AIRLINES HACKING: ADS-B VULNERABILITIES, IN-FLIGHT WIFI EXPLOITS, AND MAINTENANCE SYSTEM THREATS

Presented : Darshana Bhaud

OVERVIEW

- Introduction
- Problem
- Solution
- Tool Breakdown
- Real World cases
- Future Enhancement
- Conclusion

INTRODUCTION

- Aviation is becoming highly connected (ADS-B, in-flight WiFi, etc.).
- Cyber threats can exploit unsecured systems.
- Focus on ADS-B vulnerabilities—critical for aircraft tracking & safety.

PROBLEM

- ADS-B broadcasts unprotected data.
- Exposed to spoofing, jamming, and data manipulation.
- No authentication or encryption.
- Need tools to detect anomalies & monitor threats.

OBJECTIVE

- Simulate aircraft data broadcast (ADS-B).
- Detect suspicious activities.
- Visualize aircraft in real-time.
- Log activities for analysis.

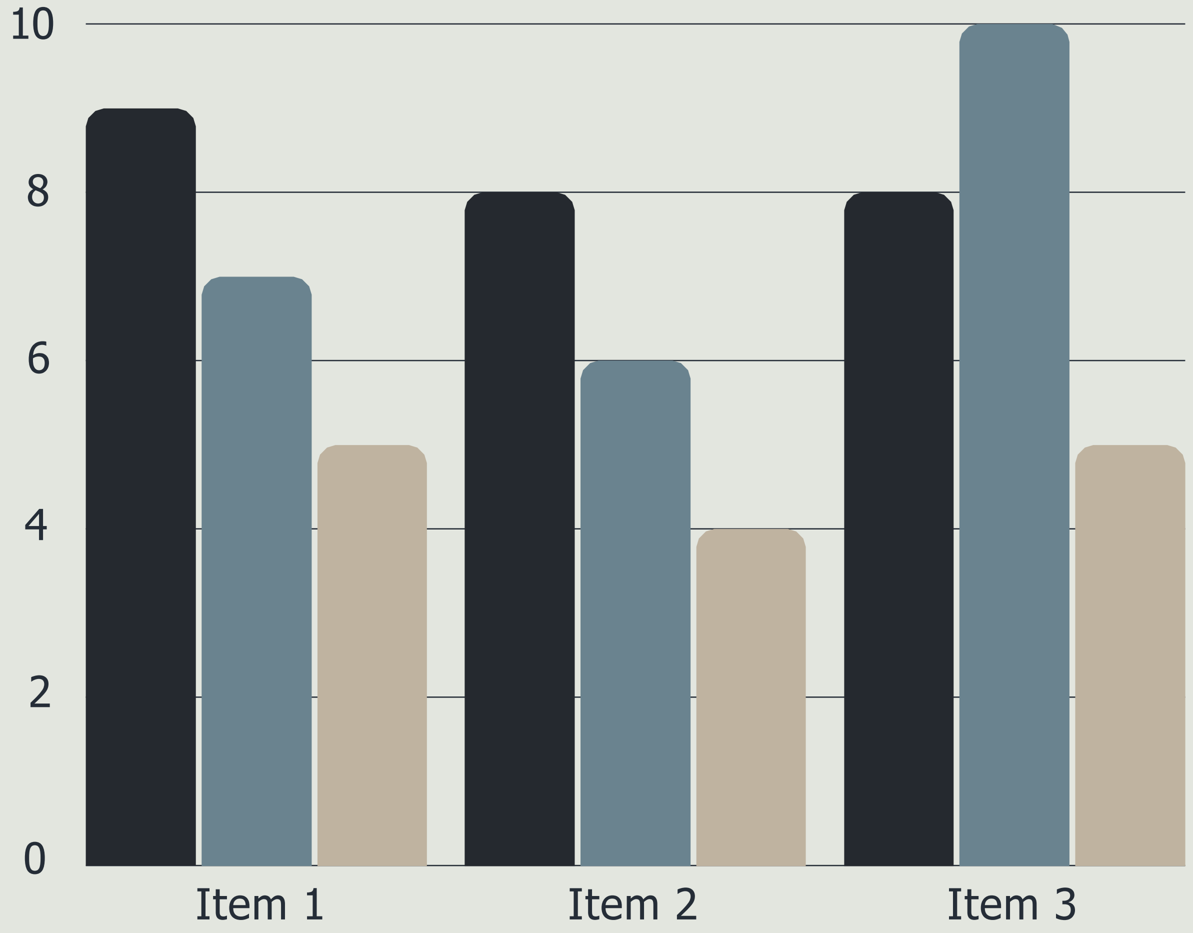
CODE & TOOL BREAKDOWN

- Data Generator: Creates random aircraft data.
- Suspicious Detection: Flags high speed & same position.

- Visualization: Live aircraft tracking on a 2D map.
- Logging: All data & anomalies saved to CSV.

REAL-WORLD USE CASES

- Air Traffic Control threat monitoring.
- Aviation security research.
- Training tool for cybersecurity teams.
- Identifying spoofed aircraft or abnormal patterns.



FUTURE ENHANCEMENTS

- Simulate advanced attacks (ghost aircraft, spoofed identity).
- Integrate with real ADS-B data via SDR.
- Use Machine Learning for smarter detection.

CONCLUSION

- ADS-B signals are open and can be easily hacked or misused.
- Attackers can send fake aircraft data or make flights appear where they don’t exist.
- Our simulator creates these fake scenarios to show how such attacks might look.

- It also detects suspicious activities like very high speeds or repeating locations.
- This helps us understand how airlines can use simple monitoring tools to catch early signs of attacks.
- The project highlights the need for stronger security, real-time alerts, and smarter systems to keep flights safe.

Thank You

For your attention