Informal Comments Rcvd 4/1

03/22/76 Decie WRP.TCL15.Comm.runoff

Comments on TCL No. 15

"Prototype Secure Multics External I/O Functional Description"

31 Jan 76

The technical note, "Prototype Secure Multics External I/O Functional Description", has been reviewed. The note represents a useful first step in the design of the external I/O design issues. However, the note contains several significant deficiencies and areas of concern. Positions are taken on several key issues without adequate substantiation. In certain areas, the exposition is vague, imprecise and incomplete. Because of these deficiencies which are discussed in more detail below, the external I/O design presented cannot be judged acceptable at this time.

The note takes the position that the certain areas of external I/O must be performed through a connection with the IOM. The note claims that the SFEP does not have the bandwidth necessary to support non-communications external I/O. A previous report, the SFEP trade study, claimed that the SFEP did have adequate capacity to perform all external I/O. Information to support the contention of inadequate

bandwidth should be presented. The constraints that the note places on external I/O make ~~use of~~ the IOM appear attractive. If the secure Multics were to maintain compatibility with existing Multics by supporting remote printers ~~and~~ RJE stations and network, it appears that certain functions would have to be duplicated in the kernel. The kernel would have to handle similar devices connected through both the IOM and SFEP.

Before the Air Force can accept a design which uses the IOM to perform external I/O, Honeywell must demonstrate that the IOM provides a suitable hardware base for secure I/O. The IOM does not currently provide such a suitable hardware base. The note alludes to proposed changes to the IOM to secure the IOM. Honeywell should describe the proposed changed and demonstrate the security of the modified IOM.

Certain areas of the report are vague and not clear. For example, one cannot immediately determine what interface the SFEP specifications are identifing -- the Multics user process to SFEP interface or the SFEP uncertified device control code to SFEP kernel interface. Sections and diagrams are omitted several places in the note.

The note eliminates the consideration of networks. This elmination is not acceptable. The Statement of Work

explicitly requires the consideration of networks. Honeywell should provide an interface to a representative packet switched network such as the ARPA net.

As is typical of Honeywell's ~~deliverables~~ reports, this external I/O note again reveals Honeywell's lack of the overall integration of the Project Guardian efforts. The note ~~contracts~~ disagrees the SFEP trade study's claim that the SFEP had the necessary capacity to perform all external I/O. The format and use of the specifications in the note appear inconsistent with previous specifications. The specifications are neither top-level nor non-procedural and ~~are~~ may not be amenable to verification. Honeywell's designers and verifiers should establish a set of guidelines for the development of specifications.

More detailed comments on the external I/O note can be found on the attached comments and on the attached annotated copy of the note.

2 Atch:

1. Detailed Comments

2. Annotated TCL #15

Detailed Comments on TCL #15

Page 4, Paragraph 1.1.1 Model Development -- Abstract models are not presented in the document.

Page 5, second paragraph -- The descriptions of all necessary kernel functions are incomplete.

Page 5, Paragraph 1.2.2 Networks not covered -- Intercomputer networks are not on the technical horizon, they are a reality.

Page 7, Paragraph 3.1 General Definitions -- The definitions of external I/O is not consistent with the previous definition of that term in the context of the ESD security program - the transfer of information between the internal (computer system) and external (people/paper system) environments.

Page 9, Paragraph 3.2.1 External I/O devices inherently ... -- While it may be reasonable to constrain user processes to operating I/O devices at their own security levels, it may still be desirable to think of some devices (e.g., printers) as being output-only, and others (e.g., card readers) as being input-only, in terms of their overall external I/O function.

Page 9, Paragraph 3.2.2 -- No simultaneous sharing ... Clause (2) appears contradictory because it is not in parallel with clause (1).

Page 9, Paragraph 3.2.4 -- I/O program must be validated . . . It is unclear what is being validated - the function of an I/O software module or a run-time check on access control.

Page 11, Paragraph 3.3.1 -- Two mechanisms needed . . . The constraint that no loss of efficiency is acceptable as a cost for achieving security seems overly restrictive.

Page 14, first paragraph -- Figure 3.4.2.1.1 is not supplied.

Page 14, Paragraph 3.4.2.2 -- All Device to Process Assignments ... Why is there no concept of a user process requesting to have a device assigned to it for communications external I/O? What is a remote printer conntected to the system by telephone lines considered?

Page 15, Paragraph 3.4.2.6 Naming of Devices -- This paragraph is not very clear. What is the security issue in device assignment?

Page 15, Paragraph 3.4.28.8 Multics - FEP Communication . . . -- Why are channels and buffers hidden?

Page 16, Paragraph 3.4.2.11 Real Delimiters -- Does the recognition by the kernel of a delimiter character imply interpretive I/O (and a performance penalty)?

Page 18, Paragraph 3.4.3.1 Attributes Maintained by Kernel -- In what sense does the kernel "validate" I/O operations? The discussion of identifier visibility is confusing.

Page 24, Paragraph 3.5 IOM External I/O -- Where is the description of the engineering considerations that are unique to the IOM? Paragraphs 3.5.1 and 3.5.2 are not adequate.

Pages 25-30, Paragraph 3.5.3.2.1 Functions . . . -- It is difficult to evaluate the specifications in this paragraph since no explanation or justification is given for any of them. It appears that the specifications are procedural and are not logically complete.