CS 556 – Computer Security
Fall 2012

Dr. Indrajit Ray
Email: indrajit@cs.colostate.edu

Department of Computer Science
Colorado State University
Fort Collins, CO 80523, USA
ACCESS CONTROL

DISCRETIONARY ACCESS CONTROL
ACCESS MATRIX MODEL
ACCESS CONTROL TRIPLES
CAPABILITIES
ACCESS CONTROL LISTS
ACCESS CONTROL ADMINISTRATION

ACCESS CONTROL
Access Control

Authentication

Access Control Models

Authorization

who should be allowed to access which protected resources?

who is trying to access a protected resource?

who should be allowed to change the access?

Access Control Architectures

Enforcement

how does the system enforce the specified authorization?
One of the most important techniques for computer security

- Often neglected

Process of expressing access policies in computer systems

Expressed in terms of *subjects* (active entities) accessing *objects* (passive as well as active entities)
Access Control Models

- Discretionary Access Control
  - Access Matrix Models
  - HRU and TAM
  - Recent Trends in DAC
  - DAC in Database Systems
- Mandatory Access Control
  - Bell LaPadula Model
  - Information Flow Model
- Access Control Models for Security in Commercial Sector
  - Mandatory Access Control for Integrity - Biba Model
  - Lippner’s Integrity Matrix Model
  - Chinese Wall for Confidentiality
  - Clark-Wilson Model
- Role-based Access Control
DISCRETIONARY ACCESS CONTROL

ACCESS CONTROL

DISCRETIONARY ACCESS CONTROL

ACCESS CONTROL MATRIX MODEL

ACCESS CONTROL TRIPLES

CAPABILITIES

ACCESS CONTROL LISTS

ACCESS CONTROL ADMINISTRATION

Dr. Indrajit Ray, Computer Science Department
Definition [Bishop p.53] If an individual user can set an access control mechanism to allow or deny access to an object, that mechanism is a *discretionary access control* (DAC), also called an *identity-based access control* (IBAC).
DAC (cont’d)

- DAC policies govern the access of subjects to objects on the basis of subjects’ identity, objects’ identity and permissions.
- When an access request is submitted to the system, the access control mechanism verifies whether there is a permission authorizing the access.
- Such mechanisms are discretionary in that they allow subjects to grant other subjects authorization to access their objects at their discretion.
ACCESS MATRIX MODEL
Access Matrix Model

- Simplest language for expressing authorizations
- Proposed in 1971 by Lampson, Graham and Denning
- A matrix is used to express the access rights that a subject has towards an object
  - Each cell in the matrix contains an expression that represents the rights
## Access Matrix Model (cont’d)

<table>
<thead>
<tr>
<th>SUBJECTS</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>r, w</td>
<td></td>
<td>r, w own</td>
<td></td>
<td>r</td>
</tr>
<tr>
<td>V</td>
<td></td>
<td>r, w</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>W</td>
<td>w, own</td>
<td></td>
<td></td>
<td>r, w</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>r</td>
<td>r</td>
<td>w</td>
<td>r, w own</td>
<td></td>
</tr>
</tbody>
</table>

**Access Control**
- Discretionary Access Control
  - Access Matrix Model
  - Access Control Triples
  - Capabilities
  - Access Control Lists
  - Access Control Administration

---

Dr. Indrajit Ray, Computer Science Department

CS 556 - Computer Security - © 2012 Colorado State University – 11 / 36
Implementing Access Matrix

- Access Control Triples
  - Most popular in database systems
- Capabilities
  - Widely used in distributed systems
- Access Control Lists (ACLs)
  - Widely used in centralized systems
Access Control Triples
## Access Control Triples

<table>
<thead>
<tr>
<th>Subjects</th>
<th>Objects</th>
<th>A[s,o]</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>A</td>
<td>r, w</td>
</tr>
<tr>
<td>U</td>
<td>C</td>
<td>r, w, own</td>
</tr>
<tr>
<td>U</td>
<td>E</td>
<td>r</td>
</tr>
<tr>
<td>V</td>
<td>B</td>
<td>r, w</td>
</tr>
<tr>
<td>W</td>
<td>A</td>
<td>w, own</td>
</tr>
<tr>
<td>W</td>
<td>E</td>
<td>r, w</td>
</tr>
<tr>
<td>X</td>
<td>A</td>
<td>r</td>
</tr>
<tr>
<td>X</td>
<td>B</td>
<td>r</td>
</tr>
<tr>
<td>X</td>
<td>C</td>
<td>w</td>
</tr>
<tr>
<td>X</td>
<td>D</td>
<td>r, w, own</td>
</tr>
</tbody>
</table>
Access Control Triples (cont’d)

- Advantages
  - Useful in database management systems that incorporates powerful secondary storage management tools as well as very good search capabilities
Access Control Triples (cont’d)

- Disadvantages
  - Grows large very quickly
    - The considered level of granularity for subjects and objects can cause this. For example, if we have a public file that is world readable and writable, then the table contains two triples (r, w) for each subject
  - It may not be convenient to keep a whole authorization table in main memory because there may be many inactive subjects / objects
CAPABILITIES
Capabilities

- Store the access matrix by rows
- With each subject $S_i$ in the access matrix a list of pairs $<O_j, A[S_i, O_j]>\) is associated for each object $O_j$, such that $A[S_i, O_j]$ is not null
  - Each element of the list indicates an object and the privileges held by the subject on that object
Capabilities

Access Control
Discretionary Access Control
Access Matrix Model
Access Control Triples
Capabilities
Access Control Lists
Access Control Administration

Dr. Indrajit Ray, Computer Science Department
Capabilities

● Advantages

✦ Easy to maintain and query system on a per subject basis
  ■ For example, it is easy to find what are all the objects that a particular subject has access to
  ■ When a new subject is introduced in the system, we need to add only one entry corresponding to that subject
Capabilities

- Disadvantages
  - It is difficult to compute the set of subjects that have access right on a given object
  - If an object is removed from the system, then the revocation of rights is time consuming; similarly if a new object is created, granting of rights is time consuming
Capabilities

- Useful in distributed systems where objects are remotely located
- Can be efficiently implemented using message passing techniques
ACCESS CONTROL
DISCRETIONARY ACCESS CONTROL
ACCESS MATRIX MODEL
ACCESS CONTROL TRIPLES
CAPABILITIES
ACCESS CONTROL LISTS
ACCESS CONTROL ADMINISTRATION

ACCESS CONTROL LISTS
Access Control Lists

- Storing the access matrix by columns
- With each object $O_j$, a list of pairs $<S_i, A[S_i, O_j]>\text{ is stored for each subject } S_i,$ such that $A[S_i, O_j]$ is not null
  - This is the Unix style
Access Control Lists

<table>
<thead>
<tr>
<th></th>
<th>U</th>
<th>W</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>r, w</td>
<td>w, own</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
<td>r</td>
</tr>
<tr>
<td>D</td>
<td>r, w, own</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>w</td>
<td></td>
</tr>
</tbody>
</table>

Dr. Indrajit Ray, Computer Science Department
Access Control Lists

- **Advantages**
  - Easy to maintain and query the system on a per object basis
    - For example, all subjects granted access to a particular object can be easily found
    - If an object is deleted, it suffices to delete only one entry in the system to reflect the change
Access Control Lists

- **Disadvantages**
  - It is difficult to compute the set of objects that a given subject can access
  - Granting and revocation of rights on a per subject basis is difficult
Access Control Lists

- Useful in centralized systems where all objects are co-located
- Useful if the number of subjects is fairly static
Limitation of Access Matrix Model

- The Access Matrix Model is not dynamic
  - No transfer of access right from one subject to another
  - No changing of access rights
  - No creation or deletion of subjects or objects

- **Authorization system** = Authorization policies + How to change them
  - Safety
ACCESS CONTROL ADMINISTRATION
## Administration of Privileges

### Unrestricted Discretion

<table>
<thead>
<tr>
<th>SUBJECTS</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>r, w</td>
<td></td>
<td>r, w own</td>
<td></td>
<td>r</td>
</tr>
<tr>
<td>V</td>
<td></td>
<td>r, w</td>
<td></td>
<td>w, own</td>
<td></td>
</tr>
<tr>
<td>W</td>
<td>w, own</td>
<td>r, w</td>
<td></td>
<td></td>
<td>r, w</td>
</tr>
<tr>
<td>X</td>
<td>r</td>
<td>r</td>
<td>w</td>
<td>r, w own</td>
<td></td>
</tr>
</tbody>
</table>
Unrestricted Discretion

- If a subject U has ownership (own) right on an object C, then U can confer any right on object C to any other subject, say V, including ownership right.
- If V gets ownership right from U then V, in turn, can confer any right on object C to itself and to any other subject, say W.
  - W, in turn, can do the same. Thus the right on C is propagated without restriction.
## Propagation of Access

### Constrained Discretion - Copy Flag

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>r, w</td>
<td></td>
<td>rc, r</td>
<td></td>
<td>r</td>
</tr>
<tr>
<td>V</td>
<td></td>
<td>r, w</td>
<td>rc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>W</td>
<td>w, own</td>
<td>r</td>
<td></td>
<td></td>
<td>r, w</td>
</tr>
<tr>
<td>X</td>
<td>r</td>
<td>r</td>
<td>w</td>
<td>r, w</td>
<td></td>
</tr>
</tbody>
</table>

**Access Control**
- Discretionary Access Control
- Access Matrix Model
- Access Control Triples
- Capabilities
- Access Control Lists
- Access Control Administration

Dr. Indrajit Ray, Computer Science Department

CS 566 - Computer Security - © 2012 Colorado State University – 33 / 36
If a subject U has a read-copy (rc) right on an object C, and U has ownership right on C, then U can confer the read-copy right on object C to any other subject, say V.

V, in turn, can then confer the read right on C to any other subject, say W. However, V cannot propagate the read-copy right to W. Thus W is prevented from propagating the access right on object C, any further.

write-copy (wc) has similar semantics
**Propagation of Access**

**Constrained Discretion - Grant / Transfer Flag**

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>S U B J E C T S</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U</td>
<td>r, w</td>
<td></td>
<td>rc, r own</td>
<td>g</td>
<td>r</td>
</tr>
<tr>
<td>V</td>
<td></td>
<td>r, w</td>
<td></td>
<td>r, w</td>
<td></td>
</tr>
<tr>
<td>W</td>
<td>w, own</td>
<td></td>
<td></td>
<td>r, w</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td></td>
<td>r</td>
<td>r</td>
<td>w</td>
<td>r, w own</td>
</tr>
</tbody>
</table>

**Access Control**
- Discretionary Access Control
- Access Matrix Model
- Access Control Triples
- Capabilities
- Access Control Lists
- Access Control Administration
If a subject $U$ has a grant right on any object $D$, then $U$ can confer any other right on object $D$ to another subject $V$, except the ownership right and grant right.

Depending on the right acquired by $V$, it can, in turn, propagate a right further to other subjects.

Transfer flag has similar semantics except that $U$ loses the privilege and the possibility to grant it once a transfer has occurred.