Published: 05/31/67

<u>Identification</u>

Dedicated Console List C. Marceau

<u>Purpose</u>

Certain consoles at an installation may be dedicated to a certain user, i.e. that user is identified merely by dialing up the computer from that console. Such a user may be either

- a) a very special user who is known to be the only user who has access to this console (e.g., the console is in a vault in his private office and only he has access to the console);
- b) an unknowable person working on a project which allows him only restricted access to the system (e.g., a transient such as a student in a large class using the system for a short time, or a random person using a demonstration console or even a pay console like a pay phone).

The dedicated console list is a list of all such consoles, and the users to whom they are dedicated. The user identification provided by the dedicated console list is simply the combination of symbolic user name and symbolic project id, used by login. In the case of users in category b) above, only the project id contains real information. The personal name is meaningless and does not appear on the Personnel List (see BQ.4.02).

<u>Discussion</u>

The dedicated console list is immediately inferior to the login directory (login_dir), which is immediately inferior to the root directory. Its path name, thus is

(root) > login_dir > dedicated_console_list

The login directory is discussed in BQ.4.00. It is of no interest here.

The dedicated console list is referenced by the user who procedure which identifies the user when he attempts to log in (see BQ.3.02). Normally a user must type a login

line in order to log in, but a user logging in from a dedicated console only needs to dial up. User who therefore first ascertains whether the console is on the dedicated console list. If it is, user who takes the user name and project id from the dedicated console list and does not expect a command line.

Note: Present consoles, specifically Teletype model 37KSR and IBM model 1050 and model 2741, do not provide completely secure console identification; a person with engineering training and a pair of pliers can easily tamper with the console's ID, making some random console indistinguishable from some dedicated console. This is not a serious problem when the dedicated console is dedicated to a severely restricted user. However, it is dangerous to identify highly privileged (or even ordinary) users by means of unreliable console ids. Therefore, for such users (defined in category "a" in the beginning of this section) it is at present necessary to combine dedicated consoles with dedicated lines. That is, the user's console is at all times connected to a particular channel of the GIOC. Needless to say, reserving a GIOC channel is expensive and a zealous spy can attempt to tap the telephone line; nevertheless, the dedicated line mechanism is the closest thing currently available to accurate identification of a console. (Another solution not yet available is a telephone exchange which permits automatic call-tracing by the called party. Such an exchange would obviate the need for more reliable console ID's.)

Consoles are identified in the dedicated console list by registry file name. When the user dials up, the Answering Service (see BQ.2.00) finds the registry file name of his console and passes it to the user_who procedure in the User Control Process (see BQ.2.03).

Access Control

The dedicated console list can be referenced by the user_who procedure and by the system administrator. The former must be able to read the list to find dedicated consoles, the latter to write in the list in order to dedicate consoles or "undedicate" them.

Access to the dedicated console list is controlled by means of the file system access control mechanism. It is possible to define the mode of access of a particular user (or even a particular user-process-group) to a segment. Further, the user's access may be limited to certain protection rings. Protection rings are discussed in BD.9.00. Three rings concern us here: the hardcore ring, containing the most sensitive modules; the administrative ring, which contains administrative modules and data bases; and the user ring, which is relatively unprotected user area. Note that the ring in which a segment resides depends on which user is trying to access it; i.e., user A may be able to access a segment from the user ring, while user B can only get at the segment from the hard core

Three usage attributes in the mode of access concern us here (two others, Execute and Trap, are discussed in BX.8.00). The Read attribute allows a user to read information from a segment. The <u>Append</u> attribute allows him to add information to a segment. The <u>Write</u> attribute allows him to change or delete information in a segment.

The system administrator has all three attributes on for the segment containing the dedicated console list. He has this access when he is working on the "system" project, i.e. working <u>qua</u> system administrator, and then only in the administrative ring. This hedge around his access rights is intended to mitigate against the possibility of his modifying the dedicated console list unintentionally.

The user who procedure operates in the User Control Process. a system process with a characteristic "user id". is because a logging-in user has not been identified (identifying him is precisely user who's job!) and cannot be known by his own name and project id. The User Control Process in which user_who executes has the <u>read</u> attribute on for the dedicated console list, when executing in the administrative ring.

<u>Implementation</u>

The dedicated console list looks like a PL/I structure:

dcl 1 dedicated_console_list ctl (p),

3 projid char (24);

2 size fixed bin (17), /* number of consoles on list */ 2 list (p dedicated_console_list.size), /* registry file name 3 rfn char (512), of console */ 3 name char (24), /* name of corresponding user */

/* project id of corresponding user */