Lecture 3 Outline

Reading: text, §3.2

1. 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.

2. 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)

3. Sharing
   a. Definition: $can\cdot share(r, x, y, G_0)$ true iff there exists a sequence of protection graphs $G_0, \ldots, G_n$ 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: $can\cdot share(r, x, y, G_0)$ iff there is an edge from $x$ to $y$ labeled $r$ 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 $I_1, \ldots, I_n$ connected by bridges for which $x' \in I_1$ and $y' \in I_n$.

4. 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 $G_0 \vdash^* G_n$ iff $G_0$ 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 part

5. Stealing
   a. Definition: $can\cdot steal(r, x, y, G_0)$ true iff there is no edge from $x$ to $y$ labeled $r$ in $G_0$, and there exists a sequence of protection graphs $G_0, \ldots, G_n$ such that $G_0 \vdash^* G_n$ in which:
   b. $G_n$ has an edge from $x$ to $y$ labeled $r$
   c. There is a sequence of rule applications $\rho_1, \ldots, \rho_n$ such that $G_i \vdash G_{i-1}$; and
   d. For all vertices $v, w \in G_i$, if there is an edge from $v$ to $y$ in $G_0$ labeled $r$, then $\rho_i$ is not of the form “$v$ grants ($r$ to $y$) to $w$”
   e. Example