BUSINESS MONDAY
HIGH TECH ◆ MANAGEMENT ◆ ECONOMY

FBI uses hackers' tools to sniff out hacker's lair

BY SIMSON L. GARFINKEL
Special to the Mercury News

JULIO Cesar Ardita is the perfect example electronic privacy advocates have been looking for in their battle with the FBI over electronic wiretapping.

The funny thing is, it's the FBI that found him.

Ardita is the 22-year-old Argentine computer hacker indicted March 29 on three counts of computer crime, suspected of breaking into countless computer systems across the country.

But what fascinates privacy advocates is that Ardita is accused of breaking into computers using the very same procedure the FBI and other government agencies use to eavesdrop on suspects. In the process, Ardita helped substantiate a long-running issue for law enforcement officers and privacy advocates: If phone systems are designed to allow law officers to listen in on phone conversation, crooks can listen in, too.

The FBI wiretapped 16,500 people to search for a suspected computer crook.

Should the government force telephone companies to "create" weaknesses in their systems so agencies such as the FBI can listen in on unsavory types? Privacy groups, like the Electronic Privacy Institute in Washington, D.C., believe computer and phone systems should be as close to impenetrable as possible.

Jonathan Littman, a journalist and author who spent more than a year talking with famed computer hacker Kevin Mitnick before his arrest last year, believes the Ardita and Mitnick cases prove the falsity of the government's contention.

"The Mitnick/Shimomura case advanced the strategy that it's easier to catch hackers than do the hard work in security to keep them out," Littman said.

This particular debate over government access vs. personal privacy dates to the 1994 passage of the Communications Assistance to Law Enforcement Act, better known as the "Digital Telephony Act."

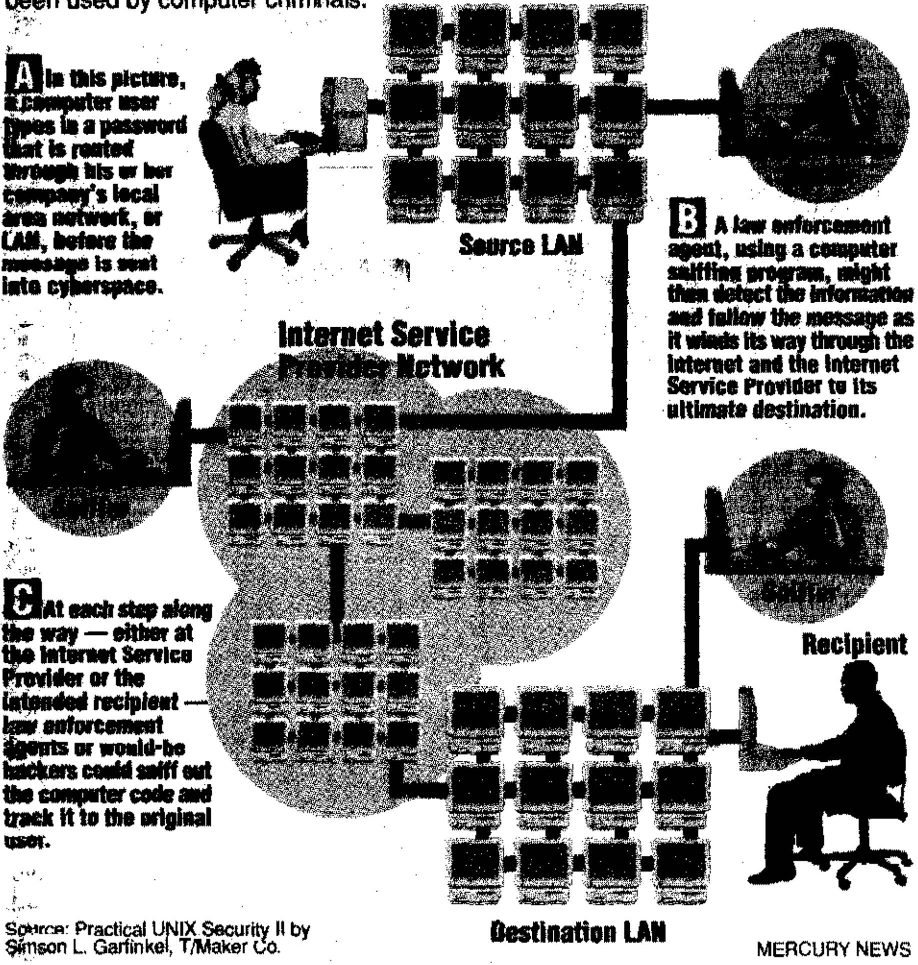
The 1994 law required sweeping changes to the nation's telecommunications infrastructure, forcing com-

*See **WIRETAP**, Page 4E*

E
MONDAY
APRIL 8, 1996
San Jose Mercury News

‘Sniffing’ out Cybercriminals

One of the newer wiretap methods that law enforcement agencies use to track computer criminals is a system known as a “sniffer.” This graphic shows how a sniffer operation might work, from various positions. The sniffer is a computer program that specifically looks for certain words or coding. Once that coding is detected, the computer system then begins to track, or sniff out, where the coding originated. This method has long been used by computer criminals.



A In this picture, a computer user types in a password that is routed through his or her company’s local area network, or LAN, before the message is sent into cyberspace.

B A law enforcement agent, using a computer sniffing program, might then detect the information and follow the message as it winds its way through the Internet and the Internet Service Provider to its ultimate destination.

C At each step along the way — either at the Internet Service Provider or the intended recipient — law enforcement agents or would-be hackers could sniff out the computer code and track it to the original user.

Source: Practical UNIX Security II by Simson L. Garfinkel, T/Maker Co.

MERCURY NEWS

Computer-crime case tread

■ WIRETAP
from Page 1

panies for the first time to build wiretap capabilities into their communications systems. But while a key aspect of the legislation was public accountability, the FBI is now more than four months late in delivering a mandated oversight report to the Congress.

"This report would be a road map to the FBI's planned revisions to the nation's telecommunications infrastructure," said David Sobel, a policy analyst at the Washington-based Electronic Privacy Information Center. "In the language of the statute, it would show the equipment facilities or services for which payment is expected to be made. This would be the first indication of what changes they are going to mandate under the authority of the new statue."

The report is "going through the administration's review process," said Barry Smith with the FBI Congressional Affairs Office. In early March, Smith said "my best guess is that it will be (released in) about a week and that's it."

Smith said that the report was delayed as a result of the two government shutdowns that occurred last fall and a major snowstorm that effectively shut down Washington for an additional week in the winter. Smith promised that as soon as the report is finished being reviewed by the Clinton administration it will be given to Congress and made available to the public.

Controversy surrounded telephony bill from the start

Since an early draft of the legislation was first circulated by the FBI in 1992, the Digital Telephony bill has been the subject of a heated controversy and cyberspace showdown between communications companies, computer irms, civil liberties groups, and aw enforcement.

The FBI maintained that rapid evelopments in the field of teleommunications were quickly utstripping law enforcement's bility to conduct electronic sureillance.

"If the technology is not fixed the future, I could bring an der (for a wiretap) to the teleone company, and because the technology wasn't designed with our requirement in mind, that person could not (comply with the court order)," said James K. Kallstrom, who was then the FBI's chief of engineering.

Civil libertarians attacked the legislation, saying that it represented an unprecedented re-engineering of the nation's telephone system for law enforcement purposes. The computer industry attacked it, saying that the wording was so broad and vague that it covered nearly anything built.

An early draft of the bill was first proposed under the Bush administration but never made it to floor of Congress. FBI Director Louis Freeh thought so highly of the revised bill that he reportedly visited every member of Congress to convince lawmakers of it's necessity.

One of the bill's most notable casualties was the fledgling cyberspace civil rights group, the Electronic Frontier Foundation. At the outset, EFF opposed the legislation, but the organization eventually switched sides and supported the bill after a series of compromises that were supposed to exclude the Internet from the legislation's coverage, and force the government to reimburse telephone companies for the estimated $500 million necessary to retrofit their existing systems to make them more easily wiretapped.

"(The legislation) limited the reach of (FBI's) design authority and excluded their reach into the Internet," said EFF's then-director, Jerry Berman, in 1994. "It places the responsibility for paying for (the modifications) where it belongs, in a publicly accountable way."

Shortly afterward, Berman left EFF with the group's top analysts and created a rival civil liberties organization, the Center for Democracy and Technology.

Two years later, the fallout is still being felt, and civil liberties groups are still battling the FBI.

While U.S. Attorney General Janet Reno hailed Ardita's indictment as proof of what electronic wiretapping can accomplish, privacy advocates say it only shows the weakness in that argument.

40-page affidavit details allegations

Although Ardita is still at large, a 40-page affidavit leased last week by the gov ment details with clinical acc cy the investigation and trac of Ardita.

The affidavit is designe support the government's a warrant for Ardita on t counts of computer crime: po sion of 15 or more unauthor access devices (computer p words), knowing and intentio ly intercepting electronic com nications, and causing more t $1,000 loss or damage to comp er systems involved in interst commerce and communications

[redacted]

The affidavit gives an unpre dented view into operations of international computer crimi with an apparently pathologi zeal for finding and targeting ne computers, taking them over, a using the capabilities gained f breaking into still more compu ers. The affidavit notes that a though there was military sens tive information on some of th computers to which Ardita alle edly gained access, there is n evidence that sensitive informa tion was taken.

'Sniffer' used to search the Internet for passwords

The government claims one of the principal techniques Ardita used to break into other computer systems is a program called a "sniffer."

A sniffer is a program that runs on a computer and monitors all of the information that passes over a computer network. The affidavit alleges that Ardita used a particular sniffer program called "sni256" which surreptitiously

n electronic privacy issues

monitored a computer network for people typing in their user names and passwords.

The affidavit alleges that Ardita's sni256 program collected people's user names and passwords, and that he used that information to log into other computer systems posing as those people.

An astonishing number of institutions had computers compromised by Ardita, according to the affidavit, including computers in Argentina and at Harvard, the University of Massachusetts, NASA's Jet Propulsion Laboratory in Pasadena, NASA Ames in Mountain View, the Naval Research Laboratory, Naval Command Control and Ocean Surveillance Center in San Diego.

ves an unprecedented view into operations of an r with an apparently pathological zeal for finding and king them over, and using the capabilities gained for uters.

For much of this work, computers at Harvard were Ardita's base of operations. And this proved to be the hacker's downfall.

Using the same sort of sniffer technology that Ardita allegedly used to sniff passwords, federal investigators placed a sniffer on Harvard University's internal network. Instead of scanning for passwords, the government's program scanned for specific sequences of letters, such as "sni256" and "griton," Ardita's alleged moniker.

Tripped up by conventional wiretaps

The government was able to trace the break-ins back to Ardita through the use of conventional wiretaps. In one case, Ardita allegedly placed a long-distance telephone call directly to Harvard's computer system; Argentine officials traced the telephone call back to Ardita's home telephone number.

In another case, Ardita allegedly placed an open invitation to other hackers to log into a bulletin board system that he operated called "Scream!" There were also numerous connections to Harvard's computer from a computer in Buenos Aires that belonged to Telecom Argentina.

"Telecom Argentina has determined that the intrusions into its host computer originated in Buenos Aires from a telephone number located in the apartment residence of Julio Cesar Ardita and his family," states the affidavit.

Apparently, few Harvard students consider the government's actions to be a violation of their privacy rights.

"The FBI checked e-mail for certain keywords before reading it. Apparently, they read only two complete messages that were not related to their case," said Gregory D. Landweber, a graduate student in Harvard's mathematics department.

Daniel Horwitz, a sophomore majoring in computer science and a member of the Harvard Computer Society, said he isn't that upset about the government's monitoring, because he never thought that the Harvard system was private in the first place.

"A Harvard system is not secure enough to keep out all potential people who wanted to read your e-mail," he said. "I don't think that there are that many people here who feel that their e-mail is important enough to keep private, and that the government shouldn't be allowed to track down these people."

Privacy advocates not placated by promises

Horowitz's comments haven't soothed the feelings of privacy advocates, who believe there is a big potential for abuse by law officers.

"The government saw what Shimomura did in the private sector, and decided that it wanted that same capability," said Littman, the author. "They wiretapped 16,500 people at, of all places, Harvard. And they have assured us that only a few innocent students or faculty members were eavesdropped on.

"Maybe that's true. But we should think about the possible far-reaching consequences. If the government can wiretap Harvard, why can't they wiretap a million people? And why isn't somebody talking about making the Net more secure, so we don't have massive wiretaps every time a juvenile starts exploiting well-known vulnerabilities that need to be fixed?"