Outline for April 7, 2006

Reading: *text*, §3.3.3—3.4

1. Greetings and felicitations!
2. Stealing
   a. Definition: *can•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, ..., G_n such that $G_0 \vdash^* G_n$:
      i. G_n has an edge from **x** to **y** labeled r
      ii. There is a sequence of rule applications ρ_1, ..., ρ_n such that $G_{n-1} \vdash G_i$; and
      iii. For all vertices **v**, **w** in G_{n-1}, if there is an edge from **v** to **y** in G_0 labeled r, then ρ_i is not of the form "**v** grants (r to **y**) to **w**"
   b. Example
   c. Theorem: *can•steal*(r, **x**, **y**, G_0) iff all of the following hold:
      i. there is no edge from **x** to **y** labeled r in G_0;
      ii. there is a subject **x′** which initially spans to **x**, or **x′** = **x**; and
      iii. there is a vertex **s** with an edge labeled r to **y** in G_0 and for which *can•share*(r, **x**, **y**, G_0) holds
3. Conspiracy
   a. Access set
   b. Deletion set
   c. Conspiracy graph
   d. I, T sets
   e. Theorem: *can•share*(r, **x**, **y**, G_0) iff there is a path from some $h(\mathbf{p}) \in I(\mathbf{x})$ to some $h(\mathbf{q}) \in T(\mathbf{Y})$
4. Schematic Protection Model
   a. Model components
   b. Link function
   c. Filter function
   d. Example: Take-Grant as an instance of SPM
   e. Create operations and attenuation