Module 5 -Computer Systems

(2021-22)

Project

UNIVERSITY OF TWENTE.

Security by Design Checklist (Requirement Analysis Phase 1)

Team ID:	**Team Members:** Rick Pluimers, Kağan Gülsüm, Kristiyan Velikov, Laurens Neinders, Aleksandar Petrov, Liran Neta
Project Name:	**Mentor(s):** Mohammed Assaad and Alex Mo

Steps to be performed:

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 or 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 with the team members and approved by your mentor(s)/TAs.

ix) Put tickmark in the last column for all verified items.

x) This document should be appended to the Software Requirement Specification (SRS) document.

Follow these 5 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.

v) Approve the document by your mentor.

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	Login system via OAuth 2.0 and OpenID Connect for the User Interface.	It enables our app to obtain a user's data and authenticate him without giving away a user’s password and other sensitive data.	As a user, I can quickly and securely log in to the system using a 3rd party account (for example google).	Our system is dependent on the functionality of a third party	Protocol OAuth 2.0 and OpenID Connect are on top of it.	
Authorization	Access control policies User-based	To keep our system more secure. Only authorized members can access the UI where they can view scores and start a race.	As a user, I can access the UI I have logged in.	An intruder can bypass the authorization control.	Persistent session using Cookies.	
Audit	Protection of Log files	It’s important to encrypt our log files so the data is free from malicious corruption	As an admin, I want to check the log files to check what happened if something is out of the ordinary.	An intruder can tamper with the log files to hide his activity.	Encryption of the log files so that they cannot be changed by anyone but the maintainers (with the key)	
	Backup files	In case of corruption or deletion of important data (recorded times), it could be recovered.	In case my files are deleted by hackers, I want to be able to recover the system’s data.	The original data could be corrupted or deleted.	backup that is often updated and separate from the main database.	
	Temporary files, software and database licenses (Legal aspect), processing of personal identifiable information on the devices (Legal aspect/GDPR policies), etc.	We are legally obligated to keep to the GDPR legislation.	As a user, I don’t want my personal information to be known by unknown parties.	Personal information can be stolen by malicious parties.	Only very little personal information is stored and as Oauth is used, No extra account data needs to be stored to make an account or log in.	

Team members' reviewed: Mentor(s) reviewed and verfied:

(Member 1, Yes), (Member 2, Yes),… (Mentor 1, Yes), (Mentor 2, Yes), …

Prepared by:

Dipti K. Sarmah (Project Coordinator)