ECS 235B Module 7
Take-Grant Model Rules
Take-Grant Protection Model

- A specific (not generic) system
  - Set of rules for state transitions
- Safety decidable, and in time linear with the size of the system
- Goal: find conditions under which rights can be transferred from one entity to another in the system
System

- objects (files, ...)
- subjects (users, processes, ...)
- don't care (either a subject or an object)

\[ G \vdash_\omega G' \quad \text{apply a rewriting rule } \omega \text{ (witness) to } G \text{ to get } G' \]

\[ G \vdash^* G' \quad \text{apply a sequence of rewriting rules (witness) to } G \text{ to get } G' \]

\[ R = \{ t, g, r, w, ... \} \quad \text{set of rights} \]
Rules

take

grant

\[ \vdash \]

\[ \vdash \]

Module 7

ECS 235B, Foundations of Computer and Information Security
More Rules

create

\[ \text{create} \quad \bullet \quad \vdash \quad \bullet \quad \alpha \]

remove

\[ \text{remove} \quad \bullet \quad \alpha \quad \otimes \quad \vdash \quad \bullet \quad \alpha - \beta \]

These four rules are called the *de jure* rules
Symmetry

1. $x$ creates ($tg$ to new) $v$
2. $z$ takes ($g$ to $v$) from $x$
3. $z$ grants ($\alpha$ to $y$) to $v$
4. $x$ takes ($\alpha$ to $y$) from $v$

Similar result for grant
Islands

- *tg*-path: path of distinct vertices connected by edges labeled *t* or *g*
  - Call them “tg-connected”

- island: maximal *tg*-connected subject-only subgraph
  - Any right one vertex has can be shared with any other vertex
Initial, Terminal Spans

- **initial span from** \(x\) **to** \(y\)
  - \(x\) subject
  - \(tg\)-path between \(x, y\) with word in \(\{\overrightarrow{t^* g}\} \cup \{ v \}\)
  - Means \(x\) can give rights it has to \(y\)

- **terminal span from** \(x\) **to** \(y\)
  - \(x\) subject
  - \(tg\)-path between \(x, y\) with word in \(\{\overrightarrow{t^*}\} \cup \{ v \}\)
  - Means \(x\) can acquire any rights \(y\) has
Bridges

• bridge: \( tg \)-path between subjects \( x, y \), with associated word in
  \( \{ t^*, \overline{t}^*, \overline{t}^*g\overline{t}^*, \overline{t}^*g\overline{t}^* \} \)
  • rights can be transferred between the two endpoints
  • \textit{not} an island as intermediate vertices are objects
Example

- islands \{ p, u \} \{ w \} \{ y, s' \}
- bridges \text{uvw; wxy}
- initial span \text{p (associated word v)}
- terminal span \text{s's (associated word t')}

Module 7  ECS 235B, Foundations of Computer and Information Security 10