

# January 16, 2014 Outline

**Reading:** *text*, §3.1–3.4

**Assignments due:** Homework #1, due January 23, 2014

1. What is the safety question?
  - a. An unauthorized state is one in which a generic right  $r$  could be leaked into an entry in the ACM that did not previously contain  $r$ . An initial state is safe for  $r$  if it cannot lead to a state in which  $r$  could be leaked.
  - b. Question: in a given arbitrary protection system, is safety decidable?
2. Mono-operational case: there is an algorithm that decides whether a given mono-operational system and initial state is safe for a given generic right.
3. General case: It is undecidable whether a given state of a given protection system is safe for a given generic right.
  - a. Approach: represent Turing machine tape as access control matrix, transitions as commands
  - b. Reduce halting problem to it
4. Related results
  - a. The set of unsafe systems is recursively enumerable
  - b. Monotonicity: no *delete* or *destroy* primitive operations
  - c. The safety question for biconditional monotonic protection systems is undecidable.
  - d. The safety question for monoconditional monotonic protection systems is decidable.
  - e. The safety question for monoconditional protection systems without the *destroy* primitive operation is decidable.
5. Take-Grant Protection Model
  - a. Counterpoint to HRU result
  - b. Symmetry of take and grant rights
  - c. Islands (maximal subject-only *tg*-connected subgraphs)
  - d. Bridges (as a combination of terminal and initial spans)
6. Sharing
  - a. Definition:  $\text{can}\bullet\text{share}(\alpha, \mathbf{x}, \mathbf{y}, G_0)$  true iff there exists a sequence of protection graphs  $G_0, \dots, G_n$  such that  $G_0 \vdash^* G_n$  using only take, grant, create, remove rules and in  $G_n$ , there is an edge from  $\mathbf{x}$  to  $\mathbf{y}$  labeled  $\alpha$
  - b. Theorem:  $\text{can}\bullet\text{share}(r, \mathbf{x}, \mathbf{y}, G_0)$  iff there is an edge from  $\mathbf{x}$  to  $\mathbf{y}$  labeled  $r$  in  $G_0$ , or all of the following hold:
    - i. there is a vertex  $\mathbf{y}'$  with an edge from  $\mathbf{y}'$  to  $\mathbf{y}$  labeled  $r$ ;
    - ii. there is a subject  $\mathbf{y}''$  which terminally spans to  $\mathbf{y}'$ , or  $\mathbf{y}'' = \mathbf{y}'$ ;
    - iii. there is a subject  $\mathbf{x}'$  which initially spans to  $\mathbf{x}$ , or  $\mathbf{x}' = \mathbf{x}$ ; and
    - iv. there is a sequence of islands  $I_1, \dots, I_n$  connected by bridges for which  $\mathbf{x}' \in I_1$  and  $\mathbf{y}' \in I_n$ .
7. Model Interpretation
  - a. ACM very general, broadly applicable; Take-Grant more specific, can model fewer situations
  - b. Example: shared buffer managed by trusted third party
8. Schematic Protection Model
  - a. Protection type, ticket, function, link predicate, filter function
  - b. Take-Grant as an instance of SPM
  - c. Create rules and attenuation
9. Safety analysis
  - a. Definitions
  - b.  $\text{path}^h$  predicate
  - c. Capacity flow function
  - d. Maximal state: definition, existence, derivability
10. Acyclic attenuating schemes and decidability