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

Engineering Secure Software Systems Winter 2020/21 **Exercise Sheet 12**

issued: February 2, 2021 **due:** February 11, 2021

Exercise 12.1, uniqueness of unwindings (10 Points)

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 $\rightarrowtail$.

Solution

1. Simply choose any non-trivial P-secure system M with a correspondings policy $\rightarrowtail$, and a corresponding unwinding $(\sim)_{u\in D}$. Then modify the system M such that all observations are identical in all states. We immediately obtain two unwindings for the new system M' and $\rightarrowtail$:
   - the unwinding for M clearly still is an unwinding for M',
   - since in M', all agents have the same observations in all states, the universal relation $S\times S$ is trivially an unwinding.
2. We prove the following fact:

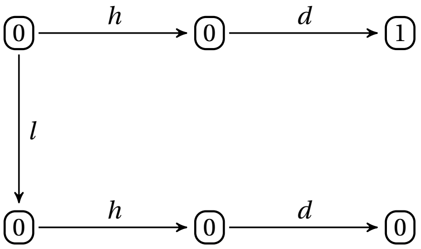
   > Let I be a non-empty set, and for each $i\in I$, let $\sim_i=(\sim_u^i)_{u\in D}$ be a P-unwinding for M and $\rightarrowtail$..
   > Then the family $(\sim_u)_{u\in D}$ defined as $\sim_u=\cap_{i\in I}\sim_u^i$ also is a P-unwinding for M and $\rightarrowtail$.

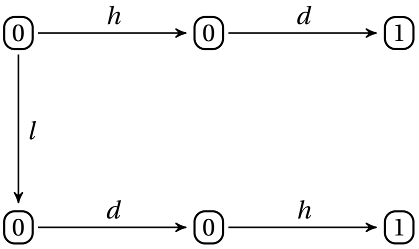
   This obviously completes the proof, since the minimal unwinding is then simply the intersection of all unwindings. Except for output consistence, the proof is an easy consequence of the fact that closure properties are invariant under intersection. Let $u\in D$, and let $\sim_u$ be defined as in the lemma. We prove that $\sim_u$ in fact satisfies all required properties: That $\sim_u$ is an equivalence relation (i.e., reflexive, symmetric, and transitive), and that $\sim_u$ satisfies output consistency, step consistency, and left respect (in their respective P-security versions).

   - *Reflexivity.* Since each $\sim_u^i$ is reflexive, we have that, for each $s\in S$, $(s,s)\in\sim_u^i$, hence $(s,s)\in\cap_{i\in I}\sim_u^i=\sim_u$.
   - *Symmetry.* Let $s\sim_u t$. By definition, then $(s,t)\in\cap_{i\in I}\sim_u^i$, i.e., $s\sim_u^i t$ for each $i\in I$. Since each $\sim_u^i$ is symmetric, it follows that $t\sim_u^i s$ for each $i\in I$, therefore, $(t,s)\in\cap_{i\in I}\sim_u^i=\sim_u$.
   - *Transitivity.* Let $s\sim_u t$ and $t\sim_u r$. As above, we then have $s\sim_u^i t$ and $t\sim_u^i r$ for each $i\in I$, the transitivity of each $\sim_u^i$ then implies that $s\sim_u^i r$ for each i, and thus $s\sim_u r$.
   - *Output Consistency.* Let $s\sim_u t$. Since $i\neq\emptyset$, there is some $i\in I$. By definition of $\sim_u$, it follows that $s\sim_u^i t$. Since $\sim_u^i$ satisfies output consistency, it follows that $\mathtt{obs}_u(s)=\mathtt{obs}_u(t)$ as required.
   - *Step Consistency.* Let $s\sim_u t$, and let $a\in A$. Since each $\sim_u^i$ satisfies step consistency, we have that $s\cdot a\sim_u^i t\cdot a$ for each $i\in I$, i.e., $(s\cdot a,t\cdot a)\in\cap_{i\in I}\sim_u^i$, therefore, $s\sim_u t$.
   - Left Respect. Let $\mathtt{dom}(a)\not\rightarrowtail u$, and let $s\in S$. Since each $\sim_u^i$ satisfies left respect, it follows that $s\sim_u^i s\cdot a$ for all $i\in I$, and hence again, $s\sim_u s\cdot a$.

Exercise 12.2, IP-Security examples (10 Points)

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.


0
h
0
d
1
l
0
h
0
d
0


0
h
0
d
1
l
0
d
0
h
1