Published: 05/29/67

Identification

User Profiles
C. Marceau

Purpose

A user is a person working on a project, and is identified by the combination of personal name (or some unique mnemonic) and project id. One person can be several users. The concept of user is a central one in Multics. For example, when a person logs in, he must give (at least implicitly) both name and project id: i.e., he logs in as a user and not simply as a person. It is quite possible that some person is known to an installation (i.e., his personal identification file is in the personnel list --- see BQ.4.02) but is not a user.

The user profile of a user is a directory whose entries contain information about the user as a user, not as a person. For example, a person's password is personal and is contained in his personal identification file (see BQ.4.02). His access to segments pertains to him as a user. He may have access to many segments when he is working on one project, and to few when he is working on another project.

Discussion

The user profile for an individual user is a directory containing segments which are of interest to the Multics system. The term "user profile" is also used to refer to the set of segments in that directory. The user profile directory is not controlled by the user himself, but by certain system personnel who determine the number and names of, and the access to, segments in all user profile directories. These segments contain information about the user, some of it supplied by the project administrator, some (possibly) by the system administrator, and some by the user himself.

A user's profile is immediately inferior to the project directory of the project on which he works (see BQ.4.00 on project directories), and has as its name the personal name of the user. Thus John Doe working on project T234 might be expected to have the user profile named John_Doe in project directory T234. The personal name on the user's profile must be the same as his name on the personnel list (see BQ.4.02).

Access Control

As explained above, only certain system personnel are allowed to write in the user profile directory (add, delete, or rename segments, or modify access control to segments). They exercise this prerogative only when working on the project "user_profiles". Thus the access control list for the user profile reflects that only users working on the project "user_profiles" modify the contents of the user profile directory (write attribute) or add segments (append attribute).

However, any user who references a segment in the user profile must be able to search the user profile directory for the entry pointing to that segment. The ability to search a directory is reflected in the fact that the user has the execute attribute on for that directory. Hence the user whose profile it is, his project administrator, and possibly other users, have the execute attribute on for the user profile.

The access for an individual segment in the user profile depends on the nature of the information in the segment. It is possible to define the mode of access of a particular user to a segment, and further to specify the protection ring(s) from which he may access the segment. The policy underlying protection rings is discussed in BD.9.00. Here we need only mention three rings--the hard core ring, which contains the most sensitive modules, such as the access control mechanism; the administrative ring, containing administrative procedures and data bases; and the user base ring, which is relatively unprotected user area. If a user has access to a segment from a certain ring his mode of access is defined by certain usage attributes: he may read the segment (Read attribute), modify the contents of the segment (Write attribute), or add to the contents of the segment (Append attribute). These access attributes are similar to those defined for directories--the system process mentioned above has the read, write, and append attributes on for all user profile directories.

(A fourth attribute has quite different meanings for directories and for non-directory segments. The Execute attribute for a directory implies the right to search the directory--e.g., each user can search his user profile. For a non-directory segment, it implies the right to execute code in the segment. A fifth attribute, Trap, causes any access to the segment to be trapped--see BG.9.00).

Segments in the User Profiles

This section describes some of the segments which are currently included in the user profile. It is expected that the number and natures of the segments will change rather rapidly until the system settles down. Even then system changes are apt to be reflected in the contents of user profiles.

One group of segments in the user profile is termed the process profile. These segments contain information needed by user processes during execution. At login time a copy is made of these segments and placed in the process directory of the Overseer process in the user's process-group (see BQ.3.00 on the process-group). All of the user's working processes refer to this process profile during execution. It contains, among other things, the permanent copies of the user's options stack (perm_op_list, see BX.12.00) and working directory table (see BX.8.12).

The user profile also contains information which can be written only by the user's project administrator and which determines the subsystem in which the user will operate after logging in, i.e., his interface with Multics. Many users will operate in the Multics Command Subsystem, issuing commands through the Listener and the Shell (see BX.0.00). Other users might see a system that considers all input as requests concerning airline reservations. To specify a subsystem the project administrator must specify the following (see BQ.3.00 for more complete information):

1. a subsystem proper, consisting of a login responder pathname, a stop responder pathname, and an automatic logout responder bit (as discussed in BQ.3.01 on the overseer);

2. an indicator specifying whether the subsystem is enforced on the user or is merely a default in case the user himself specifies no subsystem;

3. a threaded list of alternative subsystems which the user of an enforced subsystem is allowed to use;

4. a restricted Shell indicator, which specifies whether the Multics Shell (see BX.2.00) should interpret commands given as pathnames (that is, the project administrator may allow users to use the Shell, but restrict the kinds of commands which the Shell will interpret for the user);

5. an enforced searching advice indicator, specifying whether or not the project enforces searching rules on the user;

6. pathnames of segments containing enforced searching rules (if any).

The first three items are referenced just after the user has logged in and are contained in the "project_subsystem" segment. The last three are referenced often during execution of user processes, and are contained in a separate segment, the "project_restrictions" segment. Both segments can be written only by the user's project administrator (write and append attributes). The project_restrictions segment is part of the user's process profile.

If the project administrator does not enforce a subsystem on the user, the user may specify a subsystem (consisting of login responder, stop responder, and automatic logout responder bit). The user's specification is recorded in the "user_subsystem" segment in the user profile. This segment may be written only by the user. (The user can set options to restrict his Shell or to set searching rules for himself - see BX.2.00 and BX.13.00 respectively.) Table 1 lists the segments discussed in this section, together with suggested access restrictions for each segment. Other segments will be added to those in this section as the need arises.

Table 1. Segments in the User Profile Directory of user X.Y

This table lists the segments in the user profile of a user with name X working on project Y. In general, the notation "A.B" denotes user A working on project B. Users working on the system project which determines access to user profiles are denoted by "*.user_profiles". The letters R, E, W, A stand for the read, execute, write, and append attributes respectively. The access ring is the ring from which a user may access the segment.

Segment	User	User's mode of access	User's access ring
project_subsystem	X.Y	R	administrative ring
	project administrator.Y	RWA	administrative ring
user_subsystem	X.Y	RWA	administrative ring
project_restrictions	project administrator.Y	RWA	administrative ring
	X.Y	R	administrative ring
perm_op_list (options stack)	X.Y	RWA	user ring
wdt (working directory table)	X.Y	RWA	user ring
user profile directory	*.user_profiles	RWA	administrative ring
	X.Y	E (search)	user ring
	project administrator	E	user ring