To: Distribution

From: Paul A. Green

Date: May 14, 1974

Subject: Modifications to System Control Process for Security Enhancements

Reference: MTB-047

This memo is one in a series of documents describing modifications to be made to Multics. The reader is assumed to have read MTB-047, "Additional Security Controls for Multics".

The new security-related functions will be the responsibility of a person known as the System Security Officer (SSO). The SSO is the one person responsible for the overall security of the Multics system. We wish to keep the functions of the SSO and System Administrator as distinct as possible so that the SSO will not be burdened by the routine tasks of the SA, and so that the SA will not be able to perform the security-related tasks of the SSO. This will be accomplished by having the system control process differentiate between the SA and SSO; while both may install new PNTs and SATs, the SA may not modify the security attributes, and the SSO may not register new users. Further, we wish sites which do not use the security mechanisms to have no need for an SSO; we want defaults to take care of them. The responsibility of the SA is basically unchanged by these modifications; the SSO has the responsibility for:

assigning clearances to objects (persons, projects, terminals)

assigning mnemonic names for the levels and categories

performing the downgrade function on segments

physical security

reviewing the audit logs and setting audit flags

fixing security-related inconsistencies detected by the salvager

---

approving retrieval requests

monitoring the password distribution and verification mechanism

Each of these areas will be discussed in turn.

Clearances and Classifications

The abstract model of the security system assigns clearances to persons and classifications to data. The notion of a clearance is meant to imply a maximum classification which a person may access. The term "level" is often used to mean "classification". This implementation will support seven levels and sixteen categories. The total number of classifications is 7*(2**16). The classifications are partially-ordered; the relations "less than," "equal," or "greater than" may always be applied to two classifications. However, the relation less than is not anti-reflexive; it is not true that A < B implies ^(B < A). For example, "Secret Crypto" is less than "Secret Atomic," and "Secret Atomic" is less than "Secret Crypto."

User, Project and Process Clearance Assignment

The Multics concept of a user is rather diversified; the identity of a user, and the attributes which apply, are derived from three separate tables. The Person Name Table (PNT) contains strictly per-registered-person information (password, default project, last login time, etc.) Every user of Multics has an entry in the PNT, except anonymous users, and we'll get to them later. Similarly, every project is described in the System Administrators' Table (SAT), which records the per-project attributes (project administrators, load control group, project flags etc.). Finally, each project administrator controls who may use his/her project via the Project Definition Table (PDT) for that project. The attributes of a user's process are derived from the the parameters kept in the PNT, SAT, and PDT.

The security modifications will add another field to each table; the clearance of the person, project, or user. These values will be maintained by the SSO (in the case of the PNT and SAT), and by the project administrator (in the case of the PDT). Since the SSO is the only person authorized to grant clearances to registered users and projects, the default clearance value in the PNT and SAT will be level 0 (unclassified) and no categories.

The PL/I declaration is:

```
2 security
  3 categories bit (36),
  3 level fixed bin (17) unal,
  3 pad bit (18);
```

The default value for the PDT entry will be the highest level and all categories. In this way, the PDT entry will not have any effect until changed by the project administrator. The only effect a project administrator can have on the maximum level of a user's process is to lower it, as described below.

Two new login options will also be added:

-clearance string (-cl)

-change_default_clearance (-cdc)

where "string" is a list of names specifying a clearance, of the form:

name1,name2,...

A sample login might be:

login Green -clearance unclassified

A sample login which resets the default clearance is:

login Green -clearance unclassified -cdc

The initial value of the default clearance will be unclassified. The actual character strings which correspond to levels and categories will be assigned by the SSO; they are parameters in installation_parms_.

The clearances kept in the PNT, SAT, and PDT are all used when the user logs in. The level of the user's process is the minimum of the level from:

the PNT entry for the person

the SAT entry for the project

the PDT entry for the person-project combination

the clearance specified in a login option; if not given the default clearance from the PNT entry will be used

the clearance of the terminal

The category set of the process is the Boolean AND of the category sets contained in the same entries.

The final, computed value will be passed to hphcs_$create_proc in the create_info structure when the process is created, and will be placed in the pds and apte. In these two data bases, (see MTB-067, by Doug Hunt) the "pad" field of the previously mentioned PL/I declaration will be replaced by:

```
3 exceptions unaligned,
  4 segments bit (1),
  4 directories bit (1),
  4 ipc bit (1),
  4 pad bit (15);
```

These exception bits will disable the various forms of security access checking. A gate entry will be provided to turn them on and off. There is no way to change the clearance of process; the user must create a new process at a different level. All processes spawned by a user process (absentee) will be restricted to being equal to the clearance of the parent process. This is because absentee processes are really stored process descriptions, which are data just like anything else. It would be a "write-down" operation to allow a top secret process to pass arguments to an unclassified absentee process.

Anonymous users present special problems since their (optional) passwords are controlled by each project administrator, not the system administrator/system security officer. Since anonymous users are not registered, the SSO has no way of assigning a clearance for them. While it could be argued that the clearance of the project could be used, the paper system does not recognize the concept of a project clearance, only people. Therefore, anonymous users must be unclassified.

It should be noted that the system administration and accounting segments themselves will be unclassified and therefore the System Administrator and Project Administrators will perform all of their tasks at the unclassified level.

Downgrade Operation and Salvager Monitoring

Because the new access mechanisms will not allow any "write-down" operations (of data; quota, dtm, and dtu are write-down of control information) unless an escape-hatch is provided, there will be no way to declassify information. See MTB-047 for a discussion of why this is so. The system security officer has been given the authority and responsibility of performing all downgrade operations on segments. This will be a controlled write-down operation, implemented by allowing the SSO to initiate

segments and manipulate directories without being subject to the new security restrictions.

Similarly, the SSO will have to take corrective action when the salvager detects inconsistencies in the classification of segments and directories reclassifying existing ones, or downgrading entries which have crept "up." The retriever will ensure that segments and directories are reloaded at the proper level, so the SSO will not normally be concerned about retrievals. The dump maps contain a fair amount of information about the online hierarchy, however, and even though pathnames are all unclassified (by fiat), casual access to the dump maps should probably be discouraged.

Terminal Clearance Assignment

The requirements for terminal clearances may seem strange at first. But just as persons are "cleared" to a certain level, so are buildings, rooms, and equipment. This is a branch of enforcement known as physical security controls. In order to properly protect information of a certain level, all references to it, and all data paths in which it flows or is stored, must be cleared to at least the same level. If a Top Secret user is trying to type in a Top Secret coffee recipe, the room must be secure to TS (so an uncleared person can't look over his shoulder), the terminal must be cleared to TS (so a secret-cleared person can't have bugged it), the phone lines and multiplexors must be cleared to TS, and finally, Multics must mark its segment as TS. So, to force TS work to be done in TS-cleared rooms, on TS-cleared terminals, Multics will have a table which contains the clearance of each (hardwired) terminal attached to it. As an additional check, the answerback will also be recorded, and verified against the expected value. The SSO will maintain this table as well; it will be necessary to change it whenever terminals are moved or swapped for repair.

Password Distribution

Based on past experience, the weakest part of the current password mechanism is allowing users to select their own passwords. Therefore, a password generator will give each user a password when the "change password" login option is given; this will not be made mandatory for all Multics sites, rather, a system parameter will probably control whether it is used, or whether the user can choose his/her own password.

Auditing of Incorrect Login Attempts

Incorrect login attempts will continue to be carefully audited; the system will record the reason for rejection, date and time, and location and attributes of the terminal in the answering service log. Some incorrect logins may actually indicate very serious attempts to compromise physical security: If a user whose PNT clearance is only secret tries to login on a terminal which is cleared to top secret, then that user has somehow broken physical security by gaining access to a room which requires at least top secret clearance. In this case, the system will inform the operator directly, as well as filing it in the log. To provide some indication that a user (or minicomputer) is trying to guess the password of another user, via repeated unsuccessful logins, the system will report an "attempted breach of physical security" message to the operator, and log, when the number of bad passwords exceeds some system parameter.

Audit Flags

A number of flags will be maintained on a per-project and per-person basis which will cause the system to audit (in the "syserr" log) various events, such as access violations, use of "exception" privileges, initiation of classified segments, etc. These flags are under the control of the SSO, and/or are to produce the audit flags for a given process. At present, the following structure describes the flags:

```
2 audit unaligned,
  3 exception bit (1),
  3 classified_initiation bit (1),
  3 seg_violation bit (1),
  3 dir_violation bit (1),
  3 ipc_violation bit (1),
  3 illegal_opcode bit (1),
  3 pad bit (30);
```