Airline Hacking Research

Research Based Analysis By:
Haridra Bhadauria
Siddhesh Dalvi
Vaishnavi Naik

Introduction to Aviation Cybersecurity

- Critical Infrastructure: Aviation relies on interconnected digital systems—from aircraft to airports—making it a high-value cyber target.
- Growing Attack Surface: Increased use of IoT, Wi-Fi, and cloud-based services in aviation has expanded potential entry points for hackers.
- Safety & Trust at Risk: Cyberattacks can disrupt flights, leak passenger data, and damage public confidence in airline safety.

Why Aviation is a Target for Hackers ?

High Value Passenger Data

Passenger data includes names, contact details, passport numbers, payment information, travel itineraries, and frequent flyer details.

Life-critical systems

These are systems essential to the safety and operation of flights, such as avionics, air traffic control (ATC), flight management systems (FMS), and communication networks.

Why Aviation is a Target for Hackers ?

Global Infrastructure

Aviation operates globally and includes interconnected systems like airline IT networks, airport operations, radar systems, and international flight scheduling.

Legacy Systems

Many aviation systems still run on outdated software and hardware that lack modern security protocols.

System most at Risk !

ADS-B

ADS-B is a surveillance technology that allows aircraft to automatically broadcast their position, speed, and altitude to air traffic controllers and other aircraft.

Aircraft Maintain

Aircraft maintenance includes all inspection, repair, overhaul, and servicing activities to ensure aircraft are safe, airworthy, and in working condition.

System most at Risk !

Inflight Wi-Fi

In-flight Wi-Fi is a wireless internet service provided to passengers and crew during flight.

Air Traffic Control

ATC is a ground-based service that manages the safe and orderly flow of air traffic in the air and on the ground.

Airport IT

This refers to the technology systems and networks that support airport operations and services.

Common Cyber Threats In Aviation

01

Spoofing

Attackers can spoof GPS signals, Automatic Dependent Surveillance–Broadcast (ADS-B), or radio communications, misleading aircraft or ground systems about the position, identity, or instructions of planes.

02

Jamming

Jamming GPS or radio frequencies can disrupt aircraft n dense airspaces, this can pose major safety risks and force rerouting or grounding of flights.navigation and communication with air traffic control.

Common Cyber Threats In Aviation

03 Man-in-the-middle Attack

Could be used to intercept communications between pilots and ATC, or between aircraft and airline operations centers.May lead to false commands, data manipulation, or unauthorized access to sensitive systems.

04 Malware

Can infect ground-based airline systems (e.g., flight scheduling, ticketing, baggage handling).
Malware in avionics or flight planning systems could compromise flight safety and operations.

Common Cyber Threats In Aviation

05

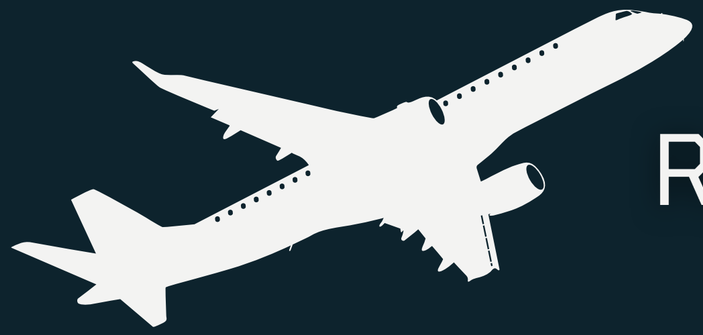
Insider Threats

Insiders might leak sensitive data, disable systems, or assist external hackers.
Their access to secure zones and systems makes them especially dangerous and hard to detect.

06

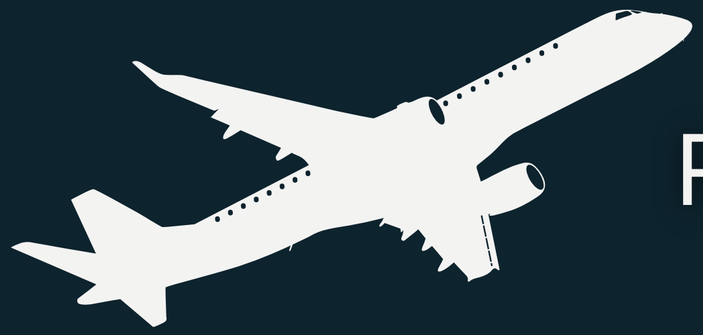
Ramsomware

Can paralyze airport operations, flight check-ins, fuel systems, or airline IT infrastructure.
Leads to mass cancellations, delays, financial losses, and reputational damage.



Real-World Incident : Air India 2021

- Incident: Global IT provider SITA was hacked in Feb 2021, affecting Air India’s passenger data.
- Data Leaked: Personal details of 4.5 million passengers—names, passports, ticket info, and partial credit card data.
- Delay in Disclosure: Air India informed the public in May, two months after being alerted.
- Root Cause: Breach occurred via third-party systems (SITA), not Air India's own infrastructure.
- Impact: Passengers advised to reset passwords; raised concerns over aviation cybersecurity and third-party risks.



Real-World Incident : Qantas 2024

1. Frequent Flyer Data Breach (Oct 2024)

- Contractors misused system access to steal frequent flyer points.
- Data of ~1,000 passengers compromised (passports, bookings).
- Breach detected via customer complaint; contractors suspended.
- No misuse of passport data confirmed.
- Highlighted third-party access risks.

2. App Privacy Glitch (May 2024)

- App bug exposed some users' booking info to others.
- No financial data leaked; issue fixed within hours.
- Caused by system update caching error.
- Qantas apologized and reinforced testing protocols.

Security Tools Used In Stimulations

1. ADS-B : dump1090,SDR

1.dump1090

- An open-source ADS-B decoder that captures and displays aircraft broadcast data (on 1090 MHz).
- Use in Research:
  - Real-time tracking of aircraft nearby.
  - Visualizing aircraft positions and messages.
  - Helps researchers understand how ADS-B works and what data is exposed.

2. SDR (Software Defined Radio)

- A radio communication system where components like tuners and filters are implemented in software (e.g., RTL-SDR).
- Use in Research:
  - Captures raw ADS-B signals from aircraft.
  - Enables replay, analysis, or spoofing simulations.
  - Low-cost tool for experimenting with aviation frequencies.

Security Tools Used In Stimulations

2.Inflight Wi-Fi: Wireshark,Aircrack-ng

Wireshark

- A powerful open-source network protocol analyzer used for capturing and inspecting data packets.
- Use in Research:
  - Monitors unencrypted traffic over in-flight Wi-Fi.
  - Analyzes HTTP, DNS, and login data for vulnerabilities.
  - Useful for identifying weak encryption and poor network segmentation.

2. Aircrack-ng

- A suite of tools for auditing and attacking Wi-Fi networks.
- Use in Research:
  - Captures and cracks WPA/WPA2 Wi-Fi passwords.
  - Performs packet injection and deauthentication attacks.
  - Simulates threats like man-in-the-middle (MITM) and denial-of-service (DoS).

Security Tools Used In Stimulations

3.Aircraft Maintenance:Burpsuite

Burp Suite

- A professional web vulnerability scanner and proxy tool used to test and exploit security flaws in web applications.
- Use in Airline Maintenance Research:
  - Intercepts and Analyzes Requests: Captures traffic between maintenance web apps and servers to inspect for vulnerabilities.
  - Authentication Testing: Identifies weak login systems, exposed credentials, and session flaws.
  - Injection Attacks: Simulates SQL injection, command injection, and XSS in backend maintenance portals.
  - Privilege Escalation Checks: Tests if low-level users can gain unauthorized access to admin controls or aircraft diagnostic data.
- Relevance:
- Many modern maintenance platforms are web-based; Burp Suite helps test their security posture without touching actual aircraft systems.

Security Tools Used In Stimulations

4.Air Traffic Control: Scapy

Scapy

- A powerful Python-based tool for packet crafting, sending, sniffing, and manipulating network traffic.
- Use in ATC Hacking Research:
  - Spoofing Packets: Simulates fake aircraft data or commands in Air Traffic Control simulations.
  - Testing Protocol Weaknesses: Crafts custom ADS-B, TCP, or other protocol packets to test system responses.
  - Replay Attacks: Sends recorded or modified traffic to simulate radar spoofing or communication interference.
  - Penetration Testing: Evaluates how ATC systems handle malformed or malicious data.

- Relevance:
- Helps researchers understand and demonstrate how ATC communications could be spoofed, jammed, or disrupted without attacking real systems.

Security Tools Used In Stimulations

5.Airport IT Infrastructure:Kali Linux

Kali Linux

- A Debian-based Linux distribution packed with cybersecurity tools for penetration testing and ethical hacking.
- Use in Airport IT Research:
  - Network Scanning: Tools like Nmap and Netdiscover identify vulnerable devices on airport networks.
  - Exploitation: Frameworks like Metasploit simulate real-world attacks on baggage systems, check-in kiosks, and internal servers.
  - Credential Cracking: Tools like Hydra and John the Ripper test for weak or default passwords used in airport systems.
  - Social Engineering: Kali includes phishing toolkits (e.g., Social Engineering Toolkit) to test human-factor vulnerabilities.
- Relevance:
- Ideal for simulating multi-layered attacks on airport infrastructure, from public Wi-Fi to backend logistics systems, in a controlled environment.

Types of Threat Actors

Nation-State Actors

Government-backed hackers targeting critical infrastructure.

Hacktivists

Attack for political or social causes (e.g., Anonymous).

Insiders

Employees or contractors misusing internal access.

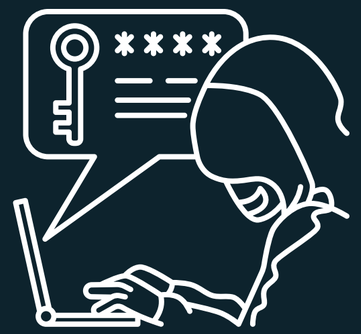
Cybercriminals

Seek financial gain (e.g., ransomware gangs).

Script Kiddies

Inexperienced hackers using existing tools to cause mischief.

ABS-B Vulnerabilities



- No Encryption – All ADS-B signals are transmitted in plain text and can be intercepted by anyone with basic equipment.
- No Authentication – The system cannot verify if a signal is from a legitimate aircraft.
- Susceptible to Spoofing – Hackers can inject fake aircraft into the system to confuse pilots or air traffic control.
- Easy Signal Jamming – ADS-B uses a known frequency, making it easy to disrupt with jamming attacks.
- Impact- Exploiting ADS-B can lead to false traffic alerts, route disruptions, and even potential mid-air collision risks

Inflight Wi-Fi Risks

- Shared Network-Passengers and crew often use the same unsecured network, increasing risk of cyber intrusion.
- Man-in-the-Middle (MITM) Attacks- Hackers can intercept data between users and websites to steal sensitive info.
- Access to Aircraft Systems - poorly segmented networks may allow attackers to move from Wi-Fi to critical flight systems.
- Data Theft- Unencrypted communications over Wi-Fi can expose login credentials and personal data.
- Malware Injection- Hackers can exploit the Wi-Fi to push malware to passenger devices or connected airline systems.

Aircraft Maintenance System Risks

- Remote Access Exploits- Maintenance systems often connect remotely, making them vulnerable to unauthorized access.
- Malware Attacks- Infection of ground systems can corrupt maintenance data or disable alerts.
- Data Manipulation- Hackers can alter maintenance logs, leading to missed inspections or false system health reports.
- Weak Authentication- Poor login controls can allow unauthorized users into critical diagnostic tools.
- Supply Chain Vulnerabilities- Third-party tools or software updates used in maintenance can be compromised.

Air Traffic Control (ATC) Threats

- Communication Hijacking- Hackers can spoof pilot-ATC radio communications, sending false instructions.
- Radar Spoofing- Fake aircraft signals can be injected, confusing controllers and pilots.
- System Jamming- Disruption of radar or ADS-B signals can impair aircraft tracking.
- Data Breaches- ATC systems store sensitive flight plans and coordination data—valuable for espionage or disruption.
- Legacy Systems- Many ATC systems run outdated software, lacking modern cybersecurity protections.

Airport IT Infrastructure Risks

- Weak Network Segmentation- Lack of separation between critical systems (e.g., baggage, check-in) and public networks increases the risk of cross-system attacks.

- Third-Party Access- Vendors and contractors with access to airport systems can be entry points for cyberattacks.

- Physical Security- Unsecured terminals and staff areas can be targeted for physical breaches, gaining access to sensitive IT systems.

- Ransomware- Attackers can lock down airport operations, causing delays, cancellations, and financial losses.

- Legacy Systems- Outdated hardware and software may be vulnerable to exploitation, exposing critical airport operations to threats.

Ethical and Legal Challenges

01

Ethical Challenges

- Risk of Misuse: Published research could be exploited by malicious hackers.
- Passenger Safety: Testing vulnerabilities on live systems can endanger lives.
- Responsible Disclosure: Balancing public awareness with protecting sensitive flaws.
- Data Privacy: Accessing real airline or passenger data raises privacy concerns.

Ethical and Legal Challenges

02

Legal Challenges

- Cybercrime Laws: Unauthorized testing or access may violate national and international laws (e.g., Computer Misuse Act, CFAA).
- Jurisdiction Issues: Airlines and systems span multiple countries with varying laws.
- NDAs and IP Protection: Research may conflict with non-disclosure or intellectual property rights.
- Liability Risks: Researchers or institutions could face lawsuits for unintended harm.

Financial and Reputational Impact

FINANCIAL IMPACT :

- Operational Disruption: Flight delays, cancellations, and rerouting costs.
- Ransom Payments: In cases of ransomware attacks.
- Regulatory Fines: For violating data protection laws (e.g., GDPR).
- Litigation Costs: Lawsuits from affected passengers or partners.
- System Recovery: High costs for investigation, patching, and restoring systems.

Financial and Reputational Impact

REPUTATIONAL IMPACT :

- Loss of Customer Trust: Fear of data misuse and safety risks.
- Brand Damage: Negative media coverage harms airline credibility.
- Business Loss: Reduced bookings and loss of corporate clients.
- Partnership Risks: Code-share or alliance partners may reconsider collaboration.

Key Observations from Stimulations

01 ADS-B Spoofing is feasible

02 Wi-Fi lacks segmentation

03 Exposed web dashboards

04 ATC endpoints are visible online

Recommendations for Stakeholders

01 Build Trust Network

02 Standardize Protocols

03 Invest in Detection tools

04 Train Staff

FUTURE SCOPE

01 AI-based Intrusion detection

02 Quantum-safe encryption

03 Red-teaming for training

04 Global legal collaboration