**Ass2-Module 5- Computer Systems (2024-2025)**

**Project**



**Requirement Analysis Phase 1**

**Security by Design Checklist**

|  |  |
| --- | --- |
| **Project Name:** | **Team Members:** |
| **Team ID:** | **Mentor(s):** |

**Instructions:**

1. **All the sections should be written in a clear, concise, and understandable way.**
2. **You must fill in the basic information about your projects such as Project Name, Team Members, Team ID, and Mentor(s).**
3. **Make sure to consider the checklist of the Requirement Analysis phase provided in the Security by Design document.**
4. **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 requirements 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 for selecting a particular mechanism for the requirements in the given column 'C'.

v) Write supplement requirement(s) in the form of a user story or Abuse case for the application (refer to the example given in 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 a tick mark 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 requirements 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** | **For example:** Checking the password | **For Example:** for granting access to multiple users and for users to have their 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 user name 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 is 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. |  |
| **Examples:** Biometric, Account security via Two-factor authentication/Multi-Factor Authentication, Smartphone communication (registered phone number), OAuth, Proof of User's physical presence for authentication (https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello-face-authentication), Proximity-based authentication, etc. |  |  |  | Follow the 4 points mentioned above. |  |
|  |  | Follow the 4 points mentioned above. |  |
| **Authorization** | Access control policies-User based, role-based, etc. |  |  |  | Follow the 4 points mentioned above. |
| **Audit** | Protection of Log files, |  |  |  | Follow the 4 points mentioned above. |  |
| Backup files, |  |  |  | Follow the 4 points mentioned above. |
| Temporary files, software, and database licenses (Legal aspect), processing of personal identifiable information on the devices (Legal aspect/GDPR policies), etc. |  |  |  | Follow the 4 points mentioned above. |  |
| **Team members' reviewed:** | (Member 1, Yes), (Member 2, Yes),… |  |  |  |  |  |

**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, the limitations of the existing system on which your project is based, etc.

* 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 namely the IOT-based home automation system is selected for the following reasons:*

* *This can digitally monitor and control the home devices such as electronic appliances, light systems, etc., from a remote location using smartphones/tablets. You have to just connect to the internet.*
* *This can be used for safety and security purposes by including the access control feature and the alarm systems in the front door.*
* *This…...”*
  1. **Limitations of the current system(If any)**:

List down the limitations of the currently existing similar systems.

***For example:***

*“The current limitations of already existing smart home automation systems 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. **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.)*

* 1. **Define SMART Goals**:

This section lists 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](https://www.youtube.com/watch?v=hXIUA2SdlAU) 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* ***system's efficiency*** *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 and Week 5.* |
| *2. To improve the* ***productivity*** *of the system by adding sensors such as door and window sensors, motion sensors, light sensors, temperature sensors, etc. for controlling the devices.* |  |  |  |  |
| *3. To improve the* ***quality*** *of the system…* |  |  |  |  |
| *4. To improve the* ***security*** *of the system…* |  |  |  |  |

* 1. **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 avoid 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: MQTT server to manage the flow of data between IoT devices, Mobile applications, Python language, HTML, PHP, Algorithms used, etc.*
  + *Hardware: Raspberry Pi 4, Sensors, Power supply, USB web camera, etc.*
* *Interfaces: To name a few such as the Internet via WiFi, backup methods such as 4G hotspots, etc.*
* *Limitations:* 
  + *This project can only monitor and control the lights of a home.*
  + *This project can only control the ‘n’ IoT devices at a time.*
  + *…”*

1. **Product features:**

Thissection 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 a 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 a* ***smart home automation system*** *are:*
    - [**L**] The system should give the option to the user to select the mode between cloud and stand-alone.
    - [**H**]The system should allow users to control and monitor their home devices using smartphones/tablets.
    - *The system should…*
    - *The system should… ”*
  + *ii) “The functional requirements of a* ***simple calculator*** *are:*
    - [**H**] The system/product should perform all the arithmetic operations according to the given keys.
    - [**M**] The system/product should have the On/Off button to switch on or switch off the calculator.
    - *The system should …”*

**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 the SBD document-Phase 1), etc.

**For example:**

* + *“The nonfunctional requirements of a* ***smart home automation system*** *are:*
    - [**L**] The system should be able to monitor the average latency between the gateway and the devices.
    - *…”*
  + *“The nonfunctional requirements of a* ***simple calculator*** *are:*
    - [**H**] The layout for the keys should not exceed more space than the layout of the calculator.
    - [**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.
    - ***…”***

**C.** **Security requirements:**

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

**For example**,

* + ​ *i) "The functional requirements of a* ***smart home automation system*** *are:*
    - [**M**] The system should perform user authentication.
    - [**H**] The system should give control of the smart devices to the authorized user.
    - *The system should… ”*
  + ​ *ii) "The functional requirements of a* ***simple calculator*** *are:*
    - [**M**] To access the application, one should require authentication.
    - *The system should …”*

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**.

1. **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 recognize.
2. **Reference**: List the existing literature (documents/articles/blogs/research papers) references you have considered for finalizing the project idea.
3. **Usage of AI tools:** State whether AI tools were used for this assignment, If yes, which AI tools are used, describe how and why you used them; alternatively, state clearly that AI tools were not used.

***Example:*** *Our team used ChatGPT to receive feedback on initial drafts and to brainstorm ideas for the assignment. We utilized this tool to refine our concepts and enhance the clarity of our writing, but we did not copy any large sections of generated text or code.*

**1Note:** ***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.***