TO: C. Clingen
F. Corbató
R. Feiertag
J. Gintell
N. Morris
R. Roach
J. Saltzer
V. Voydock
S. Webber

FROM: Mike Spier

DATE: September 21, 1971

SUBJECT: The proposed design for Multics' tape reel management procedures.

TAPE REEL MANAGEMENT

Tape reels, in a Multics installation, may typically be grouped according to their functional designation, as follows:

1) New unused tapes
2) Scratch tapes
3) Off-line segment storage tapes
4) Incremental backup tapes
5) Logical dump tapes
6) Physical save tapes
7) System bootload tapes
8) Proprietary tapes assigned to various users

The issues associated with the problem of tape reel management fall into the following three categories:

1. physical protection of the information stored on a given reel against accidental destruction. Given the unavoidable factor of human intervention, a mechanism is needed with which the system may double check on some operator's decision to mount a specific reel for the purpose of overwriting it. This kind of non-positive protection is an elementary precaution against unintentional mishap, and serves only to confer a measure of integrity to the information stored on that tape.

2. logical protection (access control) is a further refinement of the basic physical protection mechanism, by which access attributes may be associated with individual reels of tape, in the same manner in which they are associated with branches of the file system hierarchy. In this context, a reel of tape is considered the equivalent of a "segment" and may be accessed only by users featured on the reel's access control list, and only in accordance with their respective access attributes (this is a case in which usage of the 'append' attribute is both reasonable and trivially controllable). This provides positive protection of information in the sense that information is manipulated only by users who are known to have access rights to it.

Note: It is important to clearly distinguish between physical and logical protection as presented above. In the on-line file system all input/output is internal to Multics and requires no human intervention; consequently the notion of physical protection is implied by the notion of access control. Tapes, however, have to be manually selected and mounted by operators following directives displayed on some special purpose console. The function of the logical protection is to make sure that user requests for tapes are validated before the appropriate directive

for the operator is displayed. The physical protection mechanism exists in order to verify that the operator actually followed the directives without making any mistakes. Thus, the logical protection data base is internal to Multics, whereas the physical protection data base is, by necessity, "internal" to every individual reel of tape (i.e., physically written on it in the form of a control 'header').

3. physical management of reels; labeling them distinctly, storing them in an intelligent way to facilitate retrieval, establishing a reel initiation ritual by which any newly aquired reel is made known to the tape reel manager and is written with a distinct identifying header (a procedure which has to be under supervisory control because it provides a way to completely circumvent the tape protection mechanism) as well as protecting tape reels against unauthorized removal from the operations premises (possible invalidation of the entire Multics protection mechanism).

The Physical Protection Mechanism

The implementation of the physical protection mechanism is relatively trivial, in terms of cost of implementation. Every reel of tape contains, as its first record, a control header which identifies the reel and indicates the nature of its contents. A control header is distinctly recognizable, and default procedures exist for the handling of tapes which have no headers (initially all tapes on Multics, later non-Multics tapes used in inter-system communications). The header includes the following information:

1) The Installation's unique (among Multics installations) identifier.

2) The reel's unique (among tape reels of a given installation) identifier, which is a number assigned to it by the tape reel manager upon introduction into the installation.

3) A code defining the reel's functional designation, as enumerated in the beginning of this document.

4) Date on which the reel was last written, and date before which the information must not be destroyed (e.g., an incremental backup tape may not be reused for two weeks after its creation, a system bootload tape may not be overwritten for a whole year after its creation etc.).

5) The identifier of the user who "owns" this reel (i.e., in whose behalf the tape was originally written). This information may be used in order to provide some crude measure of access control, for example by restricting access to certain kinds of tapes to specific users or perhaps to members of

specific projects. Because of BOS's independance of the normal Multics environment, a special dummy user identifier "*.BOS.*" should be used to tag all reels which have been assigned to it. This point is further discussed below.

6) Functional information such as the density in which the tape was written. By convention, all headers are written in low density to minimize read errors; additional precautions, such as using checksums and/or writing the header twice and performing a logical union of the two copies, may be employed in order to further assure its readability.

The control header is followed by a tape mark separating the header from the body of the reel. All tape DIM's in Multics (including BOS) have to be upgraded to rigorously adhere to the control header checking discipline. When called to 'open' a tape, the DIM is provided with a reel number, a functional designation, an operational code defining the requested mode of access (read, write of append), and perhaps a user-id or a project-id. The DIM reads the control header and determines whether or not the desired operation is permissible. If any breach of protection is detected, the reel is unloaded and an error return is made to the DIM's caller.

Because BOS operates outside the normal Multics environment and may not share (or rather, may not trust) Multics' system data bases, BOS may only rely on a protection scheme enforced by convention, namely that only certain tapes having certain functional designations may be manipulated by it in certain predetermined ways. Thus BOS will read tapes identified (by their headers) as bootload, dump or save tapes, and will overwrite only tapes designated as available scratch tapes whose owner is "*.BOS.*". BOS will refuse to handle any other tapes whose headers feature functional designations which are not known (i.e., wired into) it.

The Logical Protection Mechanism

All requests to 'open' a reel of tape are directed to the Tape Reel Manager (TRM) which maintains a systemwide table known as the Tape Reel Table (TRT). The TRT contains an entry for every reel which belongs to that particular installation. An entry contains the respective reel's identifier, its functional designation, the date on which it was introduced into the installation, the date on which it was last written, the date before which it must not be rewritten, the number of records on it, the identifier of the user (in the case of proprietary tapes) or the project (in the case of system tapes) to whom the reel was assigned, the tape drive (and number of tracks) with which the tape was written, as well as statistical information regarding its frequency of use and frequency of errors.

Depending on the specific implementation, both TRM and TRT may reside either in the hardcore or in the administrative ring. Requests for tapes may emanate from the hardcore ring, which would indicate the necessity for a ring-0 implementation. On the other hand, a convention may be adopted that requests to write a tape may only come from outer rings, allowing proper updating of a ring-1 resident TRT, and that read requests from ring-0 need not be validated by the TRM (as in the case of restoration of off-line segments). This issue is somewhat unclear due to its contingency upon future implementation decisions. A ring-1 implementation seems much more desirable, and efforts should be made to implement the tape management package accordingly.

BOS presents another problem in that information feedback (updating the TRT to reflect the current usage of BOS tapes) is not easily implementable. It is therefore advisable that BOS tapes be ignored by the TRM, which will only be responsible for the allocation of such reels, but otherwise ignorant of their current usage.

Every TRT entry has associated with it a conventional access control list defining the users or groups of users which have the right to request the manipulation of that reel. A request to open a reel will not be passed beyond the TRM (i.e., to the DIM) unless the requesting user has been granted proper authorization.

Initially, all reels belong to the "SysAdmin" project whose identifier is known to the TRM (wired into it). Only "SysAdmin" personnel may assign ownership of a reel to some user or group of users. It is the owner of the reel which may then grant access privileges to other users.

Proposed Implementation Strategy

To achieve a painless and gradual implementation of the proposed protection mechanisms, the following upwards compatible schedule is suggested.

Stage-1: Modification of all tape DIM's to add control headers to all newly written tapes. When reading in a tape, the DIM's will be capable of recognizing, and ignoring, those new headers. Given the current relatively rapid turnover in tape reel usage on Multics, most tapes will, within a short period of time, feature the new control headers. At this stage, no extra protection is provided beyond that which is currently practised in the installation.

Stage-2: Modification of all existing tape manipulating procedures to issue the new 'open' request to a dummy TRM which passes it along to the DIM which in turn ignores ~~them~~ it. During this period, all procedure interfaces are modified in anticipation of the enforcement of the physical protection

mechanism. The ensuing delay in time is used in order to allow as many tapes as possible to be equipped with the new control headers.

Stage-3: The DIM's are upgraded to accept the 'open' request and to check the specified reel's control header. At this stage, a crude measure of access control is introduced by restricting usage of tapes to their respective owners, specified in the tape header. The successful implementation of this stage will assure that critical tapes (bootload, dump etc.) will not be mistakenly destroyed through operational mishaps. At this stage, assuming that a non-trivial number of tapes is still without headers, temporary code may be added to the DIM's to accept such tapes without protest. At some future time, a flag day may be announced following which control headers will be mandatory for all Multics tapes.

Stage-4: Implementation of the TRM and the TRT, which may be done at leisure whenever the necessary resources are available.