Outline for April 5, 2006

Reading: text, §3.1—3.3.2

1. Greetings and felicitations!
2. 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?
   c. Theorem: 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. Represent TM as ACM
   b. Reduce halting problem to it
4. Take-Grant
   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)
5. Sharing
   a. Definition: \( \text{can\textasciitilde}share(r, x, y, G_0) \) 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 \( x \) to \( y \) labeled \( r \)
   b. Theorem: \( \text{can\textasciitilde}share(r, x, y, G_0) \) iff there is an edge from \( x \) to \( y \) labelled \( r \) in \( G_0 \), or all of the following hold:
      i. there is a vertex \( y' \) with an edge from \( y' \) to \( y \) labeled \( r \);
      ii. there is a subject \( y'' \) which terminally spans to \( y' \), or \( y'' = y' \);
      iii. there is a subject \( x' \) which initially spans to \( x \), or \( x' = x \); and
      iv. there is a sequence of islands \( I_1, ..., I_n \) connected by bridges for which \( x' \) is in \( I_1 \) and \( y' \) is in \( I_n \).
6. Model Interpretation
   a. ACM very general, broadly applicable; Take-Grant more specific, can model fewer situations
   b. Theorem: \( G_0 \) protection graph with exactly one subject, no edges; \( R \) set of rights. Then \( G_0 \vdash^* G \) iff \( G \) is a finite directed graph containing subjects and objects only, with edges labeled from nonempty subsets of \( R \), and with at least one subject with no incoming edges
   c. Example: shared buffer managed by trusted third party