Module 5-Computer Systems (2021-22)
Project

UNIVERSITY OF TWENTE.

Security by Design Checklist
(Design Phase)

Team ID: 22	**Team Members:** Liran Neta, Kristiyan Velikov, Laurens Neinders, Kağan Gülsüm, Rick Pluimers, Alex Petrov
Project Name: RC Racing System	**Mentor(s):** Alex Mo, Mohammed Assaad

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** An user should only be able to access data from the database which is related to him: Challenges, Friends, Time-Laps	✔		**Check the prevention criteria:** Since we are using OAuth 2.0. We store information about the currently logged in users. We would be using cookies to keep persistent connections of the users and authorize them to access information related to them.	✔	
	Identify data flows The data coming from the sensors can not always be trusted.			**Check the mitigation criteria to reduce the impact of the risk/threat for the application.**		

2		✔		The information that comes from the sensors can not always be trusted, sensors can be tricked or malfunction so this risk should be mitigated as much as possible. The countermeasures are that we will check if the order of incoming sensor data is correct and if the given times are within reasonable boundaries. This is obviously not going to prevent every attempt of cheating, but it will help. if we would want to make this fully secure would be to have a referee validate the race.	✔	
3	**Entry and Exit points of the system** **and its components.** Only an authorised user can start a race and only system-determined results are shown to the user.	✔		**Make a data flow diagram to visualize and understand the data flow, input, output points, and trust boundary**. The data flow diagram shows a racer requesting a race and then receiving the race results back to him. Only a racer that is authorised by the O-Auth server can initiate a race and the results received are strictly the ones the system shows. The user cannot access results he is not meant to.	✔	
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).** Rc car, +-25 euro's (can we get sponsored), sensors, +- 5 euro's track material, probably made from personal materials (so free)	✔	

(Liran Neta, Yes), (Laurens Neinders, Yes), (Kağan Gülsüm, Yes),(Kristiyan Velikov, Yes),(Rick Pluimers, Yes), (Alex Petrov, Yes)

Team members' reviewed:

(Mentor 1, Yes), (Mentor 2, Yes), …

Mentor(s) reviewed and verified:

Prepared by:

Dipti K. Sarmah