Outline for April 5, 2013

Reading: §3.1–3.2   **Assignments due:** Homework #1, due April 12, 2013

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 (exercise)
   b. For protection systems without the *create* primitives, the question of safety is complete in **_P-SPACE_**.
   c. Monotonicity: no *delete* or *destroy* primitive operations
   d. The safety question for biconditional monotonic protection systems is undecidable.
   e. The safety question for monoconditional monotonic protection systems is decidable.
   f. The safety question for monoconditional protection systems without the *destroy* primitive operatin 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: $can \bullet share(\alpha, \mathbf{x}, \mathbf{y}, G_0)$ true iff there exists a sequence of protection graphs $G_0, ..., G_n$ 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 α