# A COMPARATIVE STUDY OF IBM, HONEYWELL, UNIVAC AND CONTROL DATA OPERATING SYSTEMS

January 1973

RISOS

RESEARCH IN SECURED OPERATING SYSTEMS

University of California
Lawrence Livermore Laboratory
Livermore, California
94550

Sponsored by Advanced Research Projects Agency
ARPA Order No. 2166

## INTRODUCTION

This study has a twofold purpose. The first is to present an overview of the large scale computers installed at DOD and AEC facilities. Many of these computers are operated under various types of security requirements and have operating systems designed to resist unauthorized use or control. The second purpose of this study is to supply as many facts as possible about the operating systems that predominate at DOD and AEC installations, with special reference to those aspects that particularly bear on operating system security. It can be seen from Table 1, a census of computers and their locations, that computers at DOD and AEC installations mainly come from four main sources: IBM, Univac, Control Data Corporation, and Honeywell Information Systems. In Tables 2, 3, and 4 operating systems of these four manufacturers are broken down and listed so that their characteristics can be compared. Specifically, the following four operating systems will be looked at in detail:

a. IBM's OS/MVT for the 360/370 series

b. Honeywell GCOS III

c. UNIVAC EXEC-8

d. Control Data Corporation's SCOPE 3.4

In Table 2 the basic parameters of these operating systems such as word length, size, SYSGEN times, etc. are listed and, where applicable, their derivation is explained.

Table 3 lists operating system characteristics of a more detailed nature. In this table, however, the characteristics are not only listed but are also explained or defined and basic differences between them are presented.

Table 4 compares the complete range of IBM supervisor calls (SVC's) with the equivalent operating system features of Honeywell, UNIVAC, and CDC. Supervisor calls are particularly significant from the point of view of operating system security because they are one of the most logical areas from which attempts to gain control of the system can be made.

TABLE 1. Census of Large Scale Computer Systems at DOD and AEC Facilities

| Computer System | Number at DOD Facilities | Number at AEC Facilities |
|---|---|---|
| IBM 360/50 | 61 | 6 |
| IBM 360/65 | 40 | 6 |
| IBM 360/67 | 17 | 0 |
| IBM 360/75 | 11 | 3 |
| IBM 360/85 | 2 | 0 |
| IBM 360/91 | 2 | 2 |
| IBM 360/95 | 2 | 0 |
| UNIVAC 1108 | 39 | 1 |
| CDC 6000 series | 8 | 20 |
| CDC 7600 | 0 | 6 |
| Honeywell 600 series | 14 | 0 |
| XDS Sigma 7 | 6 | 3 |
| DEC PDP-10 | 0 | 14 |

Note: For purposes of this listing, a large scale computer is defined as being roughly equivalent to or larger than an IBM 360/50 in terms of speed, computing power, throughput, etc.

TABLE 2. Comparison of Basic Operating System Parameters

| Operating System | Word Length | Instruction Length | Size of Resident OS | Size of Basic OS | Size of Total OS | SYSGEN TIME | |
|---|---|---|---|---|---|---|---|
| | | | | | | Warm Start | Cold Start |
| IBM OS-MVT | 32 Bits | 2,4 or 6 Bytes | 150K-200K Bytes | NA | 5 Million 32-Bit Words | 15-30 Minutes | 3-- Hours |
| Honeywell GCOS III | 36 Bits | 36-Bits | 19K Words | 461K Words | 2.1 Million 36-Bit Words | 5 Minutes | 30 Minutes |
| UNIVAC EXEC-8 | 36 Bits | 36 Bits | 40-50K Words | 330K Words | 2 Million 36-Bit Words | 15 Minutes | 1 Hour |
| CDC SCOPE 3.4 | 60 Bits | 15 or 30 Bits | 16K-32K Words | NA | 2.5 Million 60-Bit Words | NA | NA |

LEGEND
NA-Information not available

Notes to Table 2

Methods of estimating operating system size. The estimate given for the size of IBM's OS/MVT was based on a count of the instructions in a microfiche deck of the complete system. This method was checked against an estimate of system size based on the amount of disk space it occupies at system generation time. The size estimates for the Honeywell UNIVAC, and CDC operating systems are based on the amount of disk space they occupy at system generation time. Note the following:

a. IBM's 360/370 OS/MVT is contained on 3,000 microfiche cards. There are 45 frames per card. Assume that each card is 70% full (i.e. uses 30 frames per card) and that each frame contains about 45 instructions. Multiplying the three numbers we get a total of 4.2 million instructions. A method for cross-checking the total number of instructions is that OS/MVT occupies 75 percent of a 2314 pack containing a total of 21 million bytes. If the average instruction takes 4 bytes, and the system occupies 15.75 million bytes, the total number of instructions is 3.96 million.

b. Honewyell GCOS III with timesharing, utilities, test routines, and library occupies 545 links on disk. Each link is 3840 words. With one instruction per word, GCOS III has about 2.1 million instructions.

c. UNIVAC EXEC 8 with library and compilers occupies 400,000 words. Each word is 36 bits and each instruction is 36 bits long (i.e. one instruction per word). Thus EXEC 8 is composed of about 400,000 instructions.

d. CDC SCOPE 3.4 occupies 300 record blocks on a disc pack. Each record block contain 50 sectors and each sector contains 64 60-bit words. Thus SCOPE is composed of approximately 1 million 60-bit words. The CDC 6000 series machines have 15- or 30-bit instructions. Based on an estimated ratio of 15-bit to 30-bit instructions, the total number of instructions is about 2.5 million.

e. The core resident portion of the above operating systems depends on facility parameters. On the average, each operating system occupies about 32,000 words of core.

TABLE 3. Comparison of Detailed System Characteristics

| System Characteristic | IBM OS/MVT | HONEYWELL GCOS III | UNIVAC EXEC-8 | CDC SCOPE 3.4 |
|---|---|---|---|---|
| Multiprogramming | yes | yes | yes | yes |
| Multiprocessing | yes | yes | yes | yes |
| Batch Processing | yes | yes | yes | yes |
| Time Sharing | NO | yes | NO | no |
| Remote Batch Processing | yes | yes | yes | yes |
| Real-time Processing | yes | yes | yes | no |

Notes to Table 3

1. All of the following components are common to the above system:

a. System Startup: This is the process of initializing the operating system for normal processing. System initialization is achieved by loading a system-tailoring routine. This routine then processes system configuration information.

b. Scheduler: This module schedules job tasks into the system execution queue. Job tasks are placed in the queue after all resource requests are satisfied. Tasks are usually scheduled by priority and class.

c. Dispatcher: This module allocates CPU time to tasks queued for execution. Normally, the dispatching queue is arranged by priority. If the CPU is available, the dispatcher will remove the task from the queue and assign it to the CPU until such time as the task requires supervisor aid or terminates.

d. Peripheral Allocator: This module schedules and allocates all peripheral devices (drums, disks, tapes, etc.) requested by programs. This is done by keeping inventory tables of facilities available and facilities assigned.

e. Storage Allocator: This module is responsible for allocation of internal storage (core memory) to user tasks. Again, this is normally done by priority.

f. Interrupt Handlers: These modules provide interface (supervisor calls) between the user and the system. They also include modules which execute recovery action in the case of program or hardware faults.

g. IOS: The I/O Supervisor (IOS) is a set of modules which initiate I/O and respond to I/O termination. When an I/O request is issued, the IOS checks the channel and device for availability. If both are free, the I/O operation is initiated. If not, the request is placed on a channel or device queue. In addition, the IOS provides for I/O interrupt handling, translation of file codes to physical units, and file protection.

h. System Input and Output: This set of modules handles the input and output of user programs. When a job is entered into the system a group of modules associated with the input device will set up program files for the job. Similarly, the output modules supervise the transfer of output data from the output files.

i. File Manager: This set of modules controls the various data files within the system. File management functions are invoked to locate files, to permit or restrict user access to files, and to provide back-up and restoration services in case of file damage. Master directories or catalogs are maintained with cataloging controls available to the user.

j. Utilities and System Programs: These include library routines, compilers, assemblers, loaders, etc.

2. The following paragraphs summarize basic differences between operating systems in the categories of: I/O operations, supervisor programs, memory configuration, and storage protection:

a. I/O Operations For IBM, Honeywell, and UNIVAC, I/O commands are issued through the central processing unit in supervisor mode. Commands are executed by specialized I/O processors. For CDC, I/O commands originate and are executed through one of the peripheral processors.

b. Supervisor Programs For IBM Honeywell, and UNIVAC the supervisor is run on the central processing unit. For CDC, a good portion of the supervisor is run on Peripheral Processor 0 which sits as master control over all other processors.

c. Memory Configuration

IBM: 2048 bytes per block

Honeywell: 262,144 words per module, organized into blocks of 1024 words.

UNIVAC: 65,536 words per bank, with interleaving of even and odd words.

CDC: 4096 words per bank with phasing of 32 banks.

d. Storage Protection

IBM: Storage key for every 2048 bytes

Honeywell: Hardware register with field length control

CDC: Hardware register with field length control

UNIVAC: Storage-limits register containing upper and lower bounds of instructions and data.

## Comparison of Supervisor Calls, Master Mode Entrys, and Executive Requests (Table 4)

### General Information

IBM, Honeywell and UNIVAC. The first portion of Table 4 lists 118 IBM supervisor calls (SVC's) in numerical order and their equivalents in the Honeywell and UNIVAC systems. Included with each SVC is its description. Following this list is a list of IBM service and I/O macros along with their equivalents in the other systems. The remainder of the table consists of a listing of the Honeywell Master Mode Entrys (MME's) and UNIVAC Executive Requests (ER's) that do not correspond to any of the IBM SVC's. As with the other calls, descriptions are provided. Included in this listing is a compilation of UNIVAC subroutines and procedures and Honeywell service requests.

CDC. CDC is not included in this table of comparisons because the SCOPE operating system has a considerably different design from the other three systems. This difference stems from the fact that the CDC 6000 series machines are composed of eleven independent computers and, hence, need a much different type of operating system and service calls. CDC's SCOPE operating system has only five distinct calls. These are:

| | |
|---|---|
| TIM | Return Time |
| END | Normal End |
| ABT | Abnormal End |
| RCL | Recall |
| CIO | I/O Request |

The CIO call contains all the file management requests such as OPEN, CLOSE, READ and WRITE.

Table 4. Comparison of Supervisor Calls, Master Mode Entrys, and Executive Requests

| | Supervisor or Service Call Designation | | |
|---|---|---|---|
| NAME AND DESCRIPTION | IBM | HONEYWELL GCOS III | UNIVAC EXEC 8 |
| CP - execute channel program | SVC 0 | | |
| IT - wait for an event | SVC 1 | GERELC (M) | AWAIT$ |
| ST - signal event completion | SVC 2 | GEFINI (M) | |
| IT - SVC routine exit (return from) | SVC 3 | | EXIT$ |
| MAIN - allocate storage w/o register | SVC 4 | GEMORE *(M), ADDMEM (D) | MCORE$ |
| EEMAIN - frees storage | SVC 5 | GEMREL (M), RELMEM (D) | LCORE$ |
| NK - LOAD and transfer control | SVC 6 | CALLSS (D) | RLINK$, LINK$ |
| TL - transfer control to another load module | SVC 7 | GECALL (M) | |
| AD - loads task, no control transfer | SVC 8 | | LOAD$ |
| LETE - relinquish control of load module | SVC 9 | RETURN (D) | EXLNK$, UNLNK$ |
| EMAIN - register GETMAIN/FREEMAIN | SVC 10 | | |
| E - provides date and time | SVC 11 | GETIME (M), TIME (D) | DATE$, TDATE$, |
| NCH - synchronous exit, transfer from supervisor to user program | SVC 12 | | |
| ND - abnormally terminate a job | SVC 13 | ABORT (D) | ABORT$, EABT$, ERR$ |
| E - specify program interrupt exit, user's own fault processing | SVC 14 | | IALL$ |

Table 4 (Continued)

| | Supervisor or Service Call Designation | | |
|---|---|---|---|
| NAME AND DESCRIPTION | IBM | HONEYWELL GCOS III | UNIVAC EXEC 8 |
| ERREXCP - retry of channel program | SVC 15 | | |
| PURGE - removed specified I/O requests | SVC 16 | | |
| RESTORE - complement of PURGE | SVC 17 | | |
| BLDL/FIND - build list from information from a PDS directory/Establish beginning of a data set member | SVC 18 | | |
| OPEN - logically connect a data set | SVC 19 | | BOPEN$, IHOPN |
| CLOSE - logically disconnect a data set | SVC 20 | RETFIL (D) | BCLOF$, IHCLR, IECLF BREL RELESE, @CLOSE, BCLOR$ |
| STOW - update PDS directory | SVC 21 | | |
| OPENJ - a JFCB is supplied by user to be used during initialization (OPEN) | SVC 22 | | |
| TCLOSE - CLOSE but rewinds tape w/o updating the label | SVC 23 | | |
| DEVTYPE - locate device characteristics | SVC 24 | | |
| TRKBAL - track balancing | SVC 25 | | |
| CATALOG/INDEX/LOCATE - maintain the catalog and the VTOC | SVC 26 | | PFI$, PFS$ |
| OBTAIN - get DSCB into main storage | SVC 27 | | |
| OPENEXT - open a catalog to extend it | SVC 28 | | |
| SCRATCH - delete a data set on direct access device | SVC 29 | GERELS *(M) | PFD$ |

Table 4 (Continued)

| NAME AND DESCRIPTION | Supervisor or Service Call Designation | | |
|---|---|---|---|
| | IBM | HONEYWELL GCOS III | UNIVAC EXEC 8 |
| RENAME - change data set name | SVC 30 | | |
| FEOV - force end-of-volume condition | SVC 31 | | BBEOF$ |
| ALLOCATE - request space on I/O device | SVC 32 | GEMORE *(M) | |
| I/O HALT - stop processing on a teleprocessing device | SVC 33 | DRLDSC (D) | |
| MGCR - master command processing (scheduling routine) | SVC 34 | | |
| WTO/WTOR - write to operator/write to operator with reply | SVC 35 | CONSOL (D)** | COM$ |
| WTL - write to log | SVC 36 | | |
| SEGLD/SEGWT - segment load and segment load and wait (overlays) | SVC 37 | | |
| TTROUTER - Testran facility | SVC 38 | | |
| LABEL - write volume label sets onto tape in either EBCDIC or ASCII | SVC 39 | | LABEL$ |
| EXTRACT - extract information from the task control block (TCB) | SVC 40 | ATTRI (D) | |
| IDENTIFY - establish another entry point to a task | SVC 41 | | |
| ATTACH - create a new task | SVC 42 | | ACT$, FORK$ |
| CIRB - create interrupt request block | SVC 43 | GENEWS (M) | |
| CHAP - change dispatching priority | SVC 44 | | |
| OVLYBRCH - transfer control to another overlay segment | SVC 45 | | |

Table 4.(Continued)

| | Supervisor or Service Call Designation | | |
|---|---|---|---|
| NAME AND DESCRIPTION | IBM | HONEYWELL GCOS III | UNIVAC EXEC 8 |
| TTIMER - test interval timer | SVC 46 | GELAPS (M) | TWAIT$ |
| STIMER - set interval timer | SVC 47 | GEWAKE (M), GWAKE (D) | |
| DEQ - release a serially reusable resource | SVC 48 | | |
| TTOPEN | SVC 49 | | |
| null | SVC 50 | | |
| SNAP - snapshot dump (dump and continue) | SVC 51 | GESNAP (M) | SNAP$ |
| RESTART/SMB Reader-to help process checkpoint restarts and read SMBs | SVC 52 | | OPT$ |
| RELEX - release exclusive control after read under exclusive control | SVC 53 | | |
| DISABLE - lock out interrupts | SVC 54 | | @ENABLE |
| EOV - end-of-volume and end of data set condition, check error conditions | SVC 55 | | BMARK$, @MARK |
| ENQ - request control of a serially reusable resource | SVC 56 | | |
| FREEDBUF - free dynamically obtained buffer (obtained by READ) | SVC 57 | | |
| REQBUF/RELBUF - access to dynamic buffer management | SVC 58 | | |
| OLTEP - provide on-line test system w/facility to system control code | SVC 59 | | |
| STAE/STAI - specify task abnormal exit return control to user after ABEND | SVC 60 | | |

Table 4 (Continued)

| NAME AND DESCRIPTION | Supervisor or Service Call Designation<br>IBM | <br>HONEYWELL GCOS III | <br>UNIVAC EXEC 8 |
|---|---|---|---|
| TSAV - Used with Testran | SVC 61 | | |
| DETACH - deletes subtask (removes TCB) | SVC 62 | GEBORT (M) | DACT$ |
| CHKPT - establish checkpoint for job step | SVC 63 | GECHEK (M) | @CKPT, @RSTRT |
| RDJFCB - read job file control block from disk | SVC 64 | | |
| QWAIT - telecommunications WAIT | SVC 65 | | |
| BTAM TEST - telecommunications on-line test | SVC 66 | | |
| QPOST - telecommunications POST | SVC 67 | | |
| SYNADAF/SYNADRLS - analyze permanent I/O error/release SYNADAF buffer and save areas | SVC 68 | | |
| BSP - backspace current volume one block | SVC 69 | | |
| GSERV - graphics service | SVC 70 | | |
| ASGN BFR/RLSE BFR/BUFINQ - buffer processing and manipulation | SVC 71 | | |
| CHATR - status display interface, MCS, DIDOCS processor, 2740 processor | SVC 72 | | |
| SPAR - Specify attention. Used with GAM | SVC 73 | | |
| DAR - Damage assessment routine | SVC 74 | | |
| Dequeue routine used with GAM | SVC 75 | | |
| IFBSTAT - Statistics update | SVC 76 | | |

Table 4 (Continued)

| NAME AND DESCRIPTION | Supervisor or Service Call Designation<br>IBM | HONEYWELL GCOS III | UNIVAC EXEC 8 |
|---|---|---|---|
| CRJE | SVC 77 | | |
| LSPACE - total space still available on volume | SVC 78 | | |
| STATUS - change subtask's dispatching status | SVC 79 | | |
| GJP/GFX - graphic job processor/graphics interface task | SVC 80 | | |
| SETPRT - load character set for UCS printer | SVC 81 | | |
| DISKANAL | SVC 82 | | |
| SMFWTM | SVC 83 | | |
| Restart Address Routine | SVC 84 | | |
| SWAP - Dynamic Device Reconfiguration Processor | SVC 85 | GEFILS (M) | TSWAP$ |
| ATLAS - assign an alternate track and copy data from the defective track | SVC 86 | | |
| DOM - delete operator message from CRT | SVC 87 | | |
| MOD 88- emulator program | SVC 88 | | |
| EMSERV - emulator service | SVC 89 | | |
| XQMNGR - job management | SVC 90 | | |
| VOLSTAT | SVC 91 | | |
| TCBEXCP | SVC 92 | | |

Table 4 (Continued)

| NAME AND DESCRIPTION | Supervisor or Service Call Designation<br>IBM | <br>HONEYWELL GCOS III | <br>UNIVAC EXEC 8 |
|---|---|---|---|
| TGET/TPUT-obtain input from/transmit output to the terminal | SVC 93 | GEROUT (M) | CMI$/CMO$ |
| TERMCTL - terminal control | SVC 94 | | CMS$, CMSA$ |
| TSIP - time-sharing processing routine | SVC 95 | | |
| STAX - specific time-sharing attention exit | SVC 96 | | |
| TEST (TSO) - breakpoint handler | SVC 97 | | |
| TSO PROTECT | SVC 98 | | |
| TSO Dynamic Allocation | SVC 99 | | |
| used by SUBMIT, OUTPUT, OPERATOR, AND CANCEL/STATUS Processors | SVC 100 | | |
| QTIP - provide interface between TSO subsystem and the MCP | SVC 101 | | |
| TCAM - telecommunications access method | SVC 102 | | CMD$, CMH$ |
| XLATE - translation between ASCII and EBCDIC | SVC 103 | | |
| TCAM - telecommunications access method | SVC 104 | | CMT$ |
| IMGLIB - DEB and DCB manipulation for SYS1. IMGLIB (Image library) | SVC 105 | | |
| Type 3 and type 4 SVC routing routine | SVC 109 | | |
| Type 1 SVC routing routine | SVC 116 | | |
| Type 2 SVC routing routine | SVC 117 | | |

Table 4 (Continued)

| NAME AND DESCRIPTION | Supervisor or Service Call Designation | | |
|---|---|---|---|
| | IBM | HONEYWELL GCOS III | UNIVAC EXEC 8 |
| CHECK - wait for and test completion of a READ or WRITE operation | CHECK (macro) | | WANY$, WAIT$ |
| NOTE - Provide relative position | NOTE (macro) | | PFWL$ |
| POINT - position to a block | POINT (macro) | | PFUWL$, @FIND |
| GETBUF - obtain a buffer | GETBUF (macro) | | CADD$, CGET$ |
| GETPOOL - build a buffer pool | GETPOOL (macro) | | CPOOL$ |
| FREEPOOL - release a buffer pool | FREEPOOL (macro) | | CREL$ |
| INCLUDE - include a load module into job step | INCLUDE (macro) | | NAME$, RLIST$, IN |
| BDAM READ | READ (macro) | | BRRED$, IHRDRN, IO$ |
| BSAM and BPAM READ | READ (macro) | GERSTR (M) | BREAD$, IO$ |
| QSAM and QISAM GET | GET (macro) | | IHRD, IOW$, READ$ |
| BDAM WRITE | WRITE (macro) | | BRWRT$, IHWTRN, IO$ |
| BSAM and BPAM WRITE | WRITE (macro) | GESAVE (M) | BWRIT$, IO$ |
| QSAM and QISAM PUT | PUT (macro) | | IHWRT, IOW$, PRINT$ |
| PUTX - write record from an existing data set | PUTX (macro) | | IHDRN |
| Exit from an ESI activity, return specified buffers, activate previously named activity | | | ADACT$ |
| ASCII punch | | | APCHCA$, APCHCN$, APNCHA$<br>APUNCH$ |

Table 4 (Continued)

| NAME AND DESCRIPTION | Supervisor or Service Call Designation<br>IBM | <br>HONEYWELL GCOS III | <br>UNIVAC EXEC 8 |
|---|---|---|---|
| ASCII print | | | APRINT$, APRNTA$, APRTCA$,<br>APRTCN$ |
| ASCII read | | | AREAD$, AREADA$ |
| Contingency mode termination-notify the executive that interrupt handling is completed | | | CEND$ |
| Expand buffer pool | | | CJOIN$ |
| Allows user to define his own set of control statements and register them with the exec. | | | CLIST$ |
| Retrieve condition word | | | COND$ |
| Control statements submitted for interpretation and processing during execution | | | CSF$ |
| Retrieve file assignment information | | GEFCON (M) | FACIL$, FACIT$, FITEM$ |
| Permit unsolicited console input | | | II$ |
| Initiate arbitrary device I/O | | GEINOS (M), DIO (D) | IOARB$ |
| Initiate arbitrary device I/O simulating an exit function and control return to program | | | IOAXI$<br>IOI$ |
| Initiate I/O with interrupt activity IOI$ and wait | | | IOWI$ |

Table 4 (Continued)

| | Supervisor or Service Call Designation | | |
|---|---|---|---|
| NAME AND DESCRIPTION | IBM | HONEYWELL GCOS III | UNIVAC EXEC 8 |
| Exit and IOI$ | | | IOXI$ |
| Retrieve master configuration table | | | MCT$ |
| Master file directory manipulation | | | MSCON$ |
| Terminate real time status | | | NRT$ |
| Program Control Table retrieval | | | PCT$ |
| Processor state word control | LPSW (instr) | GEREIS (M), GESETS (M)<br>RSTSWH (D), SETSWH (D) | PSR$ |
| PUNCH | | | PNCHA$, PUNCH$ |
| PRINT ALTERNATE & CONTROL | | | PRNTA$, PRTCA$, PRTCN$ |
| READ alternate | | | READA$ |
| Line terminal transfer - altering communications paths | | CGROUT (D) | ROUTE$ |
| Establish real time status complement of NRT$ | | | RT$ |
| Set condition word | | | SETC$ |
| Retrieve time of day | | | TIME$ |
| Initialize tape file to beginning of first reel | | REW (D) | TINTL$ |
| Print then read (Field data) | | KOUTN (D) | TREAD$ |

Table 4 (Continued)

| | Supervisor or Service Call Designation | | |
|---|---|---|---|
| NAME AND DESCRIPTION | IBM | HONEYWELL GCOS III | UNIVAC EXEC 8 |
| Allow interrupt activity to reduce its priority | | | UNLCK$ |
| End courtesy call | | GEENDC (M) | |
| Physical file address request | | GEFADD (M) | |
| File System Entry Request | | GEFSYE (M), FILACT (D) | |
| File and Record Control Entry | | GEFRCE (M) | |
| Journalization and subfile page range | | GEIDSE (M) | |
| Information entry outside of BAR limits | | GEINFO (M) | |
| Load Base Register | | GELBAR (M) | |
| Loop Protection | | GELOOP (M) | |
| I/O Priority | | GEPRIO (M) | |
| Deallocate Peripherals | | GERELS (M) | |
| Causes program to be taken out until all outstanding requests (I/O, courtesy calls) are completed | | GEROAD (M) | |
| Reinstate or Roll back Program | | GEROLL (M) | |
| Supply Sequence number | | GESNUM (M), SNUMB (D) | |
| Special Interrupt Request | | GESPEC (M) | |
| Write on Sysout | | GESYOT (M) | |
| User - Supplied MME | | GEUSER (M) | |

Table 4 (Continued

| | Supervisor or Service Call Designation | | |
|---|---|---|---|
| NAME AND DESCRIPTION | IBM | HONEYWELL GCOS III | UNIVAC EXEC 8 |
| Enter Master Mode | | .EMM (M) | |
| Abort batch job from TSS | | ABTJOB (D) | |
| Access a small block of core the system maintains for each user | | CORFIL (D) | |
| Allow time-sharing subsystem to access IDS file | | IDS (D) | |
| Allow time-sharing task to obtain status of batch job | | JSTS (D) | |
| Retrieve last line of input | | KIN (D) | |
| Force Keyboard output from a partially-filled buffer | | KOTNOW (D) | |
| Keyboard output from a buffer | | KOUT (D) | |
| Object program time and size check | | OBJTZM (D) | |
| Pass list of files to subsystem | | PASAFT (D) | |
| Pass file names and descriptions | | PASDES (D) | |
| Pass file to Remote Batch Processor | | PASFLR (D) | |
| Pass program description to subsystem | | PREDES (D) | |
| Simulated Keyboard Input | | PSEUDO (D) | |
| Overlay-load a subsystem | | RESOTR (D) | |
| Save program on permanent file | | DRLSAV (D) | |
| Initiate line-numbering mode, store line number and increment value | | SETLNO (D) | |

Table 4 (Continued)

| | Supervisor or Service Call Designation | | |
|---|---|---|---|
| NAME ANDDESCRIPTION | IBM | HONEYWELL GCOS III | UNIVAC EXEC 8 |
| Pass file to batch processor | | SPAWN (D) | |
| Stop paper Tape input | | STOPPT (D) | |
| Cause subsystem to be killed | | SYSRET (D) | |
| Start paper tape input | | TAPEIN (D) | |
| Spawn Batch activity from TSS | | TASK (D) | |
| Request Terminal type and line Number | | TERMTP (D) | |
| Define and access a temporary file | | DEFIL (D) | |
| Space a linked file | | FILSP (D) | |
| Enlarge a file already opened | | GROW (D) | |
| Add links to a temporary file | | MORLNK (D) | |
| Partial Release of a temporary file | | PART (D) | |
| Switch Temporary File Names | | SWITCH (D) | |
| Do I/O on system file | | PDIO (D) ** | |
| Pass user ID and priority to Executive | | USERID (D) ** | |
| Log on New User without disconnect | | NEWUSR (D) ** | |
| Stop Execution of Master subsystem | | STPSYS (D) ** | |
| Write Statistical Collection File | | T.STAT (D) ** | |

LEGEND

*This MME performs more than one function
**These are privileged instructions
(M)-Master Mode Entrys (Batch)
(D)-Derails (Time Sharing)
w/o-Without

## ABBREVIATIONS IN TABLE 4

DIDOCS - Device independent display operator console support

DSCB - data set control block

ER - Executive Request (UNIVAC)

ESI - externally set index (not set inside machine)

GAM - Graphics Access Method

JFCB - job file control block

MCS - Multiple Console Support

MCP - Master Control Program

MME - Master Mode Entry (Honeywell)

PDS - partitioned data set

SMB - contains JCL (job control language) information

SMF - System Management Facility

TCB - task control block

VTOC - volume table of contents

2740 Processor - performs OPEN and CLOSE functions (2740 Communications Terminal)

T. Checkpoint - RESTART:

This feature is not supported on IBM O/S or Univac EXEC-8 when running in the secure mode. The weak point in checkpoint is that system tables must be written out on a mass storage device. Upon restart the system must accept as fact the information and tables recovered from mass storage, thus any piece of information that will cause the operating system to do things it should not, can be modified to give the checkpoint program special privileges.

This is a problem in GCOS III, SCOPE 3.4, IBM O/S, EXEC-8

## II. Files and Catalogs

The protecting of files and catalogs from illegal users are a problem in all systems. In the CDC 7600 SCOPE Operating System, it is possible to open the master directory of all users by knowing the name of the master directory. In IBM OS, it is possible to open a VTOC as a file thus enabling a user to modify file entries in VTOC. The modification takes the form of altering passwords and file links.

In CDC 6000 SCOPE, the system lets the user decide if he wants control back, if the password was in error. This creates the possibility of modifying and issuing passwords with no time or count limits.

Master catalogs must be protected in a special manner. Catalogs must have greater protection than files.

## III. User/System Interface

### A. Improper Parameter Checking

Because of the complexity of operating systems, the interface between user and system causes a multitude of combinations of parameter lists which are difficult to check.

For example, in IBM OS it is possible to make the system load a system overlay into an area not assigned to it. Because of hardware features and core allocation, it is possible to fool the operating system by creating phony tables and positioning them in the correct place.

### B. Improper Exit

The operating system relies on a parameter accessible by the user to determine actions, branches, or exits.

For example, in CDC SCOPE 3.2 it is possible to hang up the system by setting the done flag in the Status Field of the Fet Table.

In GCOS III, it is possible to handle your own interrupts, and fork two addition processes.

In IBM OS, issuing a STOW request which does not have a valid entry will return a pointer of the next entry, which the user should not know about. The STAE and SPIE request also cause problems with user handling interrupts. If the user exits while waiting for an interrupt request undetermine results can occur.

## IV. I/O Problems

Because the way to get the best thorough put is to have asynchrous I/O, the I/O subsystem becomes vulnerable to I/O aborts and table filling.

Any system which has features to let users handle his own interrupts must not have asynchrous events with regards to this user.

In SCOPE 3.2 CDC 6000, it is possible to disturb the I/O because of timing delays created by different peripheral processes routine executing to satisfy one request.

In OS 360, the problem is the fact that all requests to the same device are queued through an I/O handler. If the program or request is destroyed or terminated while in this queue, undertermine results will occur.

In GCOS III, it is possible to scavenge the temporary buffer space which the system uses as a work area.

## V. Improper Overlay Handling

Both system and user overlays are accomplished by table look-ups. It becomes essential that the tables be secured from the user. The order of search of the libraries are important.

Routines that use pointer values, as either a jump location or entry into a routine, should check the pointer value for lower and upper bound conditions.

## VI. Assigning Authority to System Routines

Access methods or loaders or any other routines should not run with supervisor mode, if there is no need. This restriction does not apply to a CDC 6600 with its peripheral processors because the PPUs are independent. In this case, care should be exercised by controlling the programs allowed to run in the peripheral processor.

## VII. Priority of System Jobs

If the priority of certain system jobs in the system are incorrect, an asynchrous attack on that particular area of scheduling may produce data being read that should not have been read either out of memory or mass storage.

## VIII. Loads and Preloads

If the loaders handles the libraries in a perscribed manner, it is possible to insert a look alike module name to be found in a private library instead of being found in its correct library.

An example of this, is the overlay loader which searches the userlib for a system overlay supervisor before looking for it in the system lib.

## IX. Default Conditions and Names

Default conditions and names should not be used to short cut a check. All conditions should be validified and checked.

## X. Queueing of Tables

System tables and queues should be checked to determine the end conditions to queues.

## XI. Collusion

The using of two or more programs or users to bring about any of the above conditions.

## XII. Trojan Horse