

To: Distribution
From: T. H. Van Vleck
Date: July 27, 1976
Subject: Directory Owners

INTRODUCTION

Most operating systems have some sort of access control list. Where systems differ is in who has the power to change the ACL. This memorandum proposes an addition to the current Multics rule for access to the ACL of a directory.

The current rule is that in order to change the ACL for an object, the user process must have modify access to the directory containing the object. This rule is simple but leads to some inconveniences: for example, users cannot control the ACL of their home directories, and project administrators must request the system administrators to change access to their project directories.

PROPOSAL

The new rule for ACL changing is that in order to change the ACL of a directory, the user process must have modify access to the containing directory and be the owner of the directory.

The owner of a directory will be a new data item consisting of Person.Project. It can be set by any process which has modify access to the containing directory. The initial value for the owner field will be the author of the directory.

Master directories already have owners, currently recorded in the MDCS. This change applies the concept to all directories.

If all owner fields were set to "Initializer.SysDaemon" we would have the situation which occurs in today's supervisor. Addition of the owner rule does not make any data less secure, since the user with modify access to the containing directory chooses whether to assign a new owner or to accept the default.

Multics Project Internal working documentation. Not to be reproduced or distributed outside the Multics Project.

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.

Salvager

When the online or offline salvager modifies a directory, it can log a message containing the owner name. A program running in the crank can then mail a notification to the directory owner.

Retriever

The retriever can be modified to send mail to the owner of a directory if anything is retrieved into the directory. This feature might be optional depending on the setting of a control argument.

Dumper

The error message produced by the dumper when it has trouble with a segment can be changed to include the owner name. Then the notification that items cannot be dumped can be sent to the directory owner.

Access Control List Changing

Since we suspect that it will be quite rare that any user other than the owner changes the ACL of a directory, such changes could be audited in the SYSERR log. The program running as part of the crank could notify directory owners of these ACL changes also, at installation option.

Supervisor Messages

Various supervisor messages pertaining to directories, such as directory set security out of service, can be changed to indicate the owner. Even if these messages are not processed automatically, giving the owner name will assist operations and system administration personnel in notifying the people affected by the error.

QUESTIONS

There are several unresolved questions concerning the implementation of owners.

1. Can an owner name be a starname?

This conflicts with the use as a target of mail. But if a directory's ACL is naturally maintained by several users, this choice might be useful.

2. Can segments have owners?

I can't think of a use for this offhand.

3. Can we replace the concept of author by owner?

No. The system program `up_sysctl_` depends on the unforgeability of segment owner. Some user programs may depend on directory owner in a similar way.

4. Where should the owner be stored?

If stored in the directory header, the item will be easy for the salvager to find and not likely to be overwritten.

If allocated in the parent directory and pointed to by the branch, access checking need not make the directory known to check for access to modify the ACL.

5. Who can change the owner?

Anyone with modify permission on the parent, certainly: but can the owner change the owner?