Outline for January 18, 2012

Reading: §3.3

1. Sharing
   a. Definition: \( \text{can}_\bullet \text{share}(r, x, y, G_0) \) 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: \( \text{can}_\bullet \text{share}(r, x, y, G_0) \) 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 \( I_1, ..., I_n \) connected by bridges for which \( x' \in I_1 \) and \( y' \in I_n \).

2. 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

3. Stealing
   a. Definition: \( \text{can}_\bullet \text{steal}(r, x, y, G_0) \) 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 \( G_0 \vdash^* G_n \) in which:
      i. \( G_n \) has an edge from \( x \) to \( y \) 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 \( v, w \in G_{i-1} \), if there is an edge from \( v \) to \( y \) in \( G_0 \) labeled \( r \), then \( \rho_i \) is not of the form \( \text{"v grants (r to y) to w"} \).
   b. Example

4. Conspiracy
   a. Access set
   b. Deletion set
   c. Conspiracy graph
   d. \( I, T \) sets
   e. Theorem: \( \text{can}_\bullet \text{share}(\alpha, x, y, G_0) \) iff there is a path from some \( h(p) \in I(x) \) to some \( h(q) \in T(y) \)