Exercise 3: Threat modeling and risk management framework

TDT4237 2025 Group 41
Gard Huse Storebø, Arthur Marc Jacques Saunier, Kjetil André Woll Vik

Abstract

This report presents a threat modeling and risk analysis of a web-based cybersecurity risk assessment tool designed to support Air Traffic Management (ATM) systems. The analysis follows a structured approach based on the STRIDE framework, misuse case diagrams, and a detailed Data Flow Diagram (DFD) created using OWASP Threat Dragon. Key business assets, goals, and risks were identified, followed by a comprehensive assessment of technical threats. Ten major technical risks were linked to misuse scenarios and business impacts, from SQL injection to broken access control. Based on the findings, ten corresponding security requirements were defined, and a test plan was designed to verify mitigation strategies. This work ensures a more robust and trustworthy risk assessment tool, reinforcing both system safety and operational resilience in the ATM domain.

Keywords: Security, Risk Analysis, STRIDE, Threat Modeling, Air Traffic Management, Web Application, Misuse Cases, Data Flow Diagram

Contents

1. Introduction

This report presents a threat model and risk management framework for a web-based cyber security risk assessment tool designed to support Air Traffic Management (ATM) solutions. The tool is part of the SESAR Joint Undertaking's efforts to modernize and secure European airspace systems by simplifying the process of performing standardized risk assessments on technologies such as drones, air taxis, and conventional aircraft systems.

The goal of this report is twofold: first, to identify and analyze business and technical risks associated with the tool itself, and second, to ensure the tool supports secure and efficient risk assessments for other ATM solutions. To accomplish this, we apply established risk management methodologies and threat modeling techniques, including misuse case diagrams and a data flow diagram (DFD) created with OWASP Threat Dragon.

The report is structured as follows: Section 1 defines key business assets and goals. Section 2 outlines the chosen risk scales and dimensions. Section 3 presents identified business and technical risks, including their relationships. Section 4 includes security requirements and a test plan derived from the analysis. The report concludes with a summary of findings. All models and diagrams are included as figures in the respective sections.

2. Part 1: Risk management framework

2.1. Identified Business Assets

Business Assets	
ID	Description
BA01	Stored data from completed risk assessments
BA02	Lists of known items (assets, threats, issues) used for assessments
BA03	The website/tool used to do the risk assessments

2.2. Identified Business Goals

Business Goals	
ID	Description
BG01	Make risk assessments for air traffic systems easier and faster
BG02	Help improve the security and safety of air traffic management
BG03	Be a trusted and reliable tool for users performing assessments

2.3. Risk Scales and Dimensions

Likelihood			
Low	Medium	High	Extreme
Very unlikely	Unlikely	Likely	Very likely
(e.g., ¡ once/5yrs)	(e.g., once/1-5yrs)	(e.g., few times/yr)	(e.g., weekly/daily)

Impact Dimensions

Dimension	Low	Medium	High	Extreme
Safety Impact	Minor procedure issue, no safety effect	Increased staff workload, slight safety reduction possible	Potential for significant incident (near miss)	Potential for accident, loss of life or major damage
Operational Impact	Minor annoyance, easy workaround	Tool partly unusable, some disruption	Tool mostly unusable, major work disruption	Tool completely down, work stops
Data Impact (Confidentiality / Integrity)	Minor error or small leak, easily fixed	Some data loss/leak, needs effort to fix	Major data loss/leak for one system	Critical data lost or major leak affecting many systems

2.4. Identified Business Risks

Business Risks

ID	Description	Likelihood	Impact	Risk ranking
BR01	Unauthorized access to stored risk assessments may expose sensitive information about ATM system vulnerabilities.	Medium	High (Data Impact)	High
BR02	Failure of the web tool (e.g., due to a DoS attack or server outage) leads to full disruption of ongoing risk assessments.	Low	Extreme (Operational Impact)	High
BR03	Inaccurate risk scoring due to misuse or misunderstanding of the tool could result in underestimating threats, compromising air traffic safety.	Medium	Extreme (Safety Impact)	Critical
BR04	Loss or corruption of catalog data (assets, threats, vulnerabilities) makes the tool unusable or reduces its reliability.	Low	High (Operational/Data Impact)	Medium
BR05	Users lose trust in the tool due to past performance issues or lack of transparency, leading to low adoption and reduced usage in the ATM ecosystem.	Medium	Medium (Operational/Safety Impact)	Medium

2.5. Misuse Case Diagram

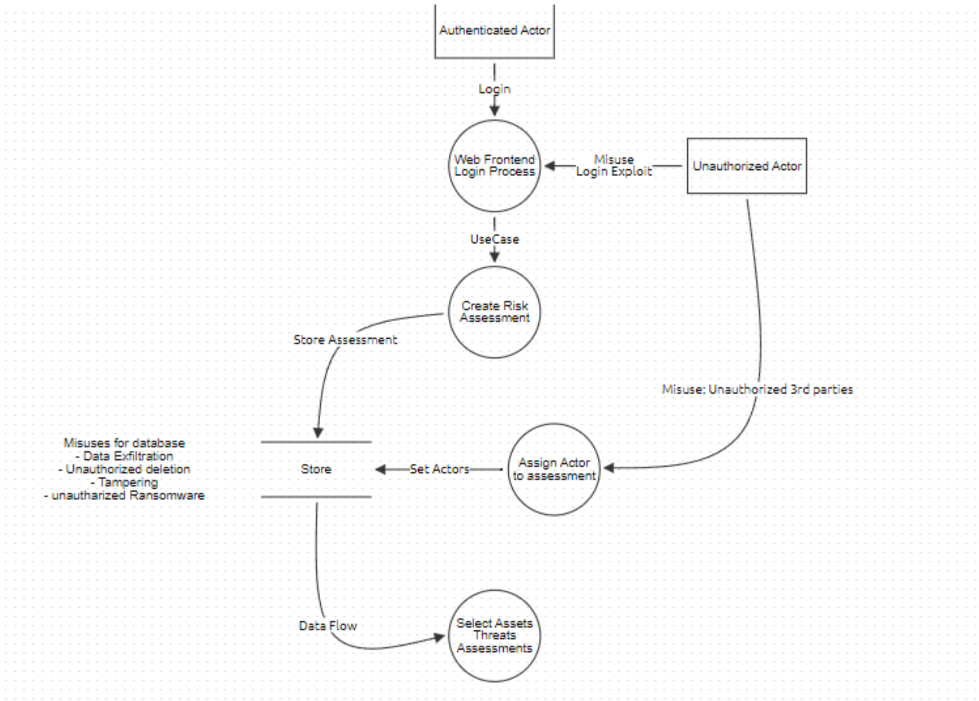

Figure 1: Misue diagram showing where Unauthorized actors could access

2.6. Data Flow Diagram

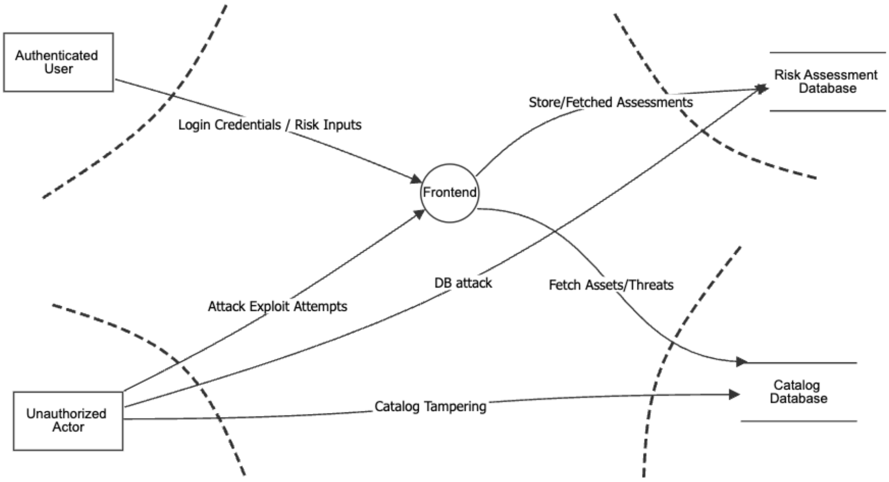

Figure 2: Data Flow Diagram

The threats listed below are based on the Data Flow Diagram of the system. The diagram shows how users interact with the tool, how data flows between components, and where attackers could target the system. It helped identify potential STRIDE threats on each element.

Threats			
Component	Threat title	Type (STRIDE)	Description
Authenticated User	Identity Spoofing	Spoofing	An attacker could impersonate a legitimate user to access sensitive risk assessment data.
Risk Inputs	Credential Interception	Information Disclosure	Credentials could be intercepted during transmission, allowing unauthorized access.
Web Frontend	Lack of Traceability	Repudiation	Actions performed by users could not be properly logged, allowing them to deny malicious activities.
Web Frontend	Privilege Escalation	Elevation of Privilege	A user could exploit flaws to gain higher-level privileges than intended.
Risk Assessment Database	Data Tampering	Tampering	An attacker could modify stored risk assessments, leading to incorrect security measures being implemented.
Risk Assessment Database	Sensitive Data Leakage	Information Disclosure	Confidential information about air traffic system vulnerabilities could be leaked from the database.
Catalog Database	Denial of Service on Catalog	Denial of Service	The catalog database could be rendered unavailable, preventing risk assessments from being performed.
Catalog Database	Catalog Corruption	Tampering	An attacker could inject false assets or threats into the catalog, degrading assessment quality.
Attack Exploit Attempts	Login Exploitation	Spoofing	Attackers could bypass authentication mechanisms to gain unauthorized access to the frontend.
DB Attack	Database Flooding Attack	Denial of Service	Attackers could flood the database with requests, causing it to crash or become unavailable.

2.7. Identified Technical Risks

Technical Risks				
ID	Description	Likelihood	Impact	Related Business Risk
TR1	SQL Injection Vulnerabilities	High	Extreme (depending on the attacker's goal; the impact could be extreme if sensitive data is accessed, risk assessments are modified, or privileges are escalated)	BR01 & BR03 & BR04
TR2	Denial-of-Service (DoS) Attacks	High	High (making the tool unavailable for a limited time, leading to the disruption of risk assessments)	BR2
TR3	Insecure Data Storage	Low	High (unencrypted data leaks ATM vulnerabilities or catalog details)	BR01 & BR04
TR4	Weak Authentication	High	High (unauthorized actors bypass login, exposing ATM vulnerabilities and reducing user trust)	BR1 & BR5
TR5	Insecure APIs	Medium	High (unsecured endpoints let attackers bypass the frontend to leak data or alter risk logic)	BR01 & BR03
TR6	Lack of logging	Medium	High (Undetected breaches and difficult incident response)	BR1 & BR5
TR7	Cross-Site Scripting XSS	Medium	High (Session Hijacking, data exfiltration)	BR1 & BR5
TR8	Vulnerable and Outdated Components	High	High (known exploits that can lead to compromise)	BR3 & BR4
TR9	Unvalidated input handling	Medium	High (leading to injection)	BR1 & BR3
TR10	Broken access control	High	High(user gaining unauthorized access, leading to information leak)	BR1 & BR3 & BR5

2.8. Security requirements

Security requirements		
Technical risk ID	Requirement ID	Requirement
TR1	SR1	Database queries must be strictly validated and sanitized.
TR2	SR2	Rate limiting and traffic filtering can mitigate Denial-of-Service (DoS) attacks.
TR3	SR3	Data storage can be encrypted using strong encryption or kept in offline storage systems.
TR4	SR4	Implement Multi-Factor Authentication (MFA) and enforce strong password policies.
TR5	SR5	Ensure proper API endpoint authentication and input validation.
TR6	SR6	Implement comprehensive, tamper-evident logging of user and admin actions. Log sensitive events like failed logins, privilege changes, and data access.
TR7	SR7	Sanitize and encode all user-generated content output to prevent XSS. Implement Content Security Policy (CSP) headers.
TR8	SR6	Regularly update and patch software and libraries to latest stable release. Perform vulnerability scanning.
TR9	SR9	Validate and sanitize all user inputs across the entire stack. Use allow-lists where possible instead of block-lists.
TR10	SR10	Implement robust access control mechanisms. Enforce the principle of least privilege. Perform access control checks server-side, not just client-side.

2.9. Test plan

Security Requirement ID	Test ID	Test Priority (1-3)	Test Description
SR1	T1	1	Perform automated SQL injection testing on all user inputs using tools like SQLMap. Manually review database access patterns to confirm prepared statements are used.
SR2	T2	2	Simulate DoS attacks with tools like LOIC or Slowloris. Confirm rate limits and mitigation triggers. Analyze server resource exhaustion thresholds.
SR3	T3	1	Review database configuration for encryption settings. Attempt unauthorized access to encrypted data and verify decryption fails without keys.
SR4	T4	1	Attempt brute force password attacks. Verify MFA enforcement. Ensure password lockout policies trigger after repeated failures.
SR5	T5	2	Use Postman or Burp Suite to send malformed or unauthorized API requests. Validate correct 401/403 responses and input validation errors.
SR6	T6	2	Perform simulated breach scenarios. Confirm that critical user actions (login, password change, privilege escalation) are logged and audit logs are protected.
SR7	T7	2	Inject common XSS payloads into input fields. Verify output encoding/sanitization and CSP header enforcement using browser developer tools.
SR8	T8	3	Run dependency vulnerability scans using OWASP Dependency-Check, npm audit, pip-audit, etc. Review project libraries for unpatched CVEs.
SR9	T9	2	Perform fuzz testing on form fields, API endpoints, and URL parameters. Validate that no injection or unexpected behavior occurs.
SR10	T10	1	Attempt privilege escalation scenarios by manipulating requests. Confirm access control checks prevent unauthorized access to restricted resources.

3. Summary of Findings

Using the risk management framework helped us better understand the possible threats to the risk assessment tool. By identifying business assets and goals early, we were able to spot relevant risks and threats using STRIDE and misuse cases. We then linked these threats to technical risks and created a set of security requirements to address them. Finally, we made a test plan to verify if the protections work as expected. This process gave us a structured way to analyze the system and improve its security.