Module 5- Computer Systems (2023-24)

Project

UNIVERSITY OF TWENTE.

Project Name:	Team ID:
Team Members:	Mentor(s):

Security by Design Checklist

Instructions:

A. **All the sections are mandatory.**
B. **Complete the sections in the below table and put a checkmark if you have done.**
C. **Think about your application and work on the sections accordingly.**
D. **Feel free to add extra requirements for reviewing security architecture and their countermeasures for your application, if needed.**

Sr. No.	Review Security Architecture	Put checkmark ✔ if you have completed the Review Security Architecture as suggested in the left column	Additional comments (If required)	Security Controls/Countermeasures	Put checkmark ✔ if you have completed the Security controls points as suggested in the left column	Additional comments (if required)
1	**Check Trust Boundaries, *for example,*** if you assign a higher privilege's level to someone to access a particular resource.			**Check the prevention criteria**, ***for example,*** if your personal information is identified by logging into an application, then either you decide to disable the application by removing your personal information and logging in. This is a prevention criterion.		
2	**Identify data flows**, ***for example***, if you read data from an untrusted source for your application.			**Check the mitigation criteria to reduce the impact of the risk/threat for the application.** ***For example*****:** Assume you have a database of users' passwords that are stored as a hash. Two users in the database who have the same password, they'll also have the same hash value. If the attacker identifies the hash value and its associated password, he'll be able to identify all the other passwords that have the same hash value. This risk can be mitigated by adding a randomly generated string, i.e. salt to each password in the database.		
3	**Entry and Exit points of the system and its components.**			**Make a data flow diagram to visualize and understand the data flow, input, output points, and trust boundary**.		

4	**Write the complete architecture in the SDD template. Review and approve among yourselves and by your assigned mentor(s).**			**Analyze the cost involved to implement the security controls (if any).**		
	Team members' reviewed:	(Member 1, Yes), (Member 2, Yes),…				

Software Design Document Template

Instructions:

i) You must explain all the given sections clearly and concisely.

ii) You must fill in the basic information about your projects such as Project Name, Team Members, Team ID, and Mentor(s).

iii) Make sure to consider the checklist of the Design phase provided in the Security by Design document.

iv) The length of the document should be 4 to 8 pages (including the diagrams).

1. Introduction

*(The **brief overview** of your application.)*

2. Functional/Non Functional Requirements

*(This section is **mandatory for those teams who have changed their project requirements** for some genuine reasons in consultation with their mentors and they have not mentioned these requirements in the Requirement Analysis document).*

3. Architectural Design

(Create diagrams to depict a high-level impression of your system using UML diagrams that should include Use case, Class, Activity, and Data flow diagrams (at least one diagram for each category).

The diagrams can be drawn using online tools, i.e. draw.io (free tool), etc.

Write the motivation for all your UML diagrams to highlight the project features and requirements.

This section aims to understand the system and its basic components, how the components interact with each other, data repositories, security requirements in design such as trust boundaries, input/output points, swapping/updating firmware for fixing bugs, and adding new features to the product, etc.).

4. **Product User Interface**

*(In this section, you should **create illustrations using Wireframing tools** (Pencil Project, Mockplus, etc.), based on the Software Requirement Specification (SRS) of your application, **for example**, the menus required for the interface, buttons, and its tasks (Toolbar), any other functionality like events, sub-events, controls, status bar, etc.)*

5. **Prevention/Mitigation Criteria (Security Controls)**

*(In this section, you should **specify the criteria to avoid/ remove the risks** identified in the design.)*

6. **The cost involved (if any):**

*(This section is used to mention the **cost involved** to implement the necessary security controls for your application. This includes both time and money related costs.)*

7. **Conclusion:**

*(You should give the **concluding remarks** of your document. You can do this by **highlighting noteworthy design decisions** and **challenges** for the next phase that you recognized.)*

Reference:

*(Utilize this section to mention the **research papers/articles** you referred to for the document.)*