IDEAS

COMPUTERS

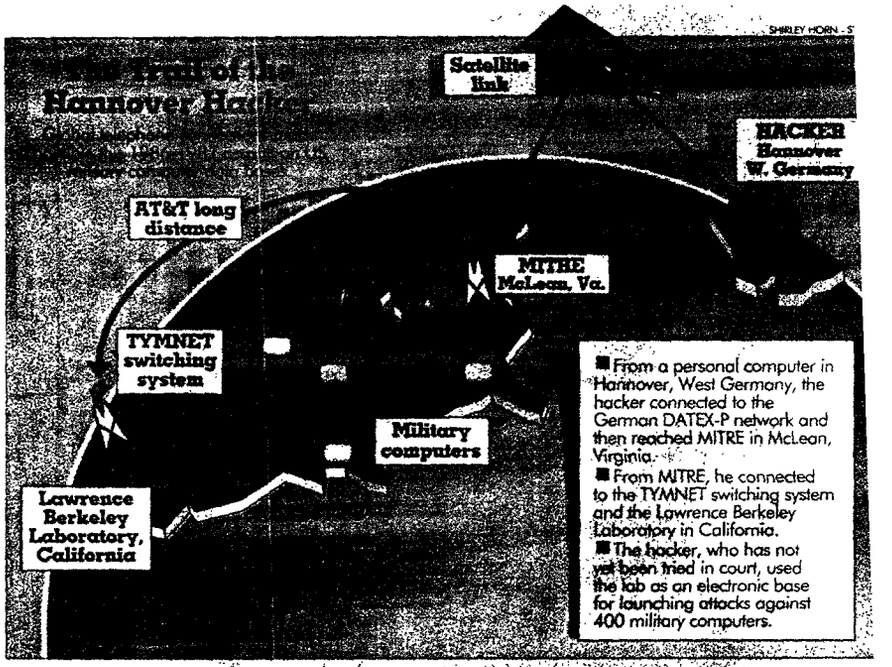
Lax Security Lets Hackers Attack

Despite alarms about 'viruses' and 'worms,' few networks take steps to prevent invasions

By Simson L. Garfinkel
Staff writer of The Christian Science Monitor
BOSTON

■ *'We've fixed the bugs and gone on our merry way as usual. We aren't really prepared for what will happen when the next bugs are discovered.'*

Donn Seeley, University of Utah systems programmer



AT 2 a.m. last November, Clifford Stoll was awakened by a panicky telephone call from the National Aeronautics and Space Administration (NASA) Ames Laboratory in Iowa: Somebody was breaking into NASA's computers. Soon Dr. Stoll discovered that his own computers were under similar attack.

Later that day, the United States news media were buzzing with reports of a computer 'worm' that had taken over the Internet, a national network of 60,000 academic, commercial, and government computer systems. It took experts more than three days to destroy the invasion completely.

In July, the worm's alleged author, Robert Morris Jr., was indicted in Syracuse, N.Y., on felony charges of violating the Computer Security Act of 1987. Morris's lawyer has filed four motions to dismiss the case; arguments will be heard October 20.

But on the Internet today, computer security at many installations has gone back to "business as usual."

"One particular customer was very worried about the Internet worm and wanted a fix for it," says Beverly Ulbrich, product manager for operating system security at Sun Microsystems in Mountainview, Calif. But now, says Miss Ulbrich, 70 percent of that customer's "several hundred" computers do not have the fix.

The day the worm hit, computer network experts at the Massachusetts Institute of Technology (MIT) in Cambridge, Mass., guessed that perhaps 6,000 computers had been affected by the program. But only one person actually counted the number of computers visited by the worm.

"Nobody has been doing real grunt research," says Stoll, who presented a paper yesterday on the worm's "epidemiology" at the 12th National Computer Security Conference in Baltimore. After nearly a year of research, Stoll found that the worm entered only about 2,600 computers.

Stoll, an astrophysicist at the Harvard Smithsonian Observatory in Cambridge, Mass., became a de facto expert on computer security when he helped US and West German officials crack a spy ring that had been using international data networks to break into US military and defense contractor systems. (See diagram.)

"Is it [the computer 'virus' threat] worth being concerned about or not?" he asked in a recent interview. The real danger, Stoll says, is not automated programs but warm-blooded people.

"No virus has been found to infect more than a few percent of computers [susceptible to attack]. The chances of being hit by a computer virus are small. . . ," he says. "It's probably cheaper to make backups and then, if hit, to clean up the mess afterwards, than it is to chase and fight off every possible infection."

One reason the Internet worm attracted so much attention is that the tricks it used could just as easily have been exploited by an individual seeking to capture or destroy information stored on a computer connected to the network. That focus on computer security has largely been lost, says Donn Seeley, a senior systems programmer at the University of Utah.

"We've fixed the bugs and gone on our merry way as usual. We aren't really prepared for what will happen when the next bugs are discovered," Mr. Seeley says. Because of the worm's notoriety, fixes for the particular security holes that it exploited were available within a matter of days, Seeley says, but other holes often remain for weeks or months after discovery. "[Computer vendors] don't really like to hear about security holes. They fix them internally as quickly as possible, and it goes though the usual slow release process to get out to the rest of the world."

When fixes are finally made available, there is no way to force computer system administrators to install them. "When you come right down to it, I think that people have short memories," says Jon Rochlis, assistant network manager at MIT.

The problem, Mr. Rochlis says, is compounded by the proliferation of desk-top computers that have the same computational power and networking capabilities that mainframes had just a few years ago. Often these desk-top wonders have a single user and no person responsible for security and maintenance.

"You have researchers sitting in their labs. . . . They don't want to take new releases of the operating system, they don't want to read security things," says Rochlis. "What right do I have to walk into their lab and say, 'You must run this new release, because I think that it is good for your security?' "

But that same proliferation of computers – most of them connected to networks that eventually connect to the Internet – has made all the computers on the network less secure by increasing the points of access for people who break into computers and making it easier for them to hide.

"People are still facing basically

How to Protect Computer Programs

TODAY is Friday, Oct. 13, the day that the Datacrime '89 computer virus is set to destroy information stored on the disk drives of IBM and compatible microcomputers running the MS-DOS operating system, according to the Computer Virus Industry Assocation.

Computer viruses are small programs that insert copies of themselves into programs commonly found on personal computers. (Computer worms, like the one that took over the Internet, make copies of themselves without modifying other programs.)

Datacrime '89 probably won't affect many people, says Linnaea Avenell of the assocation.

"We have had only seven reported incidents in the last six months. . . . We think that it is very rare, that it has been a lot of media hype, and that there are plenty of other viruses that people should be aware of. We get 30 calls a day about the Jerusalem virus," she says, referring to another computer virus that affects IBM-compatible computers.

Computer users who trade many programs with friends have a higher risk of a virus attack than those who only use programs that are obtained directly from manufacturers. Computers in public areas that are used by many people have a greater chance of being infected than those in closed offices.

The best way to protect against viruses is to make frequent backup copies of important programs and information. Backups also protect against equipment malfunction and operator error – both of which destroy far more information than viruses.

– S.L.G.

the same old security breaches that they were facing five to 10 years ago," says John Gilmore, a computer consultant in San Francisco, who has publicized many security problems. "The primary problem is a lack of awareness in the people who administer the system."

Sometimes even the security experts are lax about security on their own machines. Last year, for example, Seeley wrote a paper identifying a weakness in the computer used by the University of Utah; he suggested additional programs that could be installed to fix it. "My boss refused to install them: He thought they were overkill," says Seeley. Last month, a group of undergraduates was caught breaking into faculty accounts on the university's computer system, using the precise hole Seeley had identified in his paper.

"After an incident like this, there is an acute interest in security that lasts a few weeks, all the easy changes are made, and then we forget about it," says Seeley. "We put ourselves at the mercy of bad guys. We assume that the next people who break our security will not be so evil as to hurt us severely. . . . We have a relatively open system and rely on the fact that we are not interesting to protect us," says Seeley. He calls such practice "security through obscurity."

Many companies with equally open computers "would be wonderful targets for both industrial espionage and real espionage," Seeley says. "My suspicion is that they don't realize the danger that they are in."

Attitudes are changing, but slowly. "When I worked at Sun, I tested security on the internal network, trying to notice ways that people could break in," says Mr. Gilmore. "The reaction that I got from [management] was, 'if you are testing security, it must be because you are doing something wrong.' " Indeed, says Gilmore, some computer vendors keep their customers in the dark about holes in computer system security for fear that the information might find its way to people interested in breaking in.

Nowadays some companies are changing their attitudes, with the realization that the computer crackers already know about the holes.

"There are certain instances where it is important to tell people and there are instances where it isn't," says Sun's Ulbrich. "The issue is that if the fix is out there, the people who are concerned can put the fix in place before the hacker gets to it."

BOOKS

Computer Caper Culprit Caught

By Simson L. Garfinkel

IT all began in August 1986, when Clifford Stoll, a newly-hired astronomer and computer jockey at the Lawrence Berkeley Laboratory, discovered a mysterious account on his computer system. It was built by an intruder who had tapped into LBL's computer via an international computer network.

Who was the intruder?

So opens "The Cuckoo's Egg," Dr. Stoll's first-person account of his 10-month quest to learn the identity and the motivation of his elusive electronic visitor. In the process, Stoll opens the reader's eyes to the world of computer networks, transcontinental satellite links, and computer espionage.

THE CUCKOO'S EGG
by Clifford Stoll
New York: Doubleday
326 pp., $19.95

Although Stoll could simply have deleted the hacker's account and continued his astronomical work as if the problem were solved, he decides to build a monitoring station and watch the hacker's moves. Soon Stoll's suspicions are confirmed: The hacker knows a myriad of ways to break into LBL's computer system. Closing one door would have just pushed the hacker to another, or he might have bypassed LBL entirely, marauding around the computer network unobserved. No, Stoll realizes, the only way to stop this hacker will be to catch him.

In days that follow, Stoll learns that the hacker has done far more than spend 75-cents of computer time: With the help of computer networks that crisscross the world, the hacker has used the LBL's system as an electronic base for breaking into military and defense contractor computers all over the country.

It doesn't take genius or cunning to break into most computer systems, Stoll learns, just patience and persistence. Perhaps one in 50 computers that the hacker discovers has an account named FIELD with the password SERVICE. The hacker's plan of attack resembles a thief who walks down a row of houses, Stoll writes, methodically twisting the doorknob of each: Sooner or later, somebody is bound to have left his or her house open.

Once inside, the hacker scours the system for names and passwords of other computers. It isn't long before the hacker has built up a repertoire of systems that he can invade at a moment's notice. On many of these systems, the hacker has attained "system privileges," or the ability to change or delete any file that he chooses. For the moment, though, the intruder is content to merely read and wait.

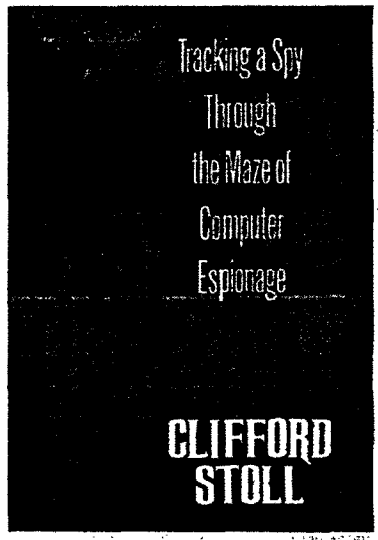
Fortunately, Stoll isn't.

In addition to following the pursuit of the wily hacker, "The Cuckoo's Egg," chronicles Stoll's inability to interest the United States security agencies in his case. Agents from the Central Intelligence Agency say all they can do is watch; the Federal Bureau of Investigation refuses to get involved until classified information is stolen or more than a half-million dollars of computer resources are lost. And, to Stoll's amazement, the chief scientist at the National Computer Security Center informs him that the NCSC's bailiwick is to design computers that are theoretically secure, not to come to the assistance of those who are having break-ins.

Stoll's calling is astronomy, not prose, and it shows in a narrative that is often self-conscious and uneven. Fast-paced dialogue and accounts of break-ins stumble into awkward descriptions of computer terminology that is neither understandable nor relevant. Undoubtedly, most readers will gloss over these page-long forays.

Another element that readers will miss is character development. "The Cuckoo's Egg" is billed as a coming-of-age-story in which Stoll, a self-described liberal living in the "People's Republic" of Berkeley, Calif., learns the importance of the FBI, CIA and the National Security Administration, even to the point of helping them, much to the chagrin of his Berkeley friends.

The book also follows the developing love story between Stoll and Martha Matthews, a law student at Berkeley and now his wife, who thinks up the ruse that Stoll finally uses to catch the hacker. If Stoll had gone into greater depth describing Martha and his friends, it would have helped the reader to empathize with his predicaments.



As a regular user of the networks mentioned in the book, I wished that Stoll had included more computer printouts in the text of the book. It would have been nice to actually "see" the hacker at work, the way Stoll did, and to read some of the sensitive-but-not-classified secrets that the hacker had learned. Since, by Stoll's own account, the information has already been sold to the KGB, there would be little harm in reprinting it.

Many of the computer security holes that Stoll writes about are still present in computers systems around the country. Indeed, Stoll says that he was asked not to put the precise details of how to exploit the holes in his book. But "the men in black hats" already know about these holes, Stoll said in a recent interview: It is only the legitimate users of the systems that are being deceived by a veil of secrecy. The title of the book comes from a trick that the hacker commonly used to take over Stoll's computer system.

The fact that everything in the book is true, and that only a handful of names have been changed, only adds to the story's excitement.

■ *Simson L. Garfinkel covers science and computer technology for the Monitor.*

Excerpt From 'The Cuckoo's Egg'

TYMNET'S idea was simple and elegant: create a digital communications backbone, let anyone connect to the backbone by making a local telephone call, then send the data to any computer on the network. Tymnet would compress dozens of users' data into a few packets, and economically send these around the country. The system was immune to noise, and each user could run as fast as he wished. Customers saved money because they could access a distant computer by making a local call. . . .

Someone was breaking in, using the Tymnet line. Since Tymnet interconnected the whole country, our hacker might be anywhere.

For the moment, though, I was fascinated not by where the hacker came from, but what he had done in three hours. My guess was right: Sventek's account was being used to break into our Unix computer.

Not just break in. This hacker was a super-user.

The hacker had sneaked through a hole in our system to become a super-user – he'd never even logged into the system manager's account. He was like a cuckoo bird.

The cuckoo lays her eggs in other birds' nests. She is a nesting parasite: some other bird will raise her young cuckoos. The survival of cuckoo chicks depends on the ignorance of other species.

Our mysterious visitor laid an egg-program into our computer, letting the system hatch it and feed it privileges.

That morning, the hacker wrote a short program to grab privileges. Normally, Unix won't allow such a program to run, since it never gives privileges beyond what a user is assigned. But run this program from a privileged account, and he'll become privileged. His problem was to masquerade this special program – the cuckoo's egg – so that it would be hatched by the system.