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, x, y, G₀) iff there is a path from some h(p) ∈ I(x) to some h(q) ∈ T(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 x to y
   a. Definition: can-know(x, y, G₀) true iff there exists a sequence of protection graphs G₀,...,Gₙ such that G₀ ⊢* Gₙ using the de jure and de facto rules and in Gₙ, there is an edge from x to y labeled r or an edge from y to x labeled w, and if the edge is explicit, its source is a subject
   b. Theorem: can-know(r, x, y, G₀) iff there is a sequence of subjects u₁,...,uₙ, n ≥ 1, in G₀, such that the following hold:
      i. u₁ = x or u₁ rw-terminally spans to x;
      ii. uₙ = y or uₙ rw-terminally spans to y; and
      iii. for all i such that 1 ≤ i < n, there is an rwtg-path between uᵢ and uᵢ₊₁ with associated word in B ∪ C.

5. Snooping
   a. Definition: can-snoop(r, x, y, G₀) true iff can-steal(r, x, y, G₀) or there exists a sequence of graphs and rule applications G₀ ⊢₁...⊢ₙ Gₙ for which all the following conditions hold:
      i. there is no explicit edge from x to y labeled r in G₀;
      ii. there is an implicit edge from x to y labeled r in Gₙ; and
      iii. neither y nor any vertex directly connected to y in G₀ is an actor in a grant rule or a de facto rule resulting in an (explicit or implicit) read edge with y as its target
   b. Example
   c. Theorem: For distinct vertices x and y in a protection graph G₀ with explicit edges only, can-snoop(x, y, G₀) iff can-steal(r, x, y, G₀) or the following hold simultaneously:
      i. there is no edge from x to y labeled r in G₀.
      ii. there is a subject x' such that x' = x or x' rw-initially spans to x in G₀;
      iii. there is a subject vertex y' such that y' ≠ y, there is no edge labeled r from y' to y in G₀, and
      iv. can-know(x', y', G₀) holds.

¹This is available in the Resources area of SmartSite; look in the folder “Handouts”