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

Definition:

\begin{itemize}
\item 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 not of the form “v grants (r to y) to w”
\end{enumerate}
\end{itemize}
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 \mathbf{s} with an edge labeled \alpha to \mathbf{y} in G_0
d) can•share(t, \mathbf{x}', \mathbf{s}, G_0) holds
Outline of Proof

\[\Rightarrow\text{: Assume conditions hold}\]

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

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

\[ \text{ Assume } can\cdot\text{steal}(\alpha, x, y, G_0) \text{ holds} \]

• First two conditions immediate from definition of \( can\cdot\text{steal}, \ can\cdot\text{share} \)

• Third condition immediate from theorem of conditions for \( can\cdot\text{share} \)

• 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 $can\cdot share$, cannot be grant

• take rule: so $can\cdot share(t, p, s, G_0)$ 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 $can\cdot share(t, x', s, G_0)$ that does not use “$s$ grants ($\alpha$ to y) to” anyone
Conspiracy

• Minimum number of actors to generate a witness for
  \( can \cdot share(\alpha, \mathbf{x}, \mathbf{y}, G_0) \)

• Access set describes the “reach” of a subject

• Deletion set is set of vertices that cannot be involved in a transfer of rights

• Build *conspiracy graph* to capture how rights flow, and derive actors from it
Example

Module 9

ECS 235B, Foundations of Computer and Information Security
Access Set

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

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

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

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

• Idea is that rights can be transferred between $y$ and $y'$ 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
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: $\text{can} \cdot \text{share}(\alpha, x, y, G_0)$ 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

\[ I(x) = \{ h(x) \}, \quad T(z) = \{ h(e) \} \]

- Path between \( h(x) \), \( h(e) \) so \( \text{can}\cdot\text{share}(r, x, z, G_0) \)
- Shortest path between \( h(x) \), \( h(e) \) has 4 vertices

\( \Rightarrow \) Conspirators are \( e, c, b, x \)
Example: Witness

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