

# ECS 235B Module 8

## Sharing in the Take-Grant Model

# can•share Predicate

Definition:

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

# *can•share* Theorem

- *can•share*( $r, \mathbf{x}, \mathbf{y}, G_0$ ) if, and only if, there is an edge from  $\mathbf{x}$  to  $\mathbf{y}$  labeled  $r$  in  $G_0$ , or the following hold simultaneously:
  - There is an  $\mathbf{s}$  in  $G_0$  with an  $\mathbf{s}$ -to- $\mathbf{y}$  edge labeled  $r$
  - There is a subject  $\mathbf{x}' = \mathbf{x}$  or initially spans to  $\mathbf{x}$
  - There is a subject  $\mathbf{s}' = \mathbf{s}$  or terminally spans to  $\mathbf{s}$
  - There are islands  $I_1, \dots, I_k$  connected by bridges, and  $\mathbf{x}'$  in  $I_1$  and  $\mathbf{s}'$  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 with 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  $\mathbf{x}_1, \dots, \mathbf{x}_n$  be subjects in  $G$
- Let  $\mathbf{x}_1$  have no incoming edges
- Now construct  $G'$  as follows:
  1. Do “ $\mathbf{x}_1$  creates  $(\alpha \cup \{g\}$  to) new subject  $\mathbf{x}_i$ ”
  2. For all  $(\mathbf{x}_i, \mathbf{x}_j)$  where  $\mathbf{x}_i$  has a rights over  $\mathbf{x}_j$ , do “ $\mathbf{x}_1$  grants  $(\alpha$  to  $\mathbf{x}_j)$  to  $\mathbf{x}_i$ ”
  3. Let  $\beta$  be rights  $\mathbf{x}_i$  has over  $\mathbf{x}_j$  in  $G$ . Do “ $\mathbf{x}_1$  removes  $((\alpha \cup \{g\} - \beta$  to)  $\mathbf{x}_j$ ”
- Now  $G'$  is desired  $G$

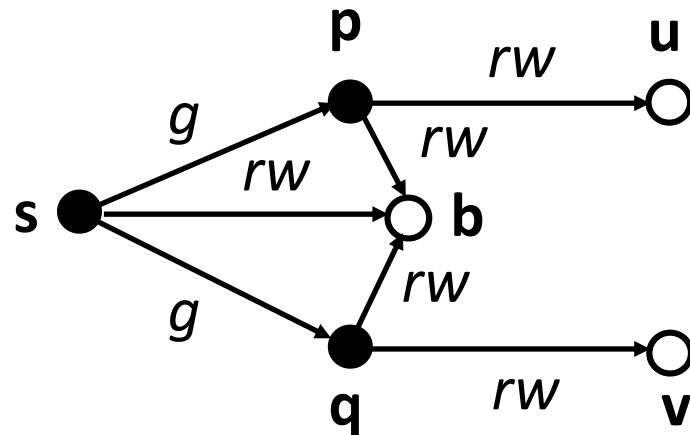
# Outline of Proof

$\Leftarrow$ : Let  $\mathbf{v}$  be initial subject, and  $G_0 \vdash^* G$

- 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**