To: Distribution

From: John W. Gintell and Jerold C. Whitmore

Date: May 22, 1974

Subject: Considerations for Evaluating Multics Security Enhancements

I. Introduction

This MTB is intended to provide a general framework in which to better understand and evaluate the proposed "Multics Security Enhancements." It is intended as a guide to help the reader evaluate future security enhancement MTBs in terms of their impact on the overall product and to stimulate readers to evaluate all future extensions to Multics in terms of their security implications.

II. Philosophy of "Security"

Security is a term which means many things to many people. The general definition of security within this project is:

> Information stored, processed or communicated within the Multics system cannot be accessed or received by a person who is not authorized; and no unauthorized person shall be able to deny access to information by authorized persons.

This definition indicates that it is a security violation if the average user can "crash," "penetrate," or "tap information from" the system directly or indirectly.

When attempting to make a system "secure," we define mechanisms which are supposed to restrict the actions of users (processes). Having chosen the mechanisms which provide the necessary control, the "security" of the system is measured by the effectiveness of these mechanisms. Let's look at some of the issues involved.

A. Multics Access Control Mechanisms

Physical security of the computer room is an obvious need to prevent sabotage and theft. Here theft involves not only listings and tapes, but also dumps, disk packs, printer ribbons, typewriter ribbons, console output, backup maps and

---

the like. Administrative procedures, physical locks, and personnel control are the mechanisms.

Within the computer system, rings are the mechanism used to separate the user process from directly affecting the supervisor and protected subsystems. The initial ring of a process is under the control of the system administrator.

The access control list mechanism is used to specify the maximum mode of access a given process may have to a segment. The contents of the ACL is under the control of any process which has an effective mode of "modify" to the ACL.

B. Effectiveness of the Mechanisms

Effective access control mechanisms must always be invoked and cannot be bypassed.

Many studies have been made to define the physical and procedural mechanisms which will provide effective control; and thus are not an issue here.

The effectiveness of rings and ACLs rests in the correctness of the ring 0 implementation and its interface to the outer rings. This assumes the correctness of the hardware, of course. To ensure the effectiveness of rings and ACLs we must all be aware of the "security" implications of system changes and be on the lookout for vulnerabilities.

These internal access control mechanisms (when effective) provide sufficient control of access to segments only if we can rely on the correct actions of all users in setting access to segments and in writing sensitive information in the correct segments. However, users are accident prone (this is charitable) and sharing makes processes prone to Trojan Horse attacks, so we cannot rely on the user processes to correctly implement administrative decisions defining which users may or may not have access to information. The proposed "security enhancements" are intended to provide additional access control mechanisms which will ensure system enforcement of these administrative decisions. This is done by limiting, effectively, who may receive (in addition to who may grant) access to information.

III. Security Enhancements

The upcoming "security enhancements" implementation will provide some new mechanisms to give the necessary control of access within the Multics system. These enhancements will not make Multics more "secure" since they will not guarantee the correctness of ring 0. However, as part of the current Honeywell

effort, a vulnerability analysis of Multics in Phoenix will begin shortly to address the "effectiveness" aspect of the Multics access control mechanisms.

The security enhancements, outlined in MTB 047, are being implemented primarily for the Air Force; to provide the necessary controls to emulate the military security system. However, an equally important goal of this effort is to provide a suitable set of access controls for the standard system that will be of general value to customers other than the military.

As part of this security enhancement effort, Honeywell is committed to incorporate all software modifications which affect the security access control decisions (in hardcore) and user authentication, as an integral part of the Multics standard product.

What is the Multics standard product? It is that portion of the Multics standard release (e.g., MR 1.0) which is fully documented and for which Honeywell software support is provided. (Note that the ARPA software, for example, is not currently part of the standard product, even though it is distributed in the standard release.)

Our committments to the enhancements outlined in MTB 047 can be grouped as follows:

A. Integral to the standard product

user control modifications
storage system changes
backup of segment security attributes
salvager support of security attributes
IPC access controls
removable hierarchy security support

B. To be included in the standard product on their merit and wide applicability to customers

accountability form terminals
printer driver control from dialed terminal
tape driver process and commands
I/O coordinator which knows about multiple security levels
additional audit mechanism
special options to existing commands
special "security" commands
special support for the SSO function

It is to our advantage to have only one Multics system to support and therefore we desire to make all changes to the standard product system instead of providing two versions of the system. On the other hand, some of the enhancements are very specialized

and would result in decreased system performance, loss of capability, or increased complexity of operation and are more suitable as an addition to the standard system, but not part of the standard product. Our preference is to add everything in group B above to the standard product, with options or defaults as needed to ease the operational burden if their use is not desired. Everything in group A will be part of the standard product and will not be capable of being "turned off", although these features will be invisible to installations not choosing to use them.

MTBs concerning items in group B, should be reviewed with the following in mind:

* Does the proposed enhancement properly solve the problem it is addressing?

* Is the proposed enhancement applicable to a wide customer base?

* Should all or part of the enhancement be included in the standard product?

IV. Conclusion

This new access control mechanism will affect each system programmer in some way at some time in the future. Therefore, we recommend that MTB 047 and the other MTBs in the "security enhancement" series be reviewed again.