Exercise Class February 11, 2021

Review Questions

When constructing an unwinding for P-security, we usually only give $\sim_L$, the equivalence relation for the Low agent. What about the others?

- (we always assume the $L \rightarrowtail H$ policy)
- H may learn everything anyway
- we usually do not even specify observations for H
- LR never gets applied, because $\texttt{dom}(a) \rightarrowtail H$
- (LR: if $\texttt{dom}(a) \not\rightarrowtail u$, then $s \sim_u s \cdot a$).
- so what is an equivalence relation for H?
- $\sim_H = \{(s,s) | s \in S\}$
- OC is clear, LR does not apply here (see above), SC: if we have $s \sim_H t$, then $s = t$. So, $s \cdot a = t \cdot a$, clearly equivalent.

For more general policies (but still P-security), for what agents does this apply?

Policy from RvdM example (motivation of TA-security):

- $H_1 \rightarrowtail D_1 \rightarrowtail L$
- $H_2 \rightarrowtail D_2 \rightarrowtail L$

Generally, the argument only applies to agents with “full information,” i.e., agents v for which $u \rightarrowtail v$ for all agents u.

Tasks

P-Security is equivalent to: $\texttt{obs}_u(s \cdot \alpha) = \texttt{obs}_u(s \cdot \texttt{purge}_u(\alpha))$

let M be P-secure, i.e., for all α_1, α_2 with $\texttt{purge}_u(\alpha_1) = \texttt{purge}_u(\alpha_2)$, we have $\texttt{obs}_u(s \cdot \alpha_1) = \texttt{obs}_u(s \cdot \alpha_2)$.

- always: $\texttt{purge}_u(\texttt{purge}_u(\alpha)) = \texttt{purge}_u(\alpha)$.
- so, use $\alpha_1 = \alpha$, $\alpha_2 = \texttt{purge}_u(\alpha)$.
- then: $\texttt{obs}_u(s \cdot \alpha_1) = \texttt{obs}_u(s \cdot \alpha_2)$, i.e., $\texttt{obs}_u(s \cdot \alpha) = \texttt{obs}_u(s \cdot \texttt{purge}_u(\alpha))$
- So, P-security implies the “alternative condition”.

Now, let M satisfy the “alternative definition,” i.e., $\texttt{obs}_u(s \cdot \alpha) = \texttt{obs}_u(s \cdot \texttt{purge}_u(\alpha))$ for all u, s, α.

- Need to show: **For any** α_1, α_2 with $\texttt{purge}_u(\alpha_1) = \texttt{purge}_u(\alpha_2)$, we have $\texttt{obs}_u(s \cdot \alpha_1) = \texttt{obs}_u(s \cdot \alpha_2)$.
- what we know (apply alternative definition for α_1 and α_2):
  - $\texttt{obs}_u(s \cdot \alpha_1) = \texttt{obs}_u(s \cdot \texttt{purge}_u(\alpha_1))$
  - $\texttt{obs}_u(s \cdot \alpha_2) = \texttt{obs}_u(s \cdot \texttt{purge}_u(\alpha_2))$
- need to show:
  - $\texttt{obs}_u(s \cdot \alpha_1) = \texttt{obs}_u(s \cdot \alpha_2)$
- we also know: $\texttt{purge}_u(\alpha_1) = \texttt{purge}_u(\alpha_2)$.

Unique (or not) unwindings

Construct system M with two different unwindings:

- M needs to be P-secure, with at least 2 states.
- Choose exactly two states, and policy $L \rightarrowtail H$.
- same observation in all states, no h-transitions.
- two equivalence relations: states are equivalent or not.
- full equivalence relation (all states are equivalent) is an unwinding always if agent has same observation in all states.

three states: all same observations:

- one initial, one final state, one unreachable state
- every transition reaches final state
- all observation 0, only one agent: L.
- equivalence relations: reflexive relation (equality relation), OR also make initial and unreachable state equivalent,