January 12, 2024 Outline

**Reading:** *text*, §3.3–3.4

**Assignments:** Homework #1, due January 19; Project selection, due January 26

---

**Module 7 (Reading: text, §3.3)**

1. Take-Grant Protection Model
   (a) Counterpoint to HRU result
   (b) Symmetry of take and grant rights
   (c) Islands (maximal subject-only $tg$-connected subgraphs)
   (d) Bridges (as a combination of terminal and initial spans)

**Module 8 (Reading: text, §3.3.2–3.3.2)**

2. Sharing
   (a) Definition: $can \cdot share(\alpha, x, y, G_0)$ true iff there exists a sequence of protection graphs $G_0, \ldots, G_n$ 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 $\alpha$
   (b) Theorem: $can \cdot share(\alpha, x, y, G_0)$ iff there is an edge from $x$ to $y$ labeled $\alpha$ in $G_0$, or all of the following hold:
      i. there is a vertex $y'$ with an edge from $y'$ to $y$ labeled $\alpha$;
      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 $I_1, \ldots, I_n$ connected by bridges for which $x' \in I_1$ and $y' \in I_n$.

3. Model Interpretation
   (a) ACM very general, broadly applicable; Take-Grant more specific, can model fewer situations
   (b) Example: shared buffer managed by trusted third party

**Module 9 (Reading: text, §3.3.3–3.3.4)**

4. $can \cdot steal(\alpha, x, y, G_0)$ definition and theorem
   (a) Definition: $can \cdot steal(\alpha, x, y, G_0)$ true iff there is no edge labeled $\alpha$ from $x$ to $y$ in $G_0$ and there exists a sequence of protection graphs $G_0, \ldots, G_n$ such that the following hold simultaneously:
      i. there is an edge from $x$ to $y$ labeled $r$ in $G_n$;
      ii. there is a sequence of rule applications $\rho_1, \ldots, \rho_n$ such that $G_{i-1} \vdash^* G_n$ using $\rho_i$; and
      iii. for all vertices $v$ and $w$ in $G_{i-1}$, $1 \leq i < n$, if there is an edge from $v$ to $y$ in $G_0$ labeled $\alpha$, then $\rho_i$ is not of the form "$v$ grants ($\alpha$ to $y$) to $w$".
   (b) Theorem: $can \cdot steal(\alpha, x, y, G_0)$ iff all of the following hold:
      i. there is an edge from $x$ to $y$ labeled $r$ in $G_n$;
      ii. there is a subject vertex $x'$ such that $x' = x$ or $x'$ initially spans to $x$; and
      iii. there is a vertex $s$ with an edge labeled $\alpha$ to $y$ in $G_0$ and for which $can \cdot share(t, x, s, G_0)$ holds.

5. Conspiracy
   (a) What is of interest?
   (b) Access, deletion sets
   (c) Conspiracy graph
   (d) Number of conspirators

**Module 10 (Reading: text, §3.4)**

6. Schematic Protection Model
(a) Protection type, ticket, function, link predicate, filter function
(b) Take-Grant as an instance of SPM