ECS 235B Module 9
Stealing in the Take-Grant Model
can\textbullet steal Predicate

Definition:

\item \textit{can\textbullet steal}(r, x, y, G_0) if, and only if, there is no edge from x to y labeled r in G_0, and there exists a sequence of protection graphs G_0, G_1, ..., G_n for which the following hold simultaneously:
\begin{enumerate}
\item There is an edge from x to y labeled r in G_n
\item There is a sequence of rule applications \( \rho_1, \ldots, \rho_n \) such that \( G_{i-1} \vdash G_i \) using \( \rho_i \)
\item For all vertices v and w in \( G_{i-1} \), \( 1 \leq i < n \), if there is an edge from v to y labeled r, then \( \rho_i \) is \textit{not} of the form “v grants (r to y) to w”
\end{enumerate}
**can•steal** Theorem

- **can•steal**($\alpha, \mathbf{x}, \mathbf{y}, G_0$) if, and only if, the following hold simultaneously:
  
  a) There is no edge from $\mathbf{x}$ to $\mathbf{y}$ labeled $\alpha$ in $G_0$
  b) There exists a subject $\mathbf{x}'$ such that $\mathbf{x}' = \mathbf{x}$ or $\mathbf{x}'$ initially spans to $\mathbf{x}$
  c) There exists a vertex $s$ with an edge labeled $\alpha$ to $\mathbf{y}$ in $G_0$
  d) **can•share**($t, \mathbf{x}', s, G_0$) holds
Outline of Proof

⇒: Assume conditions hold

• **x** subject
  • **x** gets \( t \) rights to **s**, then takes \( \alpha \) to **y** from **s**

• **x** object
  • \( can\cdot share(t, x', s, G_0) \) holds
  • If \( x' \) has no \( \alpha \) edge to \( y \) in \( G_0 \), \( x' \) takes \((\alpha \text{ to } y)\) from \( s \) and grants it to \( x \)
  • If \( x' \) has \( \alpha \) edge to \( y \) in \( G_0 \), \( x' \) creates surrogate \( x'' \), gives it \((t \text{ to } s)\) and \((g \text{ to } x'')\); then \( x'' \) takes \((\alpha \text{ to } y)\) and grants it to \( x \)
Outline of Proof

⇐: Assume $can\cdot steal(\alpha, x, y, G_0)$ holds

• First two conditions immediate from definition of $can\cdot steal$, $can\cdot share$

• Third condition immediate from theorem of conditions for $can\cdot share$

• Fourth condition: $\rho$ minimal length sequence of rule applications deriving $G_n$ from $G_0$; $i$ smallest index such that $G_{i-1} \vdash G_i$ by rule $\rho_i$ and adding $\alpha$ from some $p$ to $y$ in $G_i$
  • What is $\rho_i$?
Outline of Proof

• Not remove or create rule
  • y exists already

• Not grant rule
  • $G_i$ first graph in which edge labeled $\alpha$ to y is added, so by definition of $\text{can} \cdot \text{share}$, cannot be grant

• take rule: so $\text{can} \cdot \text{share}(t, p, s, G_0)$ holds
  • So is subject $s'$ such that $s' = s$ or terminally spans to $s$
  • Sequence of islands with $x' \in I_1$ and $s' \in I_n$

• Derive witness to $\text{can} \cdot \text{share}(t, x', s, G_0)$ that does not use “s grants ($\alpha$ to y) to” anyone
Conspiracy

- Minimum number of actors to generate a witness for $can\cdot share(\alpha, x, y, G_0)$
- Access set describes the “reach” of a subject
- Deletion set is set of vertices that cannot be involved in a transfer of rights
- Build \textit{conspiracy graph} to capture how rights flow, and derive actors from it
Example
Access Set

• *Access set* $A(\mathbf{y})$ *with focus* $\mathbf{y}$: set of vertices:
  • $\{ \mathbf{y} \}$
  • $\{ x \mid \mathbf{y} \text{ initially spans to } x \}$
  • $\{ x' \mid \mathbf{y} \text{ terminally spans to } x' \}$

• Idea is that focus can give rights to, or acquire rights from, a vertex in this set
Example

- $A(x) = \{ \text{x}, \text{a} \}$
- $A(b) = \{ \text{b}, \text{a} \}$
- $A(c) = \{ \text{c}, \text{b}, \text{d} \}$
- $A(d) = \{ \text{d} \}$
- $A(e) = \{ \text{e}, \text{d}, \text{i}, \text{j} \}$
- $A(y) = \{ \text{y} \}$
- $A(f) = \{ \text{f}, \text{y} \}$
- $A(h) = \{ \text{h}, \text{f}, \text{i} \}$
Deletion Set

• Deletion set $\delta(\mathbf{y}, \mathbf{y}')$: contains those vertices $\mathbf{z}$ in $A(\mathbf{y}) \cap A(\mathbf{y}')$ such that:
  • $\mathbf{y}$ initially spans to $\mathbf{z}$ and $\mathbf{y}'$ terminally spans to $\mathbf{z}$; or
  • $\mathbf{y}$ terminally spans to $\mathbf{z}$ and $\mathbf{y}'$ initially spans to $\mathbf{z}$; or
  • $\mathbf{z} = \mathbf{y}$; or
  • $\mathbf{z} = \mathbf{y}'$

• Idea is that rights can be transferred between $\mathbf{y}$ and $\mathbf{y}'$ if this set non-empty.
Example

- \( \delta(x, b) = \{ a \} \)
- \( \delta(b, c) = \{ b \} \)
- \( \delta(c, d) = \{ d \} \)
- \( \delta(c, e) = \{ d \} \)
- \( \delta(d, e) = \{ d \} \)
- \( \delta(y, f) = \{ y \} \)
- \( \delta(h, f) = \{ f \} \)
Conspiracy Graph

• Abstracted graph $H$ from $G_0$:
  • Each subject $x \in G_0$ corresponds to a vertex $h(x) \in H$
  • If $\delta(x, y) \neq \emptyset$, there is an edge between $h(x)$ and $h(y)$ in $H$

• Idea is that if $h(x)$, $h(y)$ are connected in $H$, then rights can be transferred between $x$ and $y$ in $G_0$
Example

\[\begin{align*}
&\text{h(x)} & \quad & \text{h(b)} & \quad & \text{h(c)} & \quad & \text{h(d)} & \quad & \text{h(e)} \\
&\text{h(y)} & \quad & \text{h(f)} & \quad & \text{h(h)} & \quad & \text{h(e)}
\end{align*}\]
Results

• $I(x)$: $h(x)$, all vertices $h(y)$ such that $y$ initially spans to $x$
• $T(x)$: $h(x)$, all vertices $h(y)$ such that $y$ terminally spans to $x$
• Theorem: $can\cdot share(\alpha, x, y, G_0)$ iff there exists a path from some $h(p)$ in $I(x)$ to some $h(q)$ in $T(y)$
• Theorem: $l$ vertices on shortest path between $h(p), h(q)$ in above theorem; $l$ conspirators necessary and sufficient to witness
Example: Conspirators

- $I(x) = \{ h(x) \}$, $T(z) = \{ h(e) \}$
- Path between $h(x)$, $h(e)$ so can share $(r, x, z, G_0)$
- Shortest path between $h(x)$, $h(e)$ has 4 vertices
  \[ \Rightarrow \] Conspirators are $e, c, b, x$
Example: Witness

1. e grants (r to z) to d
2. c takes (r to z) from d
3. c grants (r to z) to b
4. b grants (r to z) to a
5. x takes (r to z) from a
Quiz

In either 1 or 2 or both, can $y$ steal $\alpha$ rights over $x$?

1. $y \xrightarrow{t} v \xrightarrow{g} w \xrightarrow{\alpha} x$

2. $y \xrightarrow{t} v \xrightarrow{g} w \xrightarrow{\alpha} x$