Threat Model: Large International Airport (USA)

Ojabo, John Heart

Introduction and Scope

Threat modeling is a structured process for identifying potential threats, vulnerabilities, and attacks that could compromise a system or application. For critical infrastructure like a major international airport, a comprehensive threat model is essential to understand potential risks and develop effective security measures. The scope of this threat model includes:

- Physical Infrastructure
- Operational Technology (OT)
- Information Technology (IT)
- Personnel
- Processes

Identifying Assets

Key assets that require protection within the airport environment include:

- Safety, Security, Data, Physical Assets, etc

Threat Identification (Using STRIDE)

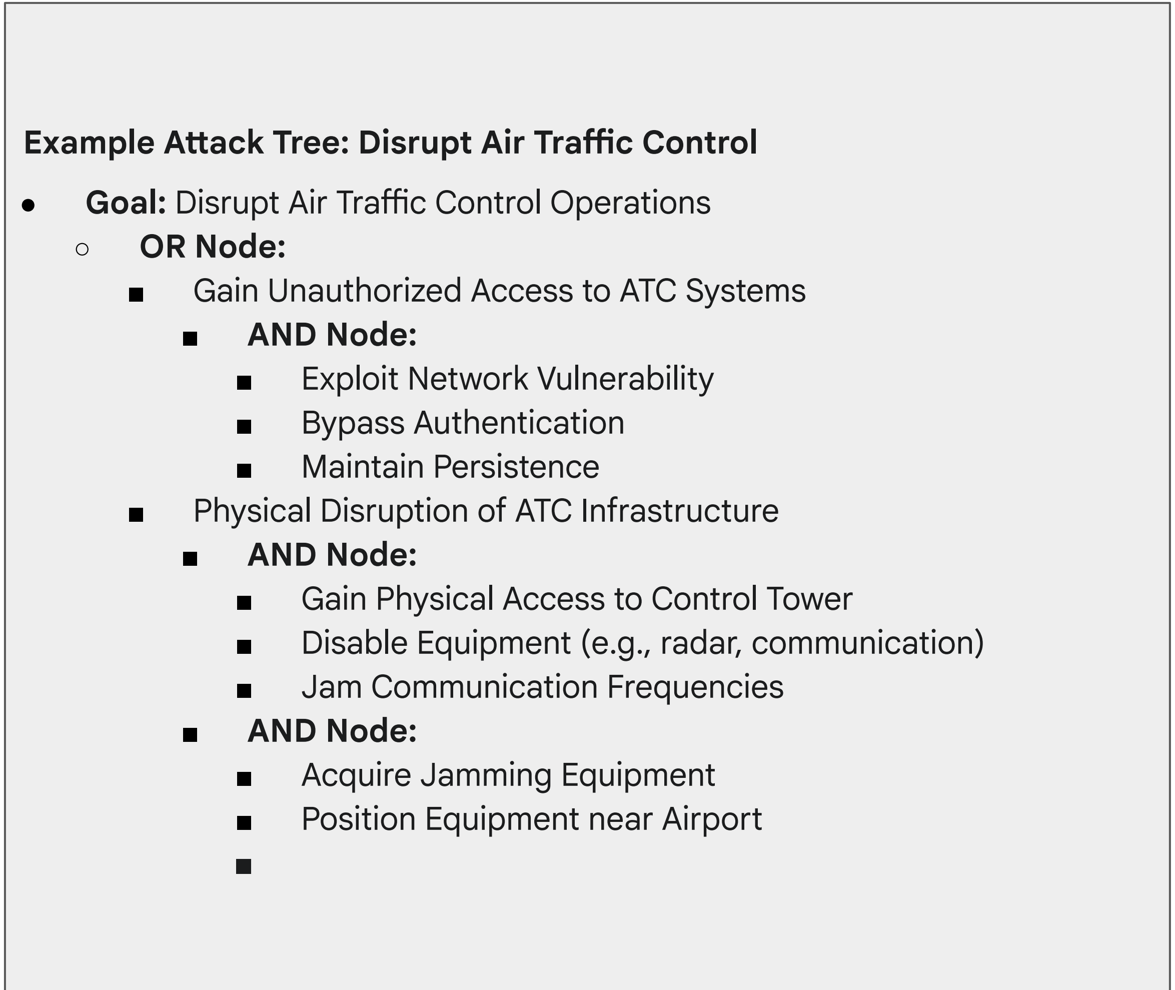
- S - Spoofing Identity
- T - Tampering with Data
- R - Repudiation
- I - Information Disclosure
- D - Denial of Service (DoS
- E - Elevation of Privilege

Attack Libraries (MITRE ATT&CK):

While STRIDE helps categorize threats, attack libraries like MITRE ATT&CK can provide detailed information on the **tactics, techniques, and procedures (TTPs)** that adversaries might use to carry out these threats

Attack Trees

Attack trees can be used to break down high-level threats into specific, achievable steps an attacker would need to take. This helps visualize attack paths and identify critical points for defense.



Example Attack Tree: Disrupt Air Traffic Control

- **Goal:** Disrupt Air Traffic Control Operations
    - **OR Node:**
        - Gain Unauthorized Access to ATC Systems
            - **AND Node:**
                - Exploit Network Vulnerability
                - Bypass Authentication
                - Maintain Persistence
        - Physical Disruption of ATC Infrastructure
            - **AND Node:**
                - Gain Physical Access to Control Tower
                - Disable Equipment (e.g., radar, communication)
                - Jam Communication Frequencies
            - **AND Node:**
                - Acquire Jamming Equipment
                - Position Equipment near Airport

Risk Assessment (Simplified)

While DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) is a quantitative risk assessment model, a simplified qualitative assessment more practical in this case. We can consider the Likelihood and Impact of each identified threat.

Threat Category	Example Threat	Likelihood	Impact	Risk Level
Spoofing	Impersonating staff for physical access	Medium	High	High
Tampering	Modifying flight data	Medium	Critical	Critical
Repudiation	Insider action without logging	Low	High	High
Information Disclosure	Leaking passenger data	Medium	High	High
Denial of Service	Disrupting air traffic control	High	Critical	Critical
Elevation of Privilege	Gaining admin access to OT systems	Medium	Critical	Critical

Mitigation Strategies

Based on the identified threats and their potential risks, mitigation strategies should be developed. These can include:

- Technical Controls
  - Implementing strong access controls and authentication for IT and OT systems.
  - Network segmentation to isolate critical systems.

- **Physical Security Controls:**
  - Perimeter security (fences, patrols, surveillance).
  - Access control systems for restricted areas

- **Administrative Controls:**
  - Security awareness training for all personnel.
  - Incident response plans and regular drills.

Threat Modelling Manifesto and OWASP Threat Modelling Cookbook

This threat model aligns with the principles of the Threat Modelling Manifesto by aiming to:

- Be **developer-friendly** (though this model is high-level, the process should involve system developers).
- Be **repeatable**.
- Be **integrated** into the development lifecycle (for new systems).
- Focus on **identifying threats** early.

The OWASP Threat Modelling Cookbook provides practical guidance and techniques for conducting threat modeling, including using methodologies like STRIDE and creating attack trees, which were utilized in this model. It emphasizes the importance of defining the scope, identifying assets, and systematically analyzing threats.

Conclusion

Threat modeling is an ongoing process, not a one-time activity. For a complex and critical environment like a large international airport, continuous threat modeling, informed by evolving threats and new vulnerabilities, is crucial to maintaining a strong security posture and ensuring the safety and security of passengers and operations. This model provides a foundational understanding of potential threats and highlights the need for a multi-layered security approach.