Engineering Secure Software Systems

February 9, 2021: Information Flow: IP and TA-Security, Wrap-Up, Discussion

Henning Schnoor

Institut für Informatik, Christian-Albrechts-Universität zu Kiel

Admin: Exam

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 → 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?

Part II: Information Flow

Overview

Part II: Information Flow

- Examples
- Introduction and Motivation
- P-Security

IP-Security

- Motivation and Definition
- Automatic Verification

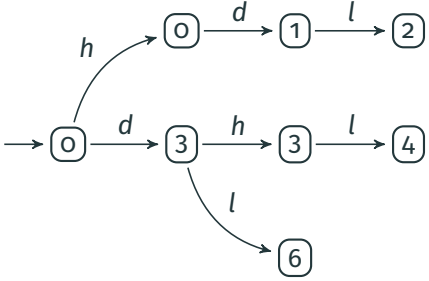
TA-Security

- Motivation and Definition

Overview

IP-Security Example I

system



specification

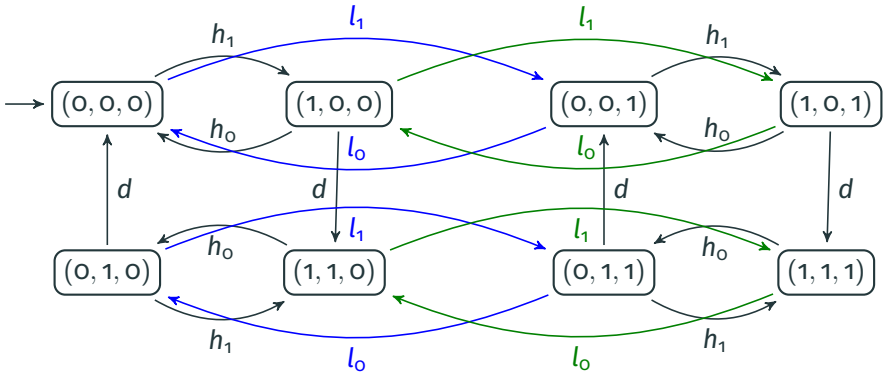
- intransitive policy: $H \rightarrowtail D \rightarrowtail L$
- actions h / d / l of agent H / D / L
- L's observations: indicated numbers

analysis

system secure?

- intuitively?
- formally?

IP-Security Example II



system

- intransitive policy $H \rightarrowtail D \rightarrowtail L$
- actions h_x, d, l_x of agents H / D / L
- $\mathtt{obs}_L(a, b, c) = (b, c)$
- system secure? intuitively, formally?

P-Security and IP-Security

question

- two security properties: P-security, IP-security
- does either implication hold? guesses?

intuition

- IP-security is “relaxation” of P-security
- agents are allowed to have more information
- leads to less-strict security property

fact

If system M is P-secure wrt. $\rightarrowtail$, then also IP-secure wrt. $\rightarrowtail$.

converse?

P-Security implies IP-Security

fact

If a system M is P-secure with respect to $\rightarrowtail$, then M is IP-secure with respect to $\rightarrowtail$. The converse is true for transitive policies.

proof

- assume M is P-secure
- agent u, state s, traces α_1, α_2 with $\mathtt{ipurge}_u(\alpha_1) = \mathtt{ipurge}_u(\alpha_2)$
- need to show: $\mathtt{obs}_u(s \cdot \alpha_1) = \mathtt{obs}_u(s \cdot \alpha_2)$
- enough to show: $\mathtt{purge}_u(\alpha_1) = \mathtt{purge}_u(\alpha_2)$, since M is P-secure
- general: $\mathtt{purge}_u(\alpha) = \mathtt{purge}_u(\mathtt{ipurge}_u(\alpha))$
- so: $\mathtt{purge}_u(\alpha_1) = \mathtt{purge}_u(\mathtt{ipurge}_u(\alpha_1)) = \mathtt{purge}_u(\mathtt{ipurge}_u(\alpha_2)) = \mathtt{purge}_u(\alpha_2)$

completes proof (see exercise for transitive case).

Exercise

Task (implications between security properties)

In the lecture, some implications between security definitions were stated without proof. Choose and prove one of the following (in the following, M is a system and $\rightarrowtail$ a policy).

1. If M is TA-secure with respect to $\rightarrowtail$, then M is also IP-secure with respect to $\rightarrowtail$.
2. If M is P-secure with respect to $\rightarrowtail$, then M is also TA-secure with respect to $\rightarrowtail$.

Exercise

Task (equivalence for transitive policies)

Show that for transitive policies, P-security, IP-security, and TA-security are equivalent. More formally: Let M be a system, and let $\rightarrowtail$ be a transitive policy. Show that the following are equivalent:

1. M is P-secure with respect to $\rightarrowtail$,
2. M is TA-secure with respect to $\rightarrowtail$,
3. M is IP-secure with respect to $\rightarrowtail$,

Exercise

Task (P-security and non-transitive policies)

Prove or disprove the following: If $M = (S, s_0, A, \texttt{step}, D, O, \texttt{obs}, \texttt{dom})$ is a system and $\rightarrowtail$ is a policy for M, then the following are equivalent:

- M is P-secure with respect to $\rightarrowtail$,
- M is P-secure with respect to the transitive closure of $\rightarrowtail$.

Overview

Unwindings for IP- (and TA-) security?

observation

- IP (and TA) security are more “complex” than P-security
- for deciding security: must keep track of “who-knows-what”
- simple unwinding as in P-security not expected

verification

- IP-security (and TA-security) can still be decided in polynomial time
- key: unwinding conditions “between several agents”

reference

Sebastian Eggert, Ron van der Meyden, Henning Schnoor, and Thomas Wilke. “The Complexity of Intransitive Noninterference”. In: IEEE Symposium on Security and Privacy. IEEE Computer Society, 2011, pp. 196–211. ISBN: 978-1-4577-0147-4

Unwindings for IP-security

definition

An IP-unwinding for a system $(S, s_0, A, \texttt{step}, D, O, \texttt{obs}, \texttt{dom})$ and a policy $\rightarrowtail$ is a family of equivalence relations $(\sim_u^v)_{u,v \in D}$ on S such that

OC^{IP} if $s \sim_u^v t$, then $\texttt{obs}_u(s) = \texttt{obs}_u(t)$

SC^{IP} if $s \sim_u^v t$ and $v \not\rightarrowtail \texttt{dom}(a)$ then $s \cdot a \sim_u^v t \cdot a$

LR^{IP} if $v \not\rightarrowtail u$ and $a \in A$ with $\texttt{dom}(a) = v$ then $s \sim_u^v s \cdot a$

intuition

- u: observer (L)
- v: potentially secret actions (H)

theorem [Egg+13]

A system M is IP-secure wrt. $\rightarrowtail$ if and only if there is an IP-unwinding for M and $\rightarrowtail$.

Polynomial-Time Algorithm for IP-Security

corollary

IP-security can be verified in polynomial time.

proof

- M IP-secure wrt $\rightarrowtail$ iff all $\sim_u^v$ satisfy output consistency, where:
  $\sim_u^v$ smallest equivalence relation satisfying SC^{IP} and LR^{IP} with respect to $\rightarrowtail$.
- algorithm: immediately from unwinding, analogous to P-security

Overview

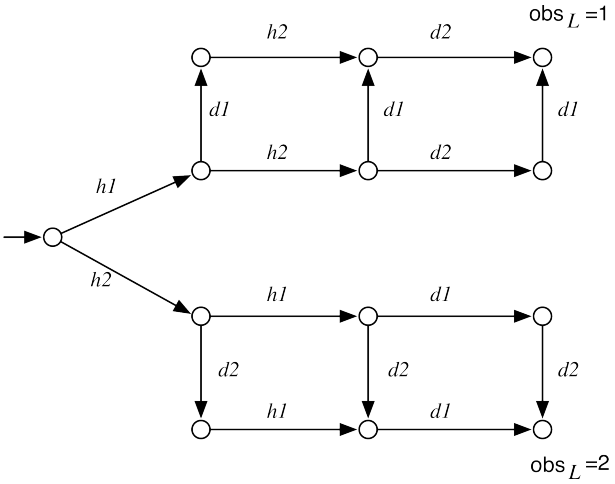
Part II: Information Flow

- Examples
- Introduction and Motivation
- P-Security
- IP-Security
  - Motivation and Definition
  - Automatic Verification
- TA-Security
  - Motivation and Definition

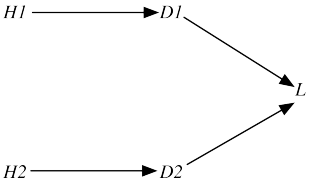
Overview

IP-Security: Is it Enough?

system [Meyo7]



policy



analysis

system secure?

- intuitively?
- formally?

From IP to TA security

observation

- P- and IP-security only model *which* actions an agent may “learn”
- not treated: information about order of actions

fixing IP security

- modify definition to add order-information
- are we then sure we captured everything?

TA-Security: Approach

overview

- $\mathtt{ta}$-function: transmission of actions
- defines *maximal information* $\mathtt{ta}_u(\alpha)$ that agent u may have about run α
- TA-Security requirement: if $\mathtt{ta}_u(\alpha) = \mathtt{ta}_u(\beta)$, then $\mathtt{obs}_u(\mathsf{s} \cdot \alpha) = \mathtt{obs}_u(\mathsf{s} \cdot \beta)$

reference (definition and basic properties of TA-Security)

Ron van der Meyden. “What, Indeed, Is Intransitive Noninterference?” In: European Symposium On Research In Computer Security (ESORICS). Ed. by Joachim Biskup and Javier Lopez. Vol. 4734. Lecture Notes in Computer Science. Springer, 2007, pp. 235–250. ISBN: 978-3-540-74834-2

Questions

Thank You!

Questions

?