Module 5-Computer Systems (2021-22)
Project

UNIVERSITY OF TWENTE.

Security by Design Checklist
(Design Phase)

Team ID: Team 31	**Team Members:** Damon Kaewborisut, Jelke Schröder, Yifan Sun, Shuhang Tian, Masis Zovikoglu, Niek Zieverink
Project Name: Raspberry Home	**Mentor(s):** Ricco Pratama Halim, Filip Ivanov

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, ***for example,*** if you assign a higher privilege's level to someone to access a particular resource.	✔	Since we don't use any external data sources we don't have trust boundaries concerning possibly untrustworthy third parties. Therefore the only real trust boundary we have is user input as this might come from an attacker. We mitigate this risk by filtering/sanitizing all user input	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.	✔	See Prevention / Mitigation Criteria (Security Controls)

2	**Identify data flows**, ***for example*** , if you read data from an untrusted source for your application.	✔	See data flow diagram	**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.	✔	See Prevention / Mitigation Criteria (Security Controls)
3	**Entry and Exit points of the system and its components.**	✔	- Entry point: User input - Exit point: User gets temperature / light data or gets broadcast message	**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).**	✔	We don’t have to incur any monetary costs for the security. Therefore the costs are all expressed in the number of hours that it will take to implement the given security measure

Team members' reviewed: Damon Kaewborisut, Jelke Schröder, Yifan Sun, Shuhang Tian, Masis Zovikoglu, Niek Zieverink

Mentor(s) reviewed and verified: Dipti K. Sarmah