ECS 235B Module 5
Primitive Operations
State Transitions

• Change the protection state of system
• |– represents transition
  • $X_i |–_\tau X_{i+1}$: command $\tau$ moves system from state $X_i$ to $X_{i+1}$
  • $X_i |–^* Y$: a sequence of commands moves system from state $X_i$ to $Y$
• Commands often called *transformation procedures*
Primitive Operations

• **create subject** $s$; **create object** $o$
  • Creates new row, column in ACM; creates new column in ACM

• **destroy subject** $s$; **destroy object** $o$
  • Deletes row, column from ACM; deletes column from ACM

• **enter** $r$ **into** $A[s, o]$
  • Adds $r$ rights for subject $s$ over object $o$

• **delete** $r$ **from** $A[s, o]$
  • Removes $r$ rights from subject $s$ over object $o$
Create Subject

• Precondition: $s \notin S$
• Primitive command: create subject $s$
• Postconditions:
  • $S' = S \cup \{s\}$, $O' = O \cup \{s\}$
  • $(\forall y \in O') [A'[s, y] = \emptyset]$, $(\forall x \in S') [A'[x, s] = \emptyset]$
  • $(\forall x \in S)(\forall y \in O) [A'[x, y] = A[x, y]]$
Create Object

- Precondition: $o \notin O$
- Primitive command: create object $o$
- Postconditions:
  - $S' = S$, $O' = O \cup \{o\}$
  - $(\forall x \in S') [A'[x, o] = \emptyset]$
  - $(\forall x \in S)(\forall y \in O) [A'[x, y] = A[x, y]]$
Add Right

• Precondition: $s \in S$, $o \in O$
• Primitive command: enter $r$ into $A[s, o]$
• Postconditions:
  • $S' = S$, $O' = O$
  • $A'[s, o] = A[s, o] \cup \{ r \}$
  • $(\forall x \in S')(\forall y \in O' - \{ o \}) [A'[x, y] = A[x, y]]$
  • $(\forall x \in S' - \{ s \})(\forall y \in O') [A'[x, y] = A[x, y]]$
Delete Right

• Precondition: $s \in S, o \in O$

• Primitive command: **delete $r$ from $A[s, o]$**

• Postconditions:
  • $S' = S, O' = O$
  • $A'[s, o] = A[s, o] - \{ r \}$
  • $(\forall x \in S')(\forall y \in O' - \{ o \}) [A'[x, y] = A[x, y]]$
  • $(\forall x \in S' - \{ s \})(\forall y \in O') [A'[x, y] = A[x, y]]$
Destroy Subject

- Precondition: \( s \in S \)
- Primitive command: **destroy subject** \( s \)
- Postconditions:
  - \( S' = S - \{ s \}, O' = O - \{ s \} \)
  - \( (\forall y \in O') [A'[s, y] = \emptyset], (\forall x \in S') [A'[x, s] = \emptyset] \)
  - \( (\forall x \in S') (\forall y \in O') [A'[x, y] = A[x, y]] \)
Destroy Object

• Precondition: \( o \in O \)

• Primitive command: \textbf{destroy object} \( o \)

• Postconditions:
  • \( S' = S, O' = O - \{ o \} \)
  • \((\forall x \in S') [A'[x, o] = \emptyset]\)
  • \((\forall x \in S')(\forall y \in O') [A'[x, y] = A[x, y]]\)
Quiz

What happens when a right is entered into a cell in the access control matrix, and that right is already there?

- Nothing; the second enter operation is ignored.
- An additional copy of the right is put into the cell.
- The second enter operation causes an error.
- It depends on the instantiation of the access control matrix.