Lecture Session 12: Janury 26, 2021

Notation

macros for copy-and-paste:

- $\texttt{purge}_u(\alpha)$
- $\texttt{obs}_u(s)$
- $\texttt{step}(s, a)$

Review Questions

The definition of P-Security requires the condition to hold from every state in the system, not only for the initial state. Does requiring the condition to only hold from the initial state s_0 lead to a different notion of security? It makes a difference because some states may be not reachable from the initial state.

Which formal concept is indicated by the "circles" in the graphical representation of the system? L-unwindings.

The definition of unwindings requires an equivalence relation $\sim_u$ for every agent u in the system. However, in the examples covered in lecture and exercise class (with the usual H/L policy), we usually only present an unwinding $\sim_L$ for the "low" agent in the system. Why do we omit discussing an unwinding $\sim_H$ for the "high" agent?

Algorithm: Computing "easier" unwinding

If a system M is P-secure with respect to $\rightarrowtail$, then the algorithm constructs an unwinding.

Proof

- assume M is P-secure
- then there is an unwinding (for M and $\rightarrowtail$), call this $(\approx_u)_{u \in D}$
- let $(\sim_u)_{u \in D}$ be the result of the algorithm (left-hand side of the slide)
- then $(\sim_u)_{u \in D}$ is an unwinding, because:
  - must prove equivalence relation (done), LR (done), SC (done)
  - must actually only prove OC (output consistency).
- Let $s \sim_u t$, then $s \approx_u t$, because (see exercise task) every equivalence in $\sim_u$ is contained in every unwinding for u, in particular, in $\approx_u$.
- Since $\approx$ satisfies OC, we know that $\texttt{obs}_u(s) = \texttt{obs}_u(t)$.

$\square$