Exercise 3: Threat modeling and risk management framework

TDT4237 2025 Group 100
Ana Barrera Novas, Andrea Cicinelli, Nicola Katja Gisela Ferger

Abstract

In this paper, we assess a web-based tool used for managing cyber risks, as well as develop a test plan for it. There are several risks involved, but using this report, the system will be able to improve its overall security.

Keywords: Insert important keywords from your report. Eg. security, webapp, risk analysis etc.

Contents

1. Introduction

This report presents a security and risk assessment of a web-based tool used for managing cyber risks in air traffic management (ATM) systems. The tool is meant to help users create, manage, and share risk assessments, making it easier to identify threats and define security needs for other ATM solutions.

We follow a structured method based on the course material, starting by identifying important system assets and goals. We then list possible risks, create diagrams showing how the system could be misused, and analyze technical threats. These results are used to suggest security requirements and a test plan to help improve the system's overall security.

2. Part 1: Risk management framework

For the following subsections, use the Risk Management Framework to fill in the tables. There is not need to write substantial text in these subsections, all information should be apparent in the tables. Latex tables are fairly easy to use, but look at Overleaf Learn (click me) for more info if you run into issues.

2.1. Identified Business Assets

Business Assets	
ID	Description
A1	Web Application Platform: the front-end and back-end systems that host the risk assessment tool.
A2	Risk Data Repository: database storing all user-generated assessments.
A3	User Credentials and Profiles: authentication records, roles, permissions and personal data

2.2. Identified Business Goals

Business Goals	
ID	Description
G1	Accurate and Comprehensive Assessments
G2	High Availability and Performance
G3	Data Confidentiality and Integrity

2.3. Risk Scales and Dimensions

Likelihood	
Low	Unlikely to occur within a year
Medium	May occur several times per year
High	Likely to occur monthly
Extreme	Expected to occur weekly

I divided the "Impact Dimensions" table in 2 because it can't contain all the information in one!

Impact Dimensions		
Dimension	Low	Medium
Financial	less than $10 k	$10 k–100 k
Operational	Minor delay	Partial service interruption
Reputational	Limited stakeholder concern	Notice within industry
Safety	No injury	First-aid only

Impact Dimensions		
Dimension	High	Extreme
Financial	$100 k–1 M	more than $1 M
Operational	Major disruption	Complete outage
Reputational	National news coverage	Corporate crisis
Safety	Lost-time injury	Permanent disability or fatality

I created possible business risks, linking the likelihood level, the impact dimension, and the risk ranking (which is the average of the two levels mentioned before).
These business risks are going to be linked in the following tables to the technical risks

2.4. Identified Business Risks

Business Risks				
ID	Description	Likelihood	Impact	Risk ranking
BR1	Inaccurate Risk Assessments: users omit key assets or threats.	High	High	High
BR2	Data Breach: unauthorized access to sensitive risk data or user profiles.	Medium	Extreme	High
BR3	System Downtime: outages or performance issues prevent assessment work.	Medium	High	High
BR4	Regulatory Non-compliance: failure to meet data-protection or industry standards.	Low	High	Medium
BR5	Safety Incident: flawed assessment leads to real-world accident or injury.	Low	Extreme	High

2.5. Misuse Case Diagram

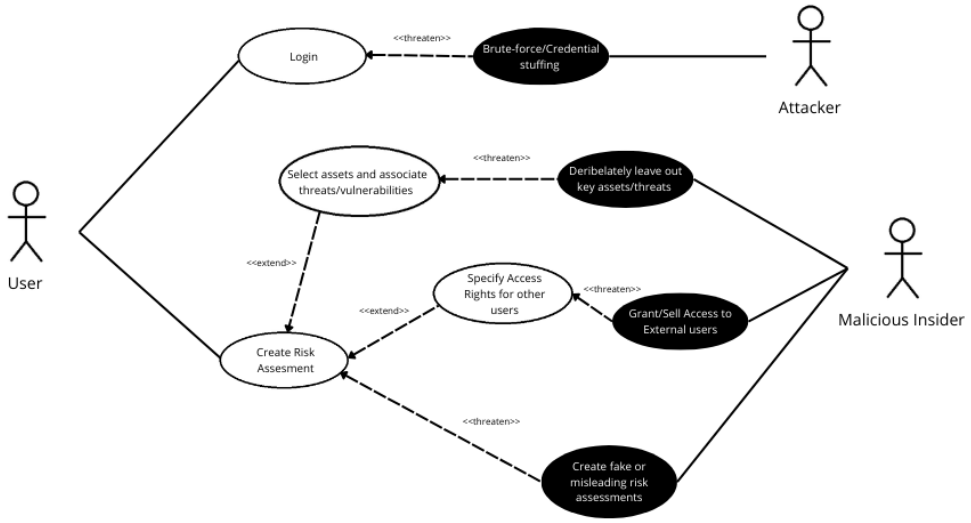

Figure 1: Relevant use cases with their misuse cases

This misuse case diagram shows how the system could be exposed to serious security issues if certain actions are not properly controlled. For example, if someone tries brute-force or credential stuffing attacks, it means the system might not be doing enough to stop repeated login attempts, putting user accounts and sensitive risk data at risk. If a malicious user creates fake or misleading risk assessments, it could lead to wrong decisions being made, especially in critical environments like air traffic management. When someone leaves out important assets or threats on purpose, it affects the quality and reliability of the whole assessment, which could hide real problems so that this could be exploited later. And the possibility of someone sharing access with unauthorized users, or even sells that access, exists, and shows how important it is to have strong rules about who can see or change certain information so that other entities can't exploit it.

2.6. Data Flow Diagram

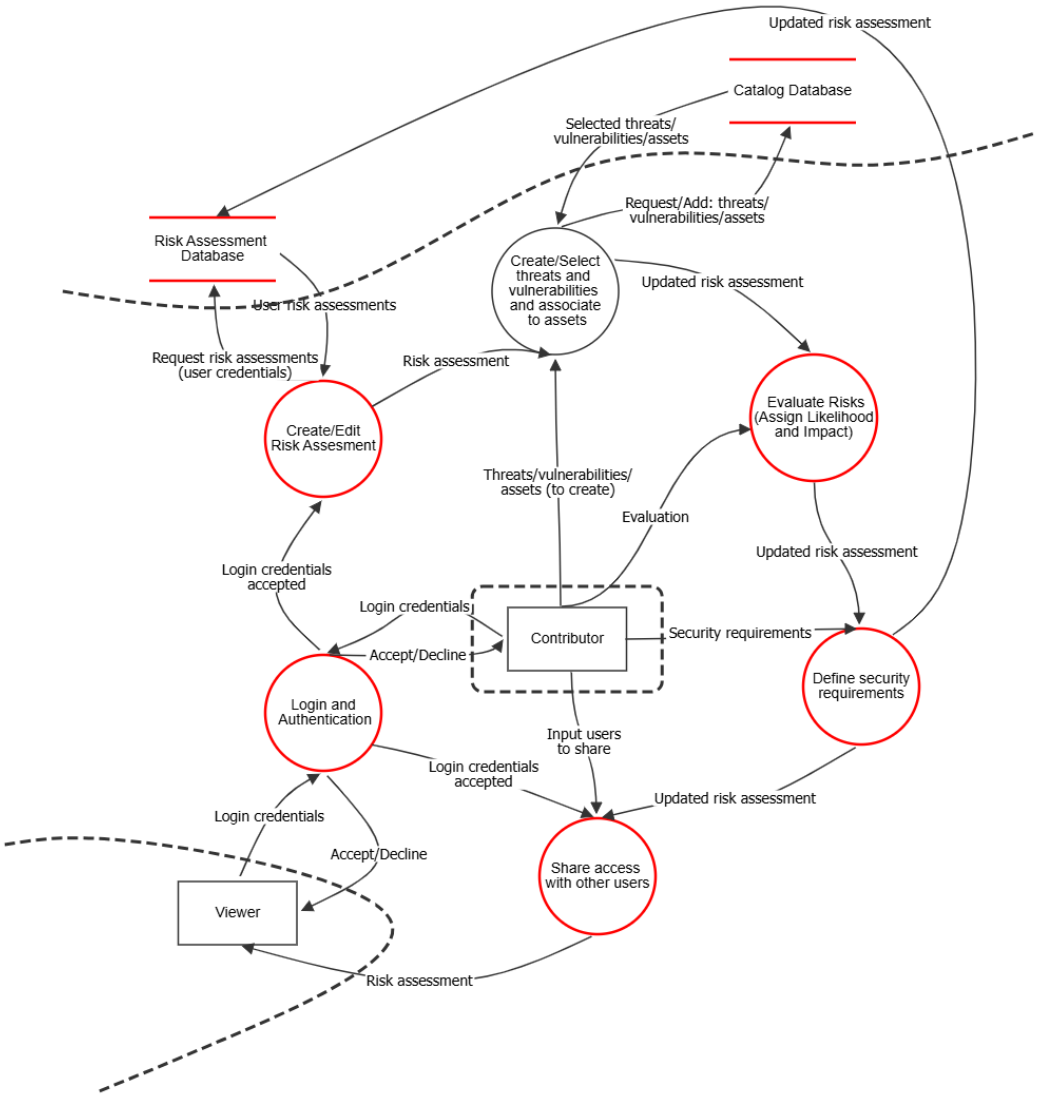

Figure 2: Threat model

The diagram outlines how different types of users interact with the tool and how data flows through its main components. External actors like the Contributor and Viewer are separated from the internal system by a trust boundary, highlighting the shift from untrusted to trusted zones. A second trust boundary surrounds the databases, emphasizing the need to protect stored data from unauthorized access or manipulation. The Contributor is the main user driving most system processes, from logging in and creating assessments to defining risks and sharing access. STRIDE threats are identified at critical points in the flow, showing where vulnerabilities may arise based on user actions, data handling, or lack of proper controls.

The application didn't let us establish correctly the type (STRIDE), as it always put Spoofing and did not let us change it, so we wrote the correct type in the description of

the threat in the diagram.

Threats			
Component	Threat title	Type (STRIDE)	Description
Login and Authentication (process)	Credential Forgery	Spoofing	Attacker tries to log in as another user using stolen or fake credentials
Login and Authentication (process)	Account Lockout Abuse	Denial of Service	Attacker repeatedly submits bad passwords to trigger lockout mechanism
Create/Edit Risk assessment (process)	No Audit Trail	Repudiation	User actions aren't logged, making it impossible to prove who edited a risk
Evaluate risks (process)	Risk Value Manipulation	Tampering	Attacker modifies likelihood or impact values to misrepresent risk level
Define security requirements (process)	Leakage of Sensitive Mitigations	Information Disclosure	Requirements are exposed to unauthorized users
Catalog DB	Inject Fake Threats	Tampering	Malicious user adds invalid or misleading entries
Risk Assessment DB	Data Exposure	Information Disclosure	Unauthorized party reads sensitive risk assessments
Share access with other users (process)	Share with untrusted user	Elevation of Privilege	User gives access to someone who should not have it
Risk Assessment DB	Undetected Data Deletion	Repudiation	A user deletes or modifies a risk assessment entry, but the system lacks proper logging to prove who made the change.
Share access with other users (process)	Untracked access sharing	Repudiation	A user shares access to a risk assessment with another person, but the system doesn't record who shared it, when, or with whom — making it impossible to track accountability or trace leaks.

2.7. Identified Technical Risks

Using the misuse case diagram, the DFD, and the STRIDE threats, we can now identify the technical risks connected to these misuse cases and threats.

Technical Risks				
ID	Description	Likelihood	Impact	Related Business Risk
TR1	Weak Authentication Mechanism lets attacks brute force credentials.	High	Attackers might get access to other users' accounts	BR1
TR2	Insufficient Input Validation at Login lets attacks put in SQL code that is then executed on the database	Medium	Susceptibility to SQL injections in the login field could lead to security breaches	BR2
TR3	Attacker types in wrong password several times to lock user accounts	Medium	Users are logged out of their accounts due to account lockout abuse	BR3
TR4	Susceptibility to DoS Attack - Network	Medium	Unexpected downtime e.g. through overwhelming the "Select assets and associate threats" functionality	BR3
TR5	Session hijacking is used to access contributor's account	Medium	Attacker can modify likelihood, impact and security requirements	BR2
TR6	No validation on catalog inputs	Low	No server-side validation allows users to insert fake threats or junk data into the threat catalog	BR1

TR7	Weak database access control, risk assessment db is not properly segmented or protected by strict permissions	Medium	sensitive data exposure.	BR2
TR8	Lack of immutable audit logs; risk modifications aren't recorded with timestamps and user IDs	Medium	undetected tampering or disputes	BR1
TR9	Access sharing happens without user role validation or periodic review	Medium	Untrusted sharing	BR4
TR10	Weak access revocation mechanism; access rights (shared users) cannot be revoked immediately	Low	ex-users could retain unwanted access longer than necessary	BR4

2.8. Security requirements

Security requirements		
Technical risk ID	Requirement ID	Requirement
TR1	SR1	Two-factor authentication should be required.
TR1	SR2	Logs should contain source and results of login attempts.
TR2	SR3	All inputs must be validated and sanitized.
TR3	SR4	The system must implement account lockout policies with throttling and altering mechanisms.

TR4	SR5	The system must rate-limit requests.
TR5	SR6	Session tokens must be transmitted only over secure channels.
TR5	SR7	Sessions must have a timeout period.
TR6	SR8	All inputs to the catalog database must be validated and sanitized.
TR7	SR9	Access to the Risk Assessment database must be restricted based on the principle of least privilege.
TR8	SR10	The system must maintain immutable, tamper-evident audit logs recording all modifications to risk assessments, including timestamps and user IDs.
TR9	SR11	When users share access, the system must validate the recipient's user role and perform periodic access reviews.
TR9	SR12	When users, sahre access the system must and perform periodic access reviews.
TR10	SR13	The system must allow immediate revocation of access rights for any shared user.

2.9. Test plan

Test Plan			
SR ID	Test ID	Test Priority (1-3)	Test Description
SR1	TC1	1	Verify that after correct username/password entry, the system requires a second factor before granting access. Try logging in without the second factor to confirm it is blocked.
SR2	TC2	2	Attempt several successful and failed logins. Verify that logs capture: username, IP address, timestamp, and login success/failure. Confirm unauthorized access attempts are logged.
SR3	TC3	1	Attempt SQL injection attacks (e.g., OR '1'='1) on login and catalog input fields. Verify that malicious inputs are either sanitized or rejected, and no database errors occur.
SR5	TC4	2	Simulate rapid repeated requests and verify the system enforces rate limiting.
SR6	TC5	1	Monitor traffic using a proxy and confirm that all session tokens are transmitted over HTTPS only (no plaintext transmission).
SR7	TC6	2	Log in as a user and stay idle. Verify that after the configured timeout period (e.g., 15 minutes), the session expires and the user must re-authenticate.
S10	TC7	2	Modify a risk assessment, then check the audit log to ensure it records the action with timestamp, user ID, and prevents any alteration of the record after it is created.

3. Summary of Findings

We found that the system has several key assets, such as the platform itself, stored risk data, and user information. These need to be protected to avoid problems like data leaks, system downtime, or misleading assessments.

Our analysis identified ten technical risks, including weak login security, missing input checks, and poor access controls. These issues can lead to business problems like incorrect risk reports or even safety incidents.

To reduce these risks, we suggest security measures such as stronger authentication, better logging, and input validation. We also designed a test plan to check that these measures would work if the system were implemented.

References