ECS 289M Lecture 5

April 10, 2006

Safety Analysis

- Goal: identify types of policies with tractable safety analyses
- Approach: derive a state in which additional entries, rights do not affect the analysis; then analyze this state
  - Called a *maximal state*

Definitions

- System begins at initial sate
- Authorized operation causes *legal transition*
- Sequence of legal transitions moves system into final state
  - This sequence is a *history*
  - Final state is *derivable* from history, initial state

More Definitions

- States represented by ^{h}
- Set of subjects SUB^h, entities ENT^h
- Link relation in context of state *h* is $link^h$
- Dom relation in context of state *h* is dom^h

$path^h$(**X**,**Y**)

- **X**, **Y** connected by one link or a sequence of links
- Formally, either of these hold:
  - for some i, $link_i^h(\mathbf{X}, \mathbf{Y})$; or
  - there is a sequence of subjects $\mathbf{X}_0, \ldots, \mathbf{X}_n$ such that $link_i^h(\mathbf{X}, \mathbf{X}_0)$, $link_i^h(\mathbf{X}_n, \mathbf{Y})$, and for $k = 1, \ldots, n$, $link_i^h(\mathbf{X}_{k-1}, \mathbf{X}_k)$
- If multiple such paths, refer to $path_j^h(\mathbf{X}, \mathbf{Y})$

Capacity $cap(path^h(\mathbf{X},\mathbf{Y}))$

- Set of tickets that can flow over $path^h(\mathbf{X},\mathbf{Y})$
  - If $link_i^h(\mathbf{X},\mathbf{Y})$: set of tickets that can be copied over the link (i.e., $f_i(\tau(\mathbf{X}), \tau(\mathbf{Y}))$)
  - Otherwise, set of tickets that can be copied over *all* links in the sequence of links making up the $path^h(\mathbf{X},\mathbf{Y})$
- Note: all tickets (except those for the final link) *must* be copyable

Flow Function

- Idea: capture flow of tickets around a given state of the system
- Let there be *m* $path^h$s between subjects **X** and **Y** in state *h*. Then *flow function*

$$flow^h: SUB^h \times SUB^h \rightarrow 2^{T \times R}$$

is:

$$flow^h(\mathbf{X},\mathbf{Y}) = \cup_{i=1,\dots,m} cap(path_i^h(\mathbf{X},\mathbf{Y}))$$

Properties of Maximal State

- Maximizes flow between all pairs of subjects
  - State is called *
  - Ticket in *flow**(**X**,**Y**) means there exists a sequence of operations that can copy the ticket from **X** to **Y**
- Questions
  - Is maximal state unique?
  - Does every system have one?

Formal Definition

- Definition: $g \leq_0 h$ holds iff for all **X**, **Y** $\in$ *SUB*^{0}, $flow^g(\mathbf{X},\mathbf{Y}) \subseteq flow^h(\mathbf{X},\mathbf{Y})$.
  – Note: if $g \leq_0 h$ and $h \leq_0 g$, then *g*, *h* equivalent
  – Defines set of equivalence classes on set of derivable states
- Definition: for a given system, state *m* is maximal iff $h \leq_0 m$ for every derivable state *h*
- Intuition: flow function contains all tickets that can be transferred from one subject to another
  – All maximal states in same equivalence class

Maximal States

- Lemma. Given arbitrary finite set of states *H*, there exists a derivable state *m* such that for all $h \in H$, $h \leq_0 m$
- Outline of proof: induction
  – Basis: $H = \varnothing$; trivially true
  – Step: $|H'| = n + 1$, where $H' = G \cup \{h\}$. By IH, there is a $g \in G$ such that $x \leq_0 g$ for all $x \in G$.

Outline of Proof

- M interleaving histories of *g*, *h* which:
  - Preserves relative order of transitions in *g*, *h*
  - Omits second create operation if duplicated
- *M* ends up at state *m*
- If $path^g(\mathbf{X},\mathbf{Y})$ for **X**, $\mathbf{Y} \in SUB^g$, $path^m(\mathbf{X},\mathbf{Y})$
  - So $g \le_0 m$
- If $path^h(\mathbf{X},\mathbf{Y})$ for **X**, $\mathbf{Y} \in SUB^h$, $path^m(\mathbf{X},\mathbf{Y})$
  - So $h \le_0 m$
- Hence *m* maximal state in *H*′

Answer to Second Question

- Theorem: every system has a maximal state *
- Outline of proof: *K* is set of derivable states containing exactly one state from each equivalence class of derivable states
  - Consider **X**, **Y** in SUB^0. Flow function's range is $2^{T \times R}$, so can take at most $2^{|T \times R|}$ values. As there are $|SUB^0|^2$ pairs of subjects in SUB^0, at most $2^{|T \times R|} |SUB^0|^2$ distinct equivalence classes; so *K* is finite
- Result follows from lemma

Safety Question

- In this model:

  Is it possible to have a derivable state with **X**/*r*:*c* in *dom*(**A**), or does there exist a subject **B** with ticket **X**/*rc* in the initial state or which can demand **X**/*rc* and τ(**X**)/*r*:*c* in *flow**(**B**,**A**)?
- To answer: construct maximal state and test
  - Consider acyclic attenuating schemes; how do we construct maximal state?

Intuition

- Consider state *h*.
- State *u* corresponds to *h* but with minimal number of new entities created such that maximal state *m* can be derived with no create operations
  - So if in history from *h* to *m*, subject **X** creates two entities of type *a*, in *u* only one would be created; surrogate for both
- *m* can be derived from *u* in polynomial time, so if *u* can be created by adding a finite number of subjects to *h*, safety question decidable.

Fully Unfolded State

- State *u* derived from state 0 as follows:
  - delete all loops in *cc*; new relation *cc*′
  - mark all subjects as folded
  - while any **X** ∈ SUB^0 is folded
    - mark it unfolded
    - if **X** can create entity **Y** of type *y*, it does so (call this the *y*-surrogate of **X**); if entity **Y** ∈ SUB^g, mark it folded
  - if any subject in state *h* can create an entity of its own type, do so
- Now in state *u*

Termination

- First loop terminates as SUB^0 finite
- Second loop terminates:
  - Each subject in SUB^0 can create at most | *TS* | children, and | *TS* | is finite
  - Each folded subject in | SUB^i | can create at most | *TS* | – *i* children
  - When *i* = | *TS* |, subject cannot create more children; thus, folded is finite
  - Each loop removes one element
- Third loop terminates as SUB^h is finite

Surrogate

- Intuition: surrogate collapses multiple subjects of same type into single subject that acts for all of them
- Definition: given initial state 0, for every derivable state *h* define *surrogate function* σ:$ENT^h \rightarrow ENT^h$ by:
  - if **X** in ENT^0, then σ(**X**) = **X**
  - if **Y** creates **X** and τ(**Y**) = τ(**X**), then σ(**X**) = σ(**Y**)
  - if **Y** creates **X** and τ(**Y**) $\neq$ τ(**X**), then σ(**X**) = τ(**Y**)-surrogate of σ(**Y**)

Implications

- τ(σ(**X**)) = τ(**X**)
- If τ(**X**) = τ(**Y**), then σ(**X**) = σ(**Y**)
- If τ(**X**) $\neq$ τ(**Y**), then
  - σ(**X**) creates σ(**Y**) in the construction of *u*
  - σ(**X**) creates entities **X**′ of type τ(**X**) = τ(σ(**X**))
- From these, for a system with an acyclic attenuating scheme, if **X** creates **Y**, then tickets that would be introduced by pretending that σ(**X**) creates σ(**Y**) are in dom^u(σ(**X**)) and dom^u(σ(**Y**))

Deriving Maximal State

- Idea
  - Reorder operations so that all creates come first and replace history with equivalent one using surrogates
  - Show maximal state of new history is also that of original history
  - Show maximal state can be derived from initial state

Reordering

- *H* legal history deriving state *h* from state 0
- Order operations: first create, then demand, then copy operations
- Build new history *G* from *H* as follows:
  - Delete all creates
  - "**X** demands **Y**/*r*:*c*" becomes "σ(**X**) demands σ(**Y**)/*r*:*c*"
  - "**Y** copies **X** /*r*:*c* from **Y**" becomes "σ(**Y**) copies σ(**X**)/*r*:*c* from σ(**Y**)"

Tickets in Parallel

- Theorem
  - All transitions in *G* legal; if **X**/*r*:*c* $\in$ *dom*^{h}(*Y*), then σ(**X**)/*r*:*c* $\in$ *dom*^{g}(σ(**Y**))
- Outline of proof: induct on number of copy operations in *H*

Basis

- *H* has create, demand only; so *G* has demand only. s preserves type, so by construction every demand operation in *G* legal.
- 3 ways for **X**/*r*:*c* to be in *dom*^{h}(**Y**):
  - **X**/*r*:*c* $\in$ *dom*^{0}(**Y**) means **X**, **Y** $\in$ *ENT*^{0}, so trivially σ(**X**)/*r*:*c* $\in$ *dom*^{g}(σ(**Y**)) holds
  - A create added **X**/*r*:*c* $\in$ *dom*^{h}(**Y**): previous lemma says σ(**X**)/*r*:*c* $\in$ *dom*^{g}(σ(**Y**)) holds
  - A demand added **X**/*r*:*c* $\in$ *dom*^{h}(**Y**): corresponding demand operation in *G* gives σ(**X**)/*r*:*c* $\in$ *dom*^{g}(σ(**Y**))

Hypothesis

- Claim holds for all histories with k copy operations
- History H has k+1 copy operations
  - H' initial sequence of H composed of k copy operations
  - h' state derived from H'

Step

- G' sequence of modified operations corresponding to H'; g' derived state
  - G' legal history by hypothesis
- Final operation is "Z copied X/r:c from Y"
  - So h, h' differ by at most $\mathbf{X}/r{:}c \in dom^h(\mathrm{Z})$
  - Construction of G means final operation is $\sigma(\mathbf{X})/r{:}c \in dom^g(\sigma(\mathbf{Y}))$
- Proves second part of claim

Step

- H' legal, so for H to be legal, we have:
  1. $\mathbf{X}/rc \in dom^{h'}(\mathbf{Y})$
  2. $link_i^{h'}(\mathbf{Y}, \mathbf{Z})$
  3. $\tau(\mathbf{X}/r{:}c) \in f_i(\tau(\mathbf{Y}), \tau(\mathbf{Z}))$
- By IH, 1, 2, as $\mathbf{X}$/r:c $\in dom^{h'}(\mathbf{Y})$,
  $\sigma(\mathbf{X})/r{:}c \in dom^{g'}(\sigma(\mathbf{Y}))$ and $link_i^{g'}(\sigma(\mathbf{Y}), \sigma(\mathbf{Z}))$
- As σ preserves type, IH and 3 imply
  $$\tau(\sigma(\mathbf{X})/r{:}c) \in f_i(\tau((\sigma(\mathbf{Y})), \tau(\sigma(\mathbf{Z})))$$
- IH says G' legal, so G is legal

Corollary

- If $link_i^h(\mathbf{X}, \mathbf{Y})$, then $link_i^g(\sigma(\mathbf{X}), \sigma(\mathbf{Y}))$

Main Theorem

- System has acyclic attenuating scheme
- For every history *H* deriving state *h* from initial state, there is a history *G* without create operations that derives *g* from the fully unfolded state *u* such that

$$(\forall \mathbf{X},\mathbf{Y} \in SUB^h)[flow^h(\mathbf{X}, \mathbf{Y}) \subseteq flow^g(\sigma(\mathbf{X}), \sigma(\mathbf{Y}))]$$

- Meaning: any history derived from an initial statecan be simulated by corresponding history applied to the fully unfolded state derived from the initial state

Proof

- Outline of proof: show that every $path^h(\mathbf{X},\mathbf{Y})$ has corresponding $path^g(\sigma(\mathbf{X}), \sigma(\mathbf{Y}))$ such that $cap(path^h(\mathbf{X},\mathbf{Y})) = cap(path^g(\sigma(\mathbf{X}), \sigma(\mathbf{Y})))$
  – Then corresponding sets of tickets flow through systems derived from *H* and *G*
  – As initial states correspond, so do those systems
- Proof by induction on number of links

Basis and Hypothesis

- Length of $path^h$(**X**, **Y**) = 1. By definition of $path^h$, $link_i^h$(**X**, **Y**), hence $link_i^g(\sigma($**X**$), \sigma($**Y**$))$. As σ preserves type, this means

$$cap(path^h(\mathbf{X}, \mathbf{Y})) = cap(path^g(\sigma(\mathbf{X}), \sigma(\mathbf{Y})))$$

- Now assume this is true when $path^h$(**X**, **Y**) has length k

Step

- Let $path^h$(**X**, **Y**) have length k+1. Then there is a **Z** such that $path^h$(**X**, **Z**) has length k and $link_j^h$(**Z**, **Y**).
- By IH, there is a $path^g(\sigma($**X**$), \sigma($**Z**$))$ with same capacity as $path^h$(**X**, **Z**)
- By corollary, $link_j^g(\sigma($**Z**$), \sigma($**Y**$))$
- As σ preserves type, there is $path^g(\sigma($**X**$), \sigma($**Y**$))$ with

$$cap(path^h(\mathbf{X}, \mathbf{Y})) = cap(path^g(\sigma(\mathbf{X}), \sigma(\mathbf{Y})))$$

Implication

- Let maximal state corresponding to *v* be #*u*
  - Deriving history has no creates
  - By theorem,

    $(\forall \mathbf{X},\mathbf{Y} \in SUB^h)[flow^h(\mathbf{X}, \mathbf{Y}) \subseteq flow^{\#u}(\sigma(\mathbf{X}), \sigma(\mathbf{Y}))]$
  - If $\mathbf{X} \in SUB^0$, $\sigma(\mathbf{X}) = \mathbf{X}$, so:

    $(\forall \mathbf{X},\mathbf{Y} \in SUB^0)[flow^h(\mathbf{X}, \mathbf{Y}) \subseteq flow^{\#u}(\mathbf{X}, \mathbf{Y})]$
- So #*u* is maximal state for system with acyclic attenuating scheme
  - #*u* derivable from *u* in time polynomial to $|SUB^u|$
  - Worst case computation for $flow^{\#u}$ is exponential in $|TS|$