CHRISTIAN-ALBRECHTS-UNIVERSITÄT ZU KIEL
Institut für Informatik · AG Software Engineering
Priv.-Doz. Henning Schnoor

Engineering Secure Software Systems Winter 2020/21
Exercise Sheet 13

issued: February 9, 2021 **due:** never (you can use these for exam preparation)

Exercise 13.1, implications between security properties (10 Points)

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 13.2, equivalence for transitive policies (10 Points)

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 13.3, P-security and non-transitive policies (10 Points)

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 $\rightarrowtail$.