LA-UR-17-30518
Approved for public release; distribution is unlimited.

Title: 414 Intrusion LANL June 1983

Author(s): Malin, Alex Barry

Intended for: Cyber Fire, 2017-11-16 (San Diego, California, United States)

Issued: 2017-11-16 (Draft)

414 Intrusion LANL June 1983

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, MPDP0, MPFG0
Accounts: NETPRIV - (used to gain access on MX G)
DECNET (gained the passwords to all open DP Vax's)
MP4NC (account set up on MPDP0 VAX)
Suspects: Adult male residing in Wisconsin
Direct Involvement: [redacted], C-8.
Interviewer : [redacted], OS-4
Interviewee: [redacted], C-8

On 28 June 1983 at approximately 2150 hours, [redacted] 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 [redacted] 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 th[redacted]e VAX's on XNET: MPDP0, ESS1, and MPFG0. The DECNET account on the M[redacted]0 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.

[redacted] 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 [redacted] 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. [redacted] immediately fixed the holes. The intruder did not identify himself.

If this person were a sophisticated user (as he apparently wa[redacted] 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.

Continued investigation of this incident by OS-4, C-8, and th[redacted] 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 MPDP0 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 b[redacted]S-4 and ADP has determined unauthorized access on two of the ADP D[redacted] 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 [redacted] essor.

[redacted] of Telenet Security called [redacted] on 29 June, 1983, and advised him of the suspected intrusions by this person at several other sites throughout the country.

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 [redacted], 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 [redacted] 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, [redacted]. 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
%PORT 45130 ON A: CHARS IN 01031 (ERR 00000); CHARS OUT 43588
@231 1983-08-19 08:43:11
$DG  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: [redacted]
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 [redacted] 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, [redacted].  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.

[redacted]

$ LO
[?5L
```

Los Alamos

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

memorandum

TO: Listed Group [redacted]

DATE: July 15, 1983

FROM: [redacted]

MAIL STOP/TELEPHONE: F679/7-1355

SYMBOL: OS4-83300

SUBJECT: Distributed Processor Security Meeting

A meeting to discuss unauthorized DP accesses and related security concerns will be held Tuesday, July 19, 1983, at 1:30 p.m., in the Tappa Room (SM-43, Room A330). It is imperative that your DP system manager(s) or an alternate attend this meeting. Attendees must bring a configuration diagram and equipment list for each DP owned by your organization.

Cy: [redacted]

OS-4 File 5.22./

Info copies sent to appropriate Division Leaders via INFORM

Los Alamos
Los Alamos National Laboratory
Los Alamos, New Mexico 87545

memorandum

DATE: 1983 August 2

TO: Listed Open DP System Managers

FROM: [redacted]

MAIL STOP/TELEPHONE: F679/1355

SYMBOL: OS-4-83303

SUBJECT: FOLLOW-UP DP SECURITY MEETING: REF: OS-4-83300 - JULY 19, 1983

A follow-up meeting to discuss Open Distributed Processing security issues will be held on Tuesday, August 9, 1983 at 1:30 pm in the TAPA Room of TA-3, SM-43, Room A330. Please be represented.

Cy: [redacted]

[redacted]

TIMES AND DATES OF INTRUSIONS

JUNE 17, Attempted but unsuccessful
June 23, 1983 at 00:56 MDT
June 24, 1983 at 00:13 MDT
June 24, 1983 at 23:33 MDT
June 25, 1983 at 00:09 MDT
June 28, 1983 at 21:36 MDT
June 28, 1983 at 22:15 MDT
June 29, 1983 at 00:08 MDT

ACCESS TECHNIQUES USED

TELENET was used to access Machine G on the ICN and DECNET was used to access the other VAX's after the passwords were obtained. Further investigation has determined one questionable access to the ADP STORES VAX from the Distributed Processor at Pacific Northwest Laboratories. This access is being investigated. Investigation found this access to probably be valid due to a program executing at Battelle designed to map the network from their DP.

OPERATIONS PERFORMED ONCE ACCESS WAS OBTAINED

After access was granted into Machine G, the perpetrator created a command file that dumped the DECNET database containing passwords to his remote terminal. The NETPRIV account had the following privileges assigned to it: DIAGNOSE, TMPMBX, OPER, NETMBX. These priviliges allowed a dump of the database to the remote terminal. Access was then gained to the other VAX's in the OPEN partition by using the "SET HOST" utility and the DECNET passwords. Continued investigation has revealed a 38 hour operation performed on the ADPDP2 VAX that is highly suspicious. The operation involved memo verification on that DP. Further investigation revealed the probability of a Los Alamos execution of a program that apparently started looping. The start time is still questionable.

TYPE OF ACCESSIBLE INFORMATION

We have not proven yet that any information other than DECNET passwords was obtained but there was certainly the opportunity for access to several types of information including the following:

Mx G - databases including clerical communications information, source files for C-Div utilities, DECNET passwords, some ICN passwords and user numbers imbedded in the system, unclassified scientific computing, Mx G accounting files.

OFVAX - Laboratory clerical information (phone book), and the Laboratory Electronic Mail System.

ESS10 - unclassified scientific word processing, databases pertaining to NASA and military satellite information and the codes that process satellite information.

MP VAX - Data analysis and support information for Los Alamos Meson Physics Facility.

ADPDP2 VAX - Laboratory mail from the following divisions:
ADP, MAT, PA

STORES - Laboratory warehouse (stock) information.

*** It has been determined through further investigation that the intruder attempted to gain access to the ZIA DP but failed. Access was gained to the S1VAX through the GUEST account but the intruder did not linger on this machine. Access was also gained to the QDVAX and we are still investigating operations performed during intrusion. Access to the Battelle DP was attempted but unsuccessful. It was possible, however, to explore the system by simply being logged on to an account with no privileges. This feature was available on the entire network, so the intruders had the ability to explore the systems without actually doing anything else.
Accounting logs were lost from
the ADPDP3 DP that contained information relating to all the information services of the Laboratory. We are fairly certain that access was attempted and possibly gained to this DP due to the access patterns previously established.

DISRUPTION, DAMAGE, OR LOSS

At this time, we have , to our knowledge, experienced no loss of information. Alterations were made to privileges on some accounts and a new account established with the ability to set privileges for all accounts.
The disruption has been extensive, requiring, up to this time, and we are still investigating, approximately 3 to 4 man months of tracking time between the groups involved.

VALUE of TELENET TIME USED
As near as we can determine, the Telenet time involved cost the Laboratory at the most approximately $150.

COST OF FUTURE PREVENTION

About 10 hours of software changes were made to all the VAX's to prevent future access. Telenet changes were made at the cost of $100 per month for future access to telenet.

PERSONS WILLING TO TESTIFY

AUG 18 1983

MA-24

Unauthorized Access of a Los Alamos National Laboratory Computer System

Those on the Attached List

The recent incident reported by the National media of an unauthorized access of a Los Alamos National Laboratory (LANL) computer system by a group of youths from Milwaukee has brought to our attention some things of which all of us in the Department of Energy should be both aware and concerned.

- The movie "War Games" is inspiring those with home computers to attempt unauthorized accesses to computer systems. The perpetrator was portrayed as a hero, not a criminal.

- The CBS television network has announced a new drama series entitled "Whiz Kids" this fall that will feature teenage computer hackers as its heroes. How many more will be inspired by this series?

- The main character of the movie "War Games" has become a real part of our society as the sale of home computers is increasing exponentially and elementary and secondary schools are teaching computer programming courses.

- Computerized "bulletin boards" are being used by computer snoopers to exchange information about how to get into various computer systems.

This incident further supports the need for a strong and effective computer security program as required by DOE Orders 1360.2 and 5636.2. LANL detected the unauthorized access, reported the incident to DOE, provided information to the Federal Bureau of Investigation which lead to the identity of the suspects, and corrected the deficiencies which permitted the unauthorized access to prevent a reoccurrence. Who can say what might have happened or how long the unauthorized accesses would have continued if LANL had not had an effective unclassified computer security program in place.

Although no classified or sensitive information was compromised, disruption was extensive requiring approximately three to four man months of tracking time and the investigation is still continuing. As near as can be determined, the TELENET time involved cost LANL approximately $150.

We learned some important things from the incident at Los Alamos. Most importantly is the need for conscientious systems management. It has been said many times that security is simply good management practice. The incident at LANL happened because of careless systems management. Unauthorized access was gained either through a default account that was part of the operating system as delivered by the vendor or through a system account required to access DECNET. There were several of these accounts, all of which are well known. Some of them are even published with their passwords in the vendor's manuals. So anyone with the vendor manual had an

account name and password to log on, once connection to the system was successful. Since the system manager at LANL had not changed the well-known passwords, the perpetrator was successful at gaining unauthorized access.

Descriptions of the techniques used by the group in Milwaukee to gain access to the LANL computer system and the actions taken or planned by LANL to correct the deficiencies and prevent reoccurrence are attached. Articles from various newspapers about the LANL incident are also attached.

I strongly suggest that you discuss this information with management and the computer protection program manager at each of your sites to evaluate their possible vulnerability to these techniques and to determine if any or all of the actions taken by LANL would be appropriate for implementation.

If you have any questions or need additional information, please call me on FTS 233-3307.

[redacted]

Attachments (3)

[redacted]

MA-24 Reader
MA-24 Official File
[redacted]

Techniques Used by the Milwaukee Youths to
Access the LANL Computer System

1. Gain access to TELENET.

   Local access numbers are available on a number of bulletin board systems. Telenet numbers in other cities can be accessed via SPRINT and MCI.

2. Obtain a valid TELENET port number.
   Again, valid port numbers are available on bulletin board systems. TELENET's algorithm for generation of port numbers is to append a two or three digit number to the Bell System area code; for example, a system in San Francisco would be 415nn or 415nnn.

3. Look for a VAX/VMS Login prompt.
   The VAX/VMS login prompt is easily recognizable. Other systems with recognizable login prompts are Digital Equipment Corporations RSTS system for PDP 11/34 and similar hardware, and Prime Computer's PRIMOS system. Other systems, including IBM's VMS and CDC's NOS, are "too difficult to crack".

4. Try gaining access to the system.
   Again, some user identification codes (UIC) and passwords (PW) can be obtained from bulletin board systems. There are some UIC/PW pairs that are standard in VAX/VMS systems: SYSTEM/MANAGER, SERVICE/FIELD, and SYSTEST/UETP. These passwords are described in DEC documentation, and should be changed by the system manager to something more secure. There are numerous UIC/PW pairs that are frequently implemented by system managers with varying degrees of privilege: DEMO/DEMO, NETWORK/NETWORK, TEST/TEST, etc. Access to the system at the lowest level of privilege allows a user to list the other users active on the system. Since users choose their password to be identical entirely too frequently, access through UIC/UIC type accounts with more privilege is possible.

5. Try to stay on the system.
   A number of methods are used by this group to retain access to a system they have penetrated. The first objective is to find a way to get one of a set of special privileges. One such privilege is CMKRNL, change mode to kernel. Given this privilege access may be gained to a SYSTEM account. Given access to a SYSTEM account the AUTHORIZE utility may be used to create new accounts on the system, or to modify the privilege of existing accounts. A second method of retaining access is to change the password on an existing account to a null password.

   A slightly more sophisticated approach involves embedding AUTHORIZE commands in files which are used in system recovery and login processes. The presence of a LOGIN.COM file in a users root directory causes the system to execute a user specified set of commands each time the user logs into the system. This user specified set of commands is executed after the commands specified in a file generated by the system manager named SYLOGIN.COM

ATTACHMENT 2

Actions Taken or Planned by LANL to Prevent Reoccurrence

1. TELENET changes were made at the cost of $100 per month. Basically, LANL eliminated the ability by its system to accept "collect" calls. Prepaid TELENET calls require the caller to provide a valid identification number and password. "Collect" calls require no identification or password and the connection is made without any screening by TELENET to ensure the caller is a valid user. By not accepting "collect" calls, LANL is assured that callers are screened by TELENET security and only those providing a valid identification and password are connected to their system. If this technique is appropriate for implementation at a site, responsible personnel at the site should contact their TELENET sales representative for assistance in completing the task.

2. About ten hours of software changes were made to all of the VAX's to prevent future access. Basically the changes involved changing passwords on the well known accounts as well as those user accounts where the account name and password were identical.

3. LANL plans to discuss the case with Digital Equipment Corporation and possibly other vendors to get improvements in the VMS system or installation procedures.

4. LANL plans to talk to other victims of the group of Milwaukee youths to determine if any other actions can be taken to reduce the vulnerability to unauthorized access.

Department of Energy
Albuquerque Operations
Los Alamos Area Office
Los Alamos, New Mexico 87544

August 17, 1983

JFM	
RES	
RP	
DB	
LHB	
JR	
DMQ	
LL	
Cys:	OS-4, CSA
File:	

[redacted]
Special Agent in Charge, FBI
United States Department of Justice
P. O. Box 25186
Albuquerque, New Mexico 87125

Dear [redacted]

CASE #LAAO-2-83

This letter formally opens a Los Alamos Area Office, U.S. Department of Energy case on the two incidents involving the Los Alamos National Laboratory's linkup with the independent commercial computer network "TELENET." The first incident occurred May 9, 1983. The second incident occurred June 28, 1983.

The details of these incidents have been provided to your staff by [redacted], Division Leader, Operational Security & Safeguards Division, Los Alamos National Laboratory.

If we can be of any further assistance in this matter, please advise.

Sincerely,

[redacted]
Chief, Security & Fire
Protection Branch

LSFP:MBP

DC	
DEC	
WSB	
CMC	
CD	
HWE	
CAG	
DGH	
TGH	
NAK	
RDK	
FHL	
NJP	
JQ	
GAS	
MLS	
RAY	
DJS	
FILE:	5,32.1
CYS:	

[redacted]

22 AUG 83 15: 42

RECEIVED OS-4

-RCVD: 03-[illegible]

18 AUG 83 9: 32

Los Alamos

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

memorandum

TO: DISTRIBUTION

DATE: August 26, 1983

FROM: Donald M. Kerr

MAIL STOP/TELEPHONE: A100/7-5101

SYMBOL: DIR

SUBJECT: SECURITY OF LABORATORY OPEN COMPUTING SYSTEMS

The open partition of the Laboratory's Integrated Computer Network and other open Laboratory computers provide a valuable and necessary mechanism for interaction between our staff and others. Although no classified or sensitive information is processed on such systems, recent events demonstrate the need for an appropriate level of protection for these computers and the information they contain.

In order to assure this, any major changes to the open partition or its associated distributed processors must have written approval from the Laboratory Computer Protection Program Manager (Dottye Camillo, OS-4, 7-4844, MS F679) prior to becoming operational. This specifically includes the connection of any external network. In addition, this approval must be obtained before external networks or remote access capabilities are added to other open Laboratory computers.

cyf	DC
	DEC
	WSB
	CMC
	CD
	HWE
	CAG
	DGH
	TGH
	NAK
	RDK
	FJH
	NJP
	JO
	GAS
	MLS
	RAY
V	DJS
FILE:	
CYS: as marked	

Distribution:

Streamline Management

[redacted]

Open Partition System Managers

[redacted]

RECEIVED OS-4

50 AUG 83 15: 57

[redacted]

Statement

to the

House Committee on Science and Technology

Unauthorized Computer Accesses at Los Alamos

J. McClary
D. Camillo
September 1983

Mr. Chairman, I am Jim McClary, Division Leader of the Operational Security and Safeguards Division at the Los Alamos National Laboratory. With me is Dorothy Camillo, Group Leader of the Computer and Telecommunications Security Group at Los Alamos. The Operational Security and Safeguards Division has responsibility for establishing and maintaining security at Los Alamos. The Computer and Telecommunications Security Group within the Division has responsibility for those specific aspects of security at the Laboratory.

I wish to thank you for the opportunity to come here today to discuss the incidents involving unauthorized accesses by the so-called "414s" to open computers at the Laboratory. I plan to discuss security in the Los Alamos Integrated Computing Network, the "414" incidents of unauthorized access, the Laboratory's response to the incidents, and some conclusions we have drawn from these events.

At the outset, Mr. Chairman, I would like to emphasize that the computers involved in this incident are not used to process classified or sensitive information. Therefore, this incident involved no compromise of such information. It did consume the time of the system managers, security personnel---and our Public Affairs Office. In a moment, I will discuss the intrusions. But first I will describe the basic security structure of our computing network at Los Alamos.

The Laboratory's Integrated Computing Network processes data of a wide range of sensitivities on many different types of computer systems. Because of the difference in data sensitivities, which range from unclassified scientific information to Secret Restricted Data related to the design of nuclear weapons, and because of the diverse user population, we place a strong emphasis on matching the level of protection in a system to the sensitivity of the data.

At Los Alamos we place computer systems into one of three categories based on the sensitivity of the data processed. In the Integrated Computing Network these categories, or partitions, are referred to as the Open Partition, the Administrative Partition, and the Secure Partition. The incident being discussed today occurred at the periphery of the Open Partition.

The Secure Partition is the only portion of the Integrated Computing Network where classified data is processed. Users of the Secure Partition must be Q cleared and authorized for access by their management. They must be located at physically protected terminals communicating over a protected distribution system and must submit a password which is itself classified in order to do classified work.

Terminals authorized only for the Administrative or Open Partitions of the Network are not allowed to access computers in the Secure Partition. There is no dial-up access to the Secure Partition.

The Administrative Partition is used to process sensitive unclassified data such as financial information and data subject to the protection of federal or state privacy acts. Users of this partition are Laboratory employees who have obtained specific management authorization. There is no dial-up access to this partition either.

In the Open Partition, we allow only work which is unclassified and is not administratively sensitive. The authorized users of this Partition are Laboratory employees and others who have legitimate reasons for computing at Los Alamos and have contractual agreements with the Laboratory. A typical non-employee user might be an employee of a Laboratory subcontractor, a University Faculty Member, or an employee of some other DOE prime contractor. Dial-up access is provided for computers in this partition, and the users need not be cleared.

Although this partition is called "Open", it does not mean that the substantial computing resources available are unprotected or are available to everyone. Each user of the Integrated Computing Network is assigned a unique identification number and sign-on password. All passwords are issued by the Computer Security Group. They are randomly generated and changed at least yearly.

Every attempt to sign on to the Network requires that the user submit his or her unique identification number and password. These are checked by a separate computer called the Network Security Controller. If they are correct, the user is allowed to access computers on which he or she can run his or her own programs. Five incorrect attempts to supply a password are allowed. After five failures, the identification number is locked out until a security officer has taken action to allow the user to try again.

In addition, each of the three Network partitions has a gateway computer which allows authorized organizations to connect their own Digital Equipment Corporation VAX computer systems to the partition.

These computers, called Distributed Processors, are operated and maintained by the user organizations. Within the Open Partition, system managers of the Distributed Processors are responsible for authorizing people to use their systems, for control of passwords, and for monitoring usage of the system. They are constrained by DOE requirements (which implement OMB Circular A71) that the system be used only for official business. However, a standard ICN user number and password are required to make use of the gateway.

Telenet is connected to one of these Open Partition Distributed Processors. This computer, referred to as Machine G, was the one initially accessed by the youths from Milwaukee. In the following discussion, the computers in question are Distributed Processors attached to the Open Partition.

Late on June 28, 1983, the system manager for Machine G discovered unauthorized activity under a privileged account. He immediately reported it to Computing Division personnel who, in turn, notified Computer Security. Investigation showed that the intruder accessed Machine G through its Telenet link. Telenet Customer Service was notified and their personnel traced the call. I was notified by Telenet the next morning that similar activities from this number were currently under investigation by the FBI. Further checks of our records revealed that the intruder had probably gained access through the use of "standard" passwords. The system managers for all the Open Partition Distributed Processors were notified and asked to examine their logs for unauthorized activity. We also learned, from a review of earlier logs, that the intruder had accessed Machine G as early as June 23rd.

The intruder appeared to be interested in developing a map of the Distributed Processors attached to the Open Partition of the Network. Having gained access through an account with full system privileges which had the password listed in the Digital Equipment Corporation manual, the intruder could access the Open Partition Distributed Processors but could not reach the worker computers in the Open Partition proper. Activity logs led us to an account which had been created by the intruder, which

we immediately destroyed. Later we found indications that a program may have been executed and that the accounting records may have been destroyed by the intruder.

Again, let me emphasize that no classified or sensitive data was available on these machines.

The Security Division reported the penetration of the Open Distributed Processor network to the DOE Area and Operations offices and the FBI on June 29th.

The Machine G system manager immediately changed passwords to all privileged accounts and the Computing Division was asked to modify Telenet access to force a sign-on check by the Network Security Controller. This change was made within 48 hours.

A meeting of Distributed Processor system managers was called on July 19th. The system managers were instructed to make sure that their systems did not have any privileged accounts with identical user numbers and passwords, or passwords published in Digital Equipment manuals. They were also instructed to review the privileged accounts and verify that users with privileges actually had a need for such access.

The Director of the Laboratory issued a memo to Laboratory management emphasizing the importance of security in our Open computers. This established the requirement that written approval from the Laboratory Computer Protection Program Manager must be obtained prior to any major changes to the Open Partition is Distributed Processors.

Further controls were initiated by the Computing Division, with the cooperation of Telenet, to assure that a Telenet user is authorized to access the Telenet link to Los Alamos.

This incident happened because we connected Telenet, a known target for hackers, to an open computer and did not take full advantage of available deterrents. These deterrents have now been implemented and we have seen no further successful intrusions.

The financial losses to the Laboratory were not large. The Telenet and computer time cost less than $300. The disruption, however, required three to four work-months of effort on the part of system managers and security personnel in establishing exactly what the intruders had done.

Now, what could they have done? I cannot to go into detail in an open forum, but the intruders could have caused confusion, delay, and perhaps incorrect results for many users of the Open Distributed Processors.

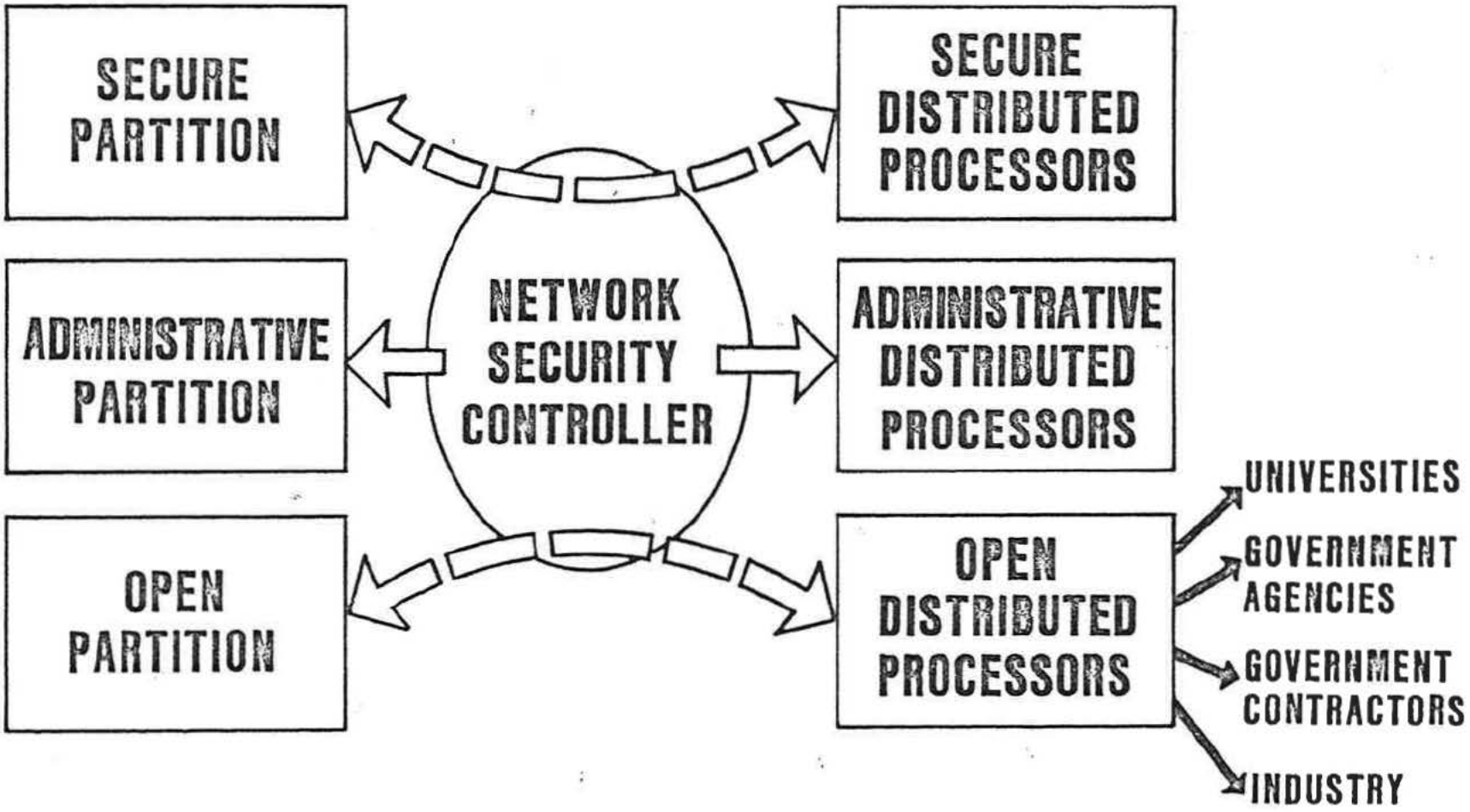
I would like to close by pointing out that we must be realistic about access to open computing systems. The Los Alamos National Laboratory is a national resource and, as such, does a great deal of unclassified, non-sensitive computing in collaboration with the rest of the academic and scientific community. This work is important and can only be accomplished by providing mutual access to appropriate computing resources for researchers around the country. The security built into our Integrated Computing Network allows us to do this without jeopardizing classified or sensitive information, but unauthorized accesses of the kind we are discussing today will occasionally occur in open computers. We must, and will, do what we can to minimize unauthorized access but we must also realistically balance the benefits of shared computing against the risk from such events.

There are areas where the entire computer security community needs help. First, there are not enough people with the proper expertise and training in computer security. Programs to develop such individuals are badly needed. Second, better-low cost methods for identifying computer

users are needed. The password systems in use today are vulnerable to attacks based on lost or stolen passwords and do not provide us with sufficient confidence that the user has been accurately identified. On the other hand, systems that can provide greater confidence are too costly for most applications. Third, a much wider use of encryption would make a major improvement in the security of computing systems. The development of inexpensive encryption devices would lead to systems which are much more secure than those currently in use. Finally, we need a realistic attitude toward those who abuse information processing systems. Obtaining unauthorized access to a government or private sector computer system is not a game. At best, it is a willful act little different from a joyride in a stolen car. Given the equipment, knowledge, and preparation necessary to accomplish even the unsophisticated intrusion being discussed today, it is more realistically compared to breaking and entering a government office. We should not dismiss the culprit because the office had windows.

Mr. Chairman and members of the committee, thank you for this opportunity to speak to you today.

INTEGRATED COMPUTER NETWORK



U.S. DEPARTMENT OF ENERGY
ALBUQUERQUE OPERATIONS OFFICE

DATE: OCT 13 1983

REPLY TO ATTN OF: SSD:RWS-281

memorandum

SUBJECT: Computer Security Information

JFM	
RES	✓
RP	✓
DB	✓
LHB	✓
JR	
DMQ	
LL	

TO: [redacted], Area Manager, Amarillo Area Office
[redacted], Acting Area Manager, Dayton Area Office
[redacted], Area Manager, Kansas City Area Office
[redacted], Area Manager, Los Alamos Area Office
[redacted], Acting Area Manager, Pinellas Area Office
[redacted], Area Manager, Rocky Flats Area Office
[redacted], Director, Information Resources Management Division, AL

Cys: OS-4

File: 1105

Attached are two newspaper articles that we recently received from DOE Headquarters relating to computer break-ins. The text of the Headquarters transmitting memorandum is quoted below.

> "Recently, there have been many newspaper articles on computer 'hackers' penetrating ADP systems (i.e., Los Alamos National Laboratory). Attached are two which appeared in the Washington Post that seem to be the most factual.
>
> These articles indicate the need to strictly enforce the existing DOE policy that no external unencrypted telephone lines be connected to any ADP system processing classified information. From time to time, I have heard that certain internal software controls are available which would preclude classified information from being transmitted to a specified terminal dedicated for unclassified traffic. As of this date, there does not exist an approved 'trusted software package' capable of protecting classified information.
>
> It is requested that you review the ADP systems under your responsibility to ensure that the existing policy is being followed."

Please insure that the above information and attachments are furnished to appropriate contractor personnel, especially security and responsible computer security personnel.

If there are any questions, please do not hesitate to call.

[redacted]
Director, Safeguards and
Security Division

2 Attachments

cc w/Attachments:
[redacted] Group Leader, OS-DO, LANL
[redacted] Manager, Computing Services
Department, Organization 2610, SNLA

GTE Telenet
Communications Corporation

1700 North Moore Street
Suite 1710
Arlington, Virginia 22209
703 243-7510

August 18, 1983

[redacted]
Los Alamos National Laboratory
Network Engineering
P.O. Box 990
Los Alamos, NM 87545

Dear Mr. [redacted]

Per your request, I am enclosing all Host Port Utilization reports for Los Alamos National Labs. Our system was able to provide reports only back to January, 1983, and, I hope this proves helpful.

Each month I will send you the current report as soon as it is available.

Sincerely,

[redacted]

Sales Administrator

[redacted]

Enclosures