Discretionary Access Control (DAC)

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 2

ravi.utsa@gmail.com
www.profsandhu.com
Authentication
Authentication, Authorization, Audit

AAA

Authentication  Authorization  Audit

Who are You?  What are You Allowed to Do?  What Did You Do?
Authentication, Authorization, Audit

AAA

- Authentication: Who are You?
- Authorization: What are You Allowed to Do?
- Audit: What Did You Do?

Siloed → Integrated
Authentication Techniques

Authentication

- Something you know: password, "secret" questions
- Something you have: smartphone, registered device
- Something you are: fingerprint, iris, keyboard dynamics, signature dynamics
Authentication Techniques

Authentication

- Something you know
  - password
  - “secret” questions

- Something you have
  - smartphone
  - registered device

- Something you are
  - fingerprint
  - iris
  - keyboard dynamics
  - signature dynamics

single factor  →  multi factor
Phishing

Personalized image to authenticate webserver to user
Phishing Man in the Middle

Personalized image passed through
Passwords
Password Attacks

Online
- Lock out
- Throttling

Offline (Dictionary Attack)
- Complex passwords
- Salting
Password Storage and Verification

Password Storage

User ID

Plaintext Password

User ID

Stored Password

Password Verification

User ID

Plaintext Password

User ID

Stored Password

Loss of stored passwords = Catastrophic failure
Password Storage and Verification

**Password Storage**

- User ID
- Plaintext Password
- Hashing Process
- Stored Hash

**Password Verification**

- User ID
- Plaintext Password
- Hashing Process
- Computed Hash
- Stored Hash

Loss of stored hashes = Attack by single dictionary
Password Storage and Verification

Password Storage

User ID → Random Salt → Plaintext Password → Hashing Process → Stored Salt → Stored Hash

Password Verification

User ID → Plaintext Password → Hashing Process → Computed Hash → Stored Salt → Stored Hash

Loss of stored hashes = Attack by different dictionary for each salt value
Access Matrix Model
# Access Matrix Model

## Objects (and Subjects)

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

**Rights**
Basic Abstractions

- Subjects
- Objects
- Rights

The rights in a cell specify the access of the subject (row) to the object (column)
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>Objects (and Subjects)</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>F</td>
</tr>
<tr>
<td>W</td>
<td>W</td>
</tr>
</tbody>
</table>

- **F**
  - r w own
  - parent

- **W**
  - r w own
Implementation

- Access Control Lists
- Capabilities
- Relations
Access Control Lists

F

U:r
U:w
U:own

G

U:r
V:r
V:w
V:own

Each column of the access matrix is stored with the object corresponding to that column.
Capabilities

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

V: G/r, G/w, G/own

Each row of the access matrix is stored with the subject corresponding to that row.
## 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
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

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 and are provided by Database Management 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
➢ Information from an object which can be read can be copied to any other object which can be written by a subject

➢ Suppose our users are trusted not to do this deliberately. It is still possible for Trojan Horses to copy information from one object to another.
Trojan Horse Vulnerability of DAC

User B cannot read file F

File F
ACL
A:r

File G
B:r
A:w
Trojan Horse Vulnerability of DAC

User A executes

Program Goodies

Trojan Horse

read

write

File F

File G

ACL

A:r

B:r

A:w

User B can read contents of file F copied to file G
Read of a digital copy is as good as read of original

Write to a digital copy is not so useful
DAC Subtleties

- Chains of grants and revokes
- Inheritance of permissions
- Negative rights