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.

Larry Martin
Office of ADP Management

Attachments (3)

cc:
Michael Orosz, MA-24
David Jones, DP-343.2
David Bailey, LANL

MA-24 Reader
MA-24 Official File
MA-24:LGMartin:ldd:353-3307:8/18/83

Addresses for Memorandum dated AUG 18 1983

D. Roberts, AL
Al Chernoff, AL
G. Lewis, NV
E. McCallum, CH
S. Ball, SAN
G. Miserendino, SR
H. Highland, RL
M. Harris, OR
J. Marmo, ID
F. Eckerson, GJ
S. Kauffman, NE-60
A. Linden, EI-10
K. Hoag, SPRO

ATTACHMENT 1

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.

ATTACHMENT 3

MILWAUK

50 Pages, 5 Parts

Thursd

FBI investigates raids by 10 on computers

By Bruce Gill

Getting some ideas from the movie "WarGames," 10 Milwaukeeans between the ages of 15 and 22 recently gained access to computers owned by a dozen US and Canadian firms, including a nuclear weapons research laboratory, The Milwaukee Sentinel learned Wednesday.

The result, sources said, is a full-fledged FBI investigation.

"We really did it this time," said a 21-year-old man involved in the incident. "It's really easy to do."

Some of the people are members of an Explorer Scout post that meets at IBM Corp., 611 E. Wisconsin Ave., but the man said the computer project had been done on home computers and was not connected with the Explorer post or IBM.

The nuclear weapons laboratory computer was at the Los Alamos (N.M.) National Laboratory, which is operated by the University of California for the US Department of Energy.

"Los Alamos has a computer connected to TELENET, a computer communication network," said James Breen, public affairs officer for the laboratory. "This computer, which processes only unclassified data, was accessed from Milwaukee by an unauthorized person. The access was detected in late June by the laboratory and reported to the Department of Energy.

Probe Turn to Page 10

FBI probes computer raids by 10

Probe From Page 1

"The incident is currently under investigation by the FBI. No classified or sensitive data was compromised in the incident."

Still, a Los Alamos Chronicle newspaper source has said the lab has changed its security codes because of the incident.

Spokesmen for the Milwaukee FBI office declined comment on the investigation.

A Los Angeles (Calif.) bank also has turned over information to the FBI, a bank spokesman said.

"Yes, the bank did some weeks ago detect what appeared to be unauthorized use of the bank's general purpose computer," said the spokesman for the Security Pacific National Bank. She said there was "a Milwaukee connection" to the break-in.

The Chronicle's source said the bank had placed a game in the computer in an attempt to trap those involved. The bank spokesman declined to explain the trap that was set, but told The Sentinel: "We did initiate a series of countermeasures to thwart the problem, and they were successful. The matter was reported to the FBI. The problem did not affect customer funds or customer records in any way."

A 15-year-old Milwaukee youth told The Sentinel Wednesday that he had been interviewed by the FBI last week. The youth was involved in an earlier incident in which he raided a computer in Milwaukee.

The organization that owned that from the youth and his parents. The youth's lawyer, Jeffrey A. Reitz, said Wednesday a somewhat smaller cash settlement was reached. Reitz said the youth had worked alone on that project and added: "There was no intent to cause damage. It was the challenge."

Referring to the recent incident, the youth told a reporter, "There's a bunch of people involved."

The 21-year-old man said 10 people ranging in age from 15 to 22 were involved. Computers from a dozen companies were broken into, he said.

"We're sort of a close group," he said. "My friends and I are in a lot of trouble for it.

"It's really easy to do," he said. "All you have to do is find someone with a computer and a modem (a device that enables a computer to transmit and receive information by telephone). And we all have computers and modems."

He said they had launched their computer raids from their homes. "It got out of hand, but it's not all our fault either. There's no security in it or nothing. It didn't take too much intelligence to get into the things."

He said the group called a local TELENET telephone number to gain access to the computers. A spokesman in that company's Virginia offices had no comment.

The man said the raids had begun about the time the movie "WarGames" was released in June. He said the 10 individuals involved had seen the movie just after they began their raids and acknowledged they had gotten "some ideas" from

The movie is about a teenage computer whiz who uses his home computer to gain access to a war-games computer, not realizing it is a Defense Department machine controlling real nuclear weapons. The game-playing almost starts a global thermonuclear war.

"We came up with a lot of our own ideas, and the movie just added to it," the man said.

The man said some members of the group had inserted the name of a Milwaukee doctor into an account in at least one computer they had broken into. The doctor, whom they had come to know through a computer hobby shop, now knows about the incident and is not pleased, he said.

One Canadian firm, which had suffered severe financial difficulties because of previous raids by teenagers at a private school in New York State several years ago, also was raided by the Milwaukee group, according to the Chronicle's source. But the source said the Milwaukeeans had not caused the firm further financial problems.

Unknown perpetrators have tried to break into computers owned by some Milwaukee businesses, said Dennis Hill, computer operator and manager at Milwaukee School of Engineering. Hill was hired by the school earlier this year to install a security system in the school's computer.

He said the school had detected unsuccessful attempts to break into the computer this year, most recently in late June.

"There are a lot of common-sense techniques that could be used" to protect

*

Life imitates 'WarGames' in computer raids

By Bruce Gill
Milwaukee Sentinel

Getting some ideas from the movie "WarGames," 10 Milwaukeans between the ages of 15 and 22 recently gained access to computers owned by U.S. and Canadian firms including the Nuclear Weapons Research Laboratory.

The result, sources said, is a full-fledged FBI investigation.

"We did it this time," said a 21-year-old man involved in the incident. "It's really easy to do."

Some of the people are members of an Explorer Scout post that meets at offices of the IBM Corporation, but the man said the computer project had been done on home computers and was not connected with the Explorer Post or IBM.

The nuclear weapons laboratory computer was at the Los Alamos National Laboratory that is operated by the University of California for the U.S. Department of Energy.

"Los Alamos has a computer connected to TELENET, a computer communication network," said James Breen, public affairs officer for the laboratory. "This computer, which processes only unclassified data was accessed

The Baltimore Sun

Nuclear lab is one target of 'WarGames'-inspired computer raids

COMPUTERS, from A1

from Milwaukee by an unauthorized person. The access was detected in late June by the laboratory and reported to the Department of Energy.

"The incident is currently under investigation by the FBI. No classified or sensitive data were compromised in the incident," Mr. Breen said. However, another laboratory spokesman said access to computers for TELENET users had been changed.

[Barbara Mulkin, a spokesperson at the Los Alamos lab, told the Associated Press that the portion of the computer "that was accessed is for records, messages and routine reports" and that "you cannot get into the classified system."

["There are elements of the security system that watch for unusual activity. They are built-in elements" which alerted the laboratory to the raid in June so the department was promptly notified, she said.

[The FBI office in Milwaukee said the U.S. attorney's office would be asked to consider warrants against adult members of the group. "There has been a violation of interstate statutes," an FBI spokesman said.]

A Los Angeles bank also has turned over information to the FBI, a bank spokesman said.

A spokesperson for the Security Pacific National Bank confirmed that "the bank did, some weeks ago, detect what appeared to be unauthorized use of the bank's general purpose computer." She said there was "a Milwaukee connection" to the break-in.

A source quoted by the Los Alamos *Chronicle* said the bank had placed a game in the computer in an attempt to trap those involved. The bank's spokesperson declined to explain the trap, but told the *Sentinal*: "We did initiate a series of countermeasures to thwart the problem and they were successful. The matter was reported to the FBI. The problem did not effect customers funds or customer records in any way."

A 15-year-old Milwaukee youth told the *Sentinal* that he had been interviewed by the FBI last week. The youth was involved in an earlier raid of a Milwaukee computer. The organization that owned that computer asked for $3,800 in restitution from the youth and his parents. The youth's lawyer, Jeffrey A. Reitz, said Wednesday a somewhat smaller cash settlement was reached. Mr. Reitz said the youth had worked alone on that project and added: "There was no intent to cause damage. It was the challenge."

Of the more recent incident, the youth told a reporter "there's a bunch of people involved."

The 21-year-old man said 10 people ranging in age from 15 to 22 were involved. Computers from a dozen companies were broken into, he said. "We're sort of a close group," he said. "My friends and I are in a lot of trouble for it. It's really easy to do," he said. "All you have to do is find someone with a computer and a modem [a device that enables a computer to transmit and receive information by telephone]. And we all have computers and modems."

He said they had launched their computer raids from their homes. "It got out of hand, but it's not all our fault either. There's no security in it or nothing. It didn't take too much intelligence to get into the things."

He said the group called a local TELENET telephone number to gain access to the computers. A spokesman in the company's Virginia offices had no comment.

The man said the raids had begun about the time the movie "WarGames" was released in June. He said the members of the group had seen the movie just after they began their raid and acknowledged they had gotten "some ideas" from it.

The movie is about a teenage computer whiz who uses his home computer to gain access to a war-games computer, not realizing it is a Defense Department machine controlling real nuclear weapons. The game-playing almost starts a global thermonuclear war. "We came up with a lot of our own ideas and the movie just added to it," the man said.

One Canadian firm that had suffered severe financial difficulties because of previous raids by teenagers at a private school in New York state several years ago also was raided by the Milwaukee group, according to the *Chronicle's* source.

8/11/83

THE WASHINGTON POST

'WarGames' Comes to Life at Nuclea

AROUND THE NATION

MILWAUKEE—A group of young people who got "some ideas" on computer raids from the movie "WarGames" succeeded in reaching a nuclear weapons laboratory computer before the government stepped in, The Milwaukee Sentinel reported yesterday.

No classified data was involved, authorities said.

"We really did it this time," an unidentified 21-year-old participant was quoted as saying. "It's really easy to do.

"It got out of hand, but it's not all our fault either. There's no security in it or nothing. It didn't take too much intelligence to get into the things."

James Breen, public affairs officer for New Mexico's Los Alamos National Laboratory, confirmed that a computer raid was made at the lab from Milwaukee by telephone.

He said the raid on the computer, which "processes only unclassified data," was detected in late June. "No classified or sensitive data was compromised," he said, but the FBI is investigating.

The 21-year-old was quoted as saying that 10 people aged 15 to 22 were involved, and that they also gained access to a dozen companies' computers from home computers.

He said the raids began shortly before the release of the movie "WarGames," in which a teen-age computer whiz supposedly gains access to a Defense Department computer and nearly starts a war.

At Los Alamos, meanwhile, security codes reportedly have been changed.

'Whiz kids' crack computers' code

Special for USA TODAY

MILWAUKEE — A group of 12 "whiz kids" — ages 15 to 22 — used their home computers to gain access to computers at a nuclear weapons lab, college files and a bank, the FBI said Thursday.

The raiders used a special telephone network — just as in the movie *WarGames*, in which a teen-ager gained access to a computer controlling nuclear weapons.

One of the group said the movie "gave us a few ideas."

The FBI, which said it isn't "treating the matter lightly," may charge them. But officials said "no classified data" was disclosed at the weapons lab.

8/11/83

USA TODAY