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 $\rightarrowtail$.

Solution

1. The proof is from the full version of [Mey07]. Assume that M is TA-secure with respect to $\rightarrowtail$, we show that IP-security holds as well. Hence let s be a state, let u be an agent, and let α_1, α_2 be action sequences with $\mathtt{ipurge}_u(\alpha_1) = \mathtt{ipurge}_u(\alpha_2)$. To show that $\mathtt{obs}_u(s \cdot \alpha_1) = \mathtt{obs}_u(s \cdot \alpha_2)$, it suffices to prove that $\mathtt{ta}_u(\alpha_1) = \mathtt{ta}_u(\alpha_2)$, then TA-security of the system implies that both have the same observations. To show this, it suffices to prove that, for all $X \subseteq D$ with $u \in X$, we have that $\mathtt{ta}_u(\alpha) = \mathtt{ta}_u(\mathtt{ipurge}_X(\alpha))$. We show the claim by induction on α. If $\alpha = \epsilon$, the claim is trivial. Hence assume the claim is true for α, we consider αa for some action $a \in A$. As usual, we consider two cases:

   - If $\mathtt{dom}(a) \not\rightarrowtail u$, then, by definition, $\mathtt{ta}_u(\alpha a) = \mathtt{ta}_u(\alpha)$. We consider two subcases, writing $v \rightarrowtail X$ is $v \rightarrowtail w$ for some $w \in X$.
     - case 1: $\mathtt{dom}(a) \not\rightarrowtail X$. Then $\mathtt{ipurge}_X(\alpha a) = \mathtt{ipurge}_X(\alpha)$. Hence

       $$\begin{array}{rcl} \mathtt{ta}_u(\mathtt{ipurge}_X(\alpha a)) & = & \mathtt{ta}_u(\mathtt{ipurge}_X(\alpha)) \\ & = & \mathtt{ta}_u(\alpha) \text{ (by induction)} \quad \text{as required.} \\ & = & \mathtt{ta}_u(\alpha a), \end{array}$$

     - case 2: $\mathtt{dom}(a) \rightarrowtail X$. Then $\mathtt{ipurge}_X(\alpha a) = \mathtt{ipurge}_{X \cup \{\mathtt{dom}(a)\}}(\alpha) \cdot a$. Hence, it follows that

       $$\begin{array}{rcl} \mathtt{ta}_u(\mathtt{ipurge}_X(\alpha a)) & = & \mathtt{ta}_u(\mathtt{ipurge}_{X \cup \{\mathtt{dom}(a)\}}(\alpha) \cdot a) \\ & = & \mathtt{ta}_u(\mathtt{ipurge}_{X \cup \{\mathtt{dom}(a)\}}(\alpha)) \text{ (recall that } \mathtt{dom}(a) \not\rightarrowtail u) \\ & = & \mathtt{ta}_u(\alpha) \text{ (by induction)} \\ & = & \mathtt{ta}_u(\alpha a). \end{array}$$

   - if $\mathtt{dom}(a) \rightarrowtail u$, then $\mathtt{ipurge}_X(\alpha a) = \mathtt{ipurge}_{X \cup \{\mathtt{dom}(a)\}}(\alpha) \cdot a$. Thus

     $$\begin{array}{rcl} \mathtt{ta}_u(\mathtt{ipurge}(\alpha a)) & = & \mathtt{ta}_u(\mathtt{ipurge}_{X \cup \{\mathtt{dom}(a)\}}(\alpha) \cdot a) \\ & = & (\mathtt{ta}_u(\mathtt{ipurge}_{X \cup \{\mathtt{dom}(a)\}}(\alpha)), \mathtt{ta}_{\mathtt{dom}(a)}(\mathtt{ipurge}_{X \cup \{\mathtt{dom}(a)\}}(\alpha)), a) \quad \text{as required.} \\ & = & (\mathtt{ta}_u(\alpha), \mathtt{ta}_{\mathtt{dom}(a)}(\alpha), a) \text{ (by induction)} \\ & = & \mathtt{ta}_u(\alpha a), \end{array}$$

   A more intuitive, but less formal, argument is as follows: As above, it suffices to show that if $\mathtt{ipurge}_u(\alpha_1) = \mathtt{ipurge}_u(\alpha_2)$, then $\mathtt{ta}_u(\alpha_1) = \mathtt{ta}_u(\alpha_2)$. To see this, consider each action a appearing in the sequence α, i.e., let $\alpha = \beta a \gamma$ that is removed by $\mathtt{ipurge}_u$. This happens when there is no “downgrading chain” from $\mathtt{dom}(a)$ to u in the sequence $a\gamma$. In this case, the event a is also not “forwarded” to u in the application of the ta-function. Therefore, the event a is not relevant to the computation of $\mathtt{ta}_u(\alpha)$, and the value $\mathtt{ta}_u(\alpha)$ does not change when we remove a from the sequence, i.e., we have that $\mathtt{ta}_u(\alpha) = \mathtt{ta}_u(\beta\gamma)$. Inductively, this shows that $\mathtt{ta}_u(\alpha_1) = \mathtt{ta}_u(\alpha_2)$.

2. Assume that M is P-secure, and let α_1, α_2 be sequences with $\mathtt{ta}_u(\alpha_1) = \mathtt{ta}_u(\alpha_2)$. Clearly, $\mathtt{ta}_u(\alpha)$ contains at least as much information about α as $\mathtt{purge}_u(\alpha)$ does. In particular, $\mathtt{purge}_u(\alpha_1) = \mathtt{purge}_u(\alpha_2)$, and from P security it follows that $\mathtt{obs}_u(s \cdot \alpha_1) = \mathtt{obs}_u(s \cdot \alpha_2)$.
3. This proof was done in the lecture.

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 $\rightarrowtail$,

Solution We know that the implications P-security to TA-security, and TA-security to IP-security, always hold. It therefore remains to show that for a transitive policy, IP-security implies P-security. Hence assume that $\rightarrowtail$ is a transitive policy, and that M is IP-secure. To show that M is also P-secure, let s be a state, let u be an agent, and let α_1, α_2 be traces with $\mathtt{purge}_u(\alpha_1) = \mathtt{purge}_u(\alpha_2)$. Since M is IP-secure, it suffices to show that $\mathtt{ipurge}_u(\alpha_1) = \mathtt{ipurge}_u(\alpha_2)$. To show this, we first prove the following claim: If v is an agent such that an action a with $\mathtt{dom}(a) = v$ appears in α, then $v \in \mathtt{sources}(\alpha, u)$ if and only if $v \rightarrowtail u$. We show the left-to-right implication inductively over α:

- In the base case $\alpha = \epsilon$, there is no such v, and the claim holds.
- Assume the claim holds for α, and let a be an action. We consider two cases:
  1. Assume there is some $v \in \mathtt{sources}(\alpha, u)$ with $\mathtt{dom}(a) \rightarrowtail v$. In this case:
     - $\mathtt{sources}(a\alpha) = \mathtt{sources}(\alpha, u) \cup \{\mathtt{dom}(a)\}$,
     - by induction, we know that $v \rightarrowtail u$. Since $\rightarrowtail$ is transitive, it also follows that $\mathtt{dom}(a) \rightarrowtail u$.

     In both cases, the claim follows.
  2. If such a v does not exist, we have that $\mathtt{sources}(a\alpha, u) = \mathtt{sources}(\alpha, u)$, and the claim follows by induction.

The right-to-left implication is trivial, and holds for intransitive policies as well.

We now use this result to show that $\mathtt{ipurge}_u(\alpha_1) = \mathtt{ipurge}_u(\alpha_2)$. In fact we show that $\mathtt{ipurge}_u(\alpha) = \mathtt{purge}_u(\alpha)$ for all sequences α. This again easily follows by induction:

- If $\alpha = \epsilon$, the claim is trivial.
- Assume the claim holds for α, we consider the trace $a\alpha$. Again, there are two cases to consider:
  - If $\mathtt{dom}(a) \in \mathtt{sources}(a\alpha, u)$, then by the above we have that $\mathtt{dom}(a) \rightarrowtail u$. Therefore, $\mathtt{ipurge}_u(a\alpha) = a\mathtt{ipurge}_u(\alpha) = a\mathtt{purge}_u(\alpha) = \mathtt{purge}(a\alpha)$. (The equalities follow from the definition of ipurge, induction, and the definition of purge.)
  - If $\mathtt{dom}(a) \notin \mathtt{sources}(a\alpha, u)$, then by the above $\mathtt{dom}(a) \rightarrowtail u$. Therefore, analogously to the above, we have that $\mathtt{ipurge}_u(a\alpha) = \mathtt{ipurge}_u(\alpha) = \mathtt{purge}_u(\alpha) = \mathtt{purge}(a\alpha)$.

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

Prove or disprove the following: If $M = (S, s_0, A, \mathtt{step}, D, O, \mathtt{obs}, \mathtt{dom})$ 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 $\rightarrowtail$.

Solution The characterization is clearly not correct. Assume a policy $\rightarrowtail = A \to B \to C \to A$. Since the transitive closure of $\rightarrowtail$ is the complete relation on the agents $\{A, B, C\}$, any system is trivially P-Secure with respect to the transitive closure. We now show that there is a system which is not secure with respect to $\rightarrowtail$ itself. For this, let M be any system that is not secure with respect to the policy $H \not\rightarrowtail L$. We can easily translate this system by mapping H's actions and observations to A, and L's actions and observations to B, without adding any actions for B. Then trivially, the system is insecure with respect to $\rightarrowtail$.