Module 3.1
Access Matrix Model

Ravi Sandhu

Spring 2021
Authentication, Authorization, Audit

AAA

Authentication
Who are You?

Authorization
What are You Allowed to Do?

Audit
What Did You Do?

siloed → integrated
Access Control Models

Discretionary Access Control (DAC) 1970

Mandatory Access Control (MAC) 1970

Role Based Access Control (RBAC) 1995

Attribute Based Access Control (ABAC) 2020s (Hopefully)

Fixed policy

Flexible policy
Access Matrix Model

Operational rights: r, w, x
Administrative rights: own
Basic Abstractions

- Subjects
- Objects
- Rights

The rights in a cell specify the access of the subject (row) to the object (column)
Users and Subjects

- A subject is a program (application) executing on behalf of a user.

- A user may at any time be idle, or have one or more subjects executing on its behalf.

- User-subject distinction is important if subject’s rights are different from a user’s rights.
  - Usually a subset
  - In many systems a subject has all the rights of a user.

- A human user may manifest as multiple users (accounts, principals) in the system.
Users and Subjects

JOE

JOE.TOP-SECRET
JOE.SECRET
JOE.CONFIDENTIAL
JOE.UNCLASSIFIED

USER

SUBJECTS
Users and Subjects

JANE

- JANE.CHAIRPERSON
- JANE.FACULTY
- JANE.EMPLOYEE
- JANE.SUPER-USER

USER

SUBJECTS
An object is anything on which a subject can perform operations (mediated by rights)

Usually objects are passive, for example:
- File
- Directory (or Folder)
- Memory segment
with CRUD operations (create, read, update, delete)

But, subjects can also be objects, with operations
- kill
- suspend
- resume
Access Matrix Model

<table>
<thead>
<tr>
<th>Subjects</th>
<th>F</th>
<th>W</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td></td>
<td></td>
</tr>
<tr>
<td>W</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Operational rights: r, w
Administrative rights: own, parent
Policy vs Enforcement

➢ POLICY
  ❖ Access Matrix

➢ ENFORCEMENT (aka Mechanism)
  ❖ Access Control Lists
  ❖ Capabilities
  ❖ Relations
Access Control Lists

Each column of the access matrix is stored with the object corresponding to that column.
each row of the access matrix is stored with the subject corresponding to that row

U  F/r, F/w, F/own, G/r

V  G/r, G/w, G/own
### Relations

<table>
<thead>
<tr>
<th>Subject</th>
<th>Access</th>
<th>Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>r</td>
<td>F</td>
</tr>
<tr>
<td>U</td>
<td>w</td>
<td>F</td>
</tr>
<tr>
<td>U</td>
<td>own</td>
<td>F</td>
</tr>
<tr>
<td>U</td>
<td>r</td>
<td>G</td>
</tr>
<tr>
<td>V</td>
<td>r</td>
<td>G</td>
</tr>
<tr>
<td>V</td>
<td>w</td>
<td>G</td>
</tr>
<tr>
<td>V</td>
<td>own</td>
<td>G</td>
</tr>
</tbody>
</table>

Commonly used in relational database management systems
ACLs versus Capabilities

- **Authentication**
  - ACL's require authentication of subjects and ACL integrity
  - Capabilities require integrity and propagation control

- **Access review**
  - ACL's are superior on a per-object basis
  - Capabilities are superior on a per-subject basis

- **Revocation**
  - ACL's are superior on a per-object basis
  - Capabilities are superior on a per-subject basis

- **Least privilege**
  - Capabilities provide for finer grained least privilege control with respect to subjects, especially dynamic short-lived subjects created for specific tasks

- **Dynamics**
  - Easier to control modification of ACL’s
ACLs versus Capabilities

- **Authentication**
  - ACL's require authentication of subjects and ACL integrity
  - Capabilities require integrity and propagation control

- **Access review**
  - ACL's are superior on a per-object basis
  - Capabilities are superior on a per-subject basis

- **Revocation**
  - ACL's are superior on a per-object basis
  - Capabilities are superior on a per-subject basis

- **Least privilege**
  - Capabilities provide for finer grained least privilege control with respect to subjects, especially dynamic short-lived subjects created for specific tasks

- **Dynamics**
  - Easier to control modification of ACL’s

Most Operating Systems use ACLs often in abbreviated form: owner, group, world
Content-Dependent Controls

- content dependent controls
  - you can only see salaries less than 50K, or
  - you can only see salaries of employees who report to you

- beyond the scope of Operating Systems
  - provided by Database Management Systems or other “content-aware” systems
Context-Dependent Controls

- context dependent controls
  - cannot access classified information via remote login
  - salary information can be updated only at year end
  - company's earnings report is confidential until announced at the stockholders meeting

- can be partially provided by the Operating System and partially by the Database Management System

- more sophisticated context dependent controls such as based on past history of accesses definitely require Database support