San Jose Mercury News

FRIDAY
FEBRUARY 6, 1998

Serving Northern California Since 1851

ITION

INSIDE: U.S. sends 2,200 Marines to Persian Gulf warships/18A

Cold calls uncover vulnerable computers

BY SIMSON L. GARFINKEL
Special to the Mercury News

Over the past two years, a few laptops in Peter Shipley's spare bedroom have continuously dialed phone numbers in the Bay Area. The laptops are searching for the telltale whistle of a computer modem. When they hear the noise, they silently assess the security of the computer on the other end, then move on to the next number.

The vulnerable computers included the Oakland Fire Department's.

So far Shipley's computers have made 2.6 million calls — and found hundreds of vulnerable systems. These are computers that contain sensitive medical records, computers that control telephone and PBX systems, and even the electronic dispatch system for a major metropolitan fire department.

Fortunately, this 32-year-old Berkeley resident is no malevolent hacker, despite the LIV2HAK license plates that adorn his black Saturn SL2. He is an independent computer security consultant with more than 13 years' experience, whose past and current clients include TRW, DHL, Wells Fargo, and the U.S. Post-

See SECURITY, Page 10A

Laptop cold calls find

■ SECURITY

from Page 1A

al Service. And he is bent on proving that many organizations are failing to take even the most basic measures to protect their computer systems.

Shipley's research demonstrates that these organizations are neglecting the most direct portal to their systems — their modem connections — even as many of them are investing time and money in stringent Internet security. It is a situation he likens to bolting the front door while leaving the back door unlocked.

"I have found hundreds of system which just let you in, without even the most basic authentication," Shipley said. "One guy said, 'Why are you doing this to me?' I said, 'You are wide open.' He said, 'No, we are not.' " Shipley convinced the man of the contrary by providing him with hidden details of his network architecture.

Shipley's audit of Bay Area computer systems appears to be the largest conducted and publicized by a legitimate security researcher. The results are alarming.

Of the more than 20,000 computers Shipley's laptops have reached, roughly 75 percent respond with enough information to allow a determined attacker to break in, he says. About 1 percent of the systems have no security at all.

Shipley's colleagues in the security business say the findings are important — and credible. "I have to say I'm not surprised by any of these findings, although it does boggle my mind that he is doing that many calls," said Dr. Sanford Sherizen, president of Data Security Systems in Natick, Mass.

The findings call to mind another, more notorious such effort from recent years — the SATAN survey. In that survey, consultant Dan Farmer used a program called SATAN to scan more than a thousand high-profile Web sites on the Internet. Farmer discovered that between 17 percent and 32 percent had significant security problems.

Shipley has found a higher percentage of vulnerable systems, giving support to his assertion that dial-up systems are more vulnerable than Internet-based systems.

"At some point people are going to wake up, but I don't know what is going to make them wake up," Sherizen said.

For Shipley — a free-spirited freelancer who spends most of his time "on various programming projects and dancing (Goth and industrial)," according to his Web site — the laptop project is a labor of business and love.

He says he undertook the "volunteer" project after wondering how many computers in the Bay Area were vulnerable to break-ins — and realizing he was unlikely to find a client who would pay for the work. Of course, publicizing the effort now may draw more clients, justifying the 14,000 hours of computer time he has invested.

To conduct his survey, Shipley has walked a careful line. The phoning technique he employs, called "war dialing," is often put to nefarious purposes. Indeed, the author of Shipley's program is now in jail, a result of putting the program's discoveries to use.

Shipley himself has maintained a hands-off approach toward the data he is collecting. "I did not break into any of these computers," he said.

In fact, because this is a research project, Shipley usually has not called up companies to alert them to their security problems.

But sometimes the system he discovers is too important to leave alone. Last fall, Shipley stumbled upon the Oakland Fire Department's dispatch system. Before his computers typed anything, the system displayed a series of help screens, describing how to display the status of fire trucks and perform other operations. Shipley's next call was to a friend at the FBI.

"I called him up and said, 'Here is a number. You don't know where you got it. You might want to call it.' They fixed (the problem) in a few days."

Don Parker, assistant chief at the Oakland Fire Department, confirmed that the department learned of its security problem from the FBI. "This was an anomaly," he said. "The problem has since been corrected."

Another open modem that Shipley discovered belonged to Cody's Books of Berkeley. "I guess you may have caught me with my pants down here," said the store's owner, Andy Ross, when informed of the discovery recently. "We were installing a new version of our system. During the process, they had reduced the level of security. . . . They probably should have increased it but they just neglected to do so. We are changing that tomorrow."

But some businesses appear to be unable — or unwilling — to correct their problems.

Last summer Shipley's computers discovered a modem belonging to

Modem security

For the past two years, consultant Peter Shipley has been conducting a random test of computer modems in the Bay Area, looking for systems that lack sufficient security. Three laptops in his spare bedroom have logged nearly 850,000 minutes (1.6 years) of machine time in the project, dialing more than 2.5 million local phone numbers. Here's a look at the results:

- Phone numbers dialed: 2,594,149
- Phones that answered with modem tone: 25,058
- Of the phones with modem tone 20,256 responded with banner from connected computer
- Approximately 250 of those had no security at all
- Approximately 75 percent are open to some form of attack.

Source: Peter Shipley

MERCURY NEWS

Culligan Water
Water conditioning and purification specialists.
FREE water analysis and estimate, call now.
408-492-9111 OR 800-273-9050

New Year's Special!!!
With Physician Supervised Weight Loss
I know I can enhance my appearance safely.
Rates as low as $5/month
DOCTORS WEIGHT LOSS CENTER
629-6188

Vulnerable systems

Pediatric Care Group, a medical facility in Berkeley. The modem apparently gives any caller the ability to inspect or change any information on the group's patient scheduling and billing system.

Shipley says he has made repeated telephone calls to the group, none of which have been returned. In more than six months, the doctors' office has still not rectified its security problem. Laveenia Shaw, a receptionist at Pediatric Care Group, declined to comment on the medical practice's inaction.

Companies aren't always to blame for their security problems, Shipley said. For example, some organizations in the Bay Area use a device called a Shiva LanRover to allow employees to access their corporate network from home. Unknown to its customers, for years the LanRover was shipped with a back door, an undocumented account that had no password. A company representative said Shiva discovered the problem more than two years ago and sent out a bulletin to its registered users.

Nevertheless, said Shipley, roughly 22 percent of the LanRovers in the Bay Area still have the problem.

One such LanRover belonged to Walker Interactive Services, a San Francisco-based business that provides financial software for large corporations. Because of the nature of its business, Shipley telephoned the company.

"We did investigate and found a loophole," said Frank Yu, Walker's vice president of research and development. A person calling Walker's modem could fully access the company's internal network without a password, circumventing the company's Internet firewall.

Yu said he was thankful that Shipley had contacted his company.

Beyond the hundreds of machines that require no user name or password to gain access, said Shipley, there are thousands more systems that provide enough information for a skilled hacker to mount a successful attack. That's because many computers display the name of their organizations before asking for a user name and password. This lets a hacker attempt to guess the password or, on some occasions, trick an employee into revealing the necessary information.

Other computer security specialists say the dangers Shipley describes are quite real. "We have not conducted a penetration test in which we failed to penetrate, both through the Internet and modems," said Steven Cobb, director of education and research at Miora Systems Consulting, an information security firm in Playa del Rey that caters to Fortune 1000 companies and regional governments.

But security is not an unsolvable problem, Cobb said. "We have the technology to create secure systems. It is not being used."

The real lesson of this study, said Shipley, is that companies shouldn't let their preoccupation with the Internet distract them from the basics of computer security. "Companies are putting a lot energy into the Internet," he said. "They are bolting the front door while leaving the back door unlocked."

IF YOU'RE INTERESTED

Peter Shipley plans to publish the results of his survey on his Web site (**http://www.internet-security.com**).

PUBLIC NOTICE

The Vendors at

National Association of Music Merchants

1998 largest trade show in history offered Colton Piano Company pianos and digital pianos from

BALDWIN, SCHIMMEL*, CHICKERING, KNABE*, YOUNG CHANG*, BOSENDORFER*, TECHNICS, PIANO DISC PLAYERS*, PETROF, CLINE* KURZWEIL, AND MANY MORE ALL AT *BELOW WHOLESALE PRICES!!!

These specially priced instruments will be liquidated

-3 DAYS ONLY-

Colton Piano Co.

•**SANTA CLARA**, 2111 Laurelwood Rd.
(Hwy. 101 at Montague, next to Levitz)
Call **408-986-9900**
•BURLINGAME, 1471 Burlingame Ave
•WALNUT CREEK, 1357 N. Main St
•SAN FRANCISCO, 4724 Geary Blvd.

Financing (OAC) & Delivery Available

Most Major Credit Cards Accepted

Open to the Public

EVERYTHING MUST BE SOLD

February 6th, 7th & 8th