Authorization

Ron Burback

Lecture 7

© Copyright Ron Burback 1997

Authorization

- What can I do?
- based on ACLs, PACs, ePACs, extended attributes
- managed by the privilege service out of the registry

© Copyright Ron Burback 1997

ACL

- Access Control List
- A list of principals and groups and their permissions
- There is NO one permission set
- There is NO one database of ACLs
- Not until DCE 1.1 was there a standard ACL manager

© Copyright Ron Burback 1997

Example ACL

- {user bach rwxid}
- {group composers rwxid}
- {any-other r-xid}
- {user brahms -----}
- bach and all members of the composers group can rwxid with the exception of brahms. All others in this cell and foreign cells can r-xid

© Copyright Ron Burback 1997

ACL Entry Types

- {**user** *principal permissions*}
  - The principal in this cell has permissions.
- {**group** *name permissions*}
  - The members of this group have permissions.
- {**foreign_user** *cell/principal permissions*}
  - The principal in a foreign cell has permissions.
- {**foreign_group** *cell/group permissions*}
  - The members in a foreign group have permissions.

© Copyright Ron Burback 1997

More ACL Entry Types

- {**foreign_other** *cell permissions*}
  - The principals in this foreign cell have permissions.
- {**any_other** *permissions*}
  - All other principals in this or foreign cells have these permissions.
- {**other_obj** *permissions*}
  - All other principals in this cells have these permissions.

© Copyright Ron Burback 1997

More ACL Entry Types

- {**user_obj** *permissions*}
  – The principals who owns this object, in this cell, has permissions.
- {**group_obj** *permissions*}
  – The group that owns this object, in this cell, have this permissions.

© Copyright Ron Burback 1997

More ACL Entry Types

- There is a special set of entries for delegation.
- user_obj_delegate, group_obj_delegate, other_obj_delegate, user_delegate, group_delegate, foreign_user_delegate, foreign_group_delegate, foreign_other_delegate, any_other_delegate.

© Copyright Ron Burback 1997

Masks

- Establish the maximum permissions to be granted.
- two masks
  - mask_obj
  - unauthenticated mask, by default an unauthenticated principal gets no permissions.
- System Administration trick to “turn off” an object or to limit human errors.

© Copyright Ron Burback 1997

How are permissions calculated?

- First check for exact principal (owner, local, or foreign). If match, exit.
- Then check for all groups. You get the logical OR of all permissions.
- Then check for others
  - cell other (other_obj)
  - foreign_other
  - all_other
- Apply masks

© Copyright Ron Burback 1997

Container ACLs

- ACL on the container
- initial ACL for objects in the container
- initial ACL for other containers in this container

© Copyright Ron Burback 1997

PACs

- Privilege Service Certificate
- List of all groups that the principal belongs to.

© Copyright Ron Burback 1997

Some Common Permissions

- r - read
- w - write
- d - delete
- t - test
- c - control
- i - insert
- a - administer

© Copyright Ron Burback 1997

Extended Registry Attributes

- ERAs
- uses the xattrschema object in the registry
- can create any kind of special information in the registry
- (name value) pair
- can be used to create many identities for a user (single site login)
- define user parameters

© Copyright Ron Burback 1997

More on ERAs

- can be mandatory
- can be single or multi valued
- can specify the type of the value
- (name value) pair

© Copyright Ron Burback 1997

EPACs

- Extended PACs
- The PAC plus the ERAs.

© Copyright Ron Burback 1997