Secure and Dependable Systems
Jacobs University Bremen
Dr. Florian Rabe

Homework 5
given: 2017-03-28

Homework 5

You have to submit your solutions as announced in the lecture.
Unless mentioned otherwise, all problems are due 2017-04-06, before the lecture.
There will be no deadline extensions unless mentioned otherwise in the lecture.

This homework is not published yet. I may still change it before publishing it.

Problem 5.1 *Verification: Class Invariants* Points: 2

Argue informally but rigorously why the formula in the stack example from the notes is a class invariant.

Problem 5.2 *Proof Assistants: Practice* Points: 4

Install either Isabelle or Coq (see the links in the lecture notes).

Write a simple pure recursive function and verify that it meets its specification using the tool. Generate executable code from your function.

Submit a reasonable combination of screen shots, shell logs, system output etc. that demonstrates you completed the task.

You may use any example that is already part of the available documentation or tutorials. But you have to prove that you actually installed the system and ran the verification. For example, you can copy an example from the tutorial, rename the function to your name, and then run the verification.