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 Douglas 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 MPDP0 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 MPFG0 from node MPDP0. 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

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 MPDP0, 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 MPDP0 and MPFG0 were modified so that they had greater privileges than they should normally be assigned. In addition, a new account existed on MPDP0 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. The bogus account which was added to MPDP0 has been removed. I 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-1983 02:17:28	PROCESS	INTERACTIVE	DECNET	02BE0045	MPDP0	00000001
23-JUN-1983 02:19:43	PROCESS	INTERACTIVE	DECNET	02910045	MPDP0	00000001
23-JUN-1983 02:19:48	PROCESS	INTERACTIVE	DECNETP	02BB0047	G	00000001
23-JUN-1983 23:36:52	PROCESS	INTERACTIVE	DECNETP	02C30046	G	00038090
23-JUN-1983 23:38:16	PROCESS	INTERACTIVE	DECNETP	02C50046	G	10000908
23-JUN-1983 23:39:03	PROCESS	INTERACTIVE	DECNETP	02C60046	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	007C0041	G	00002094
28-JUN-1983 23:10:07	PROCESS	INTERACTIVE	DECNETP	00700045	G	00000001

DECNETP ACTIVITY ON

MPDP0

Date / Time	Type	Subtype	Username	ID	Source	Status
28-JUN-1983 22:47:23	PROCESS	INTERACTIVE	DECNETP	00400051	MPDP0	00000001
28-JUN-1983 23:08:58	PROCESS	INTERACTIVE	DECNETP	00410051	MPDP0	00000001

DECNETP ACTIVITY ON

MPEG0

```
************
File SYS$SYSROOT:[SYSMGR]SYSUAFOLD.LIS;1
  256
Username:                          (b)(6)
******
File SYS$SYSROOT:[SYSMGR]SYSUAFNEW.LIS;1
  256
Username:                          (b)(6)
  257   Account:    304,005        UIC:      [304,005]
  258   CLI:        DCL            LGICMD:   SYS$SYSTEM:SYSLOG
  259   Default Device: DBA2:
  260   Default Directory: [AT6DVN]
Login Flags:
  261   Primary days:    Mon Tue Wed Thu Fri Sat Sun
Secondary days:
  262   No hourly restrictions
  263   PRIO:       4  BYTLM:        30000  BIOLM:          12
  264   PRCLM:     10  PBYTLM:          0  DIOLM:          12
  265   ASTLM:     20  WSDEFAULT:     100  FILLM:          75
  266   ENQLM:     20  WSQUOTA:       200  SHRFILLM:        0
  267   TQELM:     40  WSEXTENT:      300  CPU:     0 00:15:00.00
  268   MAXJOBS:    0  MAXACCTJOBS:     0  PGFLQUOTA:   51200
  269   Privileges:
  270     GRPNAM PRMCEB PRMMBX TMPMBX NETMBX
  271
Username:                          (b)(6)
************
************
File SYS$SYSROOT:[SYSMGR]SYSUAFOLD.LIS;1
  347   Account:    011,006        UIC:      [011,006]
  348   CLI:        DCL            LGICMD:   SYS$SYSTEM:SYSLOG
******
File SYS$SYSROOT:[SYSMGR]SYSUAFNEW.LIS;1
  362   Account:    011,010        UIC:      [011,010]
  363   CLI:        DCL            LGICMD:   SYS$SYSTEM:SYSLOG
************
************
File SYS$SYSROOT:[SYSMGR]SYSUAFOLD.LIS;1
  620   Default Directory: [DECNET]
Login Flags: DISCTLY DEFCLI LOCKPWD
  621   Primary days:    Mon Tue Wed Thu Fri Sat Sun
Secondary days:
  622   No hourly restrictions
  623   PRIO:       4  BYTLM:        30000  BIOLM:          12
  624   PRCLM:     10  PBYTLM:          0  DIOLM:          12
  625   ASTLM:     20  WSDEFAULT:     100  FILLM:          75
  626   ENQLM:     20  WSQUOTA:       200  SHRFILLM:        0
  627   TQELM:     40  WSEXTENT:      300  CPU:     0 00:15:00.00
  628   MAXJOBS:    0  MAXACCTJOBS:     0  PGFLQUOTA:   51200
  629   Privileges:
  630     GRPNAM PRMCEB PRMMBX TMPMBX NETMBX
  631
Username:  DECNETP        Owner:  SYSTEM DECNET-P
  632   Account:    011,003        UIC:      [011,003]
  633   CLI:        DCL            LGICMD:   SYS$SYSTEM:SYSLOG
  634   Default Device: SYS$SYSDEVICE:
  635   Default Directory: [DECNET]
Login Flags: DEFCLI
```

CHANGES TO SYSUAF.DAT ON MPDP0

```
   638   PRIO:      4  BYTLM:        30000  BIOLM:          12
   639   PRCLM:    10  PBYTLM:           0  DIOLM:          12
   640   ASTLM:    20  WSDEFAULT:      100  FILLM:          75
   641   ENQLM:    20  WSQUOTA:        200  SHRFILLM:        0
   642   TQELM:    40  WSEXTENT:       300  CPU:     0 00:15:00.00
   643   MAXJOBS:   0  MAXACCTJOBS:      0  PGFLQUOTA:   51200
   644   Privileges:
   645     GRPNAM DIAGNOSE PRMCEB PRMMBX TMPMBX OPER NETMBX SYSPRV
   646
Username:   DEFAULT       Owner:
******
File SYS$SYSROOT:[SYSMGR]SYSUAFNEW.LIS;1
   635   Default Directory: [DECNET]
Login Flags: DISCTLY DEFCLI LOCKPWD DISUSER
   636   Primary days:    Mon Tue Wed Thu Fri Sat Sun
Secondary days:
   637   No hourly restrictions
   638   PRIO:      4  BYTLM:        30000  BIOLM:          12
   639   PRCLM:    10  PBYTLM:           0  DIOLM:          12
   640   ASTLM:    20  WSDEFAULT:      100  FILLM:          75
   641   ENQLM:    20  WSQUOTA:        200  SHRFILLM:        0
   642   TQELM:    40  WSEXTENT:       300  CPU:     0 00:15:00.00
   643   MAXJOBS:   0  MAXACCTJOBS:      0  PGFLQUOTA:   51200
   644   Privileges:
   645     GRPNAM PRMCEB PRMMBX TMPMBX NETMBX SYSPRV
   646
Username:   DECNETP       Owner:   SYSTEM DECNET-P
   647   Account:    011,003       UIC:     [011,003]
   648   CLI:        DCL           LGICMD:  SYS$SYSTEM:SYSLOG
   649   Default Device: SYS$SYSDEVICE:
   650   Default Directory: [DECNET]
Login Flags: DISCTLY DEFCLI LOCKPWD DISUSER
   651   Primary days:    Mon Tue Wed Thu Fri Sat Sun
Secondary days:
   652   No hourly restrictions
   653   PRIO:      4  BYTLM:        30000  BIOLM:          12
   654   PRCLM:    10  PBYTLM:           0  DIOLM:          12
   655   ASTLM:    20  WSDEFAULT:      100  FILLM:          75
   656   ENQLM:    20  WSQUOTA:        200  SHRFILLM:        0
   657   TQELM:    40  WSEXTENT:       300  CPU:     0 00:15:00.00
   658   MAXJOBS:   0  MAXACCTJOBS:      0  PGFLQUOTA:   51200
   659   Privileges:
   660     GRPNAM DIAGNOSE PRMCEB PRMMBX SETPRV TMPMBX OPER NETMBX SYSPRV
   661
Username:   DEFAULT       Owner:
************
************
File SYS$SYSROOT:[SYSMGR]SYSUAFOLD.LIS;1
   665   Default Directory: [SYSMAINT]
Login Flags:
   666   Primary days:    Mon Tue Wed Thu Fri Sat Sun
Secondary days:
******
File SYS$SYSROOT:[SYSMGR]SYSUAFNEW.LIS;1
   680   Default Directory: [SYSMAINT]
Login      s: LOCKPWD
   681      imary days:    Mon Tue Wed Thu Fri Sat Sun
Seconda.y days:
************
```

```
 5013      GRPNAM PRMCEB PRMMBX TMPMBX NETMBX
 5014
Username:                                    (b)(6)
************
************
File SYS$SYSROOT:[SYSMGR]SYSUAFOLD.LIS;1
 5074
Username:                                    (b)(6)
******
File SYS$SYSROOT:[SYSMGR]SYSUAFNEW.LIS;1
 5194
Username:                                    (b)(6)
 5195   Account:    322,004        UIC:      [322,004]
 5196   CLI:        DCL            LGICMD:   SYS$SYSTEM:SYSLOG
 5197   Default Device: DBA1:
 5198   Default Directory: [MP4MWT]
Login Flags:
 5199   Primary days:    Mon Tue Wed Thu Fri Sat Sun
Secondary days:
 5200   No hourly restrictions
 5201   PRIO:       4  BYTLM:         30000  BIOLM:          12
 5202   PRCLM:     10  PBYTLM:            0  DIOLM:          12
 5203   ASTLM:     20  WSDEFAULT:       100  FILLM:          75
 5204   ENQLM:     20  WSQUOTA:         200  SHRFILLM:        0
 5205   TQELM:     40  WSEXTENT:        300  CPU:     0 00:15:00.00
 5206   MAXJOBS:    0  MAXACCTJOBS:       0  PGFLQUOTA:   51200
 5207   Privileges:
 5208     GRPNAM PRMCEB PRMMBX TMPMBX NETMBX
 5209
Username:                                    (b)(6)
 5210   Account:    322,023        UIC:      [322,023]
 5211   CLI:        DCL            LGICMD:   SYS$SYSTEM:SYSLOG
 5212   Default Device: DBA1:
 5213   Default Directory: [MP4NC]
Login Flags:
 5214   Primary days:    Mon Tue Wed Thu Fri Sat Sun
Secondary days:
 5215   No hourly restrictions
 5216   PRIO:       4  BYTLM:         30000  BIOLM:          12
 5217   PRCLM:     10  PBYTLM:            0  DIOLM:          12
 5218   ASTLM:     20  WSDEFAULT:       100  FILLM:          75
 5219   ENQLM:     20  WSQUOTA:         200  SHRFILLM:        0
 5220   TQELM:     40  WSEXTENT:        300  CPU:     0 00:15:00.00
 5221   MAXJOBS:    0  MAXACCTJOBS:       0  PGFLQUOTA:   51200
 5222   Privileges:
 5223     GRPNAM PRMCEB PRMMBX SETPRV TMPMBX NETMBX
 5224
Username:                                    (b)(6)
************
************
File SYS$SYSROOT:[SYSMGR]SYSUAFOLD.LIS;1
 5629
Username:                                    (b)(6)
******
File SYS$SYSROOT:[SYSMGR]SYSUAFNEW.LIS;1
 5779
Username                                     (b)(6)
```

← NO RECORD OF ANY SUCH ACCOUNT

```
************
File SYS$SYSROOT:[SYSMGR]SYSUAFOLD.LIS;1
  256
Username:                    (b)(6)
******
File SYS$SYSROOT:[SYSMGR]SYSUAFNEW.LIS;1
  256
Username:                    (b)(6)
  257   Account:    304,005        UIC:     [304,005]
  258   CLI:        DCL            LGICMD:  SYS$SYSTEM:SYSLOG
  259   Default Device: DRA2:
  260   Default Directory: [AT6DVN]
Login Flags:
  261   Primary days:    Mon Tue Wed Thu Fri Sat Sun
Secondary days:
  262   No hourly restrictions
  263   PRIO:       4  BYTLM:        30000  BIOLM:          12
  264   PRCLM:     10  PBYTLM:          0  DIOLM:          12
  265   ASTLM:     20  WSDEFAULT:     100  FILLM:          75
  266   ENQLM:     20  WSQUOTA:       200  SHRFILLM:        0
  267   TQELM:     40  WSEXTENT:      300  CPU:    0 00:15:00.00
  268   MAXJOBS:    0  MAXACCTJOBS:     0  PGFLQUOTA:   51200
  269   Privileges:
  270     GRPNAM PRMCEB PRMMBX TMPMBX NETMBX
  271
Username:                    (b)(6)
************
************
File SYS$SYSROOT:[SYSMGR]SYSUAFOLD.LIS;1
  590   Default Directory: [DECNET]
Login Flags: DISCTLY DEFCLI LOCKPWD
  591   Primary days:    Mon Tue Wed Thu Fri Sat Sun
Secondary days:
  592   No hourly restrictions
  593   PRIO:       4  BYTLM:        30000  BIOLM:          12
  594   PRCLM:     10  PBYTLM:          0  DIOLM:          12
  595   ASTLM:     20  WSDEFAULT:     100  FILLM:          75
  596   ENQLM:     20  WSQUOTA:       200  SHRFILLM:        0
  597   TQELM:     40  WSEXTENT:      300  CPU:    0 00:15:00.00
  598   MAXJOBS:    0  MAXACCTJOBS:     0  PGFLQUOTA:   51200
  599   Privileges:
  600     GRPNAM PRMCEB PRMMBX TMPMBX NETMBX
  601
Username:  DECNETP          Owner:  SYSTEM DECNET-P
  602   Account:    011,003        UIC:     [011,003]
  603   CLI:        DCL            LGICMD:  SYS$SYSTEM:SYSLOG
  604   Default Device: SYS$SYSDEVICE:
  605   Default Directory: [DECNET]
Login Flags: DISCTLY DEFCLI LOCKPWD
  606   Primary days:    Mon Tue Wed Thu Fri Sat Sun
Secondary days:
  607   No hourly restrictions
  608   PRIO:       4  BYTLM:        30000  BIOLM:          12
  609   PRCLM:     10  PBYTLM:          0  DIOLM:          12
  610   ASTLM:     20  WSDEFAULT:     100  FILLM:          75
  611   ENQLM:     20  WSQUOTA:       200  SHRFILLM:        0
  612   TQELM:     40  WSEXTENT:      300  CPU:    0 00:15:00.00
  613   MAXJOBS:    0  MAXACCTJOBS:     0  PGFLQUOTA:   51200
```

CHANGES TO SYSUAF.DAT ON MPFG0

```
******
File SYS$SYSROOT:[SYSMGR]SYSUAFNEW.LIS;1
  605   Default Directory:  [DECNET]
Login Flags: DISCTLY DEFCLI LOCKPWD DISUSER
  606   Primary days:    Mon Tue Wed Thu Fri Sat Sun
Secondary days:
  607   No hourly restrictions
  608   PRIO:       4  BYTLM:        30000  BIOLM:          12
  609   PRCLM:     10  PBYTLM:          0  DIOLM:          12
  610   ASTLM:     20  WSDEFAULT:     100  FILLM:          75
  611   ENQLM:     20  WSQUOTA:       200  SHRFILLM:        0
  612   TQELM:     40  WSEXTENT:      300  CPU:     0 00:15:00.00
  613   MAXJOBS:    0  MAXACCTJOBS:     0  PGFLQUOTA:   51200
  614   Privileges:
  615     GRPNAM PRMCEB PRMMBX TMPMBX NETMBX
  616
Username:  DECNETP        Owner:  SYSTEM DECNET-P
  617   Account:    011,003       UIC:      [011,003]
  618   CLI:        DCL           LGICMD:  SYS$SYSTEM:SYSLOG
  619   Default Device: SYS$SYSDEVICE:
  620   Default Directory: [DECNET]
Login Flags: DISCTLY DEFCLI LOCKPWD DISUSER
  621   Primary days:    Mon Tue Wed Thu Fri Sat Sun
Secondary days:
  622   No hourly restrictions
  623   PRIO:       4  BYTLM:        30000  BIOLM:          12
  624   PRCLM:     10  PBYTLM:          0  DIOLM:          12
  625   ASTLM:     20  WSDEFAULT:     100  FILLM:          75
  626   ENQLM:     20  WSQUOTA:       200  SHRFILLM:        0
  627   TQELM:     40  WSEXTENT:      300  CPU:     0 00:15:00.00
  628   MAXJOBS:    0  MAXACCTJOBS:     0  PGFLQUOTA:   51200
  629   Privileges:
  630     GRPNAM DIAGNOSE PRMCEB PRMMBX SETPRV TMPMBX OPER NETMBX SYSPRV
  631
Username:  DEFAULT        Owner:
*************
*************
File SYS$SYSROOT:[SYSMGR]SYSUAFOLD.LIS;1
  635   Default Directory:  [SYSMAINT]
Login Flags:
  636   Primary days:    Mon Tue Wed Thu Fri Sat Sun
Secondary days:
******
File SYS$SYSROOT:[SYSMGR]SYSUAFNEW.LIS;1
  650   Default Directory:  [SYSMAINT]
Login Flags: LOCKPWD
  651   Primary days:    Mon Tue Wed Thu Fri Sat Sun
Secondary days:
*************
*************
File SYS$SYSROOT:[SYSMGR]SYSUAFOLD.LIS;1
  919
Username:                          (b)(6)
******
File SYS$SYSROOT:[SYSMGR]SYSUAFNEW.LIS;1
  934
Usern                              (b)(6)
  935   Account:    340,113       UIC:      [340,113]
  936   CLI:        DCL           LGICMD:  SYS$SYSTEM:SYSLOG
```