Exercise for Engineering Secure Software Systems

February 4, 2021: Information Flow, Exercises 10, 11

Henning Schnoor

Institut für Informatik, Christian-Albrechts-Universität zu Kiel

Oral Exam

date

- Tuesday, February 23
- Wednesday, February 24
- Friday, March 5
- each exam: ≈ 25 minutes

preparation

- use available material: slides, notes, exercises
- **“readiness indicator:” review questions**
- only take the exam if you are prepared
- let me know if you can’t “come!”

registration

until Sunday, February 14: `https://www-ps.informatik.uni-kiel.de/pruefungsanmeldung/`, access code: 1O1BIS

Exam via BigBlueButton

Technicalities

- We use BigBlueButton, either
  - standalone,
  - as part of ESSS-Mattermost channel, or
  - as part of OLAT.
- You need a working camara/microphone, and your (student) id **with photo** readable through the camera
- Use a computer so you can draw/type in the shared working area
- Test your setup before the exam.
- TEST YOUR SETUP BEFORE THE EXAM!

Technical Issues?

- things can go wrong: internet connection, device crashes, camera, microphone, you name it!
- then: exam counts as “not taken,” not as failed
- new date probably only possible in second examination period (starting March 29)

Exam: My Expectations

I expect you to …

4,0 know central definitions, results (formally correct) and can apply them to simple examples

basic reproduction

3,0 explain relationships between and motivations for central definitions

basic understanding

2,0 explain the ideas behind the central proofs

advanced understanding

1,0 reason about alternative defintions, applications, …

application of knowledge to new situations

caveats

- this is **not** a “guaranteed performance → grade mapping”
- this is a **theory lecture**, you need to be **formally precise** when required.

Exam: Your Preparation

material

- slides
- exercises (with solutions)
- videos (of some central proofs)
- notes (contain all proofs)

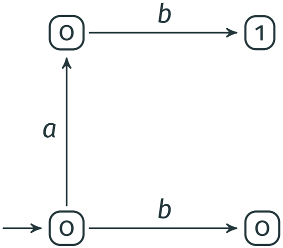
preparation: are you ready?

- Do you know the central definitions, results, **precisely**?
- Can you answer the review questions? (Answers not provided on purpose)
- Do you have ideas for most of the exercise tasks? (Most exercises have solutions, except the ones that are meant to lead to discussions)
- Can you explain the relationship between different but related concepts in the lecture?
- Can you explain the proofs of the main formal results of the lecture?

Information Flow Examples

IP-Security Example III

system



specification

- policy: $A \rightarrowtail B \rightarrowtail L$
- state labels: L observations
- actions a/b of agent A/B

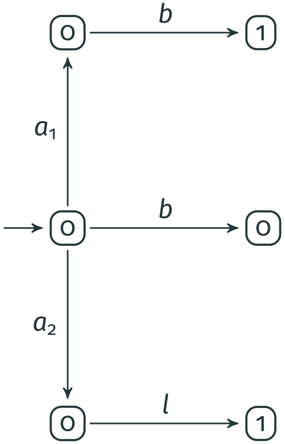
security

Is the system

- P-secure?
- IP-secure?

IP-Security Example IV

system



specification

- policy: $A \rightarrowtail B \rightarrowtail L$
- state labels: L observations
- actions $a_x/b/l$ of agent $A/B/L$

security

Is the system

- P-secure?
- IP-secure?