Airlines Hacking: ADS-B Vulnerabilities, In-flight WiFi Attacks, and Maintenance System Exploits

Abstract

This research investigates the cybersecurity threats in the aviation sector, focusing on three critical components: ADS-B broadcast systems, in-flight WiFi networks, and aircraft maintenance web systems. Through simulated environments and proof-of-concept tools, we demonstrate how attackers can exploit unsecured communication protocols, manipulate network traffic, and compromise backend systems. Our aim is to raise awareness and propose countermeasures for improving aviation cybersecurity standards.

Problem Statement & Objective

With increasing digitization in aviation, aircraft systems and connectivity are vulnerable to cyber threats. This project aims to:

- Examine how unencrypted ADS-B signals can be sniffed or spoofed.
- Simulate real-world in-flight WiFi threats using rogue AP and DNS poisoning.
- Create a vulnerable maintenance app to demonstrate web-based flaws.

Literature Review

Key references:

1. ICAO Cybersecurity Policy
2. "ADS-B Security Vulnerabilities" (IEEE)
3. DEF CON presentations on in-flight WiFi hacking
4. CVEs related to airline IT systems
5. Aviation ISAC threat reports

Research Methodology

Airlines Hacking: ADS-B Vulnerabilities, In-flight WiFi Attacks, and Maintenance System Exploits

- Tools used: Python, Flask, pyModeS, dump1090, dnschef, airmon-ng
- Testing environment: Simulated lab using Kali Linux, WiFi adapters, and Flask server
- Approach: Simulated real-world attack vectors in controlled environment

Tool Implementation

- adsb_sniffer.py: Captures and parses live ADS-B packets.
- rogue_ap.sh + dnschef: Creates fake WiFi to test phishing potential.
- vulnerable_maintenance_app.py: A login system vulnerable to SQL Injection.

Results & Observations

- ADS-B traffic is readable in plaintext.
- DNS spoofing successfully redirected traffic in the captive portal test.
- SQLi flaw allowed unauthorized access to a mock admin panel.

Ethical Impact & Market Relevance

- Ethical use only: Demonstrations were done in isolated environments.
- Relevance: Airlines, aerospace companies, and cybersecurity professionals can use these findings to reinforce cyber defenses.

Future Scope

- Simulate ADS-B spoofing (not just sniffing).
- Use machine learning to detect anomalies in aircraft signals.
- Integrate secure login and audit mechanisms in maintenance apps.

Airlines Hacking: ADS-B Vulnerabilities, In-flight WiFi Attacks, and Maintenance System Exploits

References

1. ICAO Aviation Cybersecurity Manual
2. FAA ADS-B Security Guidelines
3. "Attacking ADS-B Systems" DEF CON Talk
4. Kali Linux Wireless Tools Documentation
5. MITRE CVE Database
6. OWASP Top 10
7. ADSBExchange community tools
8. pyModeS documentation
9. DNSChef GitHub repo
10. Flask Security Best Practices