Bendix

Kansas City
Division

P O Box 1159
Kansas City, Mo 64141

The Bendix Corporation

D. E. Camillo
Los Alamos National Laboratory
P. O. Box 1663, MS 679
Los Alamos, New Mexico 87545

August 25, 1983

Dear Dottye:

Enclosed for your information are recently published Kansas City Star and Kansas City Times articles concerning computer crime. Also, you will find information on computer protection devices found in the August, 1983, issue of Security Systems Administration.

If other noteworthy information appears, I will forward it.

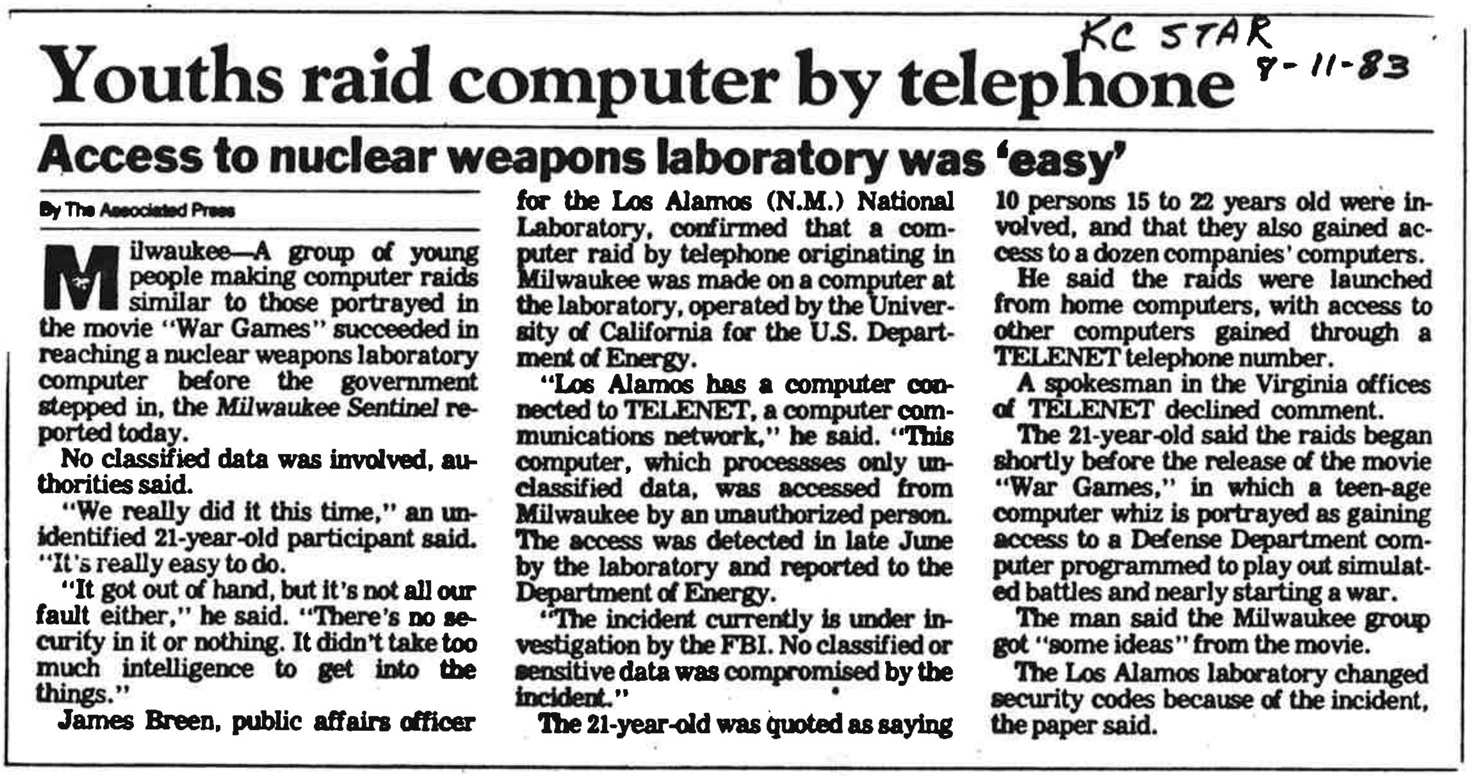
Sincerely yours,

Shirley J. Baker

Shirley J. Baker
Supervisor, ADP Security

SJB:ll

Encl.



KC STAR 8-11-83

Youths raid computer by telephone

Access to nuclear weapons laboratory was 'easy'

By The Associated Press

Milwaukee—A group of young people making computer raids similar to those portrayed in the movie "War Games" succeeded in reaching a nuclear weapons laboratory computer before the government stepped in, the *Milwaukee Sentinel* reported today.

No classified data was involved, authorities said.

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

"It got out of hand, but it's not all our fault either," he said. "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 the Los Alamos (N.M.) National Laboratory, confirmed that a computer raid by telephone originating in Milwaukee was made on a computer at the laboratory, operated by the University of California for the U.S. Department of Energy.

"Los Alamos has a computer connected to TELENET, a computer communications network," he said. "This computer, which processses 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.

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

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

He said the raids were launched from home computers, with access to other computers gained through a TELENET telephone number.

A spokesman in the Virginia offices of TELENET declined comment.

The 21-year-old said the raids began shortly before the release of the movie "War Games," in which a teen-age computer whiz is portrayed as gaining access to a Defense Department computer programmed to play out simulated battles and nearly starting a war.

The man said the Milwaukee group got "some ideas" from the movie.

The Los Alamos laboratory changed security codes because of the incident, the paper said.

Computer 'raiding' is alleged

Interference caused system on patients to fail

Chicago Tribune

Milwaukee—A 21-year-old West Allis, Wis., man used his home computer to break into a computer system at the Sloan-Kettering Memorial Cancer Center in New York City and caused the system to fail while it was monitoring treatment of the center's cancer patients, according to an affidavit filed Wednesday in U.S. District Court in Milwaukee.

The affidavit, a request for a warrant to search the home of the alleged computer intruder, Gerald Wondra, charges that he also obtained illegal access to the computer systems of several private businesses and used that access to "defraud and to obtain money and property" from the unidentified victims.

When FBI agents arrived with the search warrant at Mr. Wondra's home on July 29 he consented to the search, the affidavit said.

The affidavit said that Mr. Wondra was told that the hospital's computer system had been put out of service temporarily by his computer. He reportedly responded that "he would not do that intentionally, but that he sometimes made mistakes."

Mr. Wondra is a member of a group of Milwaukee computer enthusiasts, ranging in age from 15 to 21, who are suspected of using their home machines to break into computers nationwide, including one at the government's nuclear research laboratory at Los Alamos, N.M., and another at a Los Angeles bank.

None of the youths has been charged with a crime. Until the affidavit naming Mr. Wondra was made public Wednesday, none of the alleged computer raiders had been identified by authorities.

In the Sloan-Kettering case, the affidavit said, the intruder established unauthorized accounts and even programmed the system to make a copy of other users' passwords for his future reference, giving the intruder access to all of the cancer center's records.

Chen Chui, computer systems manager at Sloan-Kettering, told the FBI on July 8 that an unknown person had been gaining access to the center's computer since June 3. The FBI also alleged that, after the Sloan-Kettering computer system failure, Mr. Chui left a message in the computer system for the intruder "explaining the hazards of crashing the system and offering to give the intruder a free account."

Mr. Wondra received the message and telephoned Mr. Chui on June 7. Mr. Chui explained to the intruder that he was calling into a hospital computer and that what he was doing "could be dangerous to the patients" at the center, according to the affidavit.

Mr. Chui gave the intruder his own computer account, which he called "demo," and asked him to leave the rest of the system alone. According to the affidavit, however, the intruder told Mr. Chui that he was simply "curious" and was "just having fun." He said he had only been trying to make the cancer center's computer talk to his own computer, an Apple II.

A computer password? Let's try 'vulnerable'

The New York Times

MILWAUKEE — Late one night in June, a young man working at an inexpensive home computer tried to make contact with a large commercial computer.

Using a trial-and-error technique that figured in several of the recent incidents that have drawn nationwide attention to computer vulnerability, he tried various codes for gaining entry to New York City computers tied into a nationwide network.

In a short time he happened onto the combination for the computer that is used to plan and monitor treatment for patients at the Memorial Sloan-Kettering Cancer Center.

The young man entered a password that is often used to permit entry by installers and repairmen, federal authorities say, and within seconds was inside a critical system.

Using the same simple procedure, a half-dozen persons in their teens and early 20s here gained access to perhaps as many as 60 computers this summer, including ones at the nuclear weapons laboratory in Los Alamos, N.M., and a bank in Los Angeles.

The intrusions have called attention to the ease with which sophisticated computers can be entered. They have also raised questions about the effectiveness of security measures and have fueled a debate about the legal issues involved in unauthorized entry.

The young men did not "target" any of the computers, they say, but like prairie dogs popping up from holes on the plains, entered computers at random. They would go in, they say, poke through files and try to figure out where they had landed.

They did not realize they had been inside the computers at Sloan-Kettering and at Los Alamos, they say, until they were informed by the authorities or by news reports.

"I was really shocked when I heard it was a place that treated cancer patients," said 17-year-old Neal Patrick, a member of the group. Officials at Sloan-Kettering say the intruders caused administrative chaos and the deletion of records that will make it impossible to collect about $1,500 for computer services provided to other hospitals. But they say no patients were harmed.

The government has said it had no secrets stored in the computer at Los Alamos and that no damage was done.

Most of the young men have been working with computers for several years. Many hope to become professional computer specialists. They say they were eager to locate and explore new and bigger systems. "It was basic curiosity," Neal said. "We wanted to know what was going on in the world of computers. We were interested in seeing what a certain computer could actually do. It was the challenge of getting in and finding out what's there, like getting into a cave or climbing a mountain."

They maintain they saw nothing wrong with rummaging through other people's computers as long as they did no damage.

Legally they may be right. So far they have not been indicted for any federal offense. There is no specific federal law prohibiting unauthorized entry into computers, but the investigators are looking into the illegal use of telephone lines and the use of computer services without payment.

And while Wisconsin has a law, promulgated in May, that provides for up to nine months in jail for unauthorized entry into a computer, the law has no effect on surreptitious entries outside the state.

"We didn't know we were trespassing on anyone's property," said one of the young men, who, like most of the group members, agreed to talk with a reporter only with a promise of anonymity. Paul A. Piaskoski, a lawyer who has been retained by Neal's family, said the young men were stunned when FBI agents began showing up at their doors.

So far no charges have been lodged, but Mr. Piaskoski says he anticipates several indictments.

Doubts have been raised as to whether the young men really believed their actions were entirely legal.

Glenn A. Waneck, who is in charge of the computers used by students in the Milwaukee public schools, said a copy of the Wisconsin law was put into the school computers when it went into effect. He said that students were notified of the law then and that three times during the last school year they were again reminded of it.

Whatever they may have thought in the past, Neal said: "We have all learned a lesson. We don't ever want to get into any of these computers again. The potential for damage totally outweighs any curiosity I or any members of the group may have had."

As the first step in invading phisticated computers, memb the group dialed a local tel number to connect their comput leased telephone line operated GTE Telenet Communications of Vienna, Va. The corporatio vides access to 1,200 com across the country to about 150, thorized users.

When the young men located puter they would try to enter i passwords that were familiar to

"When a manfacturer ship their computers many have the password," said one of the men. "If you know something computers, it's not that hard to ine what the password could be."

"If it was particularly difficul just skip it," Neal said, "and go

Computer specialists say that puter owners are advised to c the factory-inserted passwords installation but that sometimes don't.

Dr. Radhe Mohan, director Medical Physics Computer Serv Sloan-Kettering, said that the ho computer had one of the co passwords when the young m vaded but that it was only suppo permit elementary functions. T vaders, he said, managed to throughout the computer and gram some activities, mainly to tate their re-entry.

The young men, whose home widely scattered across the city in different ways. Most are men of an Explorer post. Eventually all found themselves communic through their computers.

About eight or 10 months ago, said, they began getting togeth talk about computers. None o young men seem to recall how got the idea to invade the big con ers.

They were well along in their ac ture before the release of the m "War Games," which is the story teen-age boy who invades a N American Air Defense computer nearly — or so it seems — s World War III. But all the young have seen the film at least once.

NEWS

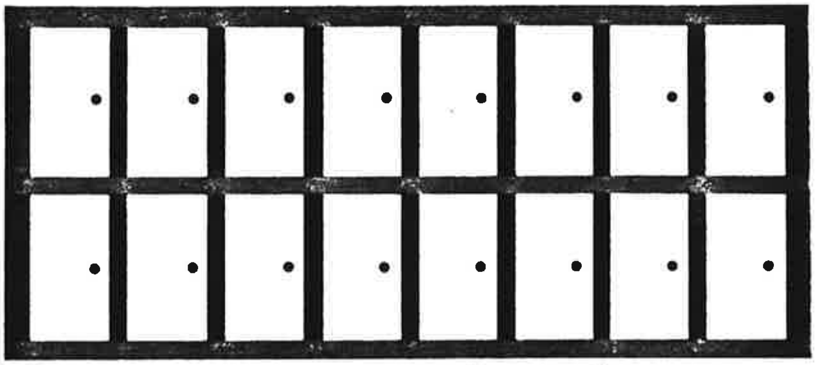
Device For Prevention of Software Piracy

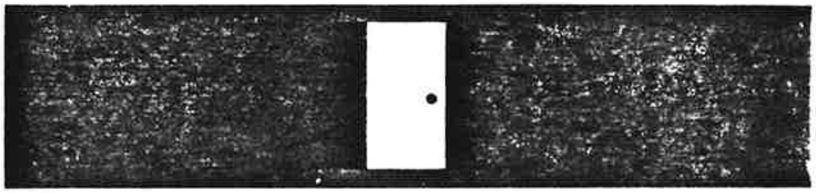
Advanced Computer Security Concepts (ADCOSEC) announced the availability of a plug-in module and associated software that will prevent software piracy on the IBM Personal Computer. The module contains a Z-80, RAM, EPROM, buffers and flags, a software implementation of the Data Encryption Standard (DES), interface software. One module can protect an unlimited number of application programs on the same IBM P.C.

The program protection software is based on ADCOSEC's patented method of using the DES. The software DES implementation was obtained from Prime Factors, Oakland, CA. The module was obtained from Cryptext, Seattle, WA., and can be inserted into any available slot in the P.C.

A demonstration package consists of an unprotected copy of a simple program and an enciphered copy of the same program, and protection software that interfaces to the module and initiates decryption of the application program. To preclude unauthorized copying of the application programs, the operational version will provide for storing and executing a small part of the application program in the module. If the software developer or distributor chooses, a different encryption key can be used with each module, substantially increasing the security level. In a financial transaction network, this approach can provide additional authentication in addition to providing for communication security.

Additional technical details and demonstration units for evaluation are available from: Marvin Sendrow, ADCOSEC, 4609 Logsdon Drive, Annandale, Va. 22003, (703) 354-0985.





SSA
Information Protection

New Computer System Handles Security Externally

This system is installed between host computer and dial-up modems

Backus Data Systems, Inc., San Jose, California recently introduced a new user programmable computer security system.

The multi-purpose, multi-channel device is easily user installed between host computers and dial-up modems and is designed to perform a high level of security checks prior to caller entry to the host.

With the majority of computer systems, remote caller connection and security password clearance is handled internally by the host computer. The fact that the caller has already gained entrance to the host computer enhances the possibility of tampering or unauthorized use.

With the Backus Security System, all log on an password recognition is handled externally to the host computer. Access to the security system directory for password changes and updates can only be done from the central side by a designated individual who is assigned the master key password which is "buried" in the systems memory.

The master password is also used to enter the system for the purpose of setting the channel configurations, i.e., baud rates, parity, bits per word and x-on x-off protocol.

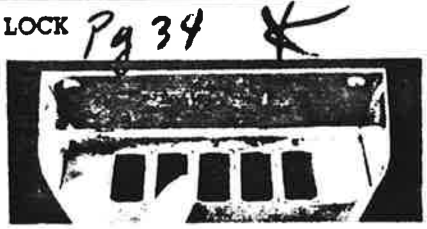
A typical six part system accommodates up to three incoming calls simultaneously. Each caller is prompted to present his designated account number and password and if desired, a telephone number for pre-programmed directory comparison. An optional program is also available whereby, one a caller leaves his telephone number and disconnects, the security system will check the number and automatically dial the caller back. Not only does the auto dial back feature provide another level of security but it also establishes a point for centralizing telephone billing.

Products And Information

Editors Note: Specifications and features of products are supplied by manufacturer or distributor.

LOCK

Pg 34



Electronic combination lock is used to unlock all types of electric door strikes and door locks. The ten-key pushbutton panel is mounted near the door outside the protected area. By entering a four-digit combination the door will unlock for a predetermined period. The system also has the capability to activate a holdup alarm if entry is made under duress. Other available options include weatherproof equipment, emergency battery standby and a selection of decorator style pushbutton panels.

Continential Instruments

More Info? On Service Card Circle Item 168

DESK TOP SHREDDER

General office shredder is a compact table top shredder that can shred continuously for 2 hours with a rate of destruction of 14 - 17 sheets per feed. It takes four computer printouts (16") at one time. High capacity torsion cutting system, ¼" shred. Comes with 6 cu.ft self contained bag holder.

Datatech

More Info? On Service Card Circle Item 169

COMPUTER SECURITY

This Telephone-Access Control Terminal, screens calls from all remote locations. The self-contained unit works in conjunction with Touch-Tone® telephones, does not require a dedicated terminal. All Computer-Sentry controls are protected by tamperproof locks. ComputerSentry's Alarm Threshold is selected by the user, who may set the unit to accept up to nine invalid attempts before an alarm is activated. The user may choose from three different alarm modes.

IMM

More Info? On Service Card Circle Item 170

COMPUTER PROTECTION

A separate piece of hardware connects between modem and telephone line. The system verifies security code via pre-programmed memory, provides port connection via "return call," and interfaces with any modem at any BAUD rate.

LeeMah

More Info? On Service Card Circle Item 171