Module 5- Computer Systems (2023-24)
Project

UNIVERSITY OF TWENTE.

Requirement Analysis Phase 1

Security by Design Checklist

Project Name: Earthquake Detector	**Team Members: Cenk Dogruer s2875144, Cuong Bui Duc s2966174, Hieu Chu s2948923, Rudolfs Neija s2975157, Carlo Fernandes de Brito s2980460**
Team ID: 15	**Mentor(s): Maxim Rosca**

Instructions:

A. **All the sections should be written in a clear, concise, and understandable way.**
B. **You must fill in the basic information about your projects such as Project Name, Team Members, Team ID, and Mentor(s).**
C. **Make sure to consider the checklist of the Requirement Analysis phase provided in the Security by Design document.**
D. **The length of the document should be between 4-8 pages.**

Steps to be performed for the checklist:

i) You should select a minimum of one security mechanism from each of the security requirements from authentication and authorization both (auditing is not included here).
ii) The auditing requirements should be considered as suggested in the table according to your application. Other than the normal check on protecting log files, backup files, etc, you should also think about the GDPR obligations, software licensing, etc. in line with your application.

iii) The given security mechanisms are for your inspiration. You can select other mechanisms also according to the requirement of your application. For example: If you select "authentication" as one of the security requirements, the mechanism can be logging/password checking, biometric, OAuth, etc. The same is applicable for authorization and auditing. iv) Justify the reason to select a particular mechanism for the requirements in the given column 'C'. v) Write supplement requirement(s) in the form of a user story ar Abuse case for the application (refer to the example given on the table, column 'D'). (The supplement requirements should be according to the goals and non-functional requirement (s) identified for your application.) vi) Write the possible risks involved for the supplement requirements (refer to the example given in the table, column 'E').

vii) Write the resources/mechanisms/tools to avoid/mitigate those risks for security controls (refer to the example of the column heading "Appropriate Security Control" (column 'F').

viii) This document must be reviewed by all the team members. ix) Put tickmark in the last column for all verified items.

Follow these 4 points for each of the Security Mechanisms and write them under Appropriate Security Controls:

i) Supplement security requirements to avoid risk**.**

ii) Write the requirement of the resources to mitigate such risks. For example: The type of Authentication software, security tokens, password management software, etc. iii) Devise a plan/method (tentative) to work on the identified risks. iv) Review the documentation within your team.

Security Policy	**Confidentiality, Integrity, and Availability**					
Security Requirements	**Security mechanisms (List down for your application)**	**Remarks on why you considered these requirements? (in a brief)**	**Supplement requirements for your application (user story/Abuse case)**	**Risk identification/Threat Assessment (at least one risk identification/abuse case)**	**Appropriate Security Controls**	**Tick ✔if you have applied the given security controls as suggested in the left column**

Authentication	Checking password	**For Example:** for granting access to multiple users and for users to have them individual profiles, we need to authenticate their username with a password. A more sophisticated authentication is not required. (Justify Why)	**Example Goal: The system verifies that there are no default passwords used by the application or any of its components. Requirement: To access the application, one should require authentication. User story: "As a user, I can enter my username and passwords to access the application." Abuse Case: As an attacker, I can enter the default passwords to access the application.**	**Example Risk identification: i) The length of the passwords are less than 4 characters., ii) The password is not very strong., iii) You enter a wrong password more than 3 times, etc.**	Follow the 4 points mentioned above.	

Checking identity	To prevent spamming, every device has their own identity, and they cannot appear at more than 1 place.	Goal: The system is not overflown with excessive data inputs coming from the same device (meaning that the device does not appear in several places at the same time so each one has their own identity. User story: As a user, I want to monitor the system without having any bugs or overflows on the website. As a user, I do not want to see duplicate devices. Abuser: As an attacker, I can enter the same ID couple of times in different places to manipulate the data through the website.	Risk: The system might be bugged, and the user might not be able to monitor its device through the website since it gives the multiple devices error. The attacker might steal someone else's identity and might prevent that person from tracking their own device.	Supplement security requirements: Provide a unique ID for each device. Requirement of the resources to mitigate the risks: Session management. Plan for the risks: Preventing any bugs that might appear from the removal of the devices. Obligating a two-factor authentication to prevent attackers from stealing identity.	

	Password checking	The data collected by the sensor and displayed in a web interface may be sensitive and should be viewable only by specific users to protect their privacy.	Goal: The data readings of the device are inaccessible to attackers. Requirement: To access the web interface, one should require username/password authentication. User story: "As a user, I can enter my network (user) name and password to monitor the readings." Abuse case: "As an attacker, I can access the unprotected data of someone else."	- The user chooses a password that is easily guessable. - Brute force password attacks.	Initially assign a secure default password to each device. If a user wishes to change it, enforce password length, special characters etc. to make the new password secure. Keep track of failed log-in attempts and enforce a policy	
Authorization on	User access	To prevent users from accessing other users' devices	Goal: Users can only access the location and the state of their own device, they are not allowed to access other users' devices. User story: "As a user, I do not want others to access and track my own device(s)." Abuse case: "As an attacker, I can manipulate the roles to access other users' devices."	Risk: The system might not be able to identify who has the authority and who does not if the roles are manipulated. The attacker might manipulate the roles to have access.	Supplement security requirements: Assign roles to the system: user and admin. User can only access their own device(s) while admin can access any device. Requirement of the resources to mitigate the risks: Role management	

					Plan for the risks: Prevent any role alteration. Having a singular account for the admin so that it will not be changed.
Audit	Protection of Log files	To prevent leaking the users' information	Goal: all data of users could be protected and avoid using for wrong purposes. Requirement: the individual information should be encoded User story: "As a user, I do not want any personal information to be used for advertising." Abuse case: "As an attacker, if I get access to the database, I can withdraw information about the users.	Risk: The data should be stored, but also needs to be protected. Attackers can try to eavesdrop the communication.	Supplement security requirements: Provide a security system which is resistant to eavesdropping, SQL injection, and man-in-the middle attacks. Requirement of the resources to mitigate the risks: Security management Plan for the risks: Prevent any type of injections by

					whitelisting or blacklisting. Having a session key between the user and the server.
Audit	Backup files,	To prevent the loss of user identifications	Goal: all users are able to log in to the system without having issues of identification crisis. User story: As a user, I want to log in to the system without having the issue of sharing the same ID with different people. As a user, I want to be able to log into the system without having my ID deleted every time after I close the session. Abuse case: "As an attacker, if I grant an access to the database, I can delete user information."	Risk: The system should store all the user information. The system should be resistant to data storage manipulations.	Supplement security requirements: Hardcopy the data Requirement of the resources to mitigate the risks: Hardcopy Plan for the risks: Hardcopy the data in case of loss. Provide a secure database for data manipulation.
	Temporary files, software and database licenses (Legal aspect)	Choosing the most suitable licensing	Goal: the licensing should be to the benefit of the software developer.	Risk: The software developer should be careful with which licensing they are planning to choose, and	Supplement security requirements: Licensing

		User story: “As a software developer, I do not want to get in trouble about the legal aspects.” Abuse case: “As an attacker, I will try to dig out any illegal movements on the website.”	they need to act based on the licensing that they have chosen.	Requirement of the resources to mitigate the risks: Obey the licensing rules Plan for the risks: Not going beyond the licensing restrictions.

Requirement Analysis Document Template

1. Introduction

There are several existing applications that you can select as a base for your project. In this section, you need to give a small background of already existing applications. In case an existing application is chosen, you need to give **at least 2 new features** and include these in the requirements.

The following points are introduced to get to know the purpose of your application, limitations of the existing system on which your project is based, etc.

1.1. **Purpose**:

You should know the purpose of creating your application. Write the reason for selecting this project by mentioning the usefulness, quality, etc. of the system.

For example:

“The project named “Earthquake Detector” is selected for multiple reasons:

- This system can detect an earthquake or any kind of an applied force (which can also be used for the security of the houses, at the door).
- This system provides a value based on the strongness of the earthquake and it creates a schema of a table based on the force that has been applied.
- This system is trackable through a website with multiple devices, allowing it to be trackable on multiple parts of the world.

Limitations of the current system (If any):

List down the limitations of the currently existing similar systems.

The current limitations of our system are

- *The accelerometer's precision is limited*
- *The device can not differentiate between seismic vibration and man-made vibrations*
- *The detection is real-time and is not predictable*

For example:

"The current limitations of already existing smart home automation system are

- *The web interface is not user-friendly.*
- *The synchronization issue, if connecting with different IoT devices at the same time.*
- *The network connectivity problem.*
- *a lot of energy/power consumption.*
- *no decision-making capability.*
- *...."*

1.2. **Intended Audience**

Write about the targeted audience who can have access to your product or the documents.

For example, *users/stakeholders (Mentor, Project Coordinator, Module Coordinator, Any specific User(s), etc.)*

Parents: They can track the earthquake detector online and see whether their house is safe or not.

House owners: They can track whether someone is trying to break-in to the house or not.

Anyone using the website: They can track whether there is an earthquake on various areas of the world.

1.3. **Define SMART Goals**:

This section is used to list down the target/expected results from the project. All the goals should be written in a SMART (Specific + Measurable + Attainable + Relevant + Time-bound) way. Here is a video for a better understanding of SMART goals!

For example

"The goals for the project IoT based smart home system are as follows:

Specific (What)	Measurable (Up to)	Attainable (How)	Relevant (Why)	Time-bound (when)
*1. To improve the **efficiency** of the system by having a user-friendly web interface.*	*To evaluate success rate/errors for improving the system.*	*To test the system with the improved web interface.*	*To ensure within the team the success of the system regarding the web interface.*	*To finish the task between Week 4-Week 5.*
2. To improve the	To evaluate whether there is any earthquake.	To attach the given sensors and adjusting it with the current existing system.	To know if there is an earthquake.	To finish the task between Week 3-Week 4

productivity *of the system by adding sensors such as door and window sensor, motion sensor, light sensor, temperature sensor, etc. for controlling the devices.*				
3. To improve the ***quality*** *of the system by applying the real-time data processing and improving data transmission*	To evaluate quickly incoming data and generate alerts.	To test the system by generating some oscillations to check if the system detects immediately.	To know the earthquake as soon as possible.	To finish between week 4 - week 5
4. To improve the ***security*** *of the system any malicious spam entries on the website will be detected and removed.*	To evaluate the real and unique values.	To test the system by applying multiple spam inputs.	To ensure the security on the website.	To finish between Week 7-Week 8

1.4. **Scope:** This section is required to write about the important resources to achieve the goals of your system. The technology used to develop your project (methods/algorithms, software requirements, hardware requirements), the duration of the project, and the project constraints should be

included here. The project constraints can be any technical hiccups, lack of resources, internal and external conditions (boundary conditions), etc. that can help further to avoid the related problems in the future during execution. In short, you can utilize this section to write about the limitations and boundaries of your project.

For example

- *"System boundaries (Software and hardware):*
- *Software: Server to keep track of multiple devices that can be put into the system.*
- *Hardware: Raspberry Pi 4, Accelerometer, Light bulb, 16x2 i2c LSD Display, breadboard, cables, GPS, Speaker*
- *Interfaces: To name a few such as the Internet via Wi-Fi, tracking device: GPS, backup methods such as 4G hotspot.*
- *Limitations:*
- *This project can only monitor and control the movements at that specific area.*
- *This project can only control the subjective activity on the device.*
- *The precision of the force acting on the object, the real-earthquake force is not precise.*
- *…"*

2. Product features:

This section describes the functionality that you want to have in your product such as the components used for the application and its functionality, appearance, performance in terms of speed/time, etc. You can specify them in the form of functional and non-functional requirements. A minimum number of 7 requirements (9 in case of selecting an existing application) is to be expected for your application. That includes functional, non-functional as well as security requirements cumulatively. However, it is highly probable that you will need more than the minimum amount to fully cover all the requirements.

While listing your requirements, you are also required to assign the level of priority to the requirements, as done in the examples below. The priority levels are: High **[H]**, Medium **[M]** and Low **[L]**.

Note: that **at least 2** should be Security Requirements.

A. Functional requirements: Write the requirements that are directly connected with the functionality of the application.

For example,

- *i) "The functional requirements of the earthquake detector **system are**:*
  - [**L**] The system should warn the user if there is a force acting which is above the threshold value.
  - [**H**]The system should allow users to monitor the changes on the devices through a website.

- [**M**] *The system should be able to detect the strength of the force.*
- [**M**] *The system should be able to track the device locations through the website. "*
- [**H**] The system should determine the strongness of the force based on the data input changes in the accelerometer.
- [**L**] The system should have the on/Off button to switch on or switch off the detector.
- [**M**] *The system should be able to neglect the force acting upon the object which is less than the threshold value."*

– *ii) "The functional requirements of a **simple earthquake detector** are:*

- [**H**] The system should be able to detect whether there is an earthquake or not.
- [**H**] The system should alarm when the earthquake is detected.

B. Nonfunctional requirements:

Write the requirements that are not the specific actions for your application but improve the quality of the system. This can be related to the storage capacity, performance requirements, Security requirements (Refer to the checklist given in SBD document-Phase 1), etc.

For example,

– *"The nonfunctional requirements of an **earthquake detector system** are:*

- [**L**] The system should be able to monitor the average latency between the gateway and the devices.
- **[H]** The system must be highly reliable, ensuring that it detects earthquakes accurately and minimizes false positive or false negative.
- **[M]** The system should be able to handle a high volume of data during a seismic event without degradation in performance.
- **[H]** The user interface should be user-friendly, making it easy for users and emergency responders to interact with system.*"*

– *"The nonfunctional requirements of a **simple earthquake detector** are:*

- [**H**] The system should be able to work with a minimum of 10 digits.
- [**M**] The system should not exceed the specified memory range.
- [**L**] The system should complete the arithmetic operation computation within t milliseconds.
- **[M]** The system should be affordable and cost-effective to acquire and maintain, especially for users in areas with limited resources**.**
- **[H]** If the detector is battery – powered, it should be designed to converse power when not actively to weather or potential physical damage.**"**

C. Security requirements:

Write the requirements that are the security requirements of your application (Refer to the checklist given in SBD document-Phase 1), etc.

For example,

- *i) "The functional requirements of an **earthquake detector system** are:*
  - [**M**] The system should perform spam blockage.
  - [**H**] The system should give control of the smart devices to the user.
  - [**M**] *A device can be invisible on the website if the user does not want to be tracked."*
- *ii) "The functional requirements of a **simple earthquake detector** are:*
  - [**L**] To access the earthquake detector and its functionality by only acquiring the device itself

Note: You are recommended to use the given priorities to produce a plan for your sprints such that you are able to deliver an **MVP** by the end of **Sprint 3**.

3. **Conclusion:** You should write the concluding remarks here. You can do this by **highlighting noteworthy design decisions** and **challenges** for the next phase that you recognized.

   - Assembling the system
   - Developing the code for the accelerometer and other connected joints to function
   - Making the calculation as precise as possible
   - Connecting every device to an actual website
   - Making a security-safe website

4. **Reference**: List the existing literature (documents/articles/blogs/research papers) references you have considered for finalizing the project idea. [1]

   - NATO Advanced Research Workshop on Earthquake Monitoring and Seismic Hazard Mitigation in Balkan Countries (2005: Borovets, Bulgaria), & Husebye, E. S. (2008). *Earthquake monitoring and seismic hazard mitigation in balkan countries: proceedings of the nato advanced*

research workshop on earthquake monitoring and seismic hazard mitigation in balkan countries, *borovetz*, *bulgaria*, *11-18 september 2005* (Ser. NATO science series. 4, earth and environmental sciences, v. 81). Springer. Retrieved September 13, 2023

- International Conference on Earthquake Engineering and Structural Dynamics (2017: Reykjavik, Iceland). (2019). Proceedings of the international conference on earthquake engineering and structural dynamics. (R. Rupakhety, S. Olafsson, & B. Bessason, Eds.) (Ser. Geotechnical, geological and earthquake engineering, volume 47). Springer. https://doi.org/10.1007/978-3-319-78187-7

- NATO Advanced Research Workshop on Earthquake Monitoring and Seismic Hazard Mitigation in Balkan Countries (2005: Borovets, Bulgaria), & Husebye, E. S. (2008). Earthquake monitoring and seismic hazard mitigation in Balkan countries: proceedings of the NATO advanced research workshop on earthquake monitoring and seismic hazard mitigation in Balkan countries, Borovetz, Bulgaria, 11-18 September 2005 (Ser. Nato science series. 4, earth and environmental sciences, v. 81). Springer. Retrieved September 18, 2023

Note: ***The security requirements should be mapped with the SBD requirement analysis (phase 1) checklist. You are free to write the security requirements in the form of a user story/abuse case.***