Chapter 2: Access Control Matrix

• Overview
• Access Control Matrix Model
  – Boolean Expression Evaluation
  – History
• Special Rights
  – Principle of Attenuation of Privilege
Overview

• Protection state of system
  – Describes current settings, values of system relevant to protection

• Access control matrix
  – Describes protection state precisely
  – Matrix describing rights of subjects
  – The model is the most precise model to describe a protection state
Description

<table>
<thead>
<tr>
<th></th>
<th>$o_1$</th>
<th>...</th>
<th>$o_m$</th>
<th>$s_1$</th>
<th>...</th>
<th>$s_n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$s_1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$s_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$s_n$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Subjects $S = \{ s_1, \ldots, s_n \}$
- Objects $O = \{ o_1, \ldots, o_m \}$
- Rights $R = \{ r_1, \ldots, r_k \}$
- Entries $A[s_i, o_j] \subseteq R$
- $A[s_i, o_j] = \{ r_x, \ldots, r_y \}$ means subject $s_i$ has rights $r_x, \ldots, r_y$ over object $o_j$
Example 1

<table>
<thead>
<tr>
<th></th>
<th>File 1</th>
<th>File 2</th>
<th>File 3</th>
<th>File 4</th>
<th>Account 1</th>
<th>Account 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>User A</td>
<td>Own R W</td>
<td>Own R W</td>
<td></td>
<td>Inquiry Credit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User B</td>
<td>R</td>
<td>Own R W</td>
<td>W</td>
<td>R</td>
<td>Inquiry Debit</td>
<td>Inquiry Credit</td>
</tr>
<tr>
<td>User C</td>
<td>R</td>
<td>R</td>
<td>Own R W</td>
<td></td>
<td>Inquiry Debit</td>
<td></td>
</tr>
</tbody>
</table>

(a) Access matrix
Access Control List

(b) Access control lists for files of part (a)
Capability Tickets

(c) Capability lists for files of part (a)
Boolean Expression Evaluation

• ACM controls access to database fields
  – Subjects have attributes
  – Verbs define type of access
  – Rules associated with objects, verb pair

• Subject attempts to access object
  – Rule for object, verb evaluated, grants or denies access
Example

- Subject annie
  - Attributes role (artist), groups (creative)
- Verb paint
  - Default 0 (deny unless explicitly granted)
- Object picture
  - Rule:
    paint: ‘artist’ in subject.role and ‘creative’ in subject.groups and time.hour ≥ 0 and time.hour < 5
Copy Right

• Allows possessor to give rights to another
• Often attached to a right, so only applies to that right
  – \( r \) is read right that cannot be copied
  – \( rc \) is read right that can be copied
• Is copy flag copied when giving \( r \) rights?
  – Depends on model, instantiation of model
Own Right

• Usually allows possessor to change entries in ACM column
  – So owner of object can add, delete rights for others
  – May depend on what system allows
    • Can’t give rights to specific (set of) users
    • Can’t pass copy flag to specific (set of) users
Examples

- Windows access control list
- Change permission
- Ownership
Attenuation of Privilege

• Principle of attenuation of privilege
  – A subject may not give rights it does not possess to another
  – Restricts addition of rights within a system
  – Usually *ignored* for owner
    • Why? Owner gives herself rights, gives them to others, deletes her rights.
Key Points

• Access control matrix simplest abstraction mechanism for representing protection state
• Transitions alter protection state
• 6 primitive operations alter matrix
  – Transitions can be expressed as commands composed of these operations and, possibly, conditions