

# Honeywell

## PROJECT GUARDIAN TECHNICAL COORDINATION LETTER

RECEIVED

MAY 26 1976

J. H. SALTZER

Date: 12 May 1976

To: Contracting Officer  
HQ/ESD/MCP  
Hanscom AFB  
Bedford, Mass. 01731

TCL: 21

Contract No: F19628-74-C-0193

Attention: C. E. Fenton, Captain, USAF

Subject : Summary of the April 29, 1976 Technical Meeting


The attached technical note summarizes the April 29 technical discussion on discretionary access control and the integrity control mechanism.

Three items in the technical note deserve special attention:

1. A kernel design exists that will meet the requirements of the AF/MITRE mathematical model, as it existed on April 29, 1976, without supporting ACL's in the kernel. This is the design that Honeywell is pursuing for the formal kernel specification.
2. The program schedule currently being developed does not include certification of the ACL mechanism. Therefore, if a revised math model is developed and certification of the ACL mechanism becomes an Air Force requirement, the change in effort must be evaluated and the program schedule must be revised accordingly.
3. If the Air Force decides to extend the mathematical model to include changing the access matrix for discretionary access control, Honeywell personnel should be involved early in the effort to ensure that the objectives will be compatible with Multics.

If there are any questions, please contact the undersigned or Mr. N. Adleman at our Cambridge, Massachusetts office.

Very truly yours,

  
R. L. Carlson  
Contract Specialist  
HONEYWELL INFORMATION  
SYSTEMS, INC.

Attachment

cc: ESD/MCI (5)  
MITRE/D73 (5)  
RADCS/ISM (3)  
NSA/R14 (3)  
AFDSC/XMS (2)  
CCTC (5)

From: J. Stern  
To: Project Guardian Distribution  
Date: May 2, 1976  
Subject: Technical Meeting Summary

On April 29, a meeting concerning Project Guardian was held at the Honeywell office in Cambridge, Mass. Present at this meeting were representatives from Honeywell, Air Force/ESD, MITRE, and MIT. Two subjects were discussed at this meeting: (1) the requirements for kernel-provided discretionary access control, and (2) the administrative and user interfaces to the integrity mechanism. The results and implications of these discussions are summarized below.

#### DISCRETIONARY ACCESS CONTROL

It was agreed that the only requirements for kernel-provided discretionary access control are the requirements of the mathematical model which was provided to Honeywell by the Air Force. With respect to discretionary controls, the model describes an access matrix that specifies the access permissions of each subject for each object. However, the model does not specify any restrictions on the modification of the access matrix. For this reason, the model can be satisfied by a kernel design which excludes the Multics access control list (ACL) mechanism.

As previously described in TCL 17, Honeywell is presently pursuing a two-layer kernel design which separates non-discretionary controls from discretionary controls. In order to satisfy the math model, it will not be necessary to certify the outer layer (which implements directories and ACLs). Therefore, formal specifications which define the kernel perimeter are being written for the interface to the inner layer only.

It was generally agreed that the lack of control over changes to the access matrix is a deficiency of the math model. However, it is not yet clear how or if this deficiency should be corrected. The most straightforward approach, of course, would be to augment the model to emulate the Multics ACL mechanism. Anything else would seem to imply an unacceptable incompatibility with the present Multics user interface. But even this approach seems uncertain with respect to certification. We, at Honeywell, still have many reservations about the prospect of attempting to certify discretionary controls. In particular, we do not know what the objectives of such an exercise would be. It is generally agreed that certification of the ACL mechanism is not

sufficient to fully enforce the need-to-know policy. Therefore, as pointed out in TCL 17, there must be some lesser objectives. But what are these objectives? What do we hope to prove?

One possible objective that was mentioned at the meeting was that of auditing. Clearly, auditing requires person identifications (i.e. user names) and object identifications (e.g. pathnames) which are, at present, thought to be features of the outer layer kernel. But do we merely want to assert the existence of an auditing mechanism, or do we want to formally prove something about it? This question, and others like it, remain unanswered.

It is apparent that the basic issues concerning discretionary controls have not been adequately considered. The very existence of such a major deficiency in the math model is evidence of this fact. We strongly recommend that before undertaking enhancements to the math model, the objectives pertaining to discretionary controls be determined. These objectives should be reviewed by all Project Guardian participants.

The program schedule currently being developed does not include certification of the ACL mechanism. Therefore, if a revised math model is developed and certification of the ACL mechanism becomes an Air Force requirement, the change in effort must be evaluated and the program schedule must be revised accordingly.

## INTEGRITY

The requirements for kernel-provided integrity controls are those of the mathematical model. The Air Force stated that no specific requirements exist for the user and administrative interfaces to the integrity mechanism. In general, these interfaces need not be so elaborate as the interfaces to the security mechanism because the application of integrity controls is recognized to be much more limited. In fact, at sites such as AFDSC, integrity controls are expected to be essentially unused. Whatever interfaces are developed must be sufficient to support a reasonable demonstration of the integrity mechanism. The design details are left to the discretion of Honeywell.