Lecture 5a: case Study DAC

DAC in UNIX

- Access control policy by Unix:
  - Authorizing requests that processes make to perform operations on files.
  - File names are used in Unix to name most other system resources, too.
  - All operations on files and other system resources are implemented by operating system code.
  - Hence, authorization is enforced by a reference monitor located in the operating system.

(cf. Schneider: Unpublished Chapter)

Authorization through DAC

- A unique user id identifies a user, and a unique group id identifies a group of users.
- Each process executes with an effective user id and an effective group id that together specify the protection domain for that process.
- Each file F has an associated access control list, a user id owner that is the file's owner, and a group id GrF that is the file's group.
  - This information is stored in the i-node for the file, along with other meta-data.
  - Only the owner of a file is permitted to change the access control list for that file, so Unix implements DAC

- ACL for a file F defines three sets of privileges:
  - owner's privileges PrivsF :owner , group's privileges PrivsF :group , and others' privileges PrivsF :other;
- A process having euid as its effective user id and egid as its effective group id is authorized to perform an operation p requiring a privilege p
- provided the following holds.

$$
\begin{aligned}
& (p \in Privs_F.owner \ \wedge \ euid = owner_F) \\
\vee \ & (p \in Privs_F.group \ \wedge \ euid \neq owner_F \ \wedge \ egid = group_F) \\
\vee \ & (p \in Privs_F.other \ \wedge \ euid \neq owner_F \ \wedge \ egid \neq group_F)
\end{aligned}
$$

Efficient if-then-else implmentation- also there is priority

- Consider a process executing with effective group id egid .
- **Can it exercise a privilege p on a file whose access control list authorizes p to group egid**?

$$Privs_F.owner = \{\mathtt{r}\}, \quad Privs_F.group = \{\mathtt{r}, \mathtt{w}\}, \quad Privs_F.other = \emptyset$$

EXPECTATION:

A process for which egid = groupF holds should be permitted to perform an operation requiring privilege w , since w is in PrivsF .group holds.

If euid = ownerF,

Then the request would be denied

Because w is not in PrivsF.owner

Already Discussed UNIX File permissions etc.

Exercise I -- DAC

Reading Suggestion: Section 7.3 of

Fred Schneider, “ Access Control”

Exercise : 7.1, 7.2, 7.3, 7.4, 7.6, 7.10, 7.13, 7.16 (9 problems)

Submission date: 20 Feb 2017