Assignment:
Verification of an Internet Mail Server

Bart Jacobs

1 Assignment

The goal of this assignment is to verify a mail server. More specifically, you must add annotations to `MailServer.c` such that the VeriFast program verifier accepts the program. Your solution is considered to be correct if you did not modify the C code itself and the command

```
verifast stringBuffers.o threading.o sockets.o MailServer.c
```

outputs

```
MailServer.c
0 errors found
Linking...
Program linked successfully.
```

This command checks that the program verifies (with overflow checking enabled), that `main` has a sound contract and that the program contains neither lemmas without proofs nor assume statements. Specifications need not express full functional correctness; you need to supply only the minimal specifications necessary to make VeriFast accept the program. Note that the `leak` command may be used in your solution.

Your final solution must be submitted to bart.jacobs@cs.kuleuven.be no later than 31 December 2022. However, I strongly encourage submitting your solution earlier. It suffices to send the annotated version of `MailServer.c`. If you get stuck, send an email describing your problem to bart.jacobs@cs.kuleuven.be and I will reply with a question that should get you unstuck, in Socratic style. In fact, I strongly encourage asking for help if you get stuck: if your final submission is incomplete, I will take into account the quantity and quality of your questions!

In your submission e-mail, state your availability during the five working days starting the second day after your submission. I will use this information to schedule an appointment for the defense of your submission. In this appointment, you must defend your solution orally and demonstrate your understanding of VeriFast by answering questions such as: describe the changes in

the symbolic state that will be made by the next step in the symbolic execution of this function. Furthermore, I will examine your knowledge and understanding of the material from the theory lectures. The appointment will take place at my office (200A 05.50).

2 Hints

- You will need fractional permissions (as discussed in the tutorial) to complete this assignment. You will need them to share a chunk among many threads (see the VeriFast Tutorial section on Leaking and Dummy Fractions).