Exercise for Engineering Secure Software Systems

February 11, 2021: Closing

Henning Schnoor

Institut für Informatik, Christian-Albrechts-Universität zu Kiel

Oral Exam

date

- first exam period: Tuesday/Wednesday, February 23/24, Friday, March 5
- second exam period: Monday, March 29 (beware DST)
- each exam: ≈ 25 minutes, be "there" 10 minutes before, I will call you in

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

(exam period 1 so far) 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: Corona Info

from Vice President for Studies & Teaching

- A **free attempt** will be granted for all examinations taken and failed during the examination periods of the winter semester 2020/21
- Please take into account that the lecturers have a significantly higher workload than in regular semesters. **We therefore ask you to only register for examinations for which you have prepared and which you wish to take.** If you will not be taking an exam at short notice, please inform the respective examiners, especially in the case of oral exams.

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 $\rightarrow$ grade mapping”
- this is a **theory lecture**, you need to be **formally precise** when required.

Exam: Your Preparation

material

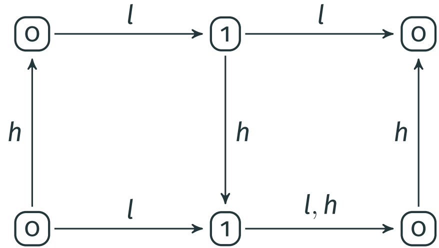
- slides
- exercises (with solutions)
- videos (of some central proofs)
- notes (contain all proofs)

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?

Task (P-Security Example I)

Is the following system P-secure? Justify your answer.



Exercise

Task (P-Security Example II)

Is the following system P-secure? Justify your answer.

$$\begin{tikzcd}
\boxed{0} \arrow[r, "l"] & \boxed{0} \arrow[r, "l"] \arrow[d, "h"] & \boxed{0} \\
\boxed{0} \arrow[u, "h"] \arrow[r, "l"] & \boxed{0} \arrow[r, "{l, h}"] & \boxed{1} \arrow[u, "h"]
\end{tikzcd}$$

Exercise

Task (alternative definition of P security I)

Let $M = (S, s_0, A, \mathtt{step}, D, O, \mathtt{obs}, \mathtt{dom})$ be a system and let $\rightarrowtail$ be a policy for M. Prove that the following are equivalent:

1. M is P-secure with respect to $\rightarrowtail$,
2. for all states $s \in S$, all $u \in D$, and all traces $\alpha \in A^*$, we have that

$$\mathtt{obs}_u(s \cdot \alpha) = \mathtt{obs}_u(s \cdot \mathtt{purge}_u(\alpha)).$$

Note: The characterization from this task is in fact the original definition of P-Security, the (equivalent, by the above) definition we work with in the lecture was later user by Ron van der Meyden.

Exercise

Task (uniqueness of unwindings)

Show that P-unwindings are not unique, but that mininal P-unwindings are, that is:

1. give an example for a system M and a policy $\rightarrowtail$ such that there are (at least) two different P-unwindings for M and $\rightarrowtail$,
2. show that if M is P-secure with respect to a policy $\rightarrowtail$, then there is a P-unwinding for M and $\rightarrowtail$ that is contained (via set inclusion) in all P-unwindings for M and $\rightarrowtail$.

Exercise

Task (IP-Security examples)

Which of the following systems are IP-secure? Assume that as usual, the state names indicate the observations made by L, that lowercase letters denote actions performed by agents with the corresponding higher-case letter name, and the policy $H \rightarrowtail D \rightarrowtail L$. Additionally, assume that H and D make the same observation in each state of the system.

$$\begin{tikzcd}
\boxed{0} \arrow[r, "h"] \arrow[d, "l"] & \boxed{0} \arrow[r, "d"] & \boxed{1} \\
\boxed{0} \arrow[r, "h"] & \boxed{0} \arrow[r, "d"] & \boxed{0}
\end{tikzcd}
\qquad
\begin{tikzcd}
\boxed{0} \arrow[r, "h"] \arrow[d, "l"] & \boxed{0} \arrow[r, "d"] & \boxed{1} \\
\boxed{0} \arrow[r, "d"] & \boxed{0} \arrow[r, "h"] & \boxed{1}
\end{tikzcd}$$

Questions

Thank You!

Questions

?