The CASE of the NETWORK MAP MAKER

INCIDENT STATISTICS

Date: 28 June 1983
Hours: 2130 - 0010 MDT
Systems: Los Alamos ICN -MX G, DP's - ESS1, MPDPO, MPFGO
Accounts: NETPRIV - (used to gain access on MX G)
DECNET (gained the passwords to all open DP Vax's)
MP4NC (account set up on MPDPO VAX)
Suspects: Adult male residing in Wisconsin
Direct Involvement: John Davis, C-8.
Interviewer : Charlene Douglass, OS-4
Interviewee: John Davis, C-8

On 28 June 1983 at approximately 2150 hours, Leo Archuleta of the CCF called me at home and advised me of an unauthorized user on Machine G. He had been advised of the presence by John Davis of C-8 who was using Machine G from home. I felt that a trace might be possible due to the fact that the penetrator's process seemed to be in a hibernating state. I came back to the Lab and called Telenet Customer Service at approximately 2215 hours. They were able to trace the call.

The perpetrator gained access through the NETPRIV account which unfortunately only had a four character password and happened to be the same as the one in the DEC manual. He then executed a command procedure that enabled him to obtain passwords to all the DECNET accounts on the Open DP's of which there are 16 on the XNET. On the evening of 28 June, he was discovered to be logged into three VAX's on XNET: MPDPO, ESS1, and MPFGO. The DECNET account on the MPDPO VAX had all system privileges.

From a brief search of the logs it appeared that the perpetrator had been logged on to our machines for the previous four evenings usually after midnight and had been very active. He had been logged into Machine G for one to two hours each evening. We don't know how long he was logged into the other machines.

John Davis of C-8 was able to enter into somewhat of a conversation with him. The person would not identify himself but said he was doing a test on our security and would be so kind to send us a full report. He was kind enough to phone John Davis on 29 June and point out some of the holes in the system. He also said at this time that he had been on the OFVAX. John immediately fixed the holes. The intruder did not identify himself.

If this person were a sophisticated user (as he apparently was), the potential was there, by logging on to these accounts, to obtain unclassified ICN passwords and Z-Numbers of users through a system dump facility. Another potential threat, through the process he was running, was to alter databases, change authorization files, set up accounts for himself, etc.

maybe we should change passwords OFE G

Continued investigation of this incident by OS-4, C-8, and the system managers of ESS1 and MP, has determined that the perpetrator did indeed gain access to the subject DP's and in the case of MPDPO did alter privileges and set up a system account for his own purposes. He also ran a program but deleted it upon completion thereby leaving no trail to the possible ramifications. Further investigation by OS-4 and ADP has determined unauthorized access on two of the ADP DP's and lots of file activity. One extended period of access for 38

hours is being reviewed. The activity occuring in this period is a verify memo process that reads all the memos on the system. It was also determined that one of the suspected unauthorized accesses to the ADP VAX was made from the Pacific Northwest Laboratories Distributed Processor.

Lee Brand of Telenet Security called Jim McClary on 29 June, 1983, and advised him of the suspected intrusions by this person at several other sites throughout the country. FBI mentioned?

On the evening of 29 June, a software change was made to MX G to require an ICN password from a Telenet user. Changes are being developed in C-5 to require another password for Telenet use.

There has been one additional unsuccessful attempt at a suspicious hour gain access to MX G through Telenet.

Tuesday evening, about 9:30, I dialed into Machine G from home. I commanded the machine to show the current interactive users and found only one other user, NETPRIV. This was suspicious because NETPRIV is a privileged account used only for DECnet network management; it should never be used interactively.

It was also suspicious because the terminal being used had a name that began with the letters NVA. This could only be our TELENET link.

I immediately logged off G and called the CCF at 667-4584. I told that person to contact OS-4.

Later I received a call from Charlene Douglas, OS-4, instructing me to log on again and try to keep the intruder on while the TELENET security office traced the call. I did log on again and was able to figure out what was going on. The image being run by the NETPRIV process on G was RTPAD, meaning that it was logged on to some other node or nodes in the open DP network. I logged on to several other VAXes and found the DECnet privileged account in use on MPDP0, MPFG0, and ESSDP1.

After about an hour, I contacted Charlene Douglass again. She told me that the call had been traced and that I should get back on the machine and either contact the intruder or get him off.

I did so and engaged in a short electronic mail dialogue with the NETPRIV user on G. I warned him that his call had been traced and that he had invaded a federal facility. I was unable to learn his name. He claimed to be only exploring our network. He offered to give us a security report, inviting us to call him back at the number we had traced. I asked him to call or write me, with the understanding that it might have some influence on further pursuance of the matter.

I received a call from an adult male about 11:45 the next day at my office, 667-4793. He explained how he had been able to get into the various DPs in spite of our security precautions. He suggested that if we gave him a normal account on our machine, he could communicate further security ideas. I turned down that suggestion but I invited him to send a written report, cautioning him that he might be wise to consult an attorney.

From: NETPRIV 28-JUN-1983 23:50
To: SYSTEM
Subj: RE: TELENET

WE WERE SPELUNKING IN YOUR ELECTRONIC CAVES AND TRYING TO SEE HOW LONG THIS COULD GO ON BEFORE BEING NOTICED.

IF YOU WOULD LIKE A FULL REPORT ABOUT YOUR SECURITY PROBLEMS PLEASE CONTACT US.

From: NETPRIV 28-JUN-1983 23:58
To: SYSTEM
Subj: RE: TELENET

MAY WE HAVE A MAIL ADDRESS, OR TELEPHONE
NUMBER WERE WE MAY CONTACT YOU.

IF YOU DO NOT WISH TO DIVULGE THIS INFORMATION
SIMPLY CALL US AT THE TRACED NUMBER

ALTHOUGH OUR ENTRY WAS UNATHORIZED IT WAS NOT
MALICOUS. WE SIMPLY WANTED TO CHECK THE SECURITY OF YOUR
SYSTEM.

AWAITING YOUR REPLY...

From: NETPRIV 29-JUN-1983 00:06
To: SYSTEM
Subj: RE: TELENET

HAVE YOU BEEN HAVING PROBLEMS WITH TELENET? WOULD YOU LIKE US TO CALL YOU TONIGHT AT THAT NUMBER?

```
BYE
BYE: COMMAND NOT FOUND.
EXIT
LOGOUT
SPORT 45130 ON A: CHARS IN 01031 (ERR 00000), CHARS OUT 43588
@231 1983-08-19 08:43:11
EDG  U 089207
@PORT 45130 ON G: @231 1983-08-19 09:11:44
MXG DP ACCESS LINE  10


DPs AVAILABLE:
ADPDP2  ADPDP3  CTRVAX  ESSDP1  ESSDP2  G       INCDP1  M6VAX
MERLIN  MFE     MPDP0   OFVAX   PNLB    QVAX2   S1VAX   STORES

DP NAME: G

USERNAME: 089207
PASSWORD:
        WELCOME TO VAX/VMS VERSION V3.3 ON NODE G

[?5H
OFFICE: N
$ SDEF .MEMO
  NEW DEFAULT: DRB3:[089207.MEMO]
$ DIR *.TXT

DIRECTORY DRB3:[089207.MEMO]

CAPTIVE.TXT;1       CONVERSE.TXT;2      CONVERSE.TXT;1      EVAL.TXT;3
  IDENT.TXT;3       INCIDENT.TXT;2      INCIDENT.TXT;1      PEN.TXT;1
  JECT2.TXT;1       SYNC.TXT;3          SYNC.TXT;2          SYNC.TXT;1
SYSMAN.TXT;1        TELENET.TXT;1

TOTAL OF 14 FILES.
$ T CONVERSE.TXT
AUGUST 5, 1983
```

THIS IS MY RECOLLECTION OF A TELEPHONE CONVERSATION ON JUNE 29, 1983 WHICH IS RELATED TO AN UNAUTHORIZED USE OF OUR OPEN NETWORK OF DISTRIBUTED PROCESSORS. I AM PREPARING THIS AT THE VERBAL REQUEST OF CHARLENE DOUGLASS, DS-4. THIS RECOLLECTION IS BASED ON NOTES WHICH I TYPED INTO THE COMPUTER ON JULY 1. I DO NOT KNOW IF THE VARIOUS SUBJECTS WERE DISCUSSED IN THE EXACT ORDER PRESENTED HERE.

I RECEIVED A CALL FROM AN ADULT MALE ABOUT 11:45 ON JUNE 29, 1983 AT MY OFFICE, 667-4793. HE DID NOT GIVE HIS NAME, BUT HE INDICATED THAT HE WAS THE PERSON WHO HAD BEEN ON OUR NETWORK THE PREVIOUS EVENING AND THAT HIS CALL WAS IN RESPONSE TO MY ELECTRONIC MAIL INVITATION. I BELIEVE HIS OPENING REMARK WAS "THIS IS YOUR PHONE CALLER".

HE EXPLAINED HOW HE HAD BEEN ABLE TO GET INTO THE VARIOUS COMPUTERS OF THE NETWORK IN SPITE OF OUR SECURITY PRECAUTIONS. HE SAID THAT HE INTENDED NO HARM, THAT HE HAD ONLY BEEN EXPLORING THE TOPOLOGY OF OUR NETWORK. HE SAID THAT OUR NETWORK WAS THE MOST COMPLEX ONE HE HAD SEEN AND THAT HE WAS PREPARING A SKETCH OF THE TOPOLOGY ON PAPER. HE SUGGESTED THAT IF WE GAVE HIM A NORMAL ACCOUNT ON OUR MACHINE, HE COULD COMMUNICATE FURTHER SECURITY IDEAS. I TURNED DOWN THAT SUGGESTION BUT I INVITED HIM TO SEND A WRITTEN REPORT, CAUTIONING HIM THAT HE MIGHT BE WISE TO CONSULT AN ATTORNEY.

JOHN F. DAVIS

```
$ LO
[?5L
```

What were the "security" flaws? We should document them

Wyden
$ computers
vs $ security

ICN User Summary -- 09/22/83 11:53

NSC Total Entries		5084	
Production Numbers		0125	
CCF Operators		0059	
Terminal Users		4900	
By Max. Level	D		1327
	U		2698
	P		0065
	C		0004
	S		0806
Data Base Total Entries		5331	
Active Users		4900	
Temporarily Inactive		0013	
Production Numbers		0125	
CCF Operators		0059	
NOS Secondary Accounts		0218	
Open Partition Only		0025	

5
4
3
4
16

PNL 250
G ?
MFEVAX 50-100
OFUAX 450
STORES 70
ADPDP2 70
AADPDP3 70
ICNDP1 ~50
ESSDP1 ?
ESSDP2 ?
QVAX2 102
SIVAX 80

MPDP0 500+
CTRVAX 150-125
MGUAX 85-90
ZIA 20

Late May 4/4
7 members

Next 10 12 th
3/4 th

3/0

Tiger team - can't answer
emanations security -
typewriter - can't
answer
a program

change pwd
leak from FA

trusted
verified
HW/SW

Magda Krance
Time
N.Y.T
Chi. 312-275-8833

temp approval
WP & computer

7/4 Times (Sunday 9.25)
article on Comp. Sec.

Nelson
Wyden
Gore
Taylor
Glickman
Carney
J. Jeffers Hirons?