble during the experiments, which may affect the interoperability of different AIS devices [4].

D. Other results and applications

We have also experimented with expanding further application horizons of our lab. In one example, we have been successful in using our lab's pentesting platform and its flexible capabilities to research, implement and demonstrate the effectiveness of multiple infamous *log4j exploits* [36] (Remote Code Execution, Denial of Service) when vulnerable components are used within aviation (ACARS, ADS-B) and maritime (AIS) infrastructure [7]. In another example, we have relied on our testlab to extend the tooling around ADS-B 1090ES, and developed the `dump1030` – an open-source tool for monitoring the uplink ADS-B interrogations on 1030 MHz [37].

V. Conclusion

We presented our *"Unified Cybersecurity Testing Lab for Satellite, Aerospace, Avionics, Maritime, Drone (SAAMD) technologies and communications"* – a cybersecurity-focused, research-oriented, and industry-capable lab featuring a flexible pentesting, attack and evaluation platform. The lab aims at offering extensive and extensible capabilities to perform complex cybersecurity analyses and tests that are otherwise challenging to perform in the real world or in similar yet domain-constrained labs.

In particular, our lab and the vision behind it bridges the space and satellite technologies with the aviation, maritime, and drone technologies and protocols, thus allowing new types and levels of research, experimentation, and innovation to be performed in a unique and highly unified manner, both for cybersecurity and non-cybersecurity purposes.

Last but not least, we invite all interested researchers and industry practitioners in these domains to elaborate their novel and experimental ideas to achieve extensive collaborations and expand the utility of the lab to its maximum potential. All such comments, requests and queries are welcome at ancostin@jyu.fi.

Acknowledgments

Minor sections and some hardware of this research were kindly supported by the cascade funding from Engage KTN (SESAR Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No 783287) project *"Engage - 204 - Proof-of-concept: practical, flexible, affordable pentesting platform for ATM/avionics cybersecurity"*. All and any results, views, opinions are authors' only and do not reflect the official position of the European Union (and it's organizations and projects, including Horizon 2020 program and Engage KTN). Major parts of this research were supported by *"Decision of the Research Dean on research funding (20.04.2022)"* within the Faculty of Information Technology of University of Jyväskylä. Hannu Turtiainen also thanks the Finnish Cultural Foundation / Suomen Kulttuurirahasto (https://skr.fi/en) for supporting his Ph.D. dissertation work and research (under grant decision no. 00221059) and the Faculty of Information Technology of the University of Jyväskylä (JYU), in particular, Prof. Timo Hämäläinen, for partly supporting and supervising his Ph.D. work at JYU in 2021–2023. Syed Khandker was partially supported by the Finnish Foundation for Technology Promotion under the PoDoCo grant program.

References

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

[2] M. Strohmeier, M. Schäfer, V. Lenders, and I. Martinovic, "Realities and challenges of nextgen air traffic management: the case of ADS-B," *IEEE Communications Magazine*, vol. 52, 2014.

[3] M. Balduzzi, A. Pasta, and K. Wilhoit, "A Security Evaluation of AIS Automated Identification System," in *Proceedings of the 30th Annual Computer Security Applications Conference*, ser. ACSAC '14. New York, USA: ACM, 2014, p. 436–445.

[4] S. Khandker, H. Turtiainen, A. Costin, and T. Hämäläinen, "Cybersecurity Attacks on Software Logic and Error Handling Within AIS Implementations: A Systematic Testing of Resilience," *IEEE Access*, vol. 10, pp. 29 493–29 505, 2022.

[5] M. Smith, M. Strohmeier, V. Lenders, , and I. Martinovic, "On the security and privacy of ACARS," *Integrated Communications Navigation and Surveillance (ICNS)*, 2016.

[6] H. Turtiainen, S. Khandker, A. Costin, and T. Hamalainen, "GDL90fuzz: Fuzzing 'GDL-90 Data Interface Specification' Within Aviation Software and Avionics Devices - A Cybersecurity Pentesting Perspective," *IEEE Access*, 2022.

[7] A. Juvonen, A. Costin, H. Turtiainen, and T. Hämäläinen, "On Apache Log4j2 Exploitation in Aeronautical, Maritime, and Aerospace Communication," *IEEE Access*, vol. 10, pp. 86 542–86 557, 2022.

[8] H. Bojinov, E. Bursztein, and D. Boneh, "Xcs: cross channel scripting and its impact on web applications," in *Proceedings of the 16th ACM conference on Computer and communications security*, 2009, pp. 420–431.

[9] M. Schäfer, V. Lenders, and I. Martinovic, "Experimental Analysis of Attacks on Next-Generation Air Traffic Communication," in *Applied Cryptography and Network Security*. Springer Berlin Heidelberg, 2013.

[10] Z. Wu, T. Shang, and A. Guo, "Security Issues in Automatic Dependent Surveillance - Broadcast (ADS-B): A Survey," *IEEE Access*, vol. 8, 2020.

[11] D. Kožović and D. Djurdjevic, "Spoofing in aviation: Security threats on GPS and ADS-B systems," *Vojnotehnicki glasnik*, vol. 69, 2021.

[12] M. Strohmeier, V. Lenders, and I. Martinovic, "On the Security of the Automatic Dependent Surveillance-Broadcast Protocol," *IEEE Communications Surveys Tutorials*, vol. 17, 2015.

[13] M. R. Manesh, M. Mullins, K. Foerster, and N. Kaabouch, "A preliminary effort toward investigating the impacts of ADS-B message injection attack," in *IEEE Aerospace Conference*. IEEE, 2018.

[14] S. Eskilsson, H. Gustafsson, S. Khan, and A. Gurtov, "Demonstrating ADS-B AND CPDLC Attacks with Software-Defined Radio," in *Integrated Communications Navigation and Surveillance Conference (ICNS)*. IEEE, 2020.

[15] D. Lundberg, B. Farinholt, E. Sullivan, R. Mast, S. Checkoway, S. Savage, A. C. Snoeren, and K. Levchenko, "On the security of mobile cockpit information systems," in *ACM SIGSAC Conference on Computer and Communications Security*, 2014.

[16] D. A. Lundberg, "Security of ADS-B Receivers," Ph.D. dissertation, UC San Diego, 2014.

[17] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection*, vol. 4, 2011.

[18] M. R. Manesh and N. Kaabouch, "Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system," *International Journal of Critical Infrastructure Protection*, vol. 19, 2017.

[19] D. L. Mccallie, *Exploring Potential ADS-B Vulnerabilities in the FAA's NextGen Air Transportation System*. BiblioScholar, 2012.

[20] M. Strohmeier, V. Lenders, and I. Martinovic, "Security of ADS-B: State of the Art and Beyond," *IEEE Communications Surveys and Tutorials*, vol. 17, 2013.

[21] C. Ray, R. Gallen, C. Iphar, A. Napoli, and A. Bouju, "DeAIS project: Detection of AIS spoofing and resulting risks," in *OCEANS Genova*. IEEE, 2015, pp. 1–6.

[22] C. Ray, C. Iphar, and A. Napoli, "Methodology for Real-Time Detection of AIS Falsification," in *Maritime Knowledge Discovery and Anomaly Detection Workshop*, 2016, pp. 74–77.

[23] S. Khandker, H. Turtiainen, A. Costin, and T. Hamalainen, "Cybersecurity attacks on software logic and error handling within ADS-B implementations: Systematic testing of resilience and countermeasures," *IEEE Transactions on Aerospace and Electronic Systems*, 2021.

[24] E. D'Afflisio, P. Braca, and P. Willett, "Malicious AIS Spoofing and Abnormal Stealth Deviations: A Comprehensive Statistical Framework for Maritime Anomaly Detection," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 57, no. 4, pp. 2093–2108, 2021.

[25] M. Strohmeier, G. Tresoldi, L. Granger, and V. Lenders, "Building an avionics laboratory for cybersecurity testing," in *Proceedings of the 15th Workshop on Cyber Security Experimentation and Test*, 2022, pp. 10–18.

[26] M. C. Kim, W. S. Oh, J. H. Lee, J. B. Yim, and Y. D. Koo, "Development of a system integration laboratory for aircraft avionics systems," in *2008 IEEE/AIAA 27th Digital Avionics Systems Conference*, 2008.

[27] A. Viana Sanchez and C. Taylor, "Reference architecture test-bed for avionics (rasta): A software building blocks overview," *DASIA 2010-Data Systems In Aerospace*, vol. 682, p. 49, 2010.

[28] V. Dey, V. Pudi, A. Chattopadhyay, and Y. Elovici, "Security Vulnerabilities of Unmanned Aerial Vehicles and Countermeasures: An Experimental Study," in *2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID)*, 2018, pp. 398–403.

[29] A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti, "A large-scale analysis of the security of embedded firmwares," in *23rd {USENIX} Security Symposium ({USENIX} Security 14)*, 2014, pp. 95–110.

[30] A. Costin, A. Zarras, and A. Francillon, "Automated dynamic firmware analysis at scale: a case study on embedded web interfaces," in *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, 2016, pp. 437–448.

[31] S. Khandker, H. Turtiainen, A. Costin, and T. Hämäläinen, "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*, vol. 10, pp. 37 718–37 730, 2022.

[32] "McMurdo Smartfind G8 AIS Smartfind G8 Smartfind E8 EPIRB-AIS USER MANUAL," https://media1.svb-media.de/media/snr/512618/pdf/manual_2019-05-28_13-09-27_8e84e6e032df7e73b7a760e7711bfe96.pdf, accessed: 2022-10-24.

[33] *Radio Frequency Regulation 4*, TRAFICOM/185774/03.04.05.00/2021, Dec 2021.

[34] A.-V. Predescu and T. H. Stelkens-Kobsch, "Aviation Security Lab: A testbed for security testing of current and future aviation technologies," in *2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC)*, 2022, pp. 1–5.

[35] A. Costin, K. Syed, T. Hannu, and T. Hämäläinen, "Cybersecurity of COSPAS-SARSAT and EPIRB: threat and attacker models, exploits, future research," in *Workshop on Security of Space and Satellite Systems (SpaceSec) Network and Distributed System Security (NDSS) Symposium*, 2023.

[36] R. Hiesgen, M. Nawrocki, T. C. Schmidt, and M. Wählisch, "he Race to the Vulnerable: Measuring the Log4j Shell Incident," *arXiv preprint arXiv:2205.02544*, 2022.

[37] L. Laaksosaari, H. Turtianen, S. Khandker, and A. Costin, "dump1030: open-source plug-and-play demodulator/decoder for 1030MHz uplink," *IEEE Aerospace and Electronic Systems Magazine*, 2023.