Risk assessment report for TrustedSitters

TDT4237 Group 21
Patrick Øivind Helvik Legendre, Gunnar Nystad, Dag Kirstihagen

Abstract

This report outlines Trustedsitters various business assets, goals and risk. The report highlights the key technical risks assosiated with the businesses goals. The dangers the application faces are detailed with misuse cases and attack trees. Security requirements and a testing plan helps Trustedsitters ensure the necessary changes are implemented, to keep the service safe and secure. Keywords: Security, webapp, risk analysis, test plan, misuse case, attack tree, technical risks, business risks. Preprint submitted to TDT4237 Review Board April 26, 2022

Keywords: Security, webapp, risk analysis, test plan, misuse case, attack tree, technical risks, business risks.

Contents

1 Introduction 3

2 Part 1: Risk management framework 3

2.1 Identified Business Assets 3
2.2 Identified Business Goals 3
2.3 Definition of risk levels 4
2.4 Business risks 6
2.5 Two misuse cases examples 6
2.6 Two attack tree examples 7
2.7 Identified Technical Risks 8
2.8 Test plan 10

3 Summary of Findings 13

1. Introduction

We have previously discovered and mitigated several of Trustedsitters' security issues. We will now assess the website according to the risk management framework. This includes detailing business assets, goals, and risks. Afterward, we will look at technical risks, misuse cases, and possible attack trees. Finally, we will propose a test plan. Based on this, Trustedsitters will have the tools to become a safe and secure service, fulfilling its business goals.

2. Part 1: Risk management framework

2.1. Identified Business Assets

Business Assets	
ID	Description
BA1	Children
BA2	Parents
BA3	Guardians
BA4	Database
BA5	Website server
BA6	Contracts
BA7	Trustedsitters reputation

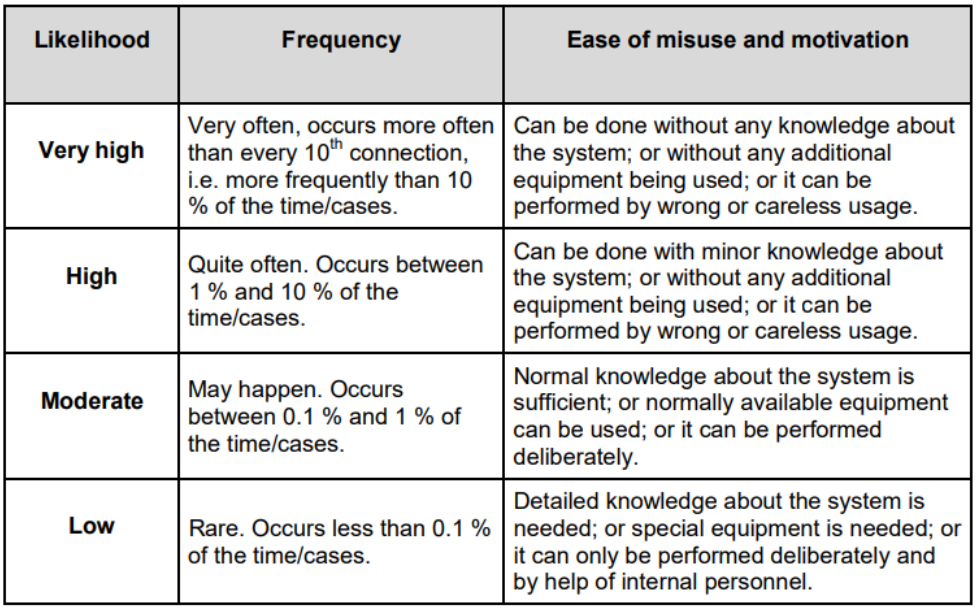
2.2. Identified Business Goals

Business Goals	
ID	Description
BG1	Trustworthy babysitters
BG2	Trustworthy parents
BG3	Able to store sensitive data securely
BG4	Share data with relevant people
BG5	Facilitate easy contact between babysitters and parents
BG6	Be available
BG7	Get more users

2.3. Definition of risk levels

For our discussion of business risks and technical risks we will evaluate the level of likelihood and impact for each risk. The scale will consist of Low, Medium, High and Extreme/Very high.

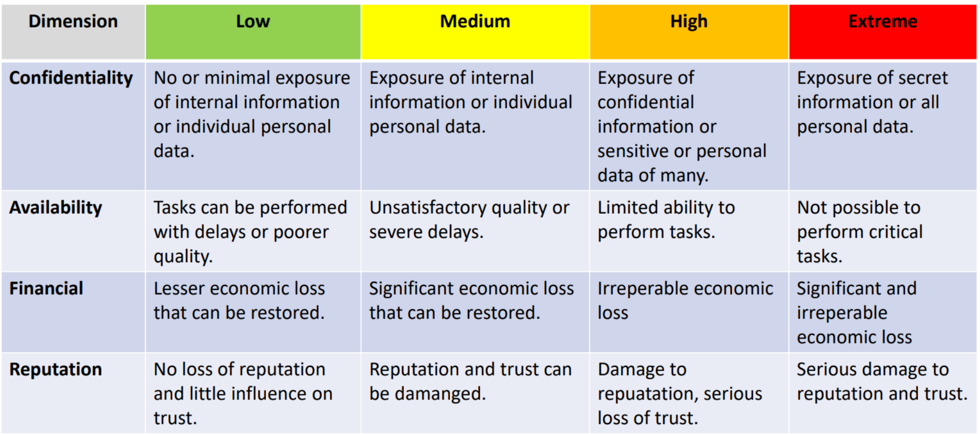
For the assessment of likelihood we have used Nasjonalt senter for e-helseforskning's scale [1]. This scale is detailed in Figure 1. The scale allows us to discuss likehood of risks across two different aspects, namely the frequency and ease of misuse and motivation. This comes in handy for Trustedsitters use case and enables us to give a tailored assesment of the risks facing the application.



Likelihood	Frequency	Ease of misuse and motivation
Very high	Very often, occurs more often than every 10th connection, i.e. more frequently than 10 % of the time/cases.	Can be done without any knowledge about the system; or without any additional equipment being used; or it can be performed by wrong or careless usage.
High	Quite often. Occurs between 1 % and 10 % of the time/cases.	Can be done with minor knowledge about the system; or without any additional equipment being used; or it can be performed by wrong or careless usage.
Moderate	May happen. Occurs between 0.1 % and 1 % of the time/cases.	Normal knowledge about the system is sufficient; or normally available equipment can be used; or it can be performed deliberately.
Low	Rare. Occurs less than 0.1 % of the time/cases.	Detailed knowledge about the system is needed; or special equipment is needed; or it can only be performed deliberately and by help of internal personnel.

Figure 1: Nasjonalt senter for e-helseforskning's likelihood assessment table.

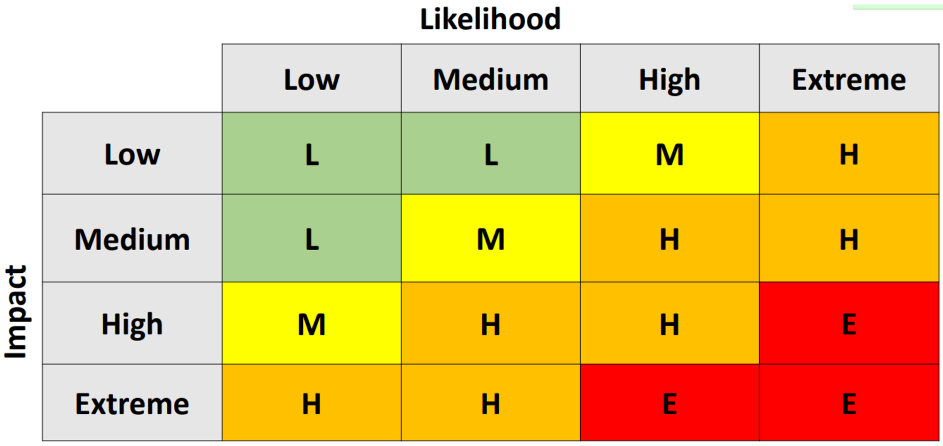
To evaluate the impact of risks we have utilized the risk assessment table presented during the "risk assessment during development"-lecture as shown in Figure 2.



Dimension	Low	Medium	High	Extreme
Confidentiality	No or minimal exposure of internal information or individual personal data.	Exposure of internal information or individual personal data.	Exposure of confidential information or sensitive or personal data of many.	Exposure of secret information or all personal data.
Availability	Tasks can be performed with delays or poorer quality.	Unsatisfactory quality or severe delays.	Limited ability to perform tasks.	Not possible to perform critical tasks.
Financial	Lesser economic loss that can be restored.	Significant economic loss that can be restored.	Irreperable economic loss	Significant and irreperable economic loss
Reputation	No loss of reputation and little influence on trust.	Reputation and trust can be damagned.	Damage to repuatation, serious loss of trust.	Serious damage to reputation and trust.

Figure 2: Risk assesment framework provided in ”risk assessment during development”-lecture.

To evaluate the total risk ranking we have utilized the risk prioritization table presented during the ”risk assessment during development”-lecture as shown in Figure 3. It should be noted ”Very high” as described in the likelihood scale corresponds to ”Extreme” in this prioritization table.



		Likelihood			
		Low	**Medium**	**High**	**Extreme**
Impact	**Low**	L	L	M	H
	Medium	L	M	H	H
	High	M	H	H	E
	Extreme	H	H	E	E

Figure 3: Risk prioritization framework provided in ”risk assessment during development”-lecture.

2.4. Business risks

Business Risks				
ID	Description	Likelihood	Impact	Risk ranking
BR1	System too difficult to use	High	High	High
BR2	System unavailable	Medium	High	High
BR3	User credentials leaked	Low	Extreme	High
BR4	User contracts and history leaked	Low	Extreme	High
BR5	Users providing incorrect information	High	High	High
BR6	Too expensive to operate the service	Medium	High	High
BR7	User identity is untrustworthy	High	High	High
BR8	Weak server security	Medium	Extreme	High

2.5. Two misuse cases examples

We provide two examples of misuse cases to provide a high-level narrative of what can happen in Figure 4 and 5. This will be easy to grasp by different stakeholders.

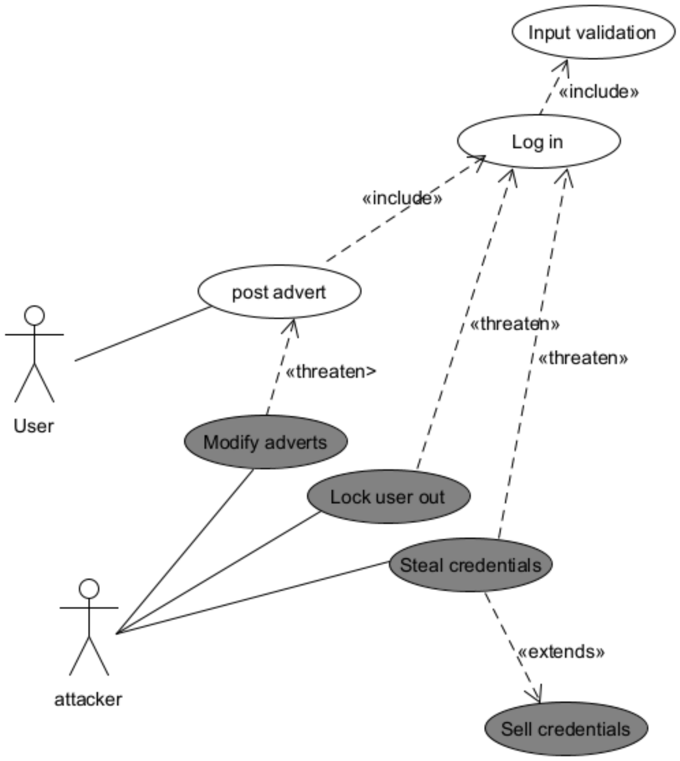


Figure 4: Misuse Case: post advert

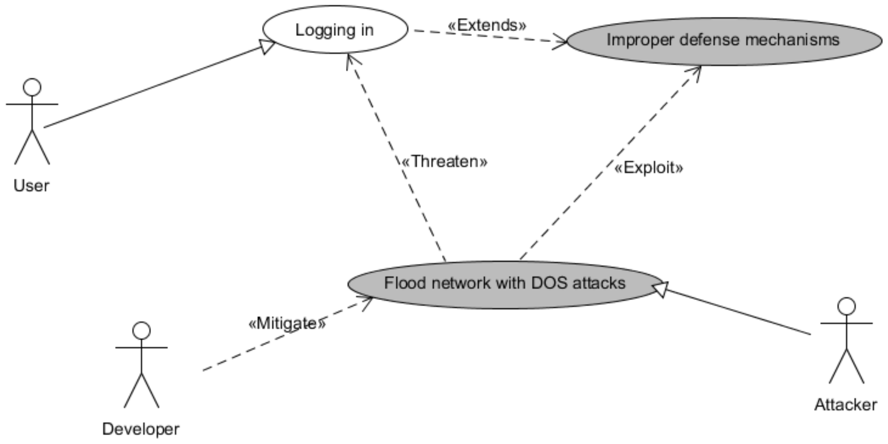


Figure 5: Misuse Case: Logging in

2.6. Two attack tree examples

We provide two attack tree examples to showcase how an attacker might exploit the technical risks in Figure 6 and 7. The discussion will not be as high levelled as the misuse cases, but will still be relatively easy to grasp for different stakeholders.

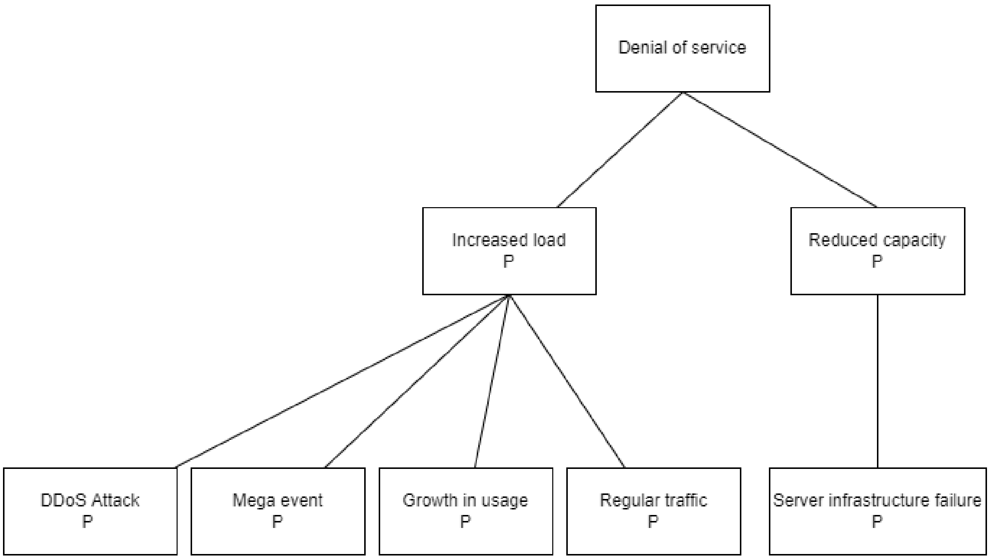


Figure 6: DoS Attack

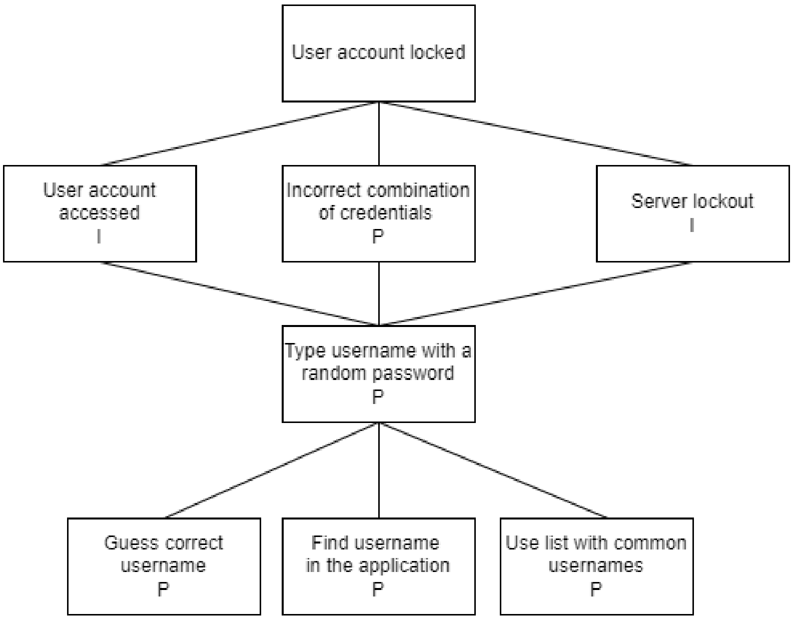

User account locked
User account accessed
I
Incorrect combination of credentials
P
Server lockout
I
Type username with a random password
P
Guess correct username
P
Find username in the application
P
Use list with common usernames
P

Figure 7: Account Lockout

2.7. Identified Technical Risks

Technical Risks					
ID	Description	Likelihood	Impact	Security Requirements	Related Business Risk
TR1	Spoofing attacks	Medium	High	Implement sign-up requiring Bank ID	BR5, BR7
TR2	Network flooded by DOS attacks	Medium	High	Implement DoS protection	BR2
TR3	Web server crashing	Low	High	Thoroughly test the application	BR2
TR4	Brute force attacks	Low	Extreme	Implement lock-out mechanism	BR3
TR5	SQL injections attacks against the database	Medium	Extreme	User inputs should always be validated and sanitized	BR3, BR4

TR6	User identity and credentials are disclosed	Low	Extreme	encrypt passwords. Database should be protected from unauthorized access. The backend should not leak any sensitive data.	BR3
TR7	A user can create multiple accounts	Medium	Medium	Implement sign-up requiring Bank ID	BR5, BR7
TR8	Attacker type in the wrong password multiple times to lock user account	Low	Low	Two-factor authentication should be required. Logs should contain the source and results of login attempts	BR2
TR9	Individual contracts and child history are disclosed	Low	High	Database should be protected from unauthorized access. The backend should not leak any sensitive data.	BR4
TR10	Not enough server capacity	Medium	High	Monitor user growth and upgrade server capacity when needed	BR2, BR6
TR11	Data loss	Low	High	Make regular backups of the system	BR2, BR6
TR12	Intrusion in the Web server	Low	Extreme	Have strong passwords for admin accounts with 2-factor authentication enabled. Log all logins of the admin accounts and all the settings that have been changed or modified	BR8

TR13	Ransomware attacks	Low	Extreme	Make regular backups of the system. Have available system restore points.	BR2, BR6, BR8

2.8. Test plan

We will now provide a suggested test plan. The plan includes the related technical risk, a description of the test and a test priority rating from 1 (low) to 3 (high).

Test Plan			
Related Technical Risk	ID	Test Priority (1-3)	Test Description
TR1: Spoofing attacks	TR1.1	2	Sign-up using someone else's name
TR2: Network flooded by DoS attacks	TR2.1	1	Attack the server by sending multiple DoS requests
TR2: Network flooded by DoS attacks	TR2.2	2	Verify that the server can discard illegitimate requests
TR2: Network flooded by DoS attacks	TR2.3	3	Test the maximum amount of request the server can handle
TR3: Web server crashing	TR3.1	3	Deploy the server and verify that is does not crash
TR3: Web server crashing	TR3.2	2	Test the amount of resources used on the server
TR4: Brute force attacks	TR4.1	3	Test the lockout system
TR5: SQL injections attacks against the database	TR5.1	3	Check if OR 1=1 possible on login
TR5: SQL injections attacks against the database	TR5.2	3	Insert metacharacters in query

Test Plan			
Related Technical Risk	ID	Test Priority (1-3)	Test Description
TR5: SQL injections attacks against the database	TR5.3	3	Automated tests-fuzzing
TR5: SQL injections attacks against the database	TR5.4	3	Static code analysis
TR6: User identity and credentials are disclosed	TR6.1	3	Test that passwords are encrypted
TR6: User identity and credentials are disclosed	TR6.2	3	Test that the admin database accounts have a strong password
TR6: User identity and credentials are disclosed	TR6.3	3	Test that the admin database accounts have 2 factor authentication
TR6: User identity and credentials are disclosed	TR6.4	2	Test post/get request for data leaks
TR6: User identity and credentials are disclosed	TR6.5	2	Test for injection that returns data leaks
TR7: A user can create multiple accounts	TR7.1	3	Test the logs for account creations
TR8: Attacker types in wrong password multiple times to lock user account	TR8.1	3	Test the connection logs

Test Plan			
Related Technical Risk	ID	Test Priority (1-3)	Test Description
TR9: Individual contracts and child history are disclosed	TR9.1	3	Test the server requests for leaks
TR9: Individual contracts and child history are disclosed	TR9.2	3	Test the strength of passwords for admin accounts
TR10: Not enough server capacity	TR10.1	2	Test the maximum amount of legitimate request the server can handle
TR11: Data loss	TR11.1	3	Verify that the system restore point is usable
TR11: Data loss	TR11.2	3	Test that the backup works
TR12: Intrusion in the Web server	TR12.1	3	Test that the admin passwords are strong enough
TR12: Intrusion in the Web server	TR12.2	3	Test 2 factor authentication on all admin accounts
TR12: Intrusion in the Web server	TR12.3	2	Perform multiple scan for vulnerabilities
TR12: Intrusion in the Web server	TR12.4	2	Perform multiple penetration tests on the server
TR13: Ransomware attacks	TR13.1	1	Perform multiple log tests
TR13: Ransomware attacks	TR13.2	1	Perform multiple privilege escalation tests
TR13: Ransomware attacks	TR13.3	2	Test protections against malicious files on the server

3. Summary of Findings

In this report, we have evaluated the Trustedsitters application based on the risk management framework. We started by analyzing the business assets and goals of Trustedsitters, including what business risks may arise. Afterward, we made example misuse cases and attack trees, detailing how a malicious actor could exploit the business risks. From this, we could look at technical risks and associate each one of them with business risks. To combat each technical risk, we have detailed an extensive test plan. Trustedsitters should seek to implement all of the suggested mitigations and base their effort on the severity and likelihood of each risk. This would make Trustedsitter be able to safely and securely deliver its service and protect its business assets and goals.

References

[1] N. senter for e helseforskning, “Definition of likelihood, consequence and risk levels,” 2009.