ESD-TR-76-165

(12) P. S.

MTR-3065

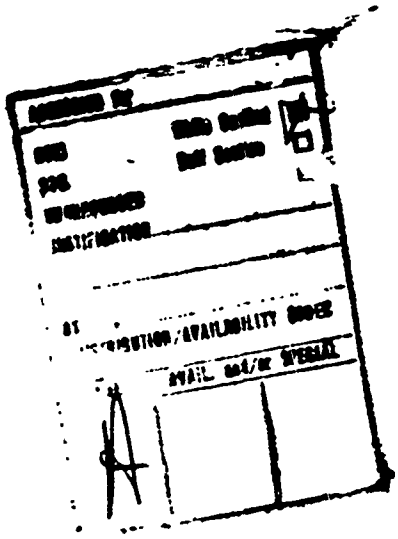
A SECURITY COMPLIANCE STUDY OF THE AIR FORCE DATA SERVICES CENTER MULTICS SYSTEM

DECEMBER 1976

Prepared for

DEPUTY FOR COMMAND AND MANAGEMENT SYSTEMS
ELECTRONIC SYSTEMS DIVISION
AIR FORCE SYSTEMS COMMAND
UNITED STATES AIR FORCE
Hanscom Air Force Base, Bedford, Massachusetts

Project No. 522C
Prepared by
THE MITRE CORPORATION
Bedford, Massachusetts
Contract No. F19628-76-C-0001



When U S Government drawings, specifications, or other data are used for any purpose other than a definitely related government procurement operation, the government thereby incurs no responsibility nor any obligation whatsoever; and the fact that the government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise, as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

Do not return this copy. Retain or destroy.

REVIEW AND APPROVAL

This technical report has been reviewed and is approved for publication.

Paul A. Karger

PAUL A. KARGER, 1Lt, USAF
Project Engineer

F. Wah Leong

F. WAH LEONG, Major, USAF
Project Officer
Air Force Data Services Center

FOR THE COMMANDER

Frank J. Emma

FRANK J. EMMA, Colonel, USAF
Director, Information Systems
Technology Applications Office
Deputy for Command & Management Systems

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

REPORT NUMBER: ESD-TR-76-165	2. GOVT ACCESSION NO.
3. RECIPIENT'S CATALOG NUMBER	
TITLE (and Subtitle): A SECURITY COMPLIANCE STUDY OF THE AIR FORCE DATA SERVICES CENTER MULTICS SYSTEM	5. TYPE OF REPORT & PERIOD COVERED
6. PERFORMING ORG. REPORT NUMBER: MTR-3065	
7. AUTHOR(s): R. C. Davis	8. CONTRACT OR GRANT NUMBER(s): F19628-76-C-0001
9. PERFORMING ORGANIZATION NAME AND ADDRESS: The MITRE Corporation, Box 208, Bedford, MA 01730	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS: Project No. 522C
11. CONTROLLING OFFICE NAME AND ADDRESS: Deputy for Command and Management Systems, Electronic Systems Division, AFSC, Hanscom Air Force Base, Bedford, MA 01731	12. REPORT DATE: DECEMBER 1976
	13. NUMBER OF PAGES: 28
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)	15. SECURITY CLASS. (of this report): UNCLASSIFIED
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

MULTICS
MULTILEVEL SECURITY
SECURITY COMPLIANCE

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

Do the hardware and software security features of the Air Force Data Services Center (AFDSC) Multics system comply with the Department of Defence security requirements? To answer this question AFDSC commissioned MITRE to undertake a study to compare intrinsic features of the AFDSC Multics system with the applicable requirements set forth in DoD Requirement 5200.28 and expanded upon in DoD Manual 5200.28-M.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

235050

ACKNOWLEDGMENT

This report has been prepared by The MITRE Corporation under Project No. 522C. The contract is sponsored by the Electronic Systems Division, Air Force Systems Command, Hanscom Air Force Base, Massachusetts.

TABLE OF CONTENTS

SECTION I

INTRODUCTION

Do the hardware and software security features of the Air Force Data Services Center (AFDSC) Multics system comply with the Department of Defense security requirements? To answer this question AFDSC commissioned MITRE to undertake a study to compare intrinsic features of the AFDSC Multics system with the applicable DoD requirements. As a result of this study we conclude that the security features of the AFDSC Multics system exhibit a high degree of compliance with all the applicable requirements set forth in DoD Directive 5200.28 and expanded upon in DoD Manual 5200.28-M.

BACKGROUND

The AFDSC has a requirement to provide Automatic Data Processing resources and services for the processing of Unclassified through Top Secret data as support to Headquarters USAF and the Office of the Secretary of the Defense. To meet this requirement AFDSC commissioned a joint Security Design Analysis team comprised of representatives from AFDSC, USAF Electronic Systems Division, The MITRE Corporation, and Honeywell Information Systems. The analysis team concluded that a Honeywell Multics system, with additional software controls, provides a reasonable assurance that no Top Secret information can be leaked to a Secret cleared individual, and that "need to know" can be implemented within these security classification categories. The analysis team also concluded that such a system is acceptable for operation in a controlled multi-level mode, where access to the system is restricted to Secret and Top Secret cleared individuals. This current MITRE study investigates whether Multics with security enhancements (henceforth referred to as Multics) complies with all the DoD security requirements.

MULTICS SECURITY CONTROLS

Multics contains a variety of hardware and software features that are supposed to provide secure operation. For the reader who is not

familiar with these controls, we provide a brief overview of the basic Multics security controls.[1]

Hardware Security Controls

Segmentation Hardware.

The most fundamental security controls in the HIS 68/80 Multics are found in the segmentation hardware. The basic instruction set of the 68/80 can directly address up to 64K segments at any one time, each segment being up to 256K words long. Segments are broken up into 1K word pages which can be moved between primary and secondary storage by software, creating a very large virtual memory.

Segments are accessed by the 68/80 CPU through segment descriptor words (SDW's) that are stored in the descriptor segment. Each SDW contains the absolute address of the page table for a segment and the access control information. The access control information determines user's access rights to the segment - read, execute, write, etc.[2] Note that by using this access control information, the supervisor can protect the descriptor segment from unauthorized modification by denying access in the SDW for the descriptor segment.

Protection Rings.

An additional hardware security control on the 68/80 Multics system is the ring mechanism. The ring mechanism extends the traditional privileged/slave mode relationship of conventional machines to permit layering within the supervisor and within user code [8]. Eight concentric rings of protection, numbered 0 - 7, are defined with higher numbered rings having less privilege than lower numbered rings, and with ring 0 containing the "hardcore" supervisor. Execution of privileged mode instructions is confined to ring 0. Each SDW specifies the allowed access to each segment, for each ring of execution.

Software Controls

One advantage of Multics over other conventional systems is that

---

[1]The contents of this section were compiled from papers written by Karger [1] and Whitmore [2]. A more complete discussion of the various security controls can be found in Lipner [3], Saltzer [4], Organick [5], and the Multics Programmers Manual [6].

[2]A more detailed description of the SDW format may be found in the processor manual [7].

the military clearance and classification[3] controls have been designed into the Multics. The basic component of these controls is the implementation of the concept of a reference monitor -- an abstract mechanism that controls access of subjects (active system elements) to objects (units of information) within the computer system [9]. An implementation of a reference monitor must meet three requirements: 1) it must be tamperproof; 2) it must always be invoked; and 3) it must be small, simple, and understandable so that it can be completely tested and certified to perform its functions properly [10]. The Multics implementation of this abstraction consists of the "ring_0" supervisor in conjunction with processor hardware protection mechanisms.

Each person registered on Multics is known to the system by his name (person-id) and his project (project-id), has a password to authenticate his identity, and a clearance used to determine the information that the user has been cleared to observe. Multics uses this information to ensure that a person cannot use the system to obtain information that he is not entitled to (i.e. that a person can only have access to information for which he has both a security clearance and a "need to know"). To obtain service the user logs in and provides the system with the necessary data for authentication. Upon completion of the authentication, Multics creates a process for the user, identified by the user's process-id[4] and by a process unique-id. Both of these identifiers are unforgeable and remain constant for the life of the process. In addition to the identifiers, Multics also assigns to a process a clearance that is constant for the life of the process. This clearance is the minimum of the following: the user's clearance, his project's clearance, the maximum clearance of the terminal from which the user is logging in, and the clearance specified by the user before the process is created. The user must change processes when he desires to change his current working clearance.

A process is the only subject on Multics. The set of objects are segments, directories, I/O channels, and interprocess messages. All objects are protected according to a classification, assigned when the object is created. Only the system security administrator is author-

---

[3]Within this paper the terms clearance and classification refer to the combination of both a level, e.g. Top Secret or Secret, and a set of categories, e.g. Crypto, NATO. The terms "access," "class," and "authorization," used in Multics documentation also refer to this combination of level and categories. Other literature on multi-level computer security use the terms clearance and classification to refer to only the level component, the dual combination being referred to as a security level.

[4]A process-id is a combination of the user's user-id, his project-id, and an instance tag.

ized to change the classification of an object.

Multics compares the clearance of the process to the classification of an object each and every time a process attempts to access an object in order to ensure that the user of the process has the proper clearance to perform the desired operation (e.g. read, write, execute, append, modify, delete, etc.) Whenever Multics compares the clearance of a process with the classification of an object four relationships are possible.

less than

equal to

greater than

isolated from

The clearance of a process is considered to be "equal to" the classification of an object if:

1. both have the same level, and

2. both have identical category sets.

The classification of an object is considered "less than" the clearance of a process if:

1. the level of the classification is less than or equal to the level of the clearance, and

2. there are no categories in the category set of the classification that are not included in the category set of the clearance, and

3. the clearance is not "equal to" the classification.

The classification of an object is considered "greater than" the clearance of a process if:

1. the level of the classification is greater than or equal the clearance, and

2. there is no category in the category set of the clearance that is not included in the category set of the classification, and

3. the clearance is not "equal to" the classification.

The classification of an object is considered to have a relationship of "isolated from" the clearance of the process if:

> the classification of the object is neither "less than", "equal to", or "greater than" the clearance of the process.

In order for a person to access information, the military security system requires that the clearance of the person be "greater than" or "equal to" the classification of the information. A sufficient condition for satisfying this requirement within the computer system environment is the enforcement of the following two rules:

1. A process having a clearance n may not "read up", i.e. read an object having a classification "greater than" n.

2. A process having clearance n may not "write down", i.e., write an object having a classification "less than" n.

The first of the rules, referred to as the simple security condition, directly implements the military security system, insofar as clearance requirements are concerned. The second rule, the *-property, prevents accidental or malicious disclosure of information due to actions of user programs. With these aforementioned two rules enforced, it is impossible for any process to: 1) extract information from an object of a higher classification; or 2) to transfer information from an object of higher classification to an object of a lower classification. Hence, no compromise of classified information can occur. A further restriction is also desirable which forbids a process to write in an object of higher classification whenever writing can be used to destroy information. In order to provide some protection against sabotage, "write up" operations are not permitted for such objects as segments, and directories.

It is important to recognize that the rules described above represent a sufficient, but not a necessary condition for achieving security. Although the *-property restrictions are strictly enforced for all user processes, they are, in certain circumstances, relaxed for trusted processes that are part of Multics. In no circumstances, however, is the security of the system violated.

In addition to the formal clearance and classification controls, the individual user is also able to specify which users have "need-to-know" for a given segment or directory by use of the Access Control List. The Access Control List is a list of users who are allowed to access the segment or directory in a given mode of access when they have the proper clearance as defined by the formal controls. No user can access a segment or directory unless someone has extended to him the proper need-to-know for that object.

Multics can be logically divided into two environments: internal and external. The internal environment is totally controlled by Multics and includes: processors, memory, disk drives, I/O multiplexors, bulk store, communication processors, and tape drives used for system functions. The external environment can be directly influenced by the actions of a process. Included in the external environment are: terminals, line printers, card readers, card punches, non-system tape drives, and other devices of the I/O class not used for system functions. To provide a "secure" pipeline between the internal and external environments, Multics performs the actual information transfer on behalf of the user, giving a reasonable assurance that failures or "software bugs" in I/O software can not be exploited by a user. The terminal is the only exception to this rule. Users may perform direct I/O to the terminal that the system has attached to the process. Terminal software has been carefully checked out in an effort to eliminate software errors. The exception for terminals is only made for the sake of efficiency.

SCOPE

This compliance study is concerned only with the DoD hardware and software security requirements. Additional requirements must also be met for the system to be considered secure. These include requirements for physical protection and policies for administration of the system [11], [12], [13]. Although these issues are important to the overall security of the system we felt the addition of Multics at the AFDSC site would have little, if any, effect on them, since AFDSC already has a secure environment. Therefore, requirements for physical security and administrative policy are only reviewed if the addition of Multics might have some effect on the controls already in effect at the AFDSC.

The remainder of this report is divided into two sections. In Section II the seven minimum requirements that "insofar as possible" must be complied with [14] are reviewed. The reviews are in the form of a quotation of the requirement followed by Multics compliances.

In Appendix I an item by item comparison is undertaken between the guidelines for the particular techniques and procedures needed to implement the seven requirements [15] and the particular security controls provided by Multics.

SECTION II

COMPLIANCE TO DoD DIRECTIVE 5200.28

Department of Defense Directive 5200.28 establishes a policy for protecting data handled by an Automatic Data Processing (ADP) System and defines administrative responsibilities for assuring the security policy is carried out. It is intended that the AFDSC Multics system process Unclassified thru Top Secret data in a controlled multi-level mode, where access to the system is restricted to Secret and Top Secret cleared individuals. Therefore the system must comply to the Minimum Requirements as set forth in DoD Directive 5200.28. Each of the following subsections consist of a requirement from Section VI of 5200.28 followed by a discussion of the compliance.

INDIVIDUAL ACCOUNTABILITY

> IV.A.1 Each user's identity shall be positively established, and his access to the system, and his activity in the system (including material accessed and actions taken) controlled and open to scrutiny.

The Multics system complies with the requirement for individual accountability by authenticating the individual before allowing access to the system and by ensuring that once access is allowed and a process for the individual is created, a correspondence can always be made between the process and the individual for whom the process was created. The principal means of making this correspondence is the process-id, an unforgeable identifier consisting of a combination of the individual's name, his project, and an instance tag. The process-id together with the process's clearance,set only when the process is created (see Section I), are characteristic datum used to control the individual's activities on the system. No action is possible unless the individual is authorized to perform the action.

Multics establishes the correspondence between the process-id and the individual by means of a system generated pronounceable password [16]. At each login the individual presents the system with his name and password. The system verifies the correctness of the password before allowing the individual to proceed. Incorrect login attempts are audited to assure that an unreasonable number of incorrect passwords

is not used to verify the correspondence between the user name and password. Periodic changing of the passwords is at the discretion of the System Security Administrator.

Upon completion of the initial login a message is sent by the system to the system log indicating the name of the individual who logged in, from what terminal the login originated, and at what time the login occurred. In this way an individual's usage of the system is open to inspection. Similarly, each logout is also recorded in the system log.

To increase the effectiveness of the controls certain other actions are recorded. These actions include an attempt to access a segment or directory with improper authorization, illegal procedure faults, attempts to "send down" an Inter-Process Communication message to a process having improper authorization, rejection of requests for attachment of I/O devices, and all setting and resetting of the system privilege bits.[5]

ENVIRONMENTAL CONTROL

> IV.A.2 The ADP system shall be externally protected to minimize the likelihood of unauthorized access to system entry points, access to classified information in the system, or damage to the system.

The addition of the Multics system to the Air Force Data Services Center Computer Center does not adversely affect the physical security controls already in effect.[6]

SYSTEM STABILITY

> IV.A.3 All elements or components of the ADP Systems shall function in a cohesive, identifiable, predictable, and reliable manner so that malfunctions are detected and reported within a known time.

---

[5] System privilege bits must be set before performing operations that bypass certain security controls.

[6] A discussion of the physical security controls appear in Wilson [12], Irvin [13], AFDSCR 171-1 [17], and AFDSCR 300-8 [11].

Multics complies with the requirement for system stability by providing cohesive documentation on system software [6] and by having available a set of test procedures that test the proper operation of the security related features.

The tests for Multics are divided into hardware tests [18] and software tests [19]. The hardware tests check the reliability of the hardware operations. Understandably each possible hardware state cannot be explicitly checked. However an extensive analysis of features closely related to security can be undertaken. The analysis of the hardware is performed by a system subverter, a utility invoked periodically to audit the status of the system. The subverter checks for the proper operation of all possible machine instructions, the segment access controls, and the ring structure. Should the result of a test indicate abnormal system behavior the operator is notified, thereby enabling corrective actions to be taken. The results of all tests are recorded to aid in determining the frequency of future tests.

The software tests are designed to aid in the verification that the security controls perform exactly as specified. On Multics the ring structure provides a mechanism for layering software controls. The software tests check the most primitive operations available to the user to ensure that a user cannot bypass the security controls. If an error is detected the operator is notified, thereby allowing corrective measures to be performed. The areas tested are the process clearance assignment, access to segments, access to directories, communication between processes, auditing, the system security administrator commands, and access to I/O.

DATA INTEGRITY

> IV.A.4 Each file or collection of data in the ADP System shall have an identifiable origin and use. Its accessibility, maintenance, movement, and disposition shall be governed on the basis of security classification and need-to-know.

As pointed out in Section I a primary advantage of the Multics system with security enhancements is that data integrity has been designed into the system. Multics bases its security policy on a mathematical model [20] [21]. The model states that an individual cannot access any information above his security clearance. In addition, even if an individual has the proper security clearance to access information, that individual must still have been extended the proper need-to-know. To prevent accidental or malicious disclosure, the model also requires that an individual's process cannot inadvertently or deliberately transfer information to an object that has a classifica-

tion lower than the process's security clearance.

By adhering to the mathematical model, Multics complies to the requirements on data accessibility, maintenance, and movement. Deletion of a file on the system is governed by security classification and need-to-know. The Model's security rules also apply to input and output. Therefore, the Multics system complies with the requirement of disposition.[7]

SYSTEM RELIABILITY

> IV.A.5 The system shall function so that each user has access to all of the information to which he is entitled, but no more.

Multics complies with the requirement for system reliability by providing clearance and classification controls, need-to-know access controls, and a hardware access control mechanism that divides the system into eight linearly ordered domains [22]. These domains, referred to as rings (see Section I), provide an additional means of restricting the process's address space. To deny direct access to system information that an individual does not have the right to observe or modify, Multics places the system information in a ring that the individual's program is not able to access directly. The hardware enforces the access control mechanisms by checking access before each and every memory reference.

COMMUNICATION LINKS

> IV.A.6 These links and lines shall be secured in a manner appropriate for the material designated for transmission through such lines or links.

Multics will handle material up to a classification of Top Secret. In order to comply with this requirement, communication lines are encrypted in a manner suitable for the information.

CLASSIFIED MATERIAL

> IV.A.7 Such material handled and produced by the ADP System or stored in or on media for recording

---

[7] See Section I for a more detailed discussion of the access controls provided by Multics.

> classified material material shall be safeguarded as appropriate for the classification assigned to the information.

On Multics, before each item of printed output is produced, a nonsuppressible security banner is printed. In addition security labels are printed, at the option of the individual user, at the top and bottom of each page of output [23]. With each piece of printed output, an accountability form is also produced containing the name of the individual who requested the output, the name of the document produced, the classification of the document, and other information useful in the distribution of classified material.

Magnetic tapes produced by the Multics system can only contain information of a single security level, defined manually by the operator before the tape is mounted [24]. Likewise card output can only occur at a single security level, defined to be the current level of the card punch. A security level banner is punched preceding each punched deck to provide a greater level of security protection. Upon removal from the system, manual security controls apply to all types of output [11].

Because all forms of output follow the guidelines set forth in 5200.28, Multics complies with the requirement that classified material produced be safeguarded as appropriate.

The security controls, mentioned in Section I, control all access to classified material handled within the computer system regardless of the media the data is stored on. All media used for the storage (including Backup Tapes and Dump Tapes) of classified material within the system is classified Top Secret [2], and may not be removed from the installation without applying the appropriate physical security controls [11].

SECTION III

CONCLUSION

After a thorough examination of the security features and measures provided by Multics, we conclude that Multics meets the objective of Department of Defense Directive 5200.28. Multics provides a combination of hardware security controls (including segmentation, rings, and a virtual memory) and software security controls (the implementation of the military clearance, classification, and need-to-know controls). In a secure environment, these controls provide the user with accountability, stability, integrity, reliability, and protection of classified material controls. Multics is thus suitable to handle Unclassified through Top Secret data in a controlled multi-level environment, where access is restricted to Secret and Top Secret cleared individuals.

APPENDIX I

COMPLIANCE TO DoD MANUAL 5200.28-M

In this appendix facilities provided by Honeywell's Multics system are compared to the techniques and procedures set forth in ADP Security Manual 5200.28-M. The purpose of 5200.28-M is to provide guidance to aid in meeting the general objective of having a dependable secure computer system. Sections of 5200.28-M discuss the developing, designing, acquiring, analyzing, testing, evaluating, establishing and approving of methodologies, standards, criteria, specifications, techniques and procedures to be used in securing an ADP computer system. Honeywell has addressed the objective of developing a secure computer system in two ways: 1) by examining any module that might deal with security to ascertain that the security controls cannot be circumvented; and 2) by developing access controls suitable for secure multilevel operation, in a controlled environment [2]. Because it's designers specifically addressed circumvention and access control mediation, Honeywell's Multics system can be expected to have a dependable secure computer system.

Following is an item by item comparison between each of the specific hardware and or software requirements set forth in 5200.28-M and the security measures provided by the Multics system. Unless otherwise stated Section numbers used within this Appendix refer to Section numbers of 5200.28-M.

PERSONNEL SECURITY SECTION II

Clearance and Access Controls II.1

Section II covers Personnel Security Clearance and Access Controls. Personnel Security Clearance and Access Control are discussed in the Security Procedures Manual [13].

PHYSICAL, COMMUNICATIONS, AND EMANATIONS SECURITY SECTION III

Section III of DoD 5200.28-M deals with Physical, Communications, and Emanations Security. The requirements covered are fulfilled by the procedures specified in the AFDSC installation Security Procedures Manual.

HARDWARE/SOFTWARE FEATURES SECTION IV

Hardware IV.2

Section IV, Part 2, of 5200.28-M presents hardware requirements for a secure computer system. Each of the 11 requirements presented is reviewed below. A more complete description of the hardware features discussed can be found in Section I of this compliance report.

4-200 Hardware Features

Paragraph 4-200.a defines the requirement for protected state variables. The Multics system provides 8 levels of isolation in the form of concentric hardware rings. A process's current ring of execution defines the set of executable instructions. The operating system and security sensitive data reside in the most protected rings.

Paragraph 4-200.b deals with the ability of a processor to access locations in memory. A processor can only access segments through segment descriptor words (SDWs) defined in a descriptor segment. Each SDW contains access bits, defining the allowable mode of access to specified memory locations, in each ring of execution. The access control bits are only set if the processor has the proper classification and need-to-know.

Paragraph 4-200.c deals with controlling the availability of certain instructions. The 68/80 processor has two modes of execution, privileged and non-privileged. Security sensitive instructions, such as the instructions performing input and output, can only be executed in privileged mode. Privileged mode is protected by restricting its use to processes executing in ring 0, the most privileged ring.

Paragraph 4-200.d states that all possible operation codes should produce known responses. Operation codes on the 68/80 are tested by a hardware subverter [18]. The subverter dynamically checks each instruction against known results. Should an unknown response ever be found the subverter notifies the system operator.

Paragraph 4-200.e deals with error detection of registers fundamental to the secure operation of the system. The use of these registers is restricted to processes in the proper mode and ring of execution [7]. In addition, the hardware subverter checks these registers for reliability errors.

Paragraph 4-200.f states that all registers that can be loaded by the operating system should also be storable. All registers on the 68/80 are storable by the operating system [7].

Paragraph 4-200.g states that error detection should be performed on each fetch cycle of an instruction. On the 68/80 each memory access is controlled by addressing a segment through a segment descriptor word (SDW). Detectable errors include address out of range and improper authorization to access [7].

Paragraph 4-200.h expands the need for error detection to include transfers of data between memory and storage devices. The 68/80 provides error detection, parity checks, and in some cases redundancy checks on transfers to and from bulk store, disk, the system controller and the CPU.

Paragraph 4-200.i deals with automatic programmed interrupts. The 68/80 provides a programmable fault vector that determines actions to be taken when system or operator malfunctions occur [7].

Paragraph 4-200.j states that the identity of remote terminals should be controlled by hardware. On the 68/80 each remote terminal is connected to a port (channel). Channel numbers are fixed in hardware allowing the operating system to positively establish the identity of each terminal [2].

Paragraph 4-200.k identifies the need for verifying the read, write, and execute access rights of a user on each fetch cycle of an instruction. As stated in Section I of this compliance report, all access to information is controlled in hardware by the use of SDWs. Included in each SDW are the user's read/write and execute rights.

Software IV.3

4-300 General

Paragraph 4-300 identifies the need to: 1) separate the control part of the operating system from the user; and 2) to keep the control part as small as possible. The Multics system complies with this requirement by: 1) only having a few central sections of the operating system execute in privileged mode; and 2) having all the modules necessary for the secure operation of the system execute in the most privilege rings, the rest of the operating system executes in the same ring as other user programs.

4-301 O/S Control

Paragraph 4-301 identifies the minimum controls the operating system shall contain. Each requirement is reviewed below. Further information on the security features of the Multics software can be found in Section I of this compliance report.

Paragraph 4-301.a requires the operating system to control all transfers of material between memory and on line storage, between the central computer facility equipment and any remote device, or between on line storage devices. The Multics system is a virtual memory system and as such the operating system controls all transfers between memory. On line storage on Multics is considered an extension of memory and thus, is controlled by the operating system. The Multics system also controls all output to and input from remote devices.

Paragraph 4-301.b requires that the operating system control allocation of all system resources, memory protection, system interrupt and shifting between user and master modes. The Multics system controls the allocation of all system resources. Memory protection is accomplished by the operating system controlling segment descriptor words. System interrupts are handled by the operating system. Privileged mode protection is controlled because the operating system receives control at a known place when the user attempts to enter privilege mode.

Paragraph 4-301.c requires that access to system utilities be controlled. The Multics system controls access to these utilities by the use of Access Control Lists (ACLs). Only those users who have a definite need to access or use these utilities are included on the ACLs.

Paragraph 4-301.d requires the operating system to control the user program's access to material and requires the operating system to control the user identification system. The Multics operating system controls user access to material by using security classification and need-to-know controls. The user identification system is also controlled by the operating system.

4-302 Test and Debugging Programs

Paragraph 4-302 requires that only programs that do not violate the security or integrity of the system may be debugged during system operation. This requirement is adhered to by the Air Force Data Services Center.

4-303 Clear System Procedures

Paragraph 4-303 requires that procedures be available for clearing from the system all classified material during operation of the system without the required protection. Although procedures exist for system clearing [13], the AFDSC Multics system always operates in a controlled environment with a maximum classification of Top Secret.

4-304 Shutdown and Restart

Paragraph 4-304 requires the operating system to provide security safeguards to cover system shutdown (both scheduled and unscheduled) and subsequent restarts On Multics shutdown and restart are under the control of the operating system. When a shutdown occurs, communication between the front-end processor and Multics is severed by the operation system. Severing the communication lines removes any possibility that a user could access the system until the system restarts.

4-305 Other Fundamental Features

Paragraph 4-305 lists other features of the operating system considered fundamental to the secure operation of the system. In addition, paragraph 4-305 requires that attempts to circumvent the security controls be detectable, reported within a known time, and recorded in the audit log. The requirement for an audit log will be discussed in the following subsection of this report. Each of the six additional features in paragraph 4-305 are reviewed below.

Paragraph 4-305.a requires that the operating system control resource allocation, memory access outside assigned areas, and the execution of master mode instructions. The Multics operating system handles resource allocation by controlling segmentation and demand paging routines. All pages are allocated or removed from memory by the operating system. Memory access outside the assigned areas is controlled by a combination of hardware and software controls. The operating system controls the fields of the hardware SDW's and page tables while the hardware performs checks on the values in these fields. Multics controls the execution of master mode instructions by: 1) only allowing execution of these instructions in the most privileged ring; and 2) by controlling the access control lists on the entry gates to this privileged ring.

Paragraph 4-305.b requires that the system ensure that classified material or critical elements of the system do not remain as accessible residue in memory or on on-line storage devices. A process can only directly access memory by accessing a segment. Multics will not let a process access a segment unless the process has the proper security clearance, the process is in the proper ring, and the name of the process is on the access control list of the segment. When a process attempts to access an authorized segment that is not in main memory, the operating system transfers the segment into addressable memory, overwriting any residual data. The operating system also removes residual data when new pages are created, by writing zeroes into all addresses in the new page, before access is allowed. Therefore accessible memory can only contain zeroes or information that the process is entitled to observe.

Paragraph 4-305.c of DoD 5200.28-M deals with the requirement for a System Security Officer. On Multics, the System Security Officer, referred to as the System Security Administrator, has the responsibility: to assign users' security clearances, to periodically force users to change their passwords, to repair any security related inconsistencies, and to downgrade information [2]. These functions comply with the requirements set forth.

Paragraph 4-305.d requires that there be appropriate security labels on all data input to, stored in, or output from the ADP system. The Multics system keeps a security label for each segment on the system. The security label: 1) identifies the sensitivity of the information; 2) is used to control the accessibility of the segment; and 3) can only be decreased by an action of the System Security Administrator. The nonsuppressible security banner, printed with each output, is never less than the security label of the segment, and is used in the determination of the label printed on the output. Security labels are discussed further in Section II of this report under the requirement for Data Integrity.

Paragraph 4-305.e states that administrative and/or hardware/software measures be established to assure that terminals are protected and are authorized access to specific levels of information. AFDSC meets these requirements by: 1) providing software controls that specify the highest level of the information that can be accessed from each terminal; 2) restricting access to terminals to properly cleared personnel; and 3) placing all terminals in areas that provide protection to the highest level of information that can be accessed.

Paragraph 4-305.f requires that the user and/or the group of users to which the individual user belongs must be accurately identified to the ADP system. Users are identified to Multics by a combination of: 1) a user name; 2) a user project; and 3) a password that was system generated. A security clearance of a process is determined by the lesser of: 1) the security clearance of the room in which his terminal resides; 2) the security clearance the user gives as a parameter when logging into the system; 3) the user's own clearance; 4) his projects clearance; and 5) his clearance on the project.

AUDIT LOG OR FILE SECTION V

5-100 Application

Paragraph 5-100 requires that an audit file or log be maintained to record security related transactions. Multics complies with this requirement by compiling two system logs: the System Log and the

Syserr Log.

The System Log records normal system entry and exit, denied system entry, and installations of new system tables dealing with user names, projects, and authorizations.

The Syserr Log contains entries for: initiations of protected segments, denied access to any segment or directory, access violation faults, illegal procedure faults, attempts to "send down" an IPC message to a process having an improper authorization inconsistencies in the file hierarchy, rejection of requests for attachment of devices, and setting and resetting the system privilege bits.

In addition to the logs compiled by the system, an accountability form is produced with each printed output. The accountability form includes the user name, project, date and time requested, classification, pathname, sequence number, printed name of document, and places for the signatures of the carrier and recipient if needed.

BASIC SAFEGUARDS SECTION VI

Section VI of the manual discusses classified material "removed from the custody of the system" and, as such, does not fall within the scope of this compliance study. Controls dealing with the removal of classified material previously in effect at AFDSC remain in effect.

ERASE AND DECLASSIFICATION PROCEDURES SECTION VII

Part 1 of Section VII requires that, "each memory location used for the storage of classified data shall be overwritten when it is no longer required, before reutilization, or before the content of the location may be read to preclude the unauthorized disclosure of classified data". Multics does exactly that by preventing unauthorized access to a segment, and by overwriting memory before a process is allowed to access an authorized segment. A user's process can only gain access to main memory by accessing a segment. The only segments accessible are active ones to which the user explicitly has access. When the user accesses a given segment, that segment, or part of it, is placed into main memory, overwriting whatever was there before. Creating a new page in a segment causes memory to be overwritten with zeroes before access to the new page is allowed. Therefore, accessible memory can only contain zeroes or information that the process is entitled to observe.

Section VII, Parts 2 and 3 discuss erase procedures. Erase procedures are operational policies outside the scope of this compliance

study. Procedures already in effect at AFDSC should require no change.

SPECIFICATIONS FOR MAGNETIC TAPE ERASE EQUIPMENT SECTION VIII

Section VIII states the specifications for magnetic tape erase equipment. Magnetic tape erase procedures were not specifically addressed by this compliance study. Procedures previously in effect continue unchanged with the addition of the Multics system.

SECURITY TESTING AND EVALUATION (ST&E) SECTION IX

Section IX, Parts 1 and 2, deal with the security testing and evaluating of the security controls provided by the ADP system. On the Multics system security testing is divided into two parts: hardware testing and software testing. The hardware tests are made by a subverter program [18] that, among other things, attempts to subvert the system by executing illegal hardware instructions. The purpose of the subverter program is to find hardware errors that a penetrator could use to bypass the software security controls. In an effort to find hardware errors in a reasonable time, the subverter is run periodically as a normal Multics job.

Software security controls are tested periodically by running a series of programs that check the correctness of the various controls [19]. Each major section of the system has its own set of test procedures. These test procedures are run each time the software is changed to reduce the possibility of introducing security errors into the system. In addition, these test procedures are run periodically to insure that the software is properly handling security related events.

REFERENCES

1. P. A. Karger and R. R. Schell, "Multics Security Evaluation: Vulnerability Analysis", ESD-TR-74-193, Volume II, Electronic Systems Divison (AFSC), L. G. Hanscom Field, Bedford, Massachusetts, June 1974.

2. Honeywell Information Systems, "Design For Multics Security Enhancements", ESD-TR-74-176, Electronic Systems Division (AFSC), L. G. Hanscom Field, bedford, Massachusetts, December 1973.

3. Steven B. Lipner, "Multics Security Evaluation: Results and Recommendations", ESD-TR-74-193, Vol. 1. (in preparation.

4. J. H. Saltzer, "Protection and the Control of Information in Multics", Communications of the ACM, Volume 17, Number 7, July 1974, pp. 388-402.

5. E. I. Organick, The Multics System: An Examination of Its Structure, MIT Press, Cambridge, Massachusetts, 1972.

6. Multics Programmers' Manual, AG91, AG92, AG93 and AK92, Honeywell Information Systems Inc., 1975.

7. Honeywell Information Systems, "Summary of the H6180 Processor", May 1973.

8. R. M. Graham, "Protection in an Information Processing Utility", Communications of the ACM, Volume 11, Number 5, May 1968, pp. 365-369.

9. "ESD 1974 Computer Security Developments Summary", MCI-75-1, Electronic Systems Division (AFSC), L. G. Hanscom Field, Bedford, Massachusetts, December 1974.

10. S.B. Lipner, "Computer Security Research & Development Requirements", MTP-142, The MITRE Corporation, Bedford, Massachusetts, February 1973.

11. Air Force Regulations, "Security Requirements for Automatic Data Processing Systems", AFR-300-8, September 1974.

12. C.A. Wilson, "Air Force Data Services Center Security Procedures", MTR-2833, Volume I, The MITRE Corporation, Bedford, Massachusetts, June 1974.

REFERENCES (Concluded)

13. W.L. Irvin, G.A. Nelson, and C.A. Wilson, "Air Force Data Services Center Security Procedures Manual", MTR-2833, Volume 2, The MITRE Corporation, Bedford, Massachusetts, June 1974.

14. Department of Defense, "Security Requirements for Automatic Data Processing (ADP) Systems", Department of Defense Directive 5200.28, December 18, 1972.

15. Department of Defense, "Techniques and Procedures for Implementing, Deactivation, Testing, and Evaluating – Secure Resource-Sharing ADP Systems", Department of Defense Manual 5200.28-M, January 1973.

16. M. Gasser, "A Random Word Generator", ESD-TR-75-97, ESD, Hanscom AFB, Bedford, Massachusetts, 1975.

17. Air Force Data Services Center Implementing Regulation, Department of Defense AFDSCR-171-1, August 1974.

18. K. Hennigan, "Hardware Subverter for the Honeywell 6180", ESD-TR-76-352, ESD, Hanscom AFB, Bedford, Massachusetts, December 1976.

19. M. Gasser, S.R. Ames, Jr., and L. Chmura, "Test Procedures for Multics Security Enhancements – Final Version", ESD-TR-76-164, ESD, Hanscom AFB, Bedford, Massachusetts, June 1975.

20. K.G. Walter, W.F. Ogden, W.C. Rounds, F.T. Bradshaw, S.R. Ames, Jr., and D.G. Shumway, "Primitive Models for Computer Security", ESD-TR-74-117, Case Western Reserve University, Cleveland, Ohio, January 1974.

21. D.E. Bell and L.J. LaPadula, "Secure Computer Systems", ESD-TR-73-278, Volume I-III, The MITRE Corporation, Bedford, Massachusetts, November 1973 – June 1974.

22. M.D. Schroeder and J.H. Saltzer, "A Hardware Architecture for Implementing Protection Rings", Communications of the ACM, Volume 15, Number 3, March 1972, pp. 157-170.

23. Honeywell Information Systems, "Third Formal Design Review for the Multics Security Controls Implementation", February 1975.

24. Honeywell Information Systems, "Minutes of the Second Formal Design Review for the Multics Security Controls Implementation", November 1974.