Outline for April 8, 2013

Reading: §3.3 **Assignments due:** Homework #1, due April 12, 2013

1. Take-Grant Protection Model
   a. Islands (maximal subject-only *tg*-connected subgraphs)
   b. Terminal and initial spans
   c. Bridges (as a combination of terminal and initial spans)
2. Sharing
   a. Definition: *can•share*(α, $\mathbf{x}$, $\mathbf{y}$, 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
   b. Theorem: *can•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 $I_1, ..., I_n$ connected by bridges for which $\mathbf{x}' \in I_1$ and $\mathbf{y}' \in I_n$.
3. 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 party
4. Stealing
   a. Definition: *can•steal*(r, $\mathbf{x}$, $\mathbf{y}$, G_0) true iff there is no edge from $\mathbf{x}$ to $\mathbf{y}$ labeled r in G_0, and there exists a sequence of protection graphs $G_0, ..., G_n$ such that $G_0 \vdash^* G_n$ in which:
      i. G_n has an edge from $\mathbf{x}$ to $\mathbf{y}$ labeled r;
      ii. There is a sequence of rule applications $\rho_1, ..., \rho_n$ such that $G_{i-1} \vdash G_i$; and
      iii. For all vertices $\mathbf{v}, \mathbf{w} \in G_{i-1}$, if there is an edge from $\mathbf{v}$ to $\mathbf{y}$ in G_0 labeled r, then ρ_i is not of the form "$\mathbf{v}$ grants (r to $\mathbf{y}$) to $\mathbf{w}$"
   b. Example
   c. Theorem: *can•steal*(r, $\mathbf{x}$, $\mathbf{y}$, G_0) iff the following hold simultaneously:
      i. there is no edge from $\mathbf{x}$ to $\mathbf{y}$ labeled α in G_0;
      ii. there is a subject $\mathbf{x}'$ such that $\mathbf{x}' = \mathbf{x}$ or $\mathbf{x}'$ initially spans to $\mathbf{x}$; and
      iii. there is a vertex $\mathbf{s}$ with an edge labeled α to $\mathbf{y}$ in G_0 and for which *can•share*(t, $\mathbf{x}$, $\mathbf{s}$, G_0) holds.
5. Conspiracy
   a. Access set
   b. Deletion set
   c. Conspiracy graph
   d. I, T sets
   e. Theorem: *can·share*(α, $\mathbf{x}$, $\mathbf{y}$, G_0) iff there is a path from some $h(\mathbf{p}) \in I(\mathbf{x})$ to some $h(\mathbf{q}) \in T(\mathbf{y})$