ECS 235B Module 41
Restrictiveness

Feedback-Free Systems

- System has n distinct components
- Components c_i, c_j are *connected* if any output of c_i is input to c_j
- System is *feedback-free* if for all c_i connected to c_j, c_j not connected to any c_i
  - Intuition: once information flows from one component to another, no information flows back from the second to the first

Feedback-Free Security

- *Theorem*: A feedback-free system composed of noninterference-secure systems is itself noninterference-secure

Some Feedback

- *Lemma*: A noninterference-secure system can feed a HIGH output *o* to a HIGH input *i* if the arrival of *o* at the input of the next component is delayed until *after* the next LOW input or output
- *Theorem*: A system with feedback as described in the above lemma and composed of noninterference-secure systems is itself noninterference-secure

Why Didn't They Work?

- For compositions to work, machine must act same way regardless of what precedes LOW input (HIGH, LOW, nothing)
- *dog* does not meet this criterion
  - If first input is *stop_count*, *dog* emits 0
  - If high level input precedes *stop_count*, *dog* emits 0 or 1

State Machine Model: 2-Bit Machine

Levels *High*, *Low*, meet 4 properties:

1. For every input i_k, state σ_j, there is an element $c_m \in C^*$ such that $T^*(c_m, \sigma_j) = \sigma_n$, where $\sigma_n \neq \sigma_j$

T^* is total function, inputs and commands always move system to a different state

Property 2

2. There is an equivalence relation $\equiv$ such that:
   a. If system in state σ_i and HIGH sequence of inputs causes transition from σ_i to σ_j, then $\sigma_i \equiv \sigma_j$
      - 2 states equivalent if either reachable from the other state using only HIGH commands
   b. If $\sigma_i \equiv \sigma_j$ and LOW sequence of inputs $i_1, \ldots, i_n$ causes system in state σ_i to transition to σ_i', then there is a state σ_j' such that $\sigma_i' \equiv \sigma_j'$ and inputs $i_1, \ldots, i_n$ cause system in state σ_j to transition to σ_j'
      - States resulting from giving same LOW commands to the two equivalent original states have same LOW projection

$\equiv$ holds if LOW projections of both states are same

- If 2 states equivalent, HIGH commands do not affect LOW projections

Property 3

- Let $\sigma_i \equiv \sigma_j$. If sequence of HIGH outputs $o_1, \ldots, o_n$ indicate system in state σ_i transitioned to state σ_i', then for some state σ_j' with $\sigma_j' \equiv \sigma_i'$, sequence of HIGH outputs $o_1', \ldots, o_m'$ indicates system in σ_j transitioned to σ_j'
  - HIGH outputs do not indicate changes in LOW projection of states

Property 4

- Let $\sigma_i \equiv \sigma_j$, let *c*, *d* be HIGH output sequences, *e* a LOW output. If output sequence *ced* indicates system in state σ_i transitions to σ_i', then there are HIGH output sequences *c*' and *d*' and state σ_j' such that *c*′*ed*′ indicates system in state σ_j transitions to state σ_j'
  - Intermingled LOW, HIGH outputs cause changes in LOW state reflecting LOW outputs only

Restrictiveness

- System is *restrictive* if it meets the preceding 4 properties

Composition

- Intuition: by 3 and 4, HIGH output followed by LOW output has same effect as the LOW input, so composition of restrictive systems should be restrictive

Composite System

- System M_1's outputs are acceptable as M_2's inputs
- μ_{1i}, μ_{2i} states of M_1, M_2
- States of composite system pairs of M_1, M_2 states (μ_{1i}, μ_{2i})
- e event causing transition
- e causes transition from state (μ_{1a}, μ_{2a}) to state (μ_{1b}, μ_{2b}) if any of 3 conditions hold

Conditions

1. M_1 in state μ_{1a} and *e* occurs, M_1 transitions to μ_{1b}; *e* not an event for M_2; and $\mu_{2a} = \mu_{2b}$
2. M_2 in state μ_{2a} and *e* occurs, M_2 transitions to μ_{2b}; *e* not an event for M_1; and $\mu_{1a} = \mu_{1b}$
3. M_1 in state μ_{1a} and *e* occurs, M_1 transitions to μ_{1b}; M_2 in state μ_{2a} and *e* occurs, M_2 transitions to μ_{2b}; *e* is input to one machine, and output from other

Intuition

- Event causing transition in composite system causes transition in at least 1 of the components
- If transition occurs in exactly 1 component, event must not cause transition in other component when not connected to the composite system

Equivalence for Composite

- Equivalence relation for composite system

$$(\sigma_a, \sigma_b) \equiv_C (\sigma_c, \sigma_d) \text{ iff } \sigma_a \equiv \sigma_c \text{ and } \sigma_b \equiv \sigma_d$$

- Corresponds to equivalence relation in property 2 for component system

Theorem

The system resulting from the composition of two restrictive systems is itself restrictive