Access Control Matrix

- Access control matrix
  - Describes protection state precisely
  - Matrix describing rights of subjects
## Description

<table>
<thead>
<tr>
<th>subjects</th>
<th>objects (entities)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$s_1$</td>
<td>$o_1$</td>
</tr>
<tr>
<td>$s_2$</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
<tr>
<td>$s_n$</td>
<td></td>
</tr>
</tbody>
</table>

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

**Objects** $O = \{ o_1, ..., o_m \}$

**Rights** $R = \{ r_1, ..., r_k \}$

**Entries** $A[s_i, o_j] \subseteq R$
Example 1

- 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>
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
Confidentiality

- $X$ set of entities, $I$ information
- $I$ has confidentiality property with respect to $X$ if no $x \in X$ can obtain information from $I$
- $I$ can be disclosed to others
- Example:
  - $X$ set of students
  - $I$ final exam answer key
  - $I$ is confidential with respect to $X$ if students cannot obtain final exam answer key
Integrity

- $X$ set of entities, $I$ information
- $I$ has *integrity* property with respect to $X$ if all $x \in X$ trust information in $I$
- Types of integrity:
  - trust $I$, its conveyance and protection (data integrity)
  - $I$ information about origin of something or an identity (origin integrity, authentication)
  - $I$ resource: means resource functions as it should (assurance)
Availability

• \( X \) set of entities, \( I \) resource
• \( I \) has availability property with respect to \( X \) if all \( x \in X \) can access \( I \)
• Types of availability:
  – traditional: \( x \) gets access or not
  – quality of service: promised a level of access (for example, a specific level of bandwidth) and not meet it, even though some access is achieved
Policy Models

• Abstract description of a policy or class of policies
• Focus on points of interest in policies
  – Security levels in multilevel security models
  – Separation of duty in Clark–Wilson model
  – Conflict of interest in Chinese Wall model
Types of Security Policies

- Military (governmental) security policy
  - Policy primarily protecting confidentiality
- Commercial security policy
  - Policy primarily protecting integrity
- Confidentiality policy
  - Policy protecting only confidentiality
- Integrity policy
  - Policy protecting only integrity
Types of Access Control

- Discretionary Access Control (DAC, IBAC)
  - individual user sets access control mechanism to allow or deny access to an object

- Mandatory Access Control (MAC)
  - system mechanism controls access to object, and individual cannot alter that access

- Originator Controlled Access Control (ORCON)
  - originator (creator) of information controls who can access information
Confidentiality Policies

• Overview
  – What is a confidentiality model

• Bell-LaPadula Model
  – General idea
  – Informal description of rules
Overview

• Goals of Confidentiality Model
• The Bell–LaPadula Model corresponds to military-style classifications.
Confidentiality Policy

• Goal: prevent the unauthorized disclosure of information
  – Deals with information flow
  – Integrity incidental

• Multi-level security models are best-known examples
  – Bell-LaPadula Model basis for many, or most, of these
Bell–LaPadula Model, Step 1

- Security levels arranged in linear ordering
  - Top Secret (TS): highest
  - Secret (S)
  - Confidential (C)
  - Unclassified (UC): lowest
- A Subject has a *security clearance* $L(s)$
- An Object has a *security classification* $L(o)$
- The goal of the Bell–LaPadula Security model is to prevent read access to objects at a security classification higher than the subject’s clearance.
Example

<table>
<thead>
<tr>
<th>security level</th>
<th>subject</th>
<th>object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Secret (TS)</td>
<td>Tamara</td>
<td>Personnel Files</td>
</tr>
<tr>
<td>Secret (S)</td>
<td>Samuel</td>
<td>E-Mail Files</td>
</tr>
<tr>
<td>Confidential (C)</td>
<td>Claire</td>
<td>Activity Logs</td>
</tr>
<tr>
<td>Unclassified (UC)</td>
<td>Ulaley</td>
<td>Telephone Lists</td>
</tr>
</tbody>
</table>

- Tamara can read all files
- Claire cannot read Personnel or E-Mail Files
- Ulaley can only read Telephone Lists
Reading Information

• Information flows *up*, not *down*
  – "Reads up" disallowed, "reads down" allowed

• Simple Security Condition (Step 1)
  – Subject $s$ can read object $o$ iff $L(o) \leq L(s)$ and $s$ has permission to read $o$
  
• Note: combines mandatory control (relationship of security levels) and discretionary control (the required permission)
  
– Sometimes called “no reads up” rule
Writing Information

• Information flows up, not down
  – “Writes up” allowed, “writes down” disallowed
• *–Property (Step 1)
  – Subject $s$ can write object $o$ iff $L(s) \leq L(o)$ and $s$ has permission to write $o$
    • Note: combines mandatory control (relationship of security levels) and discretionary control (the required permission)
  – Sometimes called “no writes down” rule
Integrity Policies

- Requirements
  - Very different than confidentiality policies
- Biba’s model
- Clark–Wilson model
Biba Integrity Model

- Set of subjects $S$, objects $O$, integrity levels $I$, relation $\leq \subseteq I \times I$ holding when second dominates first
- $\text{min}: I \times I \rightarrow I$ returns lesser of integrity levels
- $i: S \cup O \rightarrow I$ gives integrity level of entity
Intuition for Integrity Levels

• The higher the level, the more confidence
  – That a program will execute correctly
  – That data is accurate and/or reliable

• Note relationship between integrity and trustworthiness

• Important point: *integrity levels are not security levels*
Biba's Model

• Similar to Bell-LaPadula model
  1. $s \in S$ can read $o \in O$ iff $i(s) \leq i(o)$
  2. $s \in S$ can write to $o \in O$ iff $i(o) \leq i(s)$
  3. $s_1 \in S$ can execute $s_2 \in S$ iff $i(s_2) \leq i(s_1)$
Clark–Wilson Integrity Model

- Integrity defined by a set of constraints
  - Data in a *consistent* or valid state when it satisfies these
- Example: Bank
  - \( D \) today’s deposits, \( W \) withdrawals, \( YB \) yesterday’s balance, \( TB \) today’s balance
  - Integrity constraint: \( D + YB - W \)
- *Well-formed transaction* move system from one consistent state to another
- Issue: who examines, certifies transactions done correctly?
Hybrid Policies: Chinese Wall Model

Problem:

- Tony advises American Bank about investments
- He is asked to advise Toyland Bank about investments

• Conflict of interest to accept, because his advice for either bank would affect his advice to the other bank
Organization

- Organize entities into “conflict of interest” classes
- Control subject accesses to each class
- Control writing to all classes to ensure information is not passed along in violation of rules
- Allow sanitized data to be viewed by everyone
Definitions

- **Objects**: items of information related to a company
- **Company dataset (CD)**: contains objects related to a single company
  - Written $CD(O)$
- **Conflict of interest class (COI)**: contains datasets of companies in competition
  - Written $COI(O)$
  - Assume: each object belongs to exactly one $COI$ class
Example

Bank COI Class
- Bank of America
- Citibank
- Bank of the West

Gasoline Company COI Class
- Shell Oil
- Standard Oil
- Union '76
- ARCO
Temporal Element

• If Anthony reads any CD in a COI, he can never read another CD in that COI
  – Possible that information learned earlier may allow him to make decisions later
  – Let $PR(S)$ be set of objects that $S$ has already read
Sanitization

• Public information may belong to a CD
  – As is publicly available, no conflicts of interest arise
  – So, should not affect ability of analysts to read
  – Typically, all sensitive data removed from such information before it is released publicly (called sanitization)
CW–Simple Security Condition

• $s$ can read $o$ iff either condition holds:
  1. There is an $o'$ such that $s$ has accessed $o'$ and $CD(o') = CD(o)$
     - Meaning $s$ has read something in $o'$'s dataset
  2. For all $o' \in O, o' \in PR(s) \Rightarrow COI(o') \neq COI(o)$
     - Meaning $s$ has not read any objects in $o'$'s conflict of interest class
  3. $o$ is a sanitized object

• Initially, $PR(s) = \emptyset$, so initial read request granted
Writing

- Anthony, Susan work in same trading house
- Anthony can read Bank 1’s CD, Gas’ CD
- Susan can read Bank 2’s CD, Gas’ CD
- If Anthony could write to Gas’ CD, Susan can read it
  - Hence, indirectly, she can read information from Bank 1’s CD, a clear conflict of interest
**CW-Property**

- $s$ can write to $o$ iff both of the following hold:
  1. The CW-simple security condition permits $s$ to read $o$; and
  2. For all *unsanitized* objects $o'$, if $s$ can read $o'$, then $CD(o') = CD(o)$

- Says that $s$ can write to an object if all the (unsanitized) objects it can read are in the same dataset