Los Alamos

Los Alamos National Laboratory Los Alamos, New Mexico 87545

memorandum

TO: D. Camillo, OS-4 Group Leader

DATE: 14 Jul 83

FROM: Mark O. Kaletka MOK

MAIL STOP/TELEPHONE: H828/7-1359

SYMBOL: MP-1

SUBJECT: Security Incident at MP Division

This memo is to inform you of the events surrounding a recent security incident on the MP Division VAX 11/780 distributed processors, and the steps we have taken to both discover what (if any) damage was done to our systems, and to prevent any further such incidents.

On June 29, 1983 I received a telephone call from Charlene Douglas5 of OS-4 informing me that there was reason to suspect that our systems had been compromised by an unauthorized person using either the privileged DECNETP or non-privileged DECNET accounts. In checking our accounting log files for the month of June, we discovered that the privileged DECNETP account had indeed been used interactively by an unknown person on two dates in June. In both cases, this unknown user gained access to our node MPDPO through node G. The dates and times of access are contained in the first attachments. It was also evident from the log files that, on the second date, this same person was able to gain access to node MPFGO from node MPDPO. We were not able, however, to find any evidence of unauthorized activity on any of our other VAX systems.

On our systems, we have enabled image-mode accounting, and so were able to determine in detail what images had been run from the DECNETP account. The second attachment contains this information in detail. It became apparent how access had

VERIFIED UNCLASSIFIED
LANL Classification Group

initially been gained to the DECNETP account. All logins to either the DECNET or DECNETP accounts on our systems execute a command file which is intended to force an immediate logout if the process is an interactive process. This effectively blocks interactive use of these accounts, while still allowing access needed for network software. In this case, however, the individual was able to interrupt the command file (by using control-Y) before the logout process was completed, thereby gaining interactive access to the DECNETP account.

Once on our system, several system utilities were run which give access to information not otherwise available to unprivileged users. These included the NCP (Network Control Program) utility and AUTHORIZE utility. NCP is used to configure and control the DECNET network. Information available through the NCP utility includes the names of the privileged and non-privileged DECNET accounts on remote nodes known to the local node. The AUTHORIZE utility is used to create and modify user accounts and assign privileges to accounts. The RTPAD image was also run extensively. This image is executed when the command SET HOST is used to /interactively log onto a remote network node. In addition, an unknown program named NETTEST.COM was copied onto MPDPO, run, and then later deleted.

A comparison was made of the SYSUAF.DAT file which existed before June 23, and that existing after June 28. This is the file in which all user authorization information is stored, and is the file accessed by the AUTHORIZE utility. We found several descrepancies for which we were not able to account. The DECNET and DECNETP accounts on MPDPO and MPFGO were modified so that they had greater privileges than they should normally be assigned. In addition, a new account existed on MPDPO for which we had no record, and which had privileges which are not assigned to our normal accounts. This account appears to be a copy of an existing bona fide account, with a single letter changed in the account name. No directory was associated with this account, and we have no record of any access through this account.

As a result of this incident, we have severely tightened access available through the DECNET accounts. All interactive logins to these accounts have been completely disabled through flags set by the AUTHORIZE utility. The login command files have been modified to allow only network access, and now correctly disable the control-Y interrupt. In addition, these files have been removed from the default DECNET directory to prevent possible unauthorized access or modification. bogus account which was added to MPDPO has been removed. believe that these steps should eliminate further unauthorized access through these accounts. We are continuing to evaluate the damage which may have occurred due to this incident, and ways in which overall system security and integrity can be improved.

cc:

L. Rosen, MP-DO/H850 E. Hoffman, MP-1 Group Leader File

attachments:

- 1) Interactive access to DECNET and DECNETP during June.
- 2) Interactive image accounting information for DECNETP during June.
- 3) Changes to SYSUAF.DAT between June 20 and July 6.

Date /	Time	Type	Subtype	Username	ID	Source	Status	
23-JUN-1983	02: 03: 28	PROCESS	INTERACTIVE	DECNETP	02BA0047	G	10010001	
23-JUN-1903	02:17:28	PROCESS	INTERACTIVE	DECNET	028E0045	MPDPO	00000001	
23-JUN-1983	02: 19: 43	PROCESS	INTERACTIVE	DECNET	02910045	MPDPO	00000001	
23-JUN-1983	02: 19: 48	PROCESS	INTERACTIVE	DECNETP	02880047	G	00000001	
23-JUN-1983	23: 36: 52	PROCESS	INTERACTIVE	DECNETP	02030046	G	00038090	
23-JUN-1983	23: 38: 16	PROCESS	INTERACTIVE	DECNETP	02050046	C. waren	10000908	
23-JUN-1983	23: 39: 03	PROCESS	INTERACTIVE	DECNETP	02060046	G	00000001	
23-JUN-1983	23: 48: 20	PROCESS	INTERACTIVE	DECNETP	02CB0046	G	00000001	
28-JUN-1983	21:34:53	PROCESS	INTERACTIVE	DECNETP	00670045	G	00038098	
28-JUN-1983	22:11:01	PROCESS	INTERACTIVE	DECNETP	00700041	G	00002094	
28-JUN-1983	23: 10: 07	PROCESS	INTERACTIVE	DECNETP	00700045	G	00000001	

DECNETP ACTIVITY ON

MPDPP

	Date /	Time	Type	Subtype	Username	ID	Source	Status	3					•
	28-JUN-1983 28-JUN-1983	22: 47: 23 23: 08: 58	PROCESS PROCESS	INTERACTIVE INTERACTIVE	DECNETP DECNETP	00400051 00410051	MPDPO MPDPO	00000001 00000001	Action of the second of	controls.	10 14 14 1 2 14 14 14 14 14 14 14 14 14 14 14 14 14		Can and A	
						, 		s s Marring of the State of the Addisor		;			v	
etin.	**************************************	1 * * * * * * * * * * * * * * * * * * *								5				
	Parks First & American		141				2		100	3:		× ×		+
	I II PO POLICIANO		D	ECNE	TP	A	271	017	-0	01)				**********
			X		1/	mente menera fice in energia					3	5 3		
	W				M	PFE	26		(-1		**********			
		1		AAN TAN		(fee and sefer assesse) 2) /·				,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		- 1 ³⁰ - 1	
				((€)		***************************************			* ·			·		
							-	My As		1 80 × 11 8				
				3.							بالمسيد وأسيم بدوم			
20				e sam her en hjemese se e	a) - many - la m		•						Variable Control of the Control of t	
-	······································								تسيد المائدة	·	~ · · · · · · · · · · · · · · · · · · ·	4		
	TO THE STATE OF THE PARTY OF THE STATE OF TH				90 (04/9-11)	and a second distriction of the first	er er er ereit Herpegraph							
	· · · · · · · · · · · · · · · · · · ·	 	······································											
				i i i	معالمة المعالمة المعا	a amaga anga i Kapaga a	an de markement state aven ber		ومقا والمحمد المعسد ومحمد والمهرو	ean is ligared may proper and	Annah madahan da dah Manah	enter management		
			St.	<u> </u>		- AC CONTRACTOR OF THE					on a collination			
		The same of the same of			ng mingrania da	******				**************************************	********		er opriser over the personnel les	

```
File SYS$SYSROOT: [SYSMGR]SYSUAFOLD, LIS, 1
  256
Username:
                            (b)(6)
File SYS$SYSROOT: [SYSMGR]SYSUAFNEW. LIS: 1
                           (b)(6)
UIC:
Username:
                                       [304,005]
 257
       Account:
                               LGICMD: SYS$SYSTEM: SYSLOG
  258
                  DCL
       CLI:
 259
       Default Device: DBA2:
       Default Directory: [AT6DVN]
 260
Login Flags:
       Primary days: Mon Tue Wed Thu Fri Sat Sun
 261
Secondary days:
 262
       No hourly restrictions
 263
       PRIO:
                 4 BYTLM:
                                 30000 BIOLM:
                                                                     CHANGES TO SYSUAF-DAY
                                  O DIOLM:
                                                       12
                10 PBYTLM:
 264
       PRCLM:
       ASTLM:
                20 WSDEFAULT:
                                  100 FILLM:
 265
                                  200 SHRFILLM
                20 WSQUOTA:
       ENGLM:
  266
                40 WSEXTENT:
                                   300 CPU: 0 00:15:00.00
 267
       TOELM:
                                     O PGFLQUOTA: 51200
       MAXJOBS: O MAXACCTJOBS:
 268
       Privileges:
  269
         GRPNAM PRMCEB PRMMBX TMPMBX NETMBX
  271
Username:
                           (b)(6)
File SYS$SYSROOT: [SYSMGR]SYSUAFOLD. LIS: 1
       Account:
                  011,006
                               UIC:
                                       [011,006]
                               LGICMD: SYS$SYSTEM: SYSLOG
  348
File SYS$SYSROOT: [SYSMGR]SYSUAFNEW. LIS: 1
                  011,010
                               UIC:
                                       [011,010]
       Account:
                               LGICMD: SYS$SYSTEM: SYSLOG
  363 | CLI:
                  DCL
File SYS$SYSROOT: CSYSMGRISYSUAFOLD. LIS; T
 620 Default Directory: [DECNET]
Login Flags: DISCTLY DEFCLI LOCKPWD-
       Primary days: Mon Tue Wed Thu Fri Sat Sun
Secondary days:
  622
       No hourly restrictions
                              30000 BIOLM:
  623
       PRIO:
                 4 BYTLM:
                                                       12
                                     O DIOLM:
                10 PBYTLM:
  624
       PRCLM:
                                   100 FILLM:
  625
                20 WSDEFAULT:
       ASTLM:
                                   200 SHRFILLM:
  626
       ENGLM:
                20
                    WSQUOTA:
                                   300 CPU:
                                              0 00:15:00.00
                    WSEXTENT:
  627
       TOELM:
       MAXJOBS: O MAXACCTJOBS: O PGFLQUOTA: 51200
  628
  629
       Privileges:
          GRPNAM PRMCEB PRMMBX TMPMBX NETMBX
  630
  631
Username: DECNETP
                       Owner: SYSTEM DECNET-P
                               UIC:
                                       [011,003]
  632
```

LGICMD: SYS\$SYSTEM: SYSLOG

633

635

Login Flags: DEFCLI

Default Device: SYS\$SYSDEVICE: Default Directory: [DECNET]

```
608
         PRIO:
                     BYTLM:
                                   30000 BIOLM:
                                                          12
  639
        PRCLM:
                  10
                     PDYTLM:
                                       0
                                          DIOLM:
                                                         12
  640
        ASTLM:
                     WSDEFAULT:
                                                         75
                                     100
                                          FILLM:
  641
        ENGLM:
                  20
                     WSQUOTA:
                                    1200
                                          SHRFILLM:
                                                          0
  642
        TOELM:
                  40 WSEXTENT:
                                     300
                                          CPU:
                                                 0 00:15:00.00
  643
        MAXJOBS: O MAXACCTJOBS:
                                       0
                                         PGFLQUOTA: 51200
  644
        Privileges:
  645
          GRPNAM DIAGNOSE PRMCEB PRMMBX TMPMBX OPER NETMBX SYSPRV
  646
Username: DEFAULT
                        Owner:
***
File SYS$SYSROOT: [SYSMGR]SYSUAFNEW. LIS:
        Default Directory: [DECNET]
Login Flags: DISCTLY DEFCLI LUCKPWD DISUSER
  636
        Primary days: Mon Tue Wed Thu Fri Sat Sun
Secondary days:
        No hourly restrictions
  637
  638
        PRIO:
                  4 BYTLM:
                                   30000 BIOLM:
                                                         12
  639
        PRCLM:
                     PBYTLM:
                                       O DIOLM:
                                                         12
  640
        ASTLM:
                 20
                     WSDEFAULT:
                                     100 FILLM:
  641
        ENOLM:
                 20
                     WSQUDTA:
                                     200 SHRFILLM:
  642
        TQELM:
                 40
                     WSEXTENT:
                                     300 CPU:
                                                 0 00:15:00.00
  643
        MAXJOBS: O MAXACCTJOBS:
                                       O PCELQUITA 51200
  644
        Privileges:
  645
          GRPNAM PRMCED PRMMBX TMPMBX METMBX SYSPRV
  646
Username: DECNETP
                                SYSTEM DECNET-P
                        Owner:
  647
        Account: __0117003
                                UIC:
                                         [011,003]
  648
        CLI:
                   DCL
                                LGICMD: SYS$SYSTEM: SYSLOG
        Default Device: SYS$SYSDEVICE:
  649
        Default Directoru: [DECNET]
Login Flags: DISCTLY DEFCLI LOCKPWD DISUSER
        Primary days: Mon Tue Wed Thu Fri Sat Sun
Secondary days:
  652 | No hourly restrictions
  653
       PRIO:
                  4 BYTLM:
                                  30000 BIOLM:
                                                         12
  654
        PRCLM:
                 10 PBYTLM:
                                      O DIOLM:
                                                         12
  655
                                    100 FILLM:
        ASTLM:
                     WSDEFAULT:
  656
        ENGLM:
                 20
                     WSQUOTA:
                                    200 SHRFILLM:
                                                         0
  657
        TOELM:
                 40
                     WSEXTENT:
                                    300 CPU:
                                                0 00: 15: 00. 00
  658
        MAXJOBS: O MAXACCTJOBS:
                                      O PGFLQUOTA: 51200
  659
        Privileges:
        GRPNAM DIAGNOSE PRMCEB PRMMEX SETPRV THPMBX OPER NETMBX SYSPRV
  661
Username: DEFAULT
                        Owner:
File SYS$SYSROOT: [SYSMGR]SYSUAFOLD, LIS: 1
       Default Directory: [SYSMAINT]
Login Flags:
 666
       Primaru daus:
                        Mon Tue Wed Thu Fri Sat Sun
Secondary days:
File SYS$SYSROOT: [SYSMGR]SYSUAFNEW. LIS; 1
```

3

680

681

Secondary days:

Login

Default Directory: [SYSMAINT]

Mon Tue Wed Thu Fri Sat Sun

5: LOCKPWD

imary days:

```
GRPNAM PRMCEB PRMMBX TMPMBX NETMBX
 5013
 5014
                              (b)(6)
Username:
File SYS$SYSROOT: [SYSMGR]SYSUAFOLD. LIS;
 5074
Username:
                           (b)(6)
***
File SYS$SYSROOT: (SYSMGR)SYSUAFNEW. LIS; 1
 5194
Username:
                               UIC:
                                        [322,004]
 5195
       Account:
                               LGICMD: SYS$SYSTEM: SYSLOG
                  DCL
 5196
       CLI:
       Default Device: DBA1:
 5197
       Default Directory: [MP4MWT]
 5198
Login Flags:
       Primary days: Mon Tue Wed Thu Fri Sat Sun
 5199
Secondary days:
        No hourly restrictions
 5200
                                                        12
        PRIO:
                  4 BYTLM:
                                  30000 BIOLM:
 5201
                                     O DIOLM:
                 10 PBYTLM:
 5202
       PRCLM:
                                   100 FILLM:
                                                        75
                 20 WSDEFAULT:
 5203
        ASTLM:
                                   200 SHRFILLM:
                 20 WSQUOTA:
 5204
        ENGLM:
                 40 WSEXTENT:
                                  4300 CPU: 0 00:15:00.00
 5205
        TOELM:
                                 0 PGFLQUOTA: 51200
        MAXJOBS: O MAXACCTJOBS:
 5206
 5207
        Privileges:
          GRPNAM PRMCEB PRMMBX TMPMBX NETMBX
 5208
 5209
                             (b)(6)
Username:
                               UÍC:
                                        [322, 023]
 5210(
        CLI: DCL
                               LGICMD: SYS$SYSTEM: SYSLOG
 5211
                                                                          SUCH ACCOUNT
        Default Device: DBAL:
 5212
        Default Directory: [MP4NC]
 5213
Login Flags:
       'Primary days: Mon Tue Wed Thu Fri Sat Sun
 5214
Secondary days:
 5215
        No hourly restrictions
                                                        12
                                  30000 BIOLM:
        PRIO:
                 4 BYTLM:
 5216
                                      O DIOLM:
                                                        12
                 10 PBYTLM:
 5217
        PRCLM:
                 20 WSDEFAULT:
                                    100 FILLM:
 5218
        ASTLM:
                                    200 SHRFILLM:
                 20 WSQUOTA:
 5219
        ENGLM:
                                    300 CPU: 0 00:15:00.00
        TGELM:
                 40 WSEXTENT:
 5220
        MAXJOBS: O MAXACCTJOBS:
                                     O PGFLQUOTA:
 5221
 5222
        Privileges:
          GRPNAM PRMCEB PRMMBX SETPRV TMAMBX NETMBX
 5223
 5224
Username:
File SYS$SYSROOT: [SYSMGR]SYSUAFOLD. LIS: 1
 5629
Username:
                            (b)(6)
 ***
 File SYS$SYSROOT: [SYSMGR]SYSUAFNEW. LIS: 1
```

Username

(b)(6)

```
File SYS$SYSROOT: [SYSMGR]SYSUAFOLD, LIS; 1
  256
Username:
                           (b)(6)
****
File SYS$SYSROOT: [SYSMGR]SYSUAFNEW. LIS; 1
  256
Username:
  257
        Account:
                                 UIC:
                                         [304,005]
                   304,005
  258
                                LGICMD: SYS$SYSTEM: SYSLOG
        CL I:
                   DCL
  259
        Default Device: DRA2:
  260
        Default Directory: (AT6DVN]
Login Flags:
  261
        Primary days:
                        Mon Tue Wed Thu Fri Sat Sun
Secondary days:
  262
        No hourly restrictions
  263
        PRIO:
                  4 BYTLM:
                                   30000 BIOLM:
  264
       PRCLM:
                 10 PBYTLM:
                                       O DIOLM:
                                                         12
  265
        ASTLM:
                                     100 FILLM:
                     WSDEFAULT:
  266
        ENGLM:
                                     200 SHRFILLM:
                 20 WSQUOTA:
  267
        TOELM:
                 40 WSEXTENT:
                                     300 CPU:
                                                 0 00:15:00.00
  268
       MAXJOBS: 0 MAXACCTJOBS:
                                         PGFLQUOTA: 51200
  269
       Privileges:
  270
          GRPNAM PRMCEB PRMMBX TMPMBX NETMBX
  271
Username:
                           (b)(6)
File SYS$SYSROOT: CSYSMGRISYSUAFOLD. LIS: 1
        Default Directory: [DECNET]_
Login Flags: DISCTLY DEFCLI LOCKPWD
        Primary days: Mon Tue Wed Thu Fri Sat Sun
Secondary days:
       No hourly restrictions
  592
       PRIO:
  593
                  4 BYTLM:
                                   30000 BIOLM:
  594
       PRCLM:
                                      O DIOLM:
                                                         12
                 10 PBYTLM:
  595
       , ASTLM:
                 20
                    WSDEFAULT:
                                     100
                                         FILLM:
  596
       ENGLM:
                 20 WSQUOTA:
                                     200
                                          SHRFILLM:
  597
       TOELM:
                 40 WSEXTENT:
                                     300
                                         CPU:
                                                 0 00:15:00.00
  598
       MAXJOBS: O MAXACCTJOBS:
                                         PGFLQUOTA: 51200
  599
       Privileges:
          GRPNAM PRMGEB PRMMBX TMPMBX NETMBX
  600
  601
Username: DECNETP
                       Owner: SYSTEM DECNET-P
  602
        Account:
                   011,003
                                UIC:
                                         [011,003]
  603
        CLIS
                   DCL
                                LGICMD: SYS$SYSTEM: SYSLOG
  604
       Default Device: SYS$SYSDEVICE:
        Default Directory: [DECNET]
Login Flags: DISCTLY DEFCLI LOCKPWD
        Primary days: Mon Tue Wed Thu Fri Sat Sun
Secondary days:
       No hourly restrictions
  607
  808
       PRIO:
                  4 BYTLM:
                                   30000 BIOLM:
                                                         12
  609
        PRCLM:
                 10 PBYTLM:
                                      0
                                         DIOLM:
                                                         12
                 20 WSDEFAULT:
                                    100
                                         FILLM:
  610
        ASTLM:
  611
        ENGLM:
                 20
                     WSQUOTA:
                                     200
                                          SHRFILLM:
                                     300 CPU:
                                                 0 00:15:00.00
  612
        TGELM:
                 40
                    WSEXTENT:
```

MAXJOBS:

MAXACCTJOBS:

PGFLQUOTA: 51200

CHANGES TO SYSUAF. DAY
ON MPFGA

```
Login Flags: DISCTLY DEFCLI LOCKPWD DISUSER
       Primary days: Mon Tue Wed Thu Fri Sat Sun
Secondary days:
       No hourly restrictions
  607
                                 30000 BIOLM:
                 4 BYTLM:
  608
       PRIO:
                                                      12
                                   O DIOLM:
                10 PBYTLM:
       PRCLM:
  609
                                                      75
                                   100 FILLM:
                20 WSDEFAULT:
        ASTLM:
  610
                                                      0
                                   200 SHRFILLM:
                20 WSQUOTA:
  611
       ENOLM:
                                   300 CPU: 0 00:15:00.00
        TOELM:
                40 WSEXTENT:
  612
                                  O PGFLGUOTA: 51200
                   MAXACCTJOBS:
       MAXJOBS: 0
  613
       Privileges:
  614
         GRPNAM PRMCEB PRMMBX TMPMBX NETMBX
  615
  616
                       Owner: SYSTEM DECNET-P
Username: DECNETP
                                       [011,003]
                               UICE
       Account:---011,003
                               LGICMD: SYS$SYSTEM: SYSLOG
                  DCL
  618
        CLI:
        Default Device: SYS$SYSDEVICE:
  619
        Default Directory: [DECNET]
Login Flags: DISCTLY DEFCLI LOCKPWD DISUSER
        Primary days: Mon Tue Wed Thu Fri Sat Sun
Secondary days:
        No hourly restrictions
  622
                                 30000 BIOLM: 12
                '4 BYTLM:
        PRIO:
  623
                                                      12
                                     O DIOLM:
                10 PBYTLM:
  624
        PRCLM:
                                  ,100 FILLM:
                 20 WSDEFAULT:
        ASTLM:
  625
                                 200 SHRFILLM: 0
        ENGLM: 20 WSQUDTA:
  626
                                   300 CPU: 0 00:15:00.00
                 40 WSEXTENT:
        TOELM:
  627
                                     O PGFLGUOTA: 512Q0
        MAXJOBS: O MAXACCTJOBS:
  628
        Privileges:
  629
          GRPNAM DIAGNOSE PRMCEB PRMMEX SETPRV THEMBX OPER NETMBX SYSPRV
  630
  631
Username: DEFAULT
                       Owner:
 ***
File SYS$SYSROOT: [SYSMGR]SYSUAFOLD. LIS. 1
  635 Default Directory: [SYSMAINT]
 Login Flags:
                       Mon Tue Wed Thu Fri Sat"Sun
  636 Primary days:
 Secondary days:
 File SYS$SYSROOT: [SYSMGR]SYSUAFNEW. LIS: 1
  650 Default Directory: [SYSMAINT]
 Login Flags: LOCKFWD
  651 Primary days: Mon Tue Wed Thu Fri Sat Sun
 Secondary days:
 File SYS$SYSROOT: [8YSMGR]SYSUAFOLD. LIS: 1
   919
                             (b)(6)
 Username:
 ***
 File SYS$SYSROOT: [SYSMGR]SYSUAFNEW. LIS: 1
   934
```

[340,113]

LGICMD: SYS\$SYSTEM: SYSLOG

File SYS\$SYSROOT: CSYSMGRISYSUAFNEW. LIS: 1
605 Default Directory: [DECNET]

Usern

935

936

.ccount:

CLI:

340, 113

DCL