

HACKER FOR HIRE: Peter Goldis

Looking for the Loopholes

By VIN McLELLAN

BOSTON

PPETER GOLDIS spent most of mid-December in Holland, breaking into the Amsterdam computer of a major international financial services firm. Earlier in the fall, he did the same thing at corporations in Detroit, Chicago, and Los Angeles. This month, he has an assignment in Phoenix.

Mr. Goldis is a hacker in a three-piece suit, an authorized bandit who "attacks" the computer systems of banks, insurance companies and manufacturers to ferret out software loopholes that could enable employees to steal or corrupt data. The 41-year-old programmer is a master of MVS, I.B.M.'s flagship program, a huge, complex operating system considered the backbone of corporate America.

His services...are in growing demand these days at companies that rely increasingly on sophisticated computer systems. As more and more people become computer-literate - and thus have the potential to penetrate computers - concerns about security risks have multiplied as fast as the "virus attacks" that have left the computer world spinning this past year.

"You bring in someone like him to learn from him," said Louis Pintsopoulos, who supervises the auditing of electronic data processing at the Dennison Manufacturing Company in Waltham, Mass., which hired Mr. Goldis last year.

According to Mr. Pintsopoulos, Dennison tightened computer security after Mr. Goldis's visit because Mr. Goldis uncovered several "wholly unknown" vulnerabilities in purchased software products - vulnerabilities that could have enabled someone to gain control of the computer system and manipulate or change data without leaving any traces of it.

Vin McLellan writes about computers from Boston

In the computer industry, authorized hacker probes against reputedly secure computers are called "tiger team" attacks - a term borrowed from the military nickname for counter-intelligence teams that test military-base security...

Although most of Mr. Goldis's peers in the independent contracting end of the business operate in teams, Mr. Goldis is a one-man show... In the last three years, he has penetrated the computer systems of 25 major companies. In the process, he has become part of the industry's folklore.

"It's like safecrackers - you know there aren't many people with his skills, but there are some, and you can use someone like Peter to test the locks and uncover flaws," said Albert Belisle, vice chairman of the American Bankers Association's committee on information security.

Several years ago, Mr. Belisle said he brought in Mr. Goldis to "attack" the I.B.M. mainframe of a large insurance company where he worked as manager of information security. The results showing system vulnerabilities were "eye-opening," Mr. Belisle said, and had a "significant impact" on the company's computer programmers, who often



Peter Goldis

'You bring in someone like him to learn from him,' said a former client.

seemed more interested in system productivity than in security. Over all, he said, the "attack" proved to be "an extremely valuable exercise."

"Every problem Peter documented he gave us a fix for; he never put any of our systems in jeopardy, and he always kept us fully informed of everything he did," said Mr. Belisle.

MR. GOLDIS is an independent contractor, an authorized bandit hired by top management, the board of directors, or a corporate auditor to challenge employee claims that the computers in a management information system are secure... [Assignments] seem to follow tales of his doings that surface in board rooms after one of his "attacks".

As a group, Mr. Goldis's clients "are very interested in security," Mr. Goldis said. And for good reason: "They have secrets to protect," he said, "secrets that are living on the most expensive kinds of computer equipment."

What further complicates computer security is that systems are constantly evolving and being added to, and a system that is secure today could become insecure as it changes in coming weeks.

Martin King, audit manager at Computer Associates International, the largest independent software vendor, estimated that the costs of a problem that could bring down "a big manufacturing company's assembly line or put an airline reservation system out of commission" would total "thousands of dollars per minute lost."

As a result, companies are willing to pay for studies that sniff out vulnerabilities. A customer is charged about \$15,000 for Mr. Goldis's "attack", a service that includes a report and documentation on the attack methodology, he said...

The goal of such efforts is to maintain, through years of hurly-burly growth, the integrity that MVS was sold with. I.B.M. sells MVS with a formal "integrity

statement," said Don Ewing, an I.B.M. product manager.

Besides committing I.B.M. to fix any security holes uncovered in the MVS code, he said, this statement also serves as a guarantee that MVS will not allow a low-level user or unprivileged program to unilaterally upgrade its status - except where local site managers, the caretakers of a corporate computer system, fail to properly install or protect powerful or dangerous software.

In addition, most MVS systems are protected by a security program which restricts access to particular data or programs within the computer to users who have particular passwords. Three programs dominate security in the I.B.M. mainframe market: one, widely known as RACF, is made by I.B.M., and two others are sold by Computer Associates.

Kurt Meiser, one of the architects of RACF during his 22 years at I.B.M.... insists that system programmers have always known how to secure MVS, but too often have lacked the resources or the will to do the job.

Mr. Goldis agrees. "If you do all the things that you are supposed to, I won't succeed," he said.

The attack Mr. Goldis launches on his clients is a classic insider's attack - a much more sophisticated "penetration" than a simple attack by a hacker, which might involve just guessing a password. His concern is with what a hacker - or an employee who does not have such access - can do once he or she illicitly gets inside the system.

When he is brought into a company, he is given computer access of the sort given to minor clerical employees. His goal is to get to the innermost core of the onion-like MVS operating system and obtain - illicitly - the power and authority normally granted only to a small number of trusted system programmers, who can, basically, do anything to the system.

"My whole practice is based upon improperly acquiring that privilege," said Mr. Goldis.

Mr Goldis specializes in discovering and exploiting weaknesses in the way in which the million-plus lines of MVS code are installed and then linked to independent programs that call upon protected MVS resources. MVS gets extended all the time, but the flexibility of the system is both its beauty and its bane.

Each new program that makes itself an extension of the master operating system can introduce a risk to MVS integrity - and many do, with shortcuts to provide speed or new functions that give them a competitive advantage, said Mr. Goldis.

What I show is how an unprivileged user, say a data entry clerk, can get it all, including full control over all the privileges in MVS," including any security safeguards, said Mr. Goldis. "That's the trick."

The sense of vulnerability among large computer users reflects more than just a threat posed by hackers. Basic trends in the market have introduced a major new problem.

Rather than buying most of their application programs from I.B.M. - or just writing the codes themselves - corporations are purchasing more of these programs from independent developers. Even I.B.M. officials express concern about the risks of these "third-party" programs.

Industry security gurus now urge buyers to demand guarantees from software developers that their code does not

Goldis. "Their first impulse is voyeuristic: 'Gee, so-and-so has a dirty word for his password,' or stuff like that. It's like entertainment for a half-hour. Then it sinks in."

'If you do all the things you're supposed to do, I won't succeed,' Mr. Goldis said.

compromise MVS system integrity. But such demands are rare today - and guarantees even more so.

"As has always been the case, function sells - and security is often an afterthought," said William Murray, a former I.B.M. executive...

Third-party software is not the only problem. Mr. King of Computer Associates, who is perhaps the leading expert on MVS security outside of I.B.M., said he has rarely seen an MVS system that did not have special undocumented commands or trapdoors to evade security, installed by the site's system programmers to allow them to rapidly deal with any emergency that might crop up.

To Mr. Goldis, these trapdoors are bread and butter. "Almost everybody does that," he agreed. "And when they do, it makes my job very easy."

Three years ago, when he took his first independent "penetration" assignment - after making a name for himself doing systems programming... - it took him three weeks to discover such a piece of code.

"Now, it generally takes me less than half a day," he said. "I recognize it right away."

Typically Mr Goldis's clients challenge him to copy or read a specific file they have protected within the computer. But when he can, he likes to use the passwords of senior management as evidence of success.

"When you give them a list of all their passwords, they go crazy," said Mr.