ECS 235B Module 9
Stealing in the Take-Grant Model

can•steal Predicate

Definition:

- *can•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 $G_0, G_1, \ldots, G_n$ for which the following hold simultaneously:
  a) There is an edge from **x** to **y** labeled r in G_n
  b) There is a sequence of rule applications $\rho_1, \ldots, \rho_n$ such that $G_{i-1} \vdash G_i$ using ρ_i
  c) For all vertices **v** and **w** in G_{i-1}, $1 \le i < n$, if there is an edge from **v** to **y** labeled r, then ρ_i is ***not*** of the form "**v** grants (r to **y**) to **w**"

can•steal Theorem

- *can•steal*(α, **x**, **y**, G_0) if, and only if, the following hold simultaneously:
  a) There is no edge from **x** to **y** labeled α in G_0
  b) There exists a subject **x**′ such that **x**′ = **x** or **x**′ initially spans to **x**
  c) There exists a vertex **s** with an edge labeled α to **y** in G_0
  d) *can•share*(*t*, **x**′, **s**, G_0) holds

Outline of Proof

$\Rightarrow$: Assume conditions hold

- **x** subject
  - **x** gets *t* rights to **s**, then takes α to **y** from **s**
- **x** object
  - *can•share*(*t*, **x**′, **s**, G_0) holds
  - If **x**′ has no α edge to **y** in G_0, **x**′ takes (α to **y**) from **s** and grants it to **x**
  - If **x**′ has α edge to **y** in G_0, **x**′ creates surrogate **x**″, gives it (*t* to **s**) and (*g* to **x**″); then **x**″ takes (α to **y**) and grants it to **x**

Outline of Proof

$\Leftarrow$: Assume *can•steal*(α, **x**, **y**, G_0) holds

- First two conditions immediate from definition of *can•steal*, *can•share*
- Third condition immediate from theorem of conditions for *can•share*
- Fourth condition: ρ 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 ρ_i and adding α from some **p** to **y** in G_i
    - What is ρ_i?

Outline of Proof

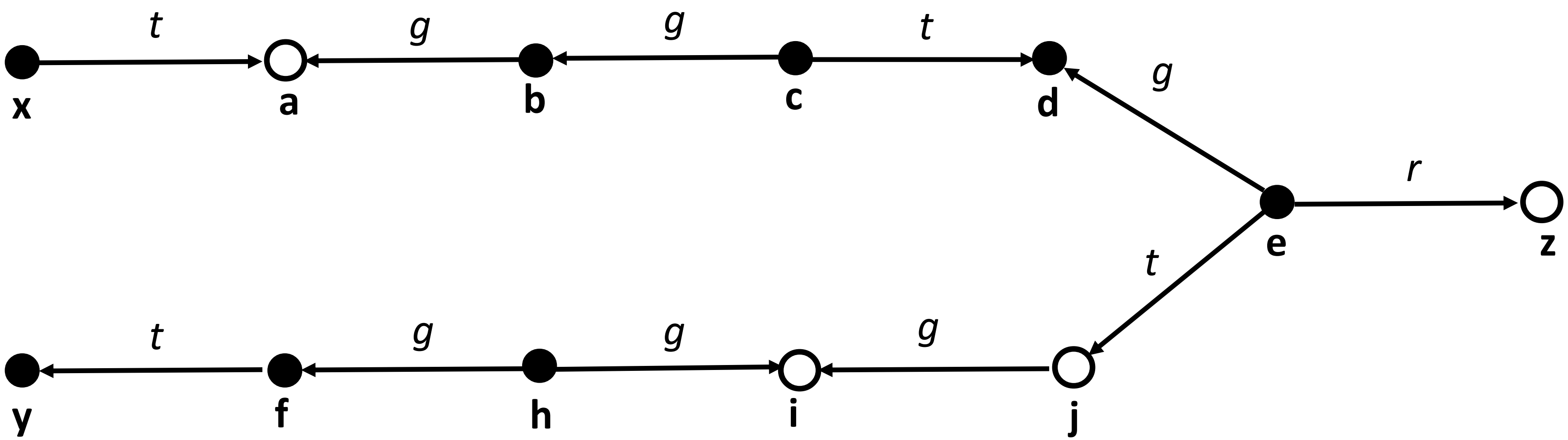
- Not remove or create rule
  - **y** exists already
- Not grant rule
  - G_i first graph in which edge labeled α to **y** is added, so by definition of *can•share*, cannot be grant
- take rule: so *can•share*(t, **p**, **s**, G_0) holds
  - So is subject **s′** such that **s′** = **s** or terminally spans to **s**
  - Sequence of islands with **x′** $\in I_1$ and **s′** $\in I_n$
- Derive witness to *can•share*(t, **x′**, **s**, G_0) that does not use "**s** grants (α to **y**) to" anyone

Conspiracy

- Minimum number of actors to generate a witness for

  can•share(α, **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 *conspiracy graph* to capture how rights flow, and derive actors from it

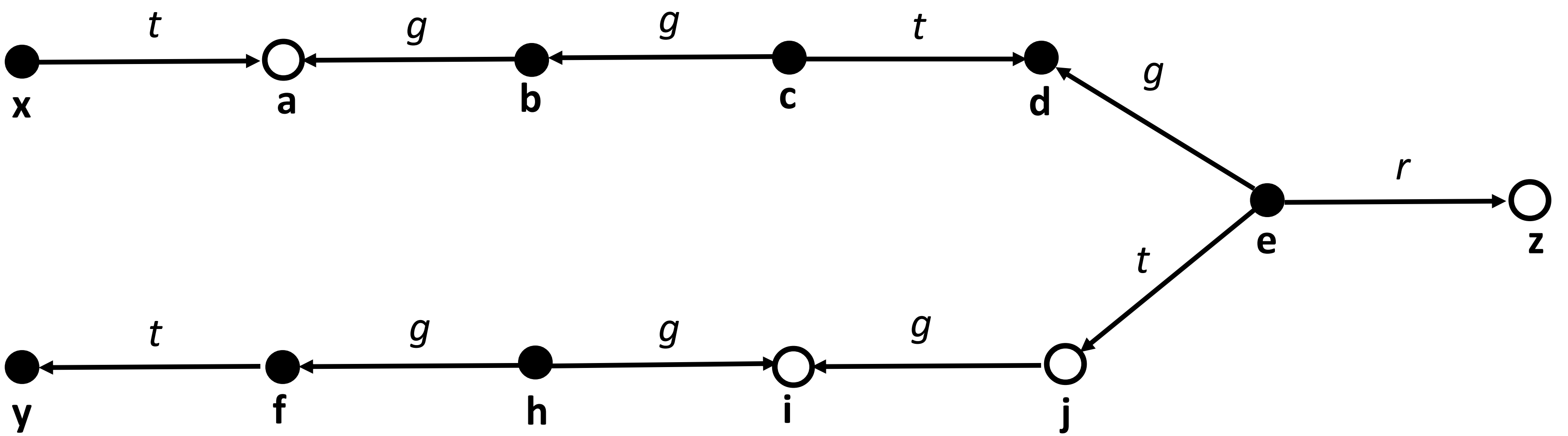
Example



Access Set

- *Access set A(**y**) with focus* **y**: set of vertices:
  - { **y** }
  - { **x** | **y** initially spans to **x** }
  - { **x′** | **y** terminally spans to **x′** }
- Idea is that focus can give rights to, or acquire rights from, a vertex in this set

Example

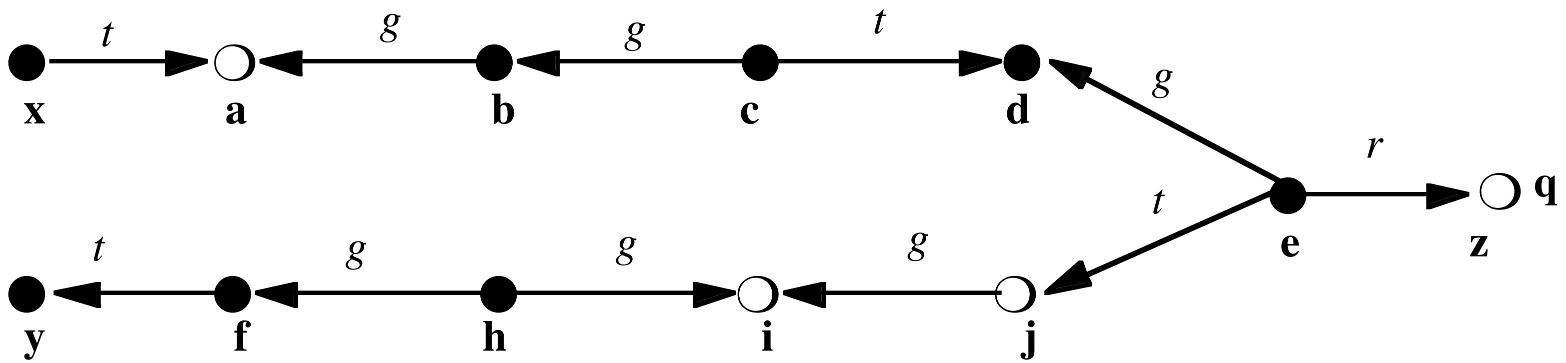


- A(**x**) = { **x**, **a** }
- A(**b**) = { **b**, **a** }
- A(**c**) = { **c**, **b**, **d** }
- A(**d**) = { **d** }
- A(**e**) = { **e**, **d**, **i**, **j** }
- A(**y**) = { **y** }
- A(**f**) = { **f**, **y** }
- A(**h**) = { **h**, **f**, **i** }

Deletion Set

- Deletion set $\delta(\mathbf{y}, \mathbf{y}')$: contains those vertices **z** in $A(\mathbf{y}) \cap A(\mathbf{y}')$ 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

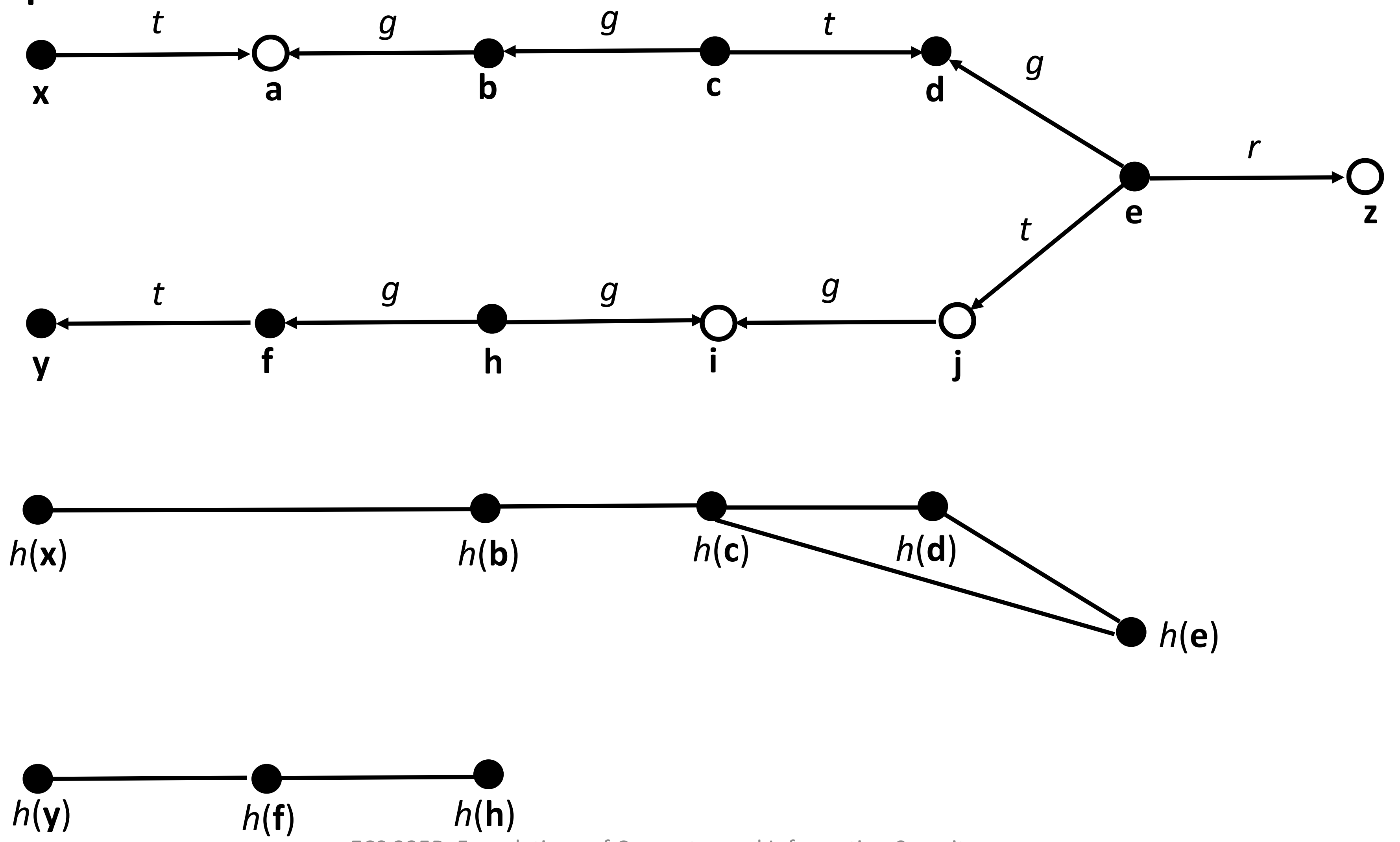


- δ(**x**, **b**) = { **a** }
- δ(**b**, **c**) = { **b** }
- δ(**c**, **d**) = { **d** }
- δ(**c**, **e**) = { **d** }
- δ(**d**, **e**) = { **d** }
- δ(**y**, **f**) = { **y** }
- δ(**h**, **f**) = { **f** }

Conspiracy Graph

- Abstracted graph H from G_0:
  - Each subject **x** $\in G_0$ corresponds to a vertex h(**x**) $\in H$
  - If δ(**x**, **y**) $\neq \varnothing$, 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

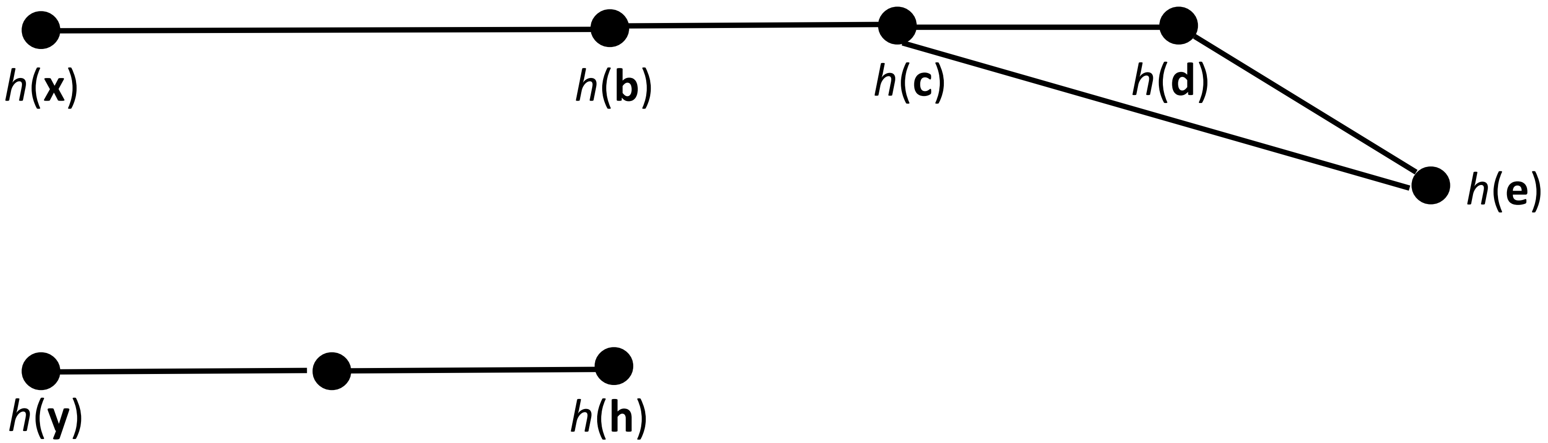
Example



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: *can•share*(α, **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

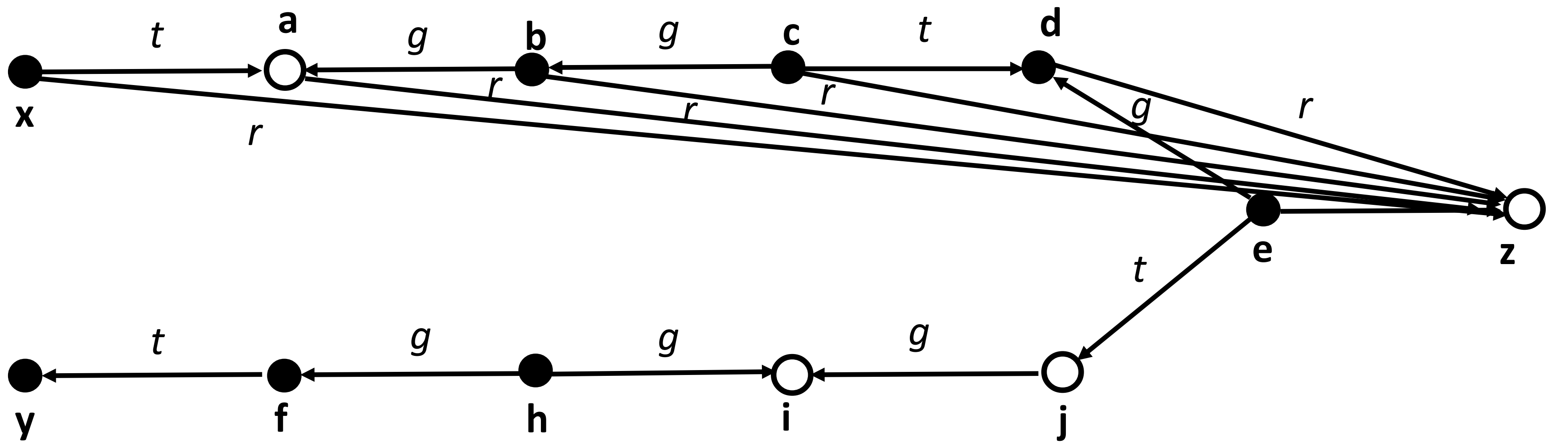
Example: Conspirators



- $I(\mathbf{x}) = \{ h(\mathbf{x}) \}$, $T(\mathbf{z}) = \{ h(\mathbf{e}) \}$
- Path between $h(\mathbf{x})$, $h(\mathbf{e})$ so *can•share*(r, **x**, **z**, G_0)
- Shortest path between $h(\mathbf{x})$, $h(\mathbf{e})$ 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**