Exercise Class February 4, 2021

Information-Flow Examples

IP-Secrity Example III example is not P-Secure, with traces $\alpha_1 = ab$, $\alpha_2 = b$, state s initial state, then

- $\texttt{purge}_L(\alpha_1) = b, \texttt{purge}_L(\alpha_2) = b$
- $\texttt{obs}(s \cdot \alpha_1) = 1 \neq 0 = \texttt{obs}(s \cdot \alpha_2)$

Proving P-insecurity with unwindings:

- apply algorithm from the lecture. Algorithm constructs a (family of) equivalence relations that is an unwinding if and only if the system is secure.
- add reflexivity (each state is its own equivalence class)
- use LR property: left two states are equivalentg
- use SC property: right two states also are equivalent
- relationship does not satisfy OC.

is the example IP-secure?

- it is (no proof here, but idea is: B downgrades information about A action)

IP-Secrity Example IV not P-Secure, use same argument as above. IP-Security?

intuition: is there a situation where L has information he should not have?

- information in states with observation "1:"
- sequences $a_1 bl$ and $a_2 bl$: observation is "1" in both cases
- (if a state does not have an outgoing edge for an action, say b, then performing this action lets the system remain in that state).
- If L observes a "1", he knows that at least one action by A has been performed.
- If L observes a change from "0" to "1" as a result of his own action l, he knows that a_2 has been performed.
- If L observes a "1," and B has not done anything, then a_2 has been performed.

- are there sequences α_1, α_2 and a state s with
  - $\texttt{ipurge}_L(\alpha_1) = \texttt{ipurge}_L(\alpha_2)$, and
  - $\texttt{obs}_L(s \cdot \alpha_1) \neq \texttt{obs}_L(s \cdot \alpha_2)$?
- choose traces $\alpha_1 = l a_2$, $\alpha_2 = a_2 l$, s as initial state
  - $\texttt{obs}_L(s \cdot \alpha_1) = 0$
  - $\texttt{obs}_L(s \cdot \alpha_2) = 1$
- $\texttt{ipurge}_L(\alpha_2) = \texttt{ipurge}_L(a_2 l) = l$ (formally: use sources-definition, informally: L is only allowed to observe actions by A if B performes an action after A's action, this does not happen here.)
- $\texttt{ipurge}_L(\alpha_1) = \texttt{ipurge}_L(l a_2) = l$ (as above: a_2-action is removed)
- α_1 and α_2 are a counter-example for IP-Security.

Minimal Unwinding

A minimal unwinding is an unwinding $\sim_u$, such that for all unwindings $\approx_u$, we have that $s \sim_u t$ implies $s \approx_u t$.