Access Control

Secure Application Development
Module 4
Konstantin Beznosov
What Do You Already Know?

- What are the main elements of access control mechanisms?
- What are the three main types of security policies?
- What access control models do you know?
Outline

- Access control mechanisms
- Access Matrix
- Security policies
  - Confidentiality models
  - Integrity models
  - Hybrid models
Authorization Mechanisms: Access Control

Definition: **enforces the rules, when rule check is possible**

Subject
Principal
User, Client
Initiator

Mix of terms:
Authorization == Access Control Decision
Authorization Engine == Policy Engine
Object System

- Subjects are objects
- Objects are not subjects

Access Matrix

<table>
<thead>
<tr>
<th></th>
<th>Subject 1</th>
<th>Subject 2</th>
<th>Subject 3</th>
<th>File 1</th>
<th>File 2</th>
<th>Process 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject 1</td>
<td>*owner</td>
<td>*owner</td>
<td>*call</td>
<td>*owner</td>
<td>*write</td>
<td></td>
</tr>
<tr>
<td>Subject 2</td>
<td></td>
<td></td>
<td></td>
<td>*read</td>
<td>write</td>
<td>wakeup</td>
</tr>
<tr>
<td>Subject 3</td>
<td></td>
<td>*owner</td>
<td></td>
<td>*write</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Subjects have access to objects
- To be protected
**Access Matrix Structure**

- **Subjects** $S = \{ s_1, \ldots, s_n \}$
- **Objects** $O = \{ o_1, \ldots, o_m \}$
- **Rights** $R = \{ r_1, \ldots, r_k \}$
- **Entries** $A[s_i, o_j] \subseteq R$
- $A[s_i, o_j] = \{ r_{x_1}, \ldots, r_{y} \}$ means subject $s_i$ has rights $r_{x_1}, \ldots, r_{y}$ over object $o_j$
Example

- Processes $p$, $q$
- Files $f$, $g$
- Rights $r$, $w$, $x$, $a$, $o$

<table>
<thead>
<tr>
<th></th>
<th>$f$</th>
<th>$g$</th>
<th>$p$</th>
<th>$q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p$</td>
<td>$rwo$</td>
<td>$r$</td>
<td>$rwxo$</td>
<td>$w$</td>
</tr>
<tr>
<td>$q$</td>
<td>$a$</td>
<td>$ro$</td>
<td>$r$</td>
<td>$rwxo$</td>
</tr>
</tbody>
</table>

**Owner-based Discretionary Access Control (DAC)**
Matrix Implementation Techniques

- Capability list (c-list)
- Access control list (ACL)
ACLs are good for revoking individual’s access to a particular file.

- How hard is it to revoke a user’s access to a particular set of, but not all, files if ACLs are used?
- Compare and contrast this with the problem of revocation using capabilities.
Access Matrix Summary

- Object System
  - Subjects, objects, access matrix
  - Objects are shared
  - All subjects are objects
    - not all objects are subjects

- Matrix implementation
  - Capability lists
  - Access control lists
Security Policies
What’s Security Policy?

- Policy partitions system states into:
  - Authorized (secure)
    - These are states the system can enter
  - Unauthorized (nonsecure)
    - If the system enters any of these states, it’s a security violation

- Secure system
  - Starts in authorized state
  - Never enters unauthorized state
Main Types of Security Policies

- **Confidentiality**
  - Bell-LaPadula

- **Integrity**
  - Biba
  - Clark-Wilson

- **Availability**
  - ?

- **Hybrid**
  - Chinese Wall
  - ORCON
  - Role-based Access Control (RBAC)
Key Points about Policies and Mechanisms

- **Policies**: describe what’s allowed
- **Mechanisms**: enforce policies
Confidentiality Policies
What’s Confidentiality Policy

- **Goal:** prevent the unauthorized disclosure of information
  - Deals with information flow
  - Integrity incidental

- **Examples**
  - Multi-level security (MLS) models
    - **Bell-LaPadula** Model basis for many
Bell-LaPadula Model

- Object and subject labels
- Categories
- “dominates” partial-order relation
- Simple security property
  - No reads up
- *-property
  - No writes down
Example for Bell–LaPadula: Controlling Access to Course Online Content
Application Description

Application:

- 10 students: \( s_1 \ldots s_{10} \)
- 3 instructors: \( i_1, i_2, i_3 \)
- 5 courses: \( c_1, \ldots, c_5 \)
  
  - \( C_1 = \{i_1, \{s_1, s_2, s_3\}\} \)
  - \( C_2 = \{i_2, \{s_3, s_4, s_5\}\} \)
  - \( C_3 = \{i_3, \{s_5, s_6, s_7\}\} \)
  - \( C_4 = \{i_1, \{s_7, s_8, s_9\}\} \)
  - \( C_5 = \{\{i_2, i_3\}, \{s_8, s_9, s_{10}\}\} \)

Policy:

1. Students can
   1. read course material and assignment instructions for the courses they are registered
   2. submit (i.e., write) their assignments for the registered courses

2. Instructors can
   1. read student submitted assignments for the courses they teach, and
   2. post (i.e., write) course material and assignment instructions for their courses

Develop configuration (i.e., label graph, and clearance and classification assignments) for access control mechanisms based on Bell-LaPadula model.
Solution

1. Security level Lattice
2. File classifications
3. User clearances
4. DAC matrix
Security level Lattice

I-C₁, C₂, C₃, C₄, C₅

I-C₁     I-C₂

I-C₃     I-C₄     I-C₅

I

S-C₁     S-C₂

S-C₃     S-C₄     S-C₅

S
# File Classifications

Course material for course $i$ == $CM_i$

Assignment Submission for course $i$ == $AS_i$

<table>
<thead>
<tr>
<th></th>
<th>S</th>
<th>S-C_1</th>
<th>S-C_2</th>
<th>S-C_3</th>
<th>S-C_4</th>
<th>S-C_5</th>
<th>I</th>
<th>I-C_1</th>
<th>I-C_2</th>
<th>I-C_3</th>
<th>I-C_4</th>
<th>I-C_5</th>
<th>I-C_1...C_5</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM_1</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AS_1</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM_2</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AS_2</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM_3</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AS_3</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM_4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AS_4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM_5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AS_5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## User Clearances

<table>
<thead>
<tr>
<th>S</th>
<th>S-C₁</th>
<th>S-C₂</th>
<th>S-C₃</th>
<th>S-C₄</th>
<th>S-C₅</th>
<th>I</th>
<th>I-C₁</th>
<th>I-C₂</th>
<th>I-C₃</th>
<th>I-C₄</th>
<th>I-C₅</th>
<th>I-C₁...C₅</th>
</tr>
</thead>
<tbody>
<tr>
<td>i₁</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i₂</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i₃</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>s₁</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₂</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₃</td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₄</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₅</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₆</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₇</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₈</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₉</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₁₀</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
</tr>
</tbody>
</table>
## DAC Matrix

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i₁</td>
<td>O</td>
<td>O</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i₂</td>
<td>O</td>
<td>O</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i₃</td>
<td>O</td>
<td>W</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₁</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₂</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₃</td>
<td>O</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₄</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₅</td>
<td>O</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₆</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₇</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₈</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₉</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s₁₀</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Assignment Submission for course i by student j == ASᵢⱼ**
Key Points About Confidentiality Models

- Control information flow
- Bell-LaPadula
- Often combine:
  - MAC (relationship of security levels) and
  - DAC (the required permission)
- Don’t deal with covert channels
Integrity Policies
Biba Integrity Model (1977)

- Integrity levels instead of security levels in MLS
- The higher the level, the more confidence
  - That a program will execute correctly
  - That data is accurate and/or reliable
Clark–Wilson Model

- Constrains who can do what
  - authorized triples: (user, TP, {CDI})

- transaction procedures (TPs): Procedures that take the system from one valid state to another
- constrained data items (CDIs): Data subject to integrity controls
Clark–Wilson Model (cont–ed)

- Integrity defined by a set of constraints
  - Data in a *consistent* or valid state when it satisfies constraints

- Example: Bank
  - $D$ today’s deposits, $W$ withdrawals, $YB$ yesterday’s balance, $TB$ today’s balance
  - Integrity constraint: $YB + D - W = TB$

- *Well-formed transaction* move system from one consistent state to another
Key Points About Integrity Models

- Integrity policies deal with trust
  - As trust is hard to quantify, these policies are hard to evaluate completely
  - Look for assumptions and trusted users to find possible weak points in their implementation
- Biba’s model is based on multilevel integrity
- Clark-Wilson’s focuses on separation of duty and transactions
Hybrid Security Models
Chinese Wall Model
If Anthony reads any *Company dataset* (CD) in a conflict of interest (COI), he can *never* read another CD in that COI.
Problem: organization creating document wants to control its dissemination

Example: Secretary of Agriculture writes a memo for distribution to her immediate subordinates, and she must give permission for it to be disseminated further. This is “originator controlled” (here, the “originator” is a person).
Role-based Access Control (RBAC)
RBAC

- Access depends on role, not identity or label
  - Example:
    - Allison, administrator for a department, has access to financial records.
    - She leaves.
    - Betty hired as the new administrator, so she now has access to those records
  - The role of “administrator” dictates access, not the identity of the individual.
RBAC (NIST Standard)

- Users
- Roles
- Operations
- Objects

Permissions

Sessions

user_sessions (one-to-many)

role_sessions (many-to-many)

UA

PA
RBAC with General Role Hierarchy

- **Users**
- **Roles**
- **Sessions**
- **Operations**
- **Objects**

- User sessions (one-to-many)
- Role sessions (many-to-many)

**Relations:**
- UA (User Authoritative)
- PA (Permission Authoritative)
- RH (Role Hierarchy)

Permissions
Example

Manager

Senior Administrator

Administrator

Employee

Senior Engineer

Engineer

\( e_{10} \)

\( e_5 \)

\( e_{3}, e_{4} \)

\( e_{1}, e_{2} \)

\( e_{8}, e_{9} \)

\( e_{6}, e_{7} \)

\( p_a, p_b \)

\( p_x, p_y \)

\( p_{1}, p_{2} \)

\( p_p \)

\( p_o \)

\( p_m, p_n \)
Constrained RBAC

Static Separation of Duty

Role Hierarchy (RH)

Dynamic Separation of Duty

User Sessions (one-to-many)

Operations → Objects

Permissions

Users → Roles

Roles → Objects

Roles → Operations

Users → Operations

Static Separation of Duty

Dynamic Separation of Duty

UA

PA
Application Description

Application:
- 10 students: s_1, ..., s_{10}
- 3 instructors: i_1, i_2, i_3
- 5 courses: c_1, ..., c_5
  - C_1 = \{i_1, \{s_1, s_2, s_3\}\}
  - C_2 = \{i_2, \{s_3, s_4, s_5\}\}
  - C_3 = \{i_3, \{s_5, s_6, s_7\}\}
  - C_4 = \{i_1, \{s_7, s_8, s_9\}\}
  - C_5 = \{\{i_2, i_3\}, \{s_8, s_9, s_10\}\}

Policy:
1. Students can
   1. read course material and assignment instructions for the courses they are registered
   2. submit (i.e., write) their assignments for the registered courses
2. Instructors can
   1. read student submitted assignments for the courses they teach, and
   2. post (i.e., write) course material and assignment instructions for their courses

Develop configuration (i.e., UA, PA, Role hierarchy) for access control mechanisms based on RBAC model
Key Points on Hybrid Models

- deal with both confidentiality and integrity
- ORCON model neither MAC nor DAC
  - Actually, a combination
- RBAC model controls access based on subject’s role(s)
Summary

- Access control mechanisms
- Access Matrix
- Security policies
  - Confidentiality models
    - Bell LaPadula confidentiality model
  - Integrity models
    - Biba integrity model
    - Clark-Wilson
  - Hybrid models
    - Chinese Wall model
    - ORCON model
    - RBAC model