CSci530: Computer Security Systems  
Security Policy Models  
12 November 2003  

Dr. Clifford Neuman, Dr. Tatyana Ryutov  
University of Southern California  
Information Sciences Institute

Administration  
• the mid-term, problems 1 and 4 are graded  
• still waiting on grades for questions 2 and 3 before the exams can be merged, a final grade assigned, and the exams returned.

Outline  
• What is policy? What is policy model?  
• Examples of security models: Bell LaPadula Model, Biba, Chinese Wall, Role Based Access Control  
• Problems with these models  
• EACL model  
• Emulation of various models  
• Policy Composition

Basic Access Control  
Security Policy  
Authorization Mechanism

Measures to protect against potential violations – unauthorized release, modification, DoS  
Can be specified informally or formally  
Rely on the basic security functions (authentication, authorization, intrusion detection, audit)

Simple Policy Example  
“Tom can read file A.”
Security Policy Model

- More formalized security policy
- Abstracts details concerning implementation
- Target is to prove system properties:
  - Consistency
  - Completeness
- Examples for security models: Access Matrix Model, Bell LaPadula Model, Biba, Chinese Wall, Role Based Access Control

Policy Development Process

1. Informal policy specification.
2. Formal policy specification.
3. Policy implementation.
4. Policy correction.

Types of Access Control

- Discretionary Access Control (DAC)
  - A user can grant or revoke access to the protected objects that he owns
- Mandatory Access Control (MAC)
  - Decisions are made based on the security labeling of objects and subjects. The security labels are assigned externally and are not determined by owner.

MAC models

- Subjects are assigned labels that reflect the security clearance (authorizations) of the user.
- Objects are assigned labels that reflect the security classification (protection requirements) of the data they contain
- MAC:
  - If the subject label and the object label cannot be compared, no access is allowed.
  - If the labels can be compared, access is determined based on rules regarding the relationship between the labels.
- Types of MAC models
  - Confidentiality (Bell-LaPadula)
  - Integrity (Biba)
  - Integrity (RBAC)

MAC Confidentiality: Bell-LaPadula Model (BLP)

- Subjects: active entities (users, processes)
- Objects: passive entities (data, files, directories)
- Access Rights (read, write)
- Security Classes (Labels) form a partially ordered lattice.
  - Lattice is a partially ordered set for which every pair of elements has a greatest lower bound and a least upper bound.
  - Partial ordering < orders some, but not all, elements of set
**BLP: Security Class**

- A security class has two parts:
  - A classification/clearance- hierarchical security level
  - A set of categories, possibly empty
- The class has two operations defined on it
  - Equals, an equivalence relation
  - Dominates, a partial ordering

**BLP: rules**

- request $q$ (object $o$, access right $r$, subject $s$) is granted if and only if all of the following properties are satisfied:
  1. **Discretionary security property:** The cell in the access matrix for row $s$ and column $o$ contains $r$.
  2. **Simple security property (read down, no read up):** A user can only read an object if the security class of the user dominates the security class of the object.
  3. **-property (write up, no write down):** A subject can only write an object if the security class of the subject is dominated by the security class of the object.

**BLP: Example 1**

- **Subjects**
  - Top Secret
  - Secret
  - Unclassified

- **Objects**
  - Top Secret
  - Secret
  - Unclassified

**BLP: Example 2**

- **Subjects**
  - Top Secret
  - Secret
  - Unclassified

- **Objects**
  - Top Secret
  - Secret
  - Unclassified

**BLP: Example 3**

- Suppose Tom’s security class is [Secret, {medical, salary}].
  - Then Tom can read the following information:
    - Any information classified Secret or lower and has no categories
    - Any information classified Secret or lower and belongs to category medical
    - Any information classified Secret or lower and belongs to the category salary
  - Tom CANNOT read information that is
    - Classified higher than Secret
    - Classified Secret or lower and has a category other than medical or salary associated with it.
- Suppose a file’s security class is [Secret, {medical, salary}].
  - It can be read only by subjects having a clearance of Secret or better, and who have read access to BOTH categories medical and salary.
The Chinese Wall model requires that a consultant not be able to read information for more than one company in any given COI class.

Chinese Wall Model (Brewer/Nash 1989)

- The Chinese wall model is deployed to avoid conflicts of interest.

- Objects are grouped into company datasets. Company datasets whose organizations are in competitions are then grouped into conflict of interest (COI) classes.

- The Chinese Wall model requires that a consultant not be able to read information for more than one company in any given COI class.

Clark-Wilson: Separation of Duty

- Static separation of duty
- Dynamic separation of duty

Clark-Wilson Model (1987)

- constrained data items (CDI).

- well formed transaction (WFT) preserves the integrity of CDI.

- The Principle of separation of duty: no single person should perform a task from beginning to end.

Clark-Wilson Triplets

- The Clark-Wilson triplets: <UserID, WFTi, (CDIk, CDIl,...,CDIn)>

- Example: CDI – bank account values
  CW policy: users and apps can modify CDIs (move money) if:
  1. The sum of all money remains constant
  2. A second user must confirm a transaction
  3. All transaction are recorded in append only log

MAC Integrity: Biba

- request q=(object o, access right r, subject s) is granted if and only if all of the following properties are satisfied:

  1. Discretionary security property: The cell in the access matrix for row s and column o contains r.
  2. Simple security property (read up, no read down):
     subject’s integrity class must be dominated by the integrity class of the object being read.
  3. *-property (write down, no write up):
     Subject’s integrity class must dominate the class of the object being written.

Integrated MAC Model

- Implementation of both Mandatory Confidentiality and Integrity rules can be based on a single security class for both confidentiality and integrity.

- This would result in a read-equal and write-equal rules.

- The drawback is reduced flexibility of the resulting system.

Copyright 2003, USC/ISI. All rights reserved.

Example: CDI – bank account values
**Chinese Wall contd.**

- An access request \( p = (o, r, s) \) is granted if all of the following properties are satisfied:
  - Discretionary security property:
    - The cell in the access matrix for row \( s \) and column \( o \) contains the requested right \( r \).
  - Mandatory security property:
    - Subject \( s \) can access object \( o \) only if \( o \) is in the same company dataset as any object already read by \( s \).
    - or
    - the object \( o \) does not belong to any of the CCI classes of objects already accessed by subject \( s \).

**The Principal of Least Privilege**

- “Each principal is given minimum access needed to accomplish its task”

**Role Based Access Control (RBAC)**

- **user**: human being / autonomous agent / computer
- **role**: job function with associated semantics regarding the authority and responsibility conferred on a member of the role.
- **permission**: an approval of a particular mode of access to one or more objects in the system.
- **user assignment**: many-to-many relation between user and role.
- **permission assignment**: many-to-many relation between role and permission.

**RBAC contd.**

```
Role Hierarchy

users  User Assignment  roles  Permission Assignment  permissions
```

**Problems with these models**

- enforce a single security policy
- do not support the specification of expressive policies
- policies are not adaptive (do not allow active actions when security violations are suspected or detected)
- provide no means to reason about the composition of policies

**Problems: Example 1**

- DAC security domain & MAC security domain
- local policies
**Problems: Example 2**

Tom can run a process on host host.bom.isi.edu. If the request fails, a notification must be sent to a system administrator. The process must not consume more than 20% of the CPU. An audit record about the completed process must be generated.

**Taxonomy of Conditions**

- Pre-conditions
  - Time
  - Access identity
- Request-result conditions
  - Write conditions
    - Value
    - T/F/U
    - New value
- Mid-conditions
  - Threshold
- Post-conditions
  - Notification

**EAACL model**

- Specify and enforce complex and fine-grained access control policies in a uniform and structured way.
- Adaptive to changes in the security requirements and assist in detecting and responding to intrusion and misuse.
- Support enforcement at various time stages of the requested action.
- Capture policy evaluation properties (such as priority and composition mode) to support policy composition in a controlled and secure manner.

**EAACL Model: Policy Representation**

<table>
<thead>
<tr>
<th>Policy</th>
<th>Authorization (ensures pre- and mid-conditions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request</td>
<td>Authorization (ensures pre- and mid-conditions)</td>
</tr>
<tr>
<td>T/F/U</td>
<td>T/F/U</td>
</tr>
<tr>
<td>Read()</td>
<td>Read()</td>
</tr>
<tr>
<td>Write()</td>
<td>Write()</td>
</tr>
<tr>
<td>System State</td>
<td>System State</td>
</tr>
</tbody>
</table>

**EAACL Model: Emulation of MAC 1**

- $C = \{c_1, c_2, ..., c_l\}$ is a partially ordered set of confidentiality labels, such as unclassified, secret, top-secret, with ordering relation $\leq$.
- $I = \{i_1, i_2, ..., i_m\}$ is a partially ordered set of integrity labels, such as low-integrity, medium-integrity, high-integrity, with ordering relation $\leq$.
- $M = \{m_1, m_2, ..., m_n\}$ is a set of single security labels for both confidentiality, such as top-secret, low-integrity, secret, medium-integrity and so on, with ordering relation $\leq$.
- Every object and subject in the system bears one of the labels from the sets $C, I, M$. Labels $c_u \in C$, $s_u \in I$, and $m_u \in M$ denote object's classification, integrity label and combined classification/integrity.
- Similarly, labels $c_s \in C$, $s_s \in I$, and $m_s \in M$ denote subject's clearance, integrity label and combined classification/integrity.
**EACL Model: Emulation of MAC 2**

- All access rights are divided into read-class and write-class.
- read pre-condition $X \text{ op } P$
  - $X$ represents the subject's security class
  - $P$ represents object's security class
  - $\text{op}$ is the operation ($\leq$ or $\geq$)

**EACL Model: Emulation of BLP Model**

Simple security property:
"Subject's confidentiality label must dominate the confidentiality label of the object being read."
represented by a read pre-condition $C_s \geq C_o$ associated with the read-type access rights.

"property:
"Subject's confidentiality label must dominate the confidentiality label of the object being written."
represented by a read pre-condition $C_s \leq C_o$ associated with the write-type access rights.

**EACL Model: Emulation of Biba Model**

Biba mandatory integrity model.

Simple security property:
"A subject's integrity label must be dominated by the integrity label of the object being read."
represented by a read pre-condition $I_s \leq I_o$ associated with the read-type access rights.

"property:
"Subject's integrity label must dominate the label of the object being written."
represented by a read pre-condition $I_s \geq I_o$ associated with the write-type access rights.

**EACL Model: Emulation of Combined MAC**

- $M_0=M_1$ associated with the read- and write-type access rights
- $C_0 \leq C_s$, $I_0 \geq I_s$ associated with the read-type access rights and is used to enforce "read down" mandatory confidentiality and "read up" mandatory integrity rule
- $C_0 \geq C_s$, $I_0 \leq I_s$ This condition block is associated with the write-type access rights and is used to enforce "write up" mandatory confidentiality and "write down" mandatory integrity rule.

**EACL Model: Emulation of Chinese Wall Model 1**

```
company information
```

**EACL Model: Emulation of Chinese Wall Model 2**

- read pre-conditions:
  - $\text{accessed_DS} = P$ and $\text{accessed_COI} = P$.
- write post-conditions:
  - $\text{update_accessed_DS, new_value:on_success}$
  - $\text{update_accessed_COI, new_value:on_success}$.
A role-based policy assigns users: Tom, Joe, and Ken role Bank_Teller

Dynamic separation of duty

A user is a member groups:

- read
  - Tom
  - Tom_Bank1

- write
  - upd_accessed_DS
  - upd_accessed_CD

A principal may be a member of several groups. By default, a principal operates with the union of privileges of all groups to which it belongs

- Role properties include:
  1. A user can be a member of several roles
  2. Role can be activated and deactivated by users at their discretion
  3. Authorizations given to a role are applicable only when that role is activated
  4. There may be various constraints placed on the use of roles, e.g. a user can activate just one role at a time

One can choose to have the subject operate with the privilege of only one group at a time.

Example:
- A user is a member groups: Programmers and System managers

- read conditions: X∈{Programmers, System_managers}
- Similarly, one may allow a subject to operate with privileges of several specified groups at a time.

Woo and Lam describe two types of policy composition:

- The Vertical Policy Composition: the policy authorities are hierarchically related in a supervisor-subordinate fashion
- The Horizontal Policy Composition: allows each authority to enforce its access control requirements independently of the others
**EACL Model: Policy Composition 2**

- Objects and policies are organized into security domains.
- Domains are organized into peer-peer and supervisor-subordinate relationships.
- Pre-determined hierarchical levels of security domains for assigning priorities to each domain’s policies.
- To compose policies with different priorities (vertical composition), use a composition mode:
  - expand
  - narrow
- To compose policies with equal priorities (horizontal composition) take a conjunction of the policies.

---

**EACL Model: Policy Composition Example 1**

- System-wide Policy
- Local Policy

System-wide policy defines a **composition mode**:

- expand
- narrow
- stop

---

**EACL Model: Policy Composition Example 2**

- USA Policy specifies narrow mode
- USC Policy specifies stop mode
- CS Policy specifies expand mode

![Diagram showing USA AND USC with stop symbol]