Risk Assessment for a Large International Airport in the USA

1. Introduction

A large international airport in the USA is a critical infrastructure, serving millions of passengers annually, with operations involving airlines, government agencies (TSA, customs, etc.), airport management, and various third-party service providers. The complexity of systems and the high volume of sensitive data processed make it a target for cyber threats.

---

2. Threat Modelling Process (OWASP)

2.1 Identify and Define the Scope

- **Scope:** All digital systems and networks within the airport, including:
  - Passenger information systems
  - Baggage handling systems
  - Air traffic control systems
  - Airport operational databases
  - Public Wi-Fi networks
  - Physical access control systems
  - Payment processing systems
- **Stakeholders:** Airport management, IT personnel, airline companies, government agencies, passengers, vendors.

2.2 Assemble Threat Model Components

2.2.1 Assets

- **Critical Systems:**
  - Air traffic control systems
  - Baggage handling systems
  - Passenger information systems
  - Security screening systems
- **Sensitive Data:**
  - Passenger personal information
  - Financial data (credit card info)
  - Employee credentials
  - Airport operational data

2.2.2 Attack Surfaces

- **Network Exposure:** Public Wi-Fi, internal networks, communication links between airport systems, external connections with airlines, remote access points.
- **Physical Exposure:** Terminals, data centers, security checkpoints, access to sensitive areas (e.g., runways).
- **Human Factors:** Insider threats, third-party contractors, social engineering vulnerabilities.

2.2.3 Threat Actors

- **Cybercriminals:** Target financial information, PII, or cause disruption.
- **Insiders:** Disgruntled employees or contractors with authorized access.
- **Hacktivists:** May target the airport for political reasons.

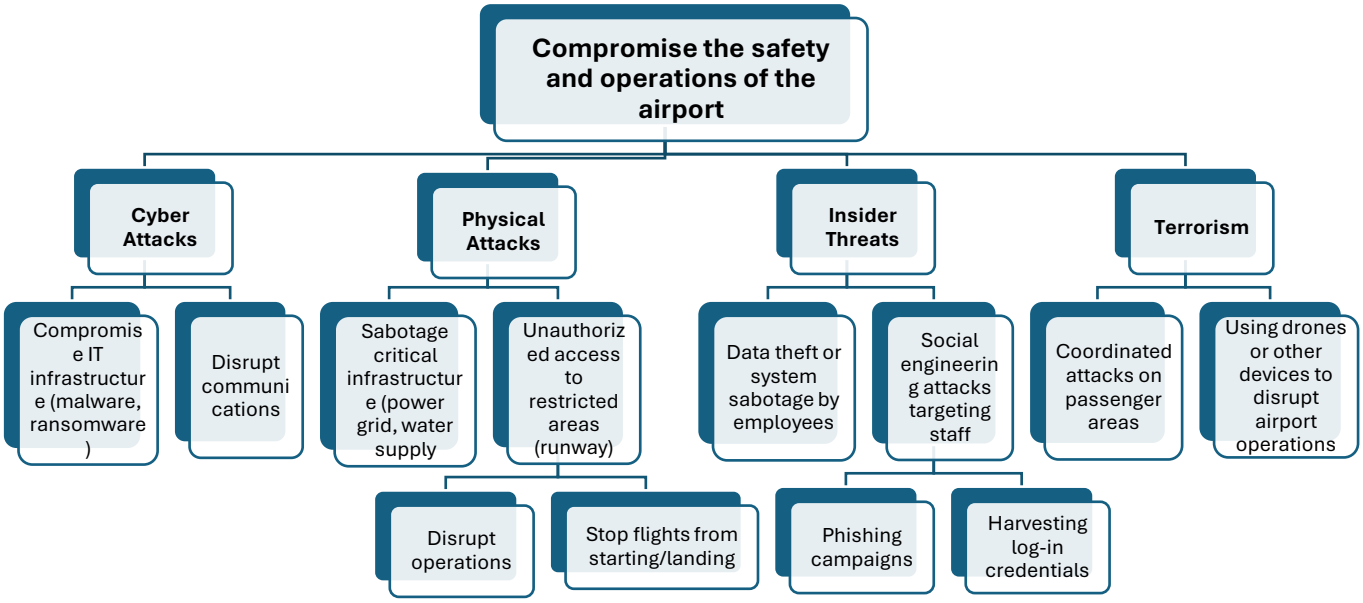
---

3. Threat Modelling Methodology

3.1 STRIDE Framework (from the Threat Modelling Manifesto)

Category	Asset/Component	Threat Description	Mitigation
Spoofing	ATC Systems	An attacker may impersonate an authorized entity to send false commands to aircraft.	Implement strong authentication (e.g., multi-factor) and encryption for communication channels.
Tampering	BHS	An attacker could alter baggage routing data, causing bags to be misrouted or lost.	Use data integrity checks (e.g., hashing) and access controls to prevent unauthorized modifications.
Repudiation	Payment Systems	An attacker denies making unauthorized transactions, leading to financial loss or disputes.	Implement strong authentication and logging mechanisms to ensure non-repudiation.
Information Disclosure	PIS	Unauthorized access to passenger PII or operational data could lead to data breaches.	Encrypt sensitive data at rest and in transit, and enforce strict access controls.
Denial of Service (DoS)	ATC Systems	An attacker may overload ATC systems, disrupting communication and endangering flights.	Deploy redundant systems and implement network traffic monitoring to detect and mitigate DoS attacks.
Elevation of Privilege	Access Control Systems	An attacker could exploit vulnerabilities to gain unauthorized access to restricted areas or systems.	Regularly update and patch systems, implement role-based access control (RBAC), and conduct security audits.

3.2 Attack Tree:



---

4. Risk Assessment Matrix

Threat	Likelihood	Impact	Risk Level
Phishing Attack on Employees	High	High	Severe
DoS Attack on ATC Systems	Medium	Critical	Severe
Data Breach of PII	High	High	Severe
Tampering with BHS	Medium	High	High
Ransomware Attack	Medium	High	High
Insider Threat	Medium	Medium	Moderate
Unauthorized Access to Secure Areas	Low	Critical	High

5. Mitigation Strategies

5.1 Technical Controls

- **Implement Multi-Factor Authentication (MFA):** Reduce the risk of unauthorized access due to compromised credentials.
- **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):** Deploy to monitor and defend against suspicious network activities.

- **Network Segmentation:** Isolate critical systems (e.g., ATC, BHS) to limit the impact of a breach.
- **Encryption:** Ensure that all sensitive data, both at rest and in transit, is encrypted.

5.2 Administrative Controls

- **Regular Security Training:** Conduct phishing awareness and social engineering resistance training for all employees.
- **Access Control Policies:** Enforce the principle of least privilege across all systems.
- **Vendor Risk Management:** Conduct thorough vetting and regular security assessments of third-party vendors.

5.3 Physical Security Controls

- **CCTV Monitoring:** Continuous surveillance of sensitive areas.
- **Biometric Access Controls:** Secure critical infrastructure areas (e.g., ATC towers, data centers) with biometric locks.
- **Security Audits:** Regular audits to ensure compliance with security policies and identify potential vulnerabilities.