Module 5 -Computer Systems

(2022-23)

Project

UNIVERSITY OF TWENTE.

Security by Design Checklist
(Requirement Analysis Phase 1)

Team ID: 4	**Team Members: Thijs Frauenfelder, Katy Radzkova, Ayolt ten Have, Victor Zugravu, Frank Bosman, Mikus Vancans**
Project Name: PSec (Portable Security)	**Mentor(s): Priya Naguine & Radu Basarabá**

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 an 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	**Username + password checking for the web interface**	For granting access to multiple users and for users to have their individual profiles, we need to authenticate their username with a password. A more sophisticated authentication is not required. Users need to be able to access the live feed quickly when they get a notification.	**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 a username and password for 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.	**Risk identification:** i) The length of the passwords is less than 8 characters. ii) The password is not very strong. iii) You enter a wrong password more than 3 times.	When making a password, the system should check the length and strength (by checking for use of numbers, uppercase & lowercase and special characters). When signing in the system will stop you after 3 wrong guesses and give you a time out.	
	A keypad with a temporary 4-number combination to access the web interface from the home	Allows the owner to control the system from home, view the camera stream and grant temporary access to people, for example when someone needs to get something from your room.	**Goal**: As an owner, I want to be able to view the stream and change the settings of the system from home. **Requirement**: To access the system from home with a dedicated access panel. **User story**: "As a user, I can check the stream at any time and customise the settings" **Abuse case:** "As an attacker, I can enter the keycode to have access/disable the system"	**Risk identification:** i) Entering a password incorrectly more than 3 times. ii) The keycode is easy to guess.	When filling in the code, the system will stop accepting tries after 3 tries. The keycode is randomly generated when the user requests it and is only valid 30 seconds, not enough time to try all 10.000 possible permutations (and you only have 3 tries)	
Authorization	**Access control policies User-based, role-based, etc.**	Our access control will be User-based as we only have one user group, the homeowners / building owners.	**Goal**: As an owner, you do not want non-owners to have access to the security system and you want to be the only one who can log in and change your security system. It is not necessary for non-affiliated people to sign in on your security page. **Requirement**: To log into the system if you are an authorised person. **User story**: "As a user of the system only I and other authorised users have access to the security system " **Abuse case:** The attacker could impersonate the owner.	**Risk identification:** i) Log-in details are shared ii) Log-in details are stolen	The camera will have a reset button which will remove all saved user accounts, so that when log-in details are leaked they won't work for long. We might also implement some kind of 2-factor for the first time log-in on a device.	
Audit	**Keeping of Log files and their protection**	Log files will be kept to see who has used the system and in what ways as a way for the user to make sure the system has not been compromised. These files will also be used for debugging.	**Goal**: As an owner, you have access to log files which allow you to check whether the security system has been compromised **Requirement**: To make a list of log files available to the user at all times **User Story**: "As a user, I can analyse the log files in case of any fears that an unauthorised person	**Risk identification**: i) Log files are not protected enough	Log files will be encrypted and only visible after signing in	

			has gained access to the camera." **Abuse case**: "As an attacker, I can manipulate the log files so as to not alert the owner "			
	Backup files	As the security system records moments where movement/sound is detected it will be uploaded to a backup location to make sure there is no loss of video in any case.	**Goal**: The system backs up recorded videos to cloud storage to prevent loss of video recordings. **Requirement**: To prevent loss of video recordings they should be uploaded to cloud storage automatically **User story**: "As a user, I don't have to worry about losing any data and can access it remotely at any time" **Abuse Case**: "As an attacker, I can corrupt or steal the video recordings"	**Risk identification**: i) The upload of the videos was unsuccessful (error / no internet connection, etc.) ii)The camera is purposefully obstructed by a malicious party	There will be an index light on the product that shows when it has no internet connection. And when it doesn't have internet connection it will back up the files locally until an internet connection is achieved. The backup files can also only be accessed when logged in.	
	Temporary files, software and database licences (Legal aspect), processing of personally identifiable information on the devices (Legal aspect/GDPR policies), etc.	Temporary files and the data models used by facial recognition will be stored offline on the Raspberry Pi.	**Goal:** Temporary files and data models will be used to process images and other data. They are kept offline so they can't be hacked. **Requirement:** none **User Story:** "users don't have to worry about the data being stolen or changed" **Abuse case:** Someone could come in and steal the SD with the data or swap it out for other data.	**Risk identification:** i) test if the SD card is still connected.	The data models will be encrypted and the temporary will only be saved offline. Furthermore the software will periodically test if the SD card is still connected and give an alert if not.	

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

Members: Mikus Vancans **yes**, Frank Bosman **yes**, Victor Zugravu **yes**,

Thijs Frauenfelder **yes** Katy Radzkova **yes**, Ayolt ten Have **yes**,

Mentors: Priya Naguine …, Radu basarabá…

Prepared by:

Dipti K. Sarmah (Project Coordinator)