ECS 235B Module 11
Sharing in the Take-Grant Model
can•share Predicate

Definition:

- $\text{can•share}(r, x, y, G_0)$ if, and only if, there is a sequence of protection graphs $G_0, \ldots, G_n$ such that $G_0 \vdash^* G_n$ using only de jure rules and in $G_n$ there is an edge from $x$ to $y$ labeled $r$. 
can\(\cdot\)share Theorem

- \(can\cdot share(r, x, y, G_0)\) if, and only if, there is an edge from \(x\) to \(y\) labeled \(r\) in \(G_0\), or the following hold simultaneously:
  - There is an \(s\) in \(G_0\) with an \(s\)-to-\(y\) edge labeled \(r\)
  - There is a subject \(x' = x\) or initially spans to \(x\)
  - There is a subject \(s' = s\) or terminally spans to \(s\)
  - There are islands \(I_1, \ldots, I_k\) connected by bridges, and \(x'\) in \(I_1\) and \(s'\) in \(I_k\)
Outline of Proof

• \( s \) has \( r \) rights over \( y \)
• \( s' \) acquires \( r \) rights over \( y \) from \( s \)
  • Definition of terminal span
• \( x' \) acquires \( r \) rights over \( y \) from \( s' \)
  • Repeated application of sharing among vertices in islands, passing rights along bridges
• \( x' \) gives \( r \) rights over \( y \) to \( x \)
  • Definition of initial span
Example Interpretation

• ACM is generic
  • Can be applied in any situation

• Take-Grant has specific rules, rights
  • Can be applied in situations matching rules, rights

• Question: what states can evolve from a system that is modeled using the Take-Grant Model?
Take-Grant Generated Systems

- Theorem: $G_0$ protection graph with 1 vertex, no edges; $R$ set of rights. Then $G_0 \vdash^* G$ iff:
  - $G$ finite directed graph consisting of subjects, objects, edges
  - Edges labeled from nonempty subsets of $R$
  - At least one vertex in $G$ has no incoming edges
Outline of Proof

$$\Rightarrow$$: By construction; $G$ final graph in theorem
- Let $x_1, \ldots, x_n$ be subjects in $G$
- Let $x_1$ have no incoming edges

- Now construct $G'$ as follows:
  1. Do "$x_1$ creates ($\alpha \cup \{ g \}$ to) new subject $x_i$"
  2. For all $(x_i, x_j)$ where $x_i$ has a rights over $x_j$, do
     "$x_1$ grants ($\alpha$ to $x_j$) to $x_i$"
  3. Let $\beta$ be rights $x_i$ has over $x_j$ in $G$. Do
     "$x_1$ removes (($\alpha \cup \{ g \} - \beta$) to) $x_j$"

- Now $G'$ is desired $G$
Outline of Proof

\(\iff: \text{Let } \mathbf{v} \text{ be initial subject, and } G_0 \vdash \star G\)

- Inspection of rules gives:
  - \(G\) is finite
  - \(G\) is a directed graph
  - Subjects and objects only
  - All edges labeled with nonempty subsets of \(R\)

- Limits of rules:
  - None allow vertices to be deleted so \(\mathbf{v}\) in \(G\)
  - None add incoming edges to vertices without incoming edges, so \(\mathbf{v}\) has no incoming edges
Example: Shared Buffer

- Goal: \( p, q \) to communicate through shared buffer \( b \) controlled by trusted entity \( s \)
  1. \( s \) creates \( \{ r, w \} \) to new object \( b \)
  2. \( s \) grants \( \{ r, w \} \) to \( b \) to \( p \)
  3. \( s \) grants \( \{ r, w \} \) to \( b \) to \( q \)
Quiz

In either 1 or 2 or both, can $x$ obtain $r$ rights over $y$?

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

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