Outline for April 10, 2013

Reading: [Bis96][1] **Assignments due:** Homework #1, due April 12, 2013

1. 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 $h(\mathbf{q}) \in T(\mathbf{y})$
2. *de facto* rules
   a. Explicit edges
   b. Implicit edges

   a. Pass
   b. Post
   c. Spy
   d. Find
3. Paths and spans
   a. rw-path, $rwtg$-path
   b. rw-initial span
   c. rw-terminal span
   d. Connection
4. Information flow from $\mathbf{x}$ to $\mathbf{y}$
   a. Definition: *can•know*($\mathbf{x}$, $\mathbf{y}$, G_0) true iff there exists a sequence of protection graphs $G_0, ..., G_n$ such that $G_0 \vdash^* G_n$ using the *de jure* and *de facto* rules and in G_n, there is an edge from $\mathbf{x}$ to $\mathbf{y}$ labeled r or an edge from $\mathbf{y}$ to $\mathbf{x}$ labeled w, and if the edge is explicit, its source is a subject
   b. Theorem: *can•know*(r, $\mathbf{x}$, $\mathbf{y}$, G_0) iff there is a sequence of subjects $\mathbf{u}_1, \ldots, \mathbf{u}_n$, $n \geq 1$, in G_0, such that the following hold:
      i. $\mathbf{u}_1 = \mathbf{x}$ or $\mathbf{u}_1$ rw-terminally spans to $\mathbf{x}$;
      ii. $\mathbf{u}_n = \mathbf{y}$ or $\mathbf{u}_n$ rw-terminally spans to $\mathbf{y}$; and
      iii. for all i such that $1 \leq i < n$, there is an rwtg-path between $\mathbf{u}_i$ and $\mathbf{u}_{i+1}$ with associated word in $B \cup C$.
5. Snooping
   a. Definition: *can•snoop*(r, $\mathbf{x}$, $\mathbf{y}$, G_0) true iff *can•steal*(r, $\mathbf{x}$, $\mathbf{y}$, G_0) or there exists a sequence of graphs and rule applications $G_0 \vdash_{\rho_1} \ldots \vdash_{\rho_n} G_n$ for which all the following conditions hold:
      i. there is no explicit edge from $\mathbf{x}$ to $\mathbf{y}$ labeled r in G_0;
      ii. there is an implicit edge from $\mathbf{x}$ to $\mathbf{y}$ labeled r in G_n; and
      iii. neither $\mathbf{y}$ nor any vertex directly connected to $\mathbf{y}$ in G_0 is an actor in a grant rule or a *de facto* rule resulting in an (explicit or implicit) read edge with $\mathbf{y}$ as its target
   b. Example
   c. Theorem: For distinct vertices $\mathbf{x}$ and $\mathbf{y}$ in a protection graph G_0 with explicit edges only, *can•snoop*($\mathbf{x}$, $\mathbf{y}$, G_0) iff *can•steal*(r, $\mathbf{x}$, $\mathbf{y}$, G_0) or the following hold simultaneously:
      i. there is no edge from $\mathbf{x}$ to $\mathbf{y}$ labeled r in G_0.
      ii. there is a subject $\mathbf{x}'$ such that $\mathbf{x}' = \mathbf{x}$ or $\mathbf{x}'$ rw-initially spans to $\mathbf{x}$ i G_0;
      iii. there is a subject vertex $\mathbf{y}'$ such that $\mathbf{y}' \neq \mathbf{y}$, there is no edge labeled r from $\mathbf{y}'$ to $\mathbf{y}$ in G_0, and $\mathbf{y}'$ rw-terminally spans to $\mathbf{y}$ in G_0; and
      iv. *can•know*($\mathbf{x}'$, $\mathbf{y}'$, G_0) holds.

[1] This is available in the Resources area of SmartSite; look in the folder "Handouts"