ECS 235B Module 8
Attribute-Based Access Control Matrix
Attributes

- **attribute**: variable of a specific data type associated with an entity
- **att(o)**: set of attribute values associated with *o*, called the *attribute value tuple* of *o*
  - Each attribute is written *o.a_i*, with value *v* drawn from set *Va_i*
- **attribute predicate**: boolean expression built from attributes and constants with appropriate operation and relation symbols
  - Unary predicate: built from one attribute
  - Binary predicate: built from two attributes
  - Can have as many attributes in a predicate as needed
  - Example: *Alice.credit* ≥ $100.00
Attribute Based Access Control Matrix (ABAM)

• Change access control matrix so rows correspond to subjects and their attributes, and columns correspond to objects and their attributes

• Note access control matrix discussed previously is special case
  • Just make the attribute sets be empty
Primitive Operations

• **enter, delete** as before

• **create subject** $s$ **with attribute tuple** $\text{att}(s)$: create subject $s$ with given attribute tuple; additionally, add an identity attribute with a unique value

• **create object** $o$ **with attribute tuple** $\text{att}(o)$: create object $o$ with given attribute tuple; additionally, add an identity attribute with a unique value

• **destroy** as before except it also deletes the associated attribute tuple

• **update attribute** $o.a_i$: update $\text{att}(o) = (v_1, \ldots, v_i, \ldots, v_n)$ to $\text{att}(o)' = (v_1, \ldots, v_i', \ldots, v_n)$, where $v_i, v_i' \in Va_i$, and $v_i \neq v_i'$
Commands

• Like previous commands, except that conditions may include attribute predicates
• Let \( p \) give \( q \) \( r \) rights over \( f \), if \( p \) owns \( f \) and value of \( p \)'s attribute \textit{jobcode} is between 3 and 5 inclusive

\[
\text{command grant\{read\}file\{attribute\}\{3to5\}(p, f, q) }
\]
\[
\text{if own in } A[p, f] \text{ and } 3 \leq p.\text{jobcode and } p.\text{jobcode} \leq 5
\]
\[
\text{then enter } r \text{ into } A[q, f];
\]
end
Consider an alternate form of the access control matrix. In this matrix, a subject corresponds to a (subject, attribute) pair with the attributes having fixed values. For example, one subject could be “px=3” and another “px=4”, the notation meaning that attribute “x” has the values 3 and 4, respectively. Which of the following is true?

• This alternate form is equivalent to an attribute-based access control matrix.

• This alternate form is not equivalent to the attribute-based access control matrix, because there are many subjects and objects that do not really exist, namely those with attributes having values other than the current value.