Module 5-Computer Systems (2022-23)

Project

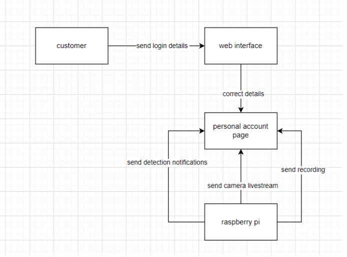
UNIVERSITY OF TWENTE.

Security by Design Checklist (Design Phase)

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

Instructions:

1. Complete the sections in the below table and put a checkmark if you have done.
2. Think about your application and work on the sections accordingly.
3. Feel free to add extra requirements for reviewing security architecture and their countermeasures for your application, if needed.
4. This document should be reviewed and approved by your team members and mentors before submission.
5. Make sure to submit this checklist along with the Software design document (SDD) on Canvas.

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,** The thrust boundaries are checked when the user tries to log in or when the user performs an action, like turning on the lifestream.			**Check the prevention criteria**, When the user logs in his credentials are checked and a token to show that this process was successful at that time will be stored. then every time the user loads a page, requests data or sends data the token is checked as well.		
2	**Identify data flows**, Every time data is requested the user's token is sent to verify the user.			**Check the mitigation criteria to reduce the impact of the risk/threat for the application.** The passwords are salted and peppered to ensure that even if the database is compromised and the intruder knows the most often used password they won't manage to decrypt the other passwords.		
3	**Entry and Exit points of the system and its components.** Web interface and its connections with the Raspberry Pi.			**Make a data flow diagram to visualize and understand the data flow, input, output points, and trust boundary.** The trust boundary is the connection with the pi, the data retrieved from it and the requests sent.  customer send login details web interface correct details personal account page send detection notifications send recording send camera livestream raspberry pi		

4	**Write the complete architecture in the SDD template. Review and approve among yourselves and by your assigned mentor(s).** Written in the SDD file			**Analyze the cost involved to implement the security controls (if any).** See table 2 Costs for security and table 3 Costs for hardware.		

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

Port closing, done by week 7
HTTPS encryption, done by week 8
Password handling, done by week 8
Streaming encryption (AES-128), done by week
Authorisation, done by week 7
Input sanitisation, done by week 7

Table 2 Costs for security

Item	Price	Comments
Raspberry Pi 4	/	Already attained
Web camera	16€	Web camera
Microphone	8€	Microphone
Small display	/	Display, already attained
Keypad	/	Keypad, already attained
Power supply	/	Already attained
Motion sensor	2.30€	Motion Sensor
Total:	~27€	

Table 3 Costs for hardware.