

CMPUT 299 (B1) Winter 2008

Security in a Networked World

Some Notes on ACLs

yannis@cs.ualberta.ca

More on Access Control Mechanisms

- ▶ Access Control List
 - ▶ Each object is associated with a set of pairs. Each pair is an identity (*subject*) and a right.
- ▶ Unix file access rights are an example of coarse granularity ACL. Some more expressive varieties have been attempted as well, e.g., IBM's AIX extended permissions.
- ▶ (Some) Questions
 - ▶ Are there “default rights” (are they modifiable?)
 - ▶ Which subjects can modify an object's ACL.
 - ▶ Should ACLs apply to a “super-user”
 - ▶ Is grouping/wildcards allowed
 - ▶ Are contradictory ACLs allowed

ACL Modification

- ▶ ACL Modification?
 - ▶ Usually the initiator of an object bears the “own” right over the object. By convention if you “own” then you can modify the ACL of the object.
- ▶ “Super-Users”?
 - ▶ Some systems, e.g. Solaris, apply the full ACLs (not the “abbreviated” Unix ACLs).
- ▶ Grouping/Wildcards?
 - ▶ Usually supported (one or the other) in some restricted sense to save space.
- ▶ Contradictions?
 - ▶ Preference to deny, or to allow, or pick first one found.

More on Access Control Mechanisms (cont'd)

- ▶ Capabilities
 - ▶ Each subject is associated with a set of pairs. Each pair represents an object and a set of rights on the object.
- ▶ Note that the subjects need to be “aware” of the object identities/names. Memory access in a region of the logical address space of a process is based on a C-list.
- ▶ Access control mechanisms return “capabilities” (usually opaque pointers/descriptors) tightly bound to the object being manipulated. Access is indirect – hence incurring higher overhead.

The Problem with CAPs

- ▶ In ACLs process identities and ACLs are under control of the OS. However, C-Lists are under (some) control of the user processes. How are capabilities safeguarded then?
- ▶ Some mechanisms
 - ▶ Memory protection mechanism.
 - ▶ Cryptography
- ▶ What about copying and amplifying capabilities?
 - ▶ Copy inhibit bit field?
 - ▶ Changing capabilities over time?
- ▶ Revocation of rights?