



“Proof of concept: practical, flexible, affordable  
pentesting platform for ATM/avionics cybersec”

Andrei Costin ([ancostin@jyu.fi](mailto:ancostin@jyu.fi))

15.9.2021

# Agenda (15 min talk)

- Background
- Experiments and Results
- Acknowledgements
- Conclusion

# Background – #whoami

- Andrei Costin
  - PhD from EURECOM (2012-2015)
  - Senior Lecturer/Docent Assistant Professor at JYU (2017-present)
    - IoT/IIoT/embedded/CPS/CI security
    - System security, offensive security, vulnerabilities&exploitation, MLsec
    - Digital privacy
  - CEO/co-founder of [binare.io](https://binare.io) (2020-present)
    - Deep-tech cybersecurity spinoff from JYU

# Background – State of the Art

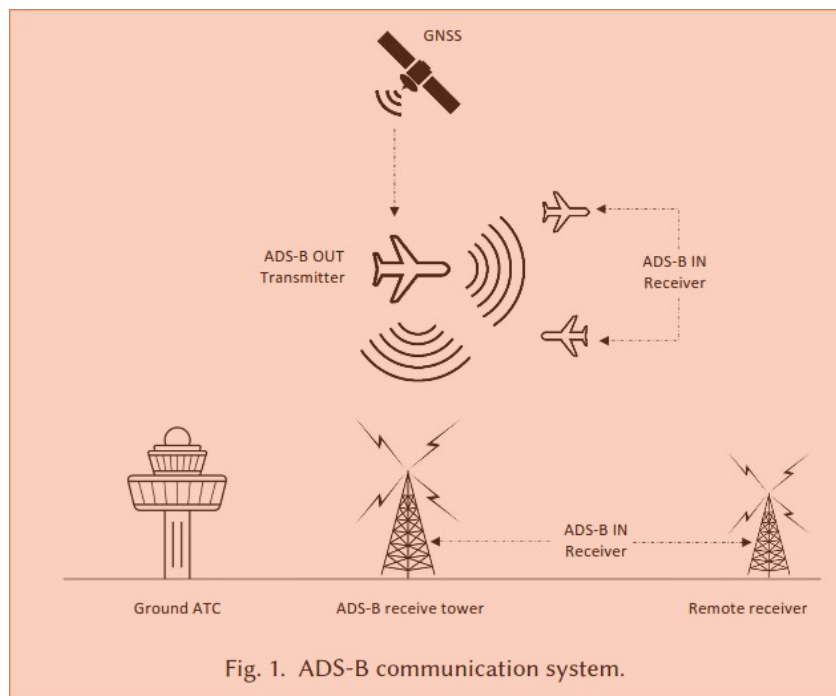
- Costin and Francillon (2012)

Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices	244	2012
A Costin, A Francillon		
BlackHat USA, 1-12		

- Strohmeier, Schäfer, Lenders, Martinovic et al. (2013+)

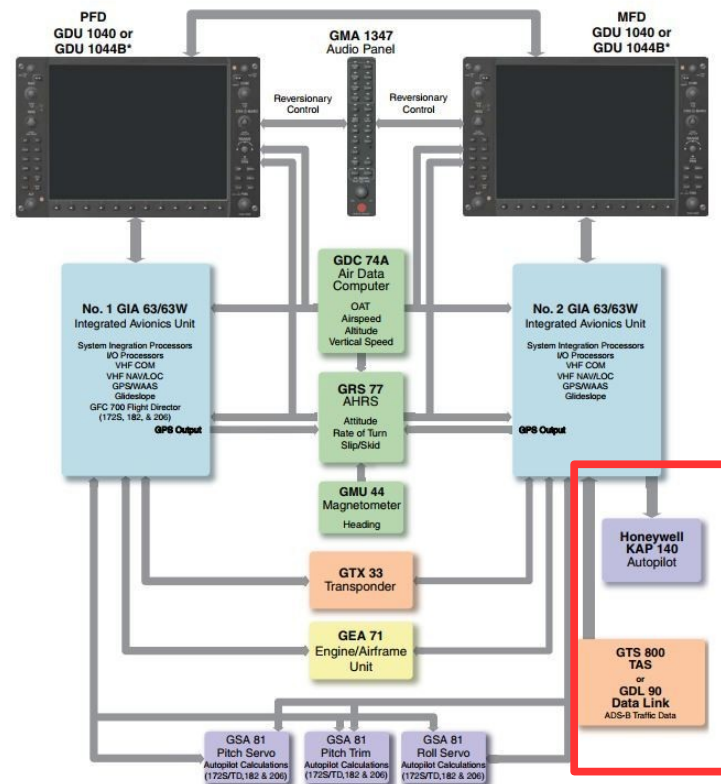
Realities and Challenges of NextGen Air Traffic Management: The Case of ADS-B	241	2014
M Strohmeier, M Schäfer, V Lenders, I Martinovic		
Communications Magazine, IEEE 52 (5), 111-118		
Bringing up OpenSky: A large-scale ADS-B sensor network for research	239	2014
M Schäfer, M Strohmeier, V Lenders, I Martinovic, M Wilhelm		
Proceedings of the 13th International Symposium on Information Processing in ...		
On the Security of the Automatic Dependent Surveillance-Broadcast Protocol	217	2014
M Strohmeier, V Lenders, I Martinovic		
IEEE Communications Surveys & Tutorials 17 (2), 1066-1087		
On Perception and Reality in Wireless Air Traffic Communication Security	98	2017
M Strohmeier, M Schäfer, R Pinheiro, V Lenders, I Martinovic		
IEEE Transactions on Intelligent Transportation Systems 18 (6), 1338-1357		

# Background – ADS-B, GDL-90



15.9.2021

(C)opyright. All Rights Resen  
Costin (ATM-cybersec)



\* The GDU 1040 is available in systems not using the GFC 700 Automatic Flight Control System.  
The GDU 1044B is available in systems using the Garmin GFC 700 Automatic Flight Control System.

Figure 1-1 Basic G1000 System

# Background – ADS-B, GDL-90

- What: airplanes, ATM/ATC, **satellites(!!)**, amateurs (RTL-SDR)
- Coverage: global, high + 2020 FAA mandate
- Unauthenticated: ADS-B, GDL-90
- Unencrypted: ADS-B, GDL-90
- Wireless: ADS-B
- Broadcast: ADS-B
- **Autopilots (KAP-140/IAU): ADS-B, GDL-90**



# Experiments and Results

- ADS-B Denial of Service (paper [1])
  - 68 configurations (hardware + software), with 11 distinct hardware chipsets
    - ~52% affected (crashed, unresponsive, unusable UI/UX)
      - **~25% crashed (within 0.5-2 minutes)**

Table 3. Percentage distribution of total setups and impacted/crashed setups, according to ADS-B type as well as Platform type, respectively.

Categorization →	ADS-B		Platform	
	1090ES	UAT978	Mobile/smartphone	Non-Mobile
Total systems	64.70%	35.30%	73.52%	26.28%
Impacted	41.17%	10.30%	32.35%	19.11%
Crashed	14.70%	10.30%	22.05%	2.95%

- Vendors: [redacted] (responsible disclosure)

# Experiments and Results

- GDL-90 Denial of Service (paper [3])
  - 16 configurations
    - Not all hardware/software support GDL-90 (e.g., proprietary protocols)
    - ~56% (9) affected (crashed, unresponsive, unusable UI/UX)
      - ~44% (7) crashed
  - Very common in most Garmin avionics devices
  - Vendors: [redacted] (responsible disclosure)



# Experiments and Results

- ADS-B – Novel coordinated attack (paper [2])

TABLE V: Summary of the effects of “Coordinated attack” on ADS-B 1090ES software with N=2 attackers impersonating the same ICAO address but injecting different values for other fields.

Configurations		Effects							
Hardware	Software	ICAO	Squawk	Flight	Velocity	Altitude	Latitude	Longitude	Latitude and Longitude
R	[REDACTED]	08.14	CDA	FLC	FLC	FLC	FLC	WRG	WRG
		08.14	CDA	FLC	FLC	FLC	FLC	WRG	WRG
		08.14	CDA	FLC	FLC	FLC	FLC	FST	FST
		08.14	(DNT)	(DNT)	(DNT)	(DNT)	(DNT)	(DNT)	(DNT)
P	[REDACTED]	08.14	CDA	FLC	FLC	FLC	FLC	FST	FLC
		08.14	CDA	FLC	FLC	FLC	FLC	FST	FLC
P	[REDACTED]	08.14	CDA	FLC	FLC	FLC	FLC	FLC	FLC
A	[REDACTED]	08.14	CDA	INA	FLC	FLC	FLC	WRG	WRG
A	[REDACTED]	08.14	CDA	INA	FLC	FLC	FLC	WRG	WRG
P	[REDACTED]	08.14	CDA	FST	FLC	FLC	WRG	FLC	FLC
P	[REDACTED]	08.14	CDA	INA	INA	INA	FLC	FLC	FLC
C	[REDACTED]	08.14	CDA	FST	FLC	FLC	WRG	FLC	FLC
C	[REDACTED]	08.14	CDA	INA	INA	INA	FLC	FLC	FLC

# Experiments and Results

- [Video Demo]

# Results – Publications (25.1.2022)

- <https://ieeexplore.ieee.org/abstract/document/9667309>

@article{khandker2021cybersecurity,  
title={Cybersecurity attacks on software logic and error handling within ADS-B implementations: Systematic testing of resilience and countermeasures},  
author={Khandker, Syed and Turtiainen, Hannu and Costin, Andrei and Hamalainen, Timo},  
journal={IEEE Transactions on Aerospace and Electronic Systems},  
year={2021},  
publisher={IEEE}  
}

Journals & Magazines > IEEE Transactions on Aerospace... > Early Access

## Cybersecurity attacks on software logic and error handling within ADS-B implementations: Systematic testing of resilience and countermeasures

Publisher: IEEE [Cite This](#) [PDF](#)

Syed Khandker ; Hannu Turtiainen ; Andrei Costin ; Timo Hamalainen [All Authors](#)

[Full Text Views](#)

[Open Access](#)  
Under a [Creative Commons License](#)

**Abstract**

[Authors](#)

[Keywords](#)

[Metrics](#)

**Abstract:**  
Automatic Dependent Surveillance-Broadcast (ADS-B) is a cornerstone of the next-generation digital sky and is now mandated in several countries. However, there have been many reports of serious security vulnerabilities in the ADS-B architecture. In this paper, we demonstrate and evaluate the impact of multiple cyberattacks on ADS-B via remote radio frequency links that affected various network, processing, and display subsystems used within the ADS-B ecosystem. Overall we implemented and tested 12 cyberattacks on ADS-B in a controlled environment, out of which 5 attacks were presented or implemented for the first time. For all these attacks, we developed a unique testbed that consisted of 13 hardware devices and 22 software that ran on Android, iOS, Linux, and Windows operating systems, which result in a total of 36 tested configurations. Each of the attacks was successful on various subsets of the tested configurations. In some attacks, we discovered wide qualitative variations and discrepancies in how particular configurations react to and treat ADS-B inputs that contain errors or contradicting flight information, with the main culprit almost always being the software implementation. In some other attacks, we managed to cause Denial of Service (DoS) by remotely crashing/impacting more than 50% of the test-set that corresponded to those attacks. Besides demonstrating successful attacks, we also implemented, investigated, and report herein some practical countermeasures to these attacks. We demonstrated that the strong relationship between the received signal strength and the distance-to-emitter might help verify the aircrafts advertised ADS-B position and distance. For example, our best machine learning models achieved 90% accuracy in detecting spoofed ADS-B signals, which may be effectively used to distinguish ADS-B signals of real aircraft from spoofed signals of attackers.

Published in: IEEE Transactions on Aerospace and Electronic Systems ( Early Access )

Page(s): 1 - 1 [DOI: 10.1109/TAES.2021.3139559](#)

Date of Publication: 31 December 2021 [Publisher: IEEE](#)

# Results – Publications

- [1] *“Practical denial-of-service and combined high-level attacks on real-world ADS-B, ATC, ATM hardware and software”*
  - ACM TOPS, under review
- [2] *“Cybersecurity attacks against software logic and error handling within ADS-B implementations: systematic testing of resilience, and implementation of some countermeasures”*
  - IEEE TAES, under review
- [3] *“Fuzzing ‘GDL-90 Data Interface Specification’ within aviation software and avionics devices – a cybersecurity perspective”*
  - Elsevier COSE, under review

# Acknowledgements

- Team (University of Jyväskylä)
  - Andrei Costin, Hannu Turtiainen, Syed Khandker, Timo Hamalainen

# Acknowledgements

- Funding

- EngageKTN – *project 204 (1.7.2020-30.6.2021)*



- JYU: *Decision of the Research Dean on research funding within the IT Faculty (07.04.2021)*
  - Finnish Cultural Foundation / Suomen Kulttuurirahasto: *grant decision 00211119*

# Conclusion

- Attacks on ADS-B are **feasible, more dangerous and (very likely) imminent**
- Attacks (by Costin, Turtiainen, Khandker, Hamalainen):
  - Demonstrated: DoS – OK for SocialNetworks, **catastrophic for safety-critical**
  - Work-in-progress: RCE (Remote Code Execution) – **(sub-)system takeover**
    - Similar: “DHS says it remotely hacked a Boeing 757 sitting on a runway” (2017)
- Most/all ADS-B detect/protect solutions mainly on paper :(
- Mobile EFBs **unregulated** – used by pilots, checked/guaranteed by **nobody!**
- For collaborations (research/funding, business): [ancostin@jyu.fi](mailto:ancostin@jyu.fi)
- Q&A



“Proof of concept: practical, flexible, affordable  
pentesting platform for ATM/avionics cybersec”

Andrei Costin ([ancostin@jyu.fi](mailto:ancostin@jyu.fi))

15.9.2021