THE MITRE CORPORATION

BEDFORD, MASS.

MEMORANDUM

TO: E. L. Burke

DATE: 14 February 1975

FROM: K. J. Biba

MEMO NO.: D73-M783

SUBJECT: Multics Design Note #9 - The Secure Generation of Unique Names

COPIES TO: Distribution

The structure of the storage hierarchy assures that the generation (activation) of segment names (represented as a vector of directory entry names) is secure. Such name generation is only observable to processes having a security level greater than or equal to that of the generating process (which, in turn, is equal to the security level of the directory). However, these benefits of a control hierarchy are not available to other multi-level name pools supported by the Multics security kernel. Of particular note are message (within message segment) and process names. Unique identifiers for segments, if supported by the kernel and observable outside the kernel domain, constitute a third instance of a multi-level name pool. Two properties must be satisfied by such multi-level name pools: 1) all names must be unique (the supply must be inexhaustible over the life of the system) and 2) the generation of names must not be modulatable so as to insecurely transmit information through the availability of names (system resources). Thus we find the problem to be a variant of the confinement problem.

While instances of the confinement problem appear, in general, to be difficult problems, the name generation issue apparently has a straightforward solution. The "apparently" caveat results since the proposed solution is stated without proof.

Let us consider a V_function "UNIQUE_NAME" as the generator of the required multi-level name pool. An instance of this function is used in the specification contained in Multics Design Note #7. We then require: 1) no two invocations of this function are equal in value; 2) the value returned by any given invocation is independent of the number of previous invocations (strictly, it is independent of all information maintained by the system). The first condition insures that the generated name is unique and the latter condition insures that its value is not modulatable. A practical realization of this function is a clock having a submicrosecond quantum (resolution). The current value of the clock may then be assigned as the name of an object. It is anticipated that the "UNIQUE_NAME" function will be realized, in Multics, by such a clock.

R. J. Biba

K. J. Biba
Intelligence and
Information Systems

KJB:jkl

Distribution
S. R. Ames, Jr.
D. E. Bell
E. H. Bensley
E. L. Burke
C. S. Chandersekaran
M. Gasser
C. D. Jordan
L. J. LaPadula
S. B. Lipner
J. K. Millen
R. D. Rhode
W. L. Schiller
D. F. Stork
J. C. C. White