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

FROM: Mike Spier

DATE: October 12, 1971

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

This second (and hopefully final) draft of the Multics tape reel management design document includes a number of changes worked out during the discussions held on Sept 30 and October 7. The main changes are in the area of the Tape Reel Table implementation, which is now distributed and consists of a dedicated segment per reel of tape. This design provides the benefit of all existing file system mechanisms (especially those of access control) and moreover, consistent with Multics practises, it allows tape reels to be addressed by symbolic pathname.

- Not clear how it fits into IOS system and into tape drive management.

Should make a +RDs be available via an internal linkage section, so that they can be found.

Need longer reel identifiers

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
9) External tapes from other installations

Functional designations 1-8 apply to internal tapes, designation 9 covers all tapes which are not internal to a given Multics installation. 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., physicall 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 acquired 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). Special administrative procedures are required in order to a) allow usage of external tapes which may not conform to the standard Multics tape format, b) distinguish between internal and external tapes (otherwise a major loophole in the protection scheme), and 3) still convey a measure of protection to external tapes against operational mistakes.

Design Overview

Associated with each reel of tape in a Multics installation, there is a ring-1 dedicated segment known as Tape Reel Descriptor Segment (TRDS) which resides in some directory of the file system hierarchy. Every reel has an 'owner', namely a user to whom the tape was allocated. By convention, the owner of a tape is the user whose name appears in the TRDS 'owner' item. Access to the TRDS is given to those users who are allowed to share the reel. Such users are given 'rwa' access in ring-1, however their actual access mode to the tape reel per-se is specified through the extended access mechanism, as interpreted by the Tape Reel Manager. Such extended access can only be granted by the owner of the reel, who may be a single user or perhaps a group of users. All TRDS's have, by convention, a symbolic name suffixed with '.trds'. Also, by convention, a user may access a reel of tape only by specifying that reel's TRDS. Thus, from the user's point of view, the reel has a symbolic pathname, namely that of the TRDS.

The physical reel is identified by a unique (within a Multics installation) identifier which designates its physical

storage location. A systemwide ring-1 database, known as the Tape Reel Table (TRT) associates all reel identifiers with the current pathname of their respective TRDS, allowing a reel to be correctly accessed by either name. Access by reel identifier is restricted to the operational staff.

A ring-1 software package, known as the Tape Reel Manager (TRM) provides the interpretive interface to both TRT and TRDS. Because of the possibility of error caused by a disk reload following a system crash (e.g., the reappearance of an obsolete TRDS), all user requests are validated by the TRM which first looks up the TRT to ascertain that a given TRDS is currently valid. Additional assurance is provided by a standard 36-bit unique identifier which is used to validate the relationship between a TRDS, a TRT entry and a tape reel control header. By their nature, tape reels provide their own backup; thus the control information contained in the reel's header can be used to regenerate an inconsistent TRT entry or TRDS.

The Physical Protection Mechanism

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 is written on the tape, automatically, whenever a) the reel is 'attached' in the 'write' mode, and b) whenever a reel attached in the 'append' mode contains zero data records. Needless to say, in either case the attach call first reads the reel's current header in order to determine whether or not a new header may be written on it. The control header contains the following items:

1) The Installation's unique (among Multics installations) identifier which is a 168-character string.

2) The reel's unique (among tape reels of a given installation) identifier, which is an 8-character string representation of a number assigned to it by the tape reel manager upon introduction into the installation and which designates the reel's physical storage location.

3) The header's unique identifier, which is a standard Multics 36-bit unique identifier used to verify the relationship between a reel header, the reel's TRT entry and its associated TRDS.

4) A format version identifier. This is a fixed binary constant identifying the current structure of the header. Whenever the

header declaration is modified, this constant is also modified, allowing software recognition of possibly incompatible header formats.

5) A 32-character string code defining the reel's functional designation which is one of designations 2 through 8 as enumerated in the beginning of this document.

6) The reel's intrinsic access mode, which may be either 'read', 'write' or 'append'. This mode, specified by the user when the reel is first written, adds an additional measure of protection, preventing a user from accidentally destroying one of his own tapes. The reel will not be accessed in violation of this mode, unless the user chooses to override it.

7) Date on which this reel was last written from scratch ('write' access, as opposed to 'append' access).

8) 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.). This restriction relates to 'write' but not to 'append' access; the user may override this restriction.

9) The identifier of the user who "owns" this reel. 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 independence 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.

The control header is followed by a EOF 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 'attach' a tape, the DIM is provided with a reel number, a functional designation, and an operational code defining the requested mode of access (read, write or append). 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 to (i.e., wired into) it.

Need an override for emergency.

The Logical Protection Mechanism

All requests to 'attach' 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:

1) A format version identifier for this structure.

2) The reel's identifier.

3) The current header's unique identifier.

4) An authentication code for external tapes, as discussed below.

5) The date on which this TRT entry was last modified.

6) Binary control indicators for special cases, e.g., an indicator that this reel has no TRDS (for example BOS tapes), an indicator that this is an unused entry, an indicator that this reel is available for assignment, an indicator to distinguish between internal and external reels, etc. The number and usage of these indicators is largely implementation dependent.

why not an ordering path name?

7) The condensed tree-name (i.e., concatenation of file system branches' unique identifiers) of the reel's Tape Reel Descriptor Segment. As explained earlier, associated with each reel of tape is a segment which defines that reel; the segment resides in the directory of the user to whom that reel is currently allocated.

The TRT describes all the tape reels which currently belong to the installation. More detailed information about those reels can be found in the individual TRDS's pointed to by their respective TRT entries. The Tape Reel Manager, executing under some administrative process may allocate a reel of tape to some user by moving the reel's TRDS into the user's directory.

what is the definition of allocation? having access?

The Tape Reel Descriptor Segment

From the user's point of view, a reel of tape is identified by a symbolic pathname which is the pathname of the reel's associated TRDS. The 'attach' call, specifying the TRDS as the

device-ID, is directed to the ring-1 Tape Reel Manager which initiates the TRDS and checks to see whether or not the user is privileged to perform the requested operation. An access violation, be it a file system violation (user specified a TRDS which is inaccessible to him) or a simulated extended access violation, results in the normal signaling of an access violation condition.

If the user has access to that reel, a further check is made to determine whether or not an attempt is made to violate the reel's intrinsic access, e.g., a violation of either the intrinsic access mode or the period of time during which the information on the reel is not to be destroyed. If a violation is detected, then an error return is made displaying an appropriate error message. The user may then override both the intrinsic access mode or the conservation period if he so chooses, provided that he has proper access privileges to do so.

If all the checks have been satisfied, the TRM signals to the operator to mount the requested reel, specified in terms of its reel identifier, and the user process is blocked until signaled that the reel has been properly mounted. The TRM then calls into the hardcore ring to read the reel's control header, and validates the information specified in the TRDS against the information contained in the header. Any protection violation causes the immediate detachment and unloading of the reel, and the signaling of an access violation condition. If the header proved satisfactory, the TRM returns to its caller and the user is allowed to make read/write request calls directly into the hardcore ring.

Note: Because of the user's ability to directly read or write a tape without the intermediary of the TRM, any backward repositioning of the tape (rewind) or change in access mode (from read to write) has to be intercepted by the TRM in order to preserve the consistency of the tape protection scheme. Thus, the ring-0 DCM must not accept any requests which have not previously been validated by the TRM.

If the tape is attached for writing ('write' or 'append' mode) and the protection checks were satisfactory, then if the requested access mode is 'append' and the reel contains one or more data record then the tape is advanced to its logical end (following the last data record); otherwise, the tape is rewound and a new control header is written onto it.

At the termination of the tape operation, a 'detach' call is made to the TRM which updates the TRDS if necessary, writes (if necessary) a trailer record at the end of the tape and unloads it. A message is displayed on the operator's console instructing him what to do with the reel.

A Tape Reel Descriptor Segment contains the following items of information:

1) A lock variable. Only one user at a time may manipulate a (potentially shared) reel of tape. A reel's owner may perhaps be given preemption privileges over non-owners, if necessary.

2) A format version identifier for this structure.

3) The reel's identifier.

4) The reel header's unique identifier. If this identifier matches the one read from the reel's control header then it is assumed that this TRDS is valid. One reason for this control item is that sometimes a user may wish to enter into the TRDS control information which contradicts the information in the header, for example reset the date before which the reel must not be re-written, or override the reel's intrinsic access mode, etc. Thus the unique identifier protects the reel from supposed control changes which were in fact caused by the TRDS's inconsistency (e.g., due to a disk reload).

5) The user identifier of the user (or group of users) who 'owns' this reel.

6) The date on which this reel was allocated to its present owner.

7) The date on which the TRDS was last modified through user request.

8) The reel's functional designation code.

9) The reel's intrinsic access mode. This is set during the 'attach' of a newly written reel and applies to all subsequent attempts to access the information on the reel. For example, when generating an MST, its intrinsic access mode may be set to 'read', assuring that Multics' supervisor will never accept a 'write' request for that reel. If, however, it happens that the MST was erroneously generated and has to be redone, the intrinsic access in the TRDS entry may be set to 'write', overriding the access mode specified in the reel's control header, and the tape may be reused for another MST generation.

10) The intrinsic access mode parameter; when a tape is written, this item is used as parameter for the attach call and is written into the reel's header, whereupon it is copied into item 9 of the TRDS.

11) The date on which the reel was last written from scratch; that is, the date on which its current control header was generated.

12) The date on which the reel was last written at all ('append' access).

13) The date before which the reel must not be rewritten (but may be appended to).

14) Indicator as to whether the reel is written in 7-track or 9-track.

15) Counters of the number of valid and invalid records on the tape, as well as the number of logical records.

16) Historical information concerning the reel's frequency of usage, the number of error spots on it, etc.

17) Additional application oriented information. Given the unavoidable sacrifice of an entire page of memory per TRDS, the unused part of the page may be utilized to store additional information of interest. For user archive tapes as well as for off-line segment tapes this may be a directory of the tape's contents, for MST's perhaps descriptive information of the characteristics of this specific system, etc. The ring-1 residency of the TRDS implies of course that this information be manipulated by some dedicated caretaker procedure.

Certain tapes, such as backup or BOS tapes, do not have associated TRDS's for obvious reasons. The Tape Reel Manager must therefore be sufficiently flexible to allow the circumvention of the logical protection mechanism. The most straightforward way to do so is to allow several such reels of similiar functional designation (e.g., all incremental backup tapes) to share a single dummy template TRDS, allowing all tape manipulating procedures in Multics to have a standard interface to the TRM.

Physical Management of Reels

Within a given Multics installation, all reels of tape (both internal and external) are known by their unique identifier which designates their physical storage location.

Every reel introduced into the installation must first be registered and given an identifier. A special registration command is available to the operational staff, which invokes the Tape Reel Manager executing in some system process. The reel is mounted on a tape drive and the TRM is notified whether the reel is external or internal. An internal reel is mounted for writing, an external reel is mounted for reading only.

The TRM reads the reel's first record (if it exists) to determine whether or not it is a standard Multics tape control header. This check assures against redundant registration of

You can't try to read a blank tape!

internal tapes in violation of the protection mechanism. The TRM creates a new TRT entry for this reel and assigns it a unique reel identifier. An internal reel is then written with a control header in accordance with the physical protection scheme.

What about reels to be carried to another Multics installation?

Physical protection of external reels which by definition must not be written with a control header is achieved through usage of a reel authentication code. This code is generated by the TRM and stored in the reel's TRT entry. In the future, when this reel is to be mounted by an operator, the TRM will request the operator to type in this authentication code as displayed on the reel's label, and will check it against the code stored in the TRT entry.

The tape is then unloaded, and a message to the operator displays the new reel identifier and, in the case of an external reel, the authentication code, which the operator physically marks on the reel, probably by using a combination of preprinted standard character stickers. Reel identifier markings are uniform for all reels. Additionally, depending on the reel's designation and usage, additional markings on distinctly colored labels are used in order to visually differentiate between tapes.

Removal of tapes from the installation premises is a priori forbidden. Only tapes which do not contain any protected information might be released for removal. In principle, only the Tape Reel Manager knows whether or not a reel of tape contains any protected information, and that only after having read the reel's control header to validate the reel's identity. Clearly, in order to allow tapes to be removed from the operational premises, certain administrative procedures, going as far as a formal request to the TRM, have to be worked out in order to assure against any breach of protection.

Should go on a set