To: Distribution

From: T. H. Van Vleck

Date: January 18, 1977

Subject: New Access Control Rules

INTRODUCTION

MTB-296 proposed the introduction of a new attribute, the owner of a directory. It was then observed that a generalization of this concept solved another problem which we have had since the beginning: that of the over-powerful administrator.

The hierarchical organization of the Multics storage system provides a method of delegating responsibility for resource management to successive layers of administrators and sub-administrators. But although an administrator may have responsibility for managing a block of storage resources, the administrator may not have the right to inspect all the data stored in these resources. In the current system, a user who has modify access on a directory has potential access to every branch inferior to the directory, and cannot be prevented from forcing access.

This memorandum proposes a new branch attribute, "private," and a new ACL mode, "o," ("owner") for both segments and directories; and a new branch attribute, "private-ok," for directories. Private segments and directories cannot have their access forced by an administrator with access further up: only a user with "o" access to a private branch may modify its ACL.

Some administrators may legitimately own the data belonging to their subordinates. Indeed, some sites may find that the possibility of users sequestering information from the computer system management would interfere with the mission of the system. Therefore, the ability to make a branch "private" is a privilege which need not be propagated downward in the hierarchy.

PROPOSAL

In order to change the ACL of a non-private branch, the user process must have modify access to the containing directory or have "o" effective access to the branch.

In order to change the ACL of a private branch, the user process must have "c" effective access to the branch.

A branch can be made private by a process with "m" to the parent directory only if it is "private-ok."

A branch can be made private-ok by a process with "m" to the parent directory only if its parent directory is private-ok. Thus, if a site does not wish to have any private segments or directories, it does not make project directories private-ok. If a project administrator wishes to be able to force access to a particular user's storage, he does not make that user's directory private-ok.

Private subtrees may be deleted by means of hcs_$del_dir_tree, by a user who has modify access to the directory which contains the subtree.

CONSEQUENCES

Directory control primitives must check that the ACL for a private object contains at least one "o" entry, and reject operations which would create a branch whose ACL cannot be modified.

Special privileged operations will be made available to the administrative utility programs so that they may sweep a disk storage hierarchy for the purpose of visiting quota cells, without requiring any kind of access. This change will vastly improve the speed and simplicity of the disk storage parts of the crank.

Similar special primitives will be provided for the support of statistical programs such as sweep_disk_.

A "locksmith" function will be available for the cases where a private branch has no "o" term in its ACL, or where the "o" term names a person no longer at the site. This will be implemented as a highly-privileged operation which turns off the private attribute for a branch and logs a message saying it did so. The primitive will send mail to all users with "o" access to the branch, by going through ring 1.

The salvager will be modified to check for inconsistencies between private and private-ok, and to repair them by turning off private. The same action will be taken for private objects with no "o" term in their ACL.

For a private branch, one can determine the set of users who have access to it by examining the branch ACL only. Various programs may have to be modified to operate correctly when they encounter a private object; for example, the delete_dir command, which attempts to force access to a branch in order to delete it, must be modified to use del_dir_tree.

APPLICATIONS

In addition to the increase in convenience provided by the new rule, there will be an opportunity to make several useful extensions to the supervisor and administrative procedures. As mentioned in MTB-296, various system messages pertaining to directories can be changed to indicate the name or names of users with "o" access (if any). These messages can be placed in the SYSERR log and mailed to users by a program running in the crank.

Since it will be quite rare that any user other than one with "o" access changes the ACL of a (non-private) directory, such changes will be audited in the SYSERR log. The program running as part of the crank will notify users with "o" access of these ACL changes also. The create_dir command will be modified to give the creator of a directory "o" access.

POSSIBLE CALLING SEQUENCES

```
   dcl hcs_$allow_private entry (char (*), char (*),
       fixed bin (35));

   call hcs_$allow_private (dn, en, ec);
```

This call turns on the private-ok flag for a directory.

```
   dcl hcs_$make_private entry (char (*), char (*),
       fixed bin (35));

   call hcs_$make_private (dn, en, ec);
```

This call makes a segment or directory private. An error is indicated if the ACL of the branch has no "o" terms.

```
    dcl hphcs_$list_quotas entry (char (*), char (*),
        ptr, fixed bin, fixed bin (35));

    call hphcs_$list_quotas (dn, en, addr (data), n, ec);

    dcl 1 data aligned,
        2 version fixed bin,
        2 dirs (n),
          3 primary_name char (32),
          3 quota fixed bin (35),
          3 used fixed bin (35),
          3 trp fixed bin (71);
```

This call is used by the accounting system to list the subdirectories of a directory, with their quotas.

```
    dcl ring1_admin_$reset_private entry (char (*), char (*),
        fixed bin (35)):

    call ring1_admin_$reset_private (dn, en, ec);
```

This call is the "locksmith" operation. It enters ring 1 and sends mail to all owners before calling admin_gate_$reset_private.