CASE OF THE PURLOINED PASSWORD

By Vin McLellan

July 26, 1981


Case of the Purloined Password

The F.B.I. wants to know who swiped an electronic file opening access to all sorts of data at a subsidiary of Dun & Bradstreet.

Profit in your pocket (not your broker's)

About the Archive

This is a digitized version of an article from The Times's print archive, before the start of online publication in 1996. To preserve these articles as they originally appeared, The Times does not alter, edit or update them.

Occasionally the digitization process introduces transcription errors or other problems; we are continuing to work to improve these archived versions.

BOSTON S INCE last fall, the Federal Bureau of Investigation has been conducting a criminal investigation into a curious computer-age crime - the theft of an information file called a password directory from the electronic memory of National CSS Inc., one of the nation's largest timesharing companies.

A password directory is essentially a list of the secret words used by customers to identify themselves and signal the timesharing company's computer to unlock and release information they have stored within the system. With the passwords, a thief would have access to the private files of the more than 8,000 companies that are NCSS customers and, in effect, use it as their computer center. So armed, he or she would also be able to manipulate and change that data without leaving any telltale evidence.

While the potential for this kind of crime has worried experts for years, the opportunity to unravel an actual case history is so rare that the cadre of F.B.I. agents trained for computer fraud discuss the NCSS case as a ''learning experience.''

In the timesharing industry, the issue of system vulnerability has become much more sensitive in recent years. With cheaper electronic storage, remote computing centers are now often used as information vaults. Timesharing clients, which once stored only processing instructions, ''programs,'' within such systems, now often store whole data banks.

No significant cash or data loss has yet been associated with the theft, but with its ominous possibilities, the NCSS security scandal has badly jarred the huge $8 billion-a-year remote processing industry.

The tale has its odd angles. Bemused F.B.I. agents have found themselves confronted with a tradition of almost ritual thievery among computer programers. Dun & Bradstreet, the credit rating service that has expanded into a business information conglomerate and is now NCSS's parent, drew the

wrath of many industry professionals for not covering up the incident - even as it infuriated some NCSS clients by warning them they had a security problem, but refusing to give them any details of the ''problem.''

The industry tradition has been to handle security problems quietly and privately. ''Everybody in this business has dealt with penetration,'' said Chester Bartholomew, protection and control director for Boeing Computer Services, a Seattle timesharing concern. ''Usually, we have enough information to take a rifle shot at it rather than let loose with a shotgun blast.''

But D.& B. required NCSS to notify all its remote processing clients that there was some sort of security problem and that all passwords should be changed, according to NCSS sources. It was the first ''broadcast'' security alert to the entire customer base of a major timesharing company in the 25-year history of the industry - but it made no mention of stolen passwords.

D.& B. also vetoed a news story on the NCSS incident prepared for Datamation, a major computer industry trade magazine. Datamation staff members said that this was the first incidence of editorial intervention since D.& B. acquired the magazine in 1977. (John L. Kirkley, Datamation's editor, said policy was for D.& B.'s technical publication subsidiary to review any story concerning D.& B. affiliates and that the NCSS instance was Datamation's first such piece. After review, he said, a more general treatment of the security issue was requested, and ''that's what we're doing.'')

Last week, NCSS spokesman Daniel Benson said that it was ''company policy'' not to discuss the case while the F.B.I. inquiry continues. D.& B. officials did not respond to repeated requests for comment.

But extensive interviews with Justice Department officials and present and former NCSS people, outline a history of widespread unauthorized access to password directories. An F.B.I. report on the case to the United States Attorney's Office in Connecticut, where NCSS is based, is expected before the

fall, according to Justice Department sources.

D.& B. is itself a major user of the NCSS service; perhaps, according to former NCSS officials, its ''most vulnerable'' client. Since it acquired the timesharing company in 1979, the traditional D.& B. credit services have become increasingly dependent on NCSS technology and the network.

For example, in the large ''multi-access'' data base used in D.& B.'s new ''DunsVue'' system, anyone who had obtained the NCSS password directory would have been able to change or erase or create data, according to NCSS technicians familiar with the D.& B. software. In other words, temporarily, at least, a thief could create or diminish credit.

Unfortunately, when you attach communication links to a computer, even with passwords, ''you really don't know who is at the other end of the line,'' said Harold Feinleib, until recently NCSS vice president for advanced systems. ''The only secure computer centers are those without telecommunications.''

With the password-based security systems used in most timesharing systems, security is a relative thing, measured by the willingness of all participants to accept security discipline. ''It's like the seatbelt problem,'' Mr. Bartholomew said. That is, how does one get people to take precautions?

National CSS, based in Wilton, Conn., with revenues of $100 million last year, is regarded as one of the most technically sophisticated companies in the business. ''I don't have a feeling that other systems are any better than NCSS on security,'' mused Mr. Feinleib. ''Most are worse. You wonder. Do these things happen all over?''

The theft, apparently, was an all-electronic one. Someone, somehow, penetrated several levels of the system's internal security and plucked the directories from three NCSS computers in Connecticut and another in California - the four big machines in the network - then ordered the system to

shuttle the passwords around the country over telephone circuits.

L AW enforcement officials say it is unclear how many times the system was raided. As is common with computer data-theft, NCSS apparently had no idea the company had been robbed until told of the directories being found in someone else's computer.

NCSS got the first hint of the problem on Oct. 31, 1979, Halloween, when Larry Smith, an independent business consultant and former NCSS manager for advanced product design, placed an angry phone call to the company.

Someone, he charged, had used his NCSS password and I.D. and billed him $30 for the use of a ''program product'' called RAMIS, a product for which Mr. Smith had developed a successor while at NCSS. Mr. Smith said that where the computer usually recorded RAMIS accounting information, a four-letter obscenity appeared.

''It's like somebody wrote, 'Kilroy was here,' '' Mr. Smith said. Mr. Smith, like many other NCSS executives and senior technicians, had made a tidy profit when D.& B. bought the company. He then teamed up with James Morley, a business consultant, plus several NCSS programmers to form a software consulting firm, called the Guild, in Richfield, Conn.

Within months, the Guild had attracted from NCSS a client called Media Metrics, a small advertising research concern in Moraga, Calif. Soon thereafter, Mr. Smith and an associate resigned from the Guild to start a competing company, Hanson-Smith Ltd., in Shelton, Conn. (''My attorney insists it was a friendly split because nobody sued anybody else,'' Mr. Smith said. ''But that is the extent to which it was friendly.'')

A week and a half after Mr. Smith's angry phone call, a technician at Media Metrics went rummaging through the memory of the Media Metrics computer in search of extra storage space. There, according to Mr. Smith and F.B.I. sources, he happened upon the NCSS directory - which, of course, had

no business being there. Media Metrics president John Putnam was notified, and he called the Guild and then NCSS, according to NCSS sources. (Mr. Putnam declines to discuss the incident.)

On a Saturday night in November, an NCSS attorney placed a frantic call to the F.B.I., according to Justice Department and NCSS sources. But when the F.B.I. proved unwilling to guarantee to ''handle the situation quietly'' and unable to move directly against the suspected thieves to reclaim the password data, said a Justice Department source, NCSS officials suddenly became defensive and ''uncooperative,'' hiding behind a phalanx of corporate lawyers.

''Getting information was like pulling teeth,'' said an official close to the investigation. After the F.B.I. threatened NCSS executives with grand jury subpoenas, cooperation improved, he added, but the inquiry has largely gone around, rather than through, corporate channels.

The theft seemed at first to indicate only that the NCSS system was vulnerable to its 100-odd ''system programmers'' - the elite technical staff.

''With current procedures, if the system programmer wants to breach security, there is no way to stop him,'' said Robert Jesserum, former director of development at NCSS, now president of Electronic Information Systems in Stamford. ''It's a matter of trusting a lot of people,'' he said.

But reports soon developed that some sophisticated, lower-level field technicians - even without NCSS system programming experience - had been able to penetrate NCSS security.

According to former NCSS executives, there have also been incidents in which programmers working for NCSS clients have also managed to breach directory security in recent years. Three years ago at the Bank of America in San Francisco, which leases a copy of the NCSS ''operating system'' to

manage its own internal computer network, a six-month security review was initiated after one of its programmers proved he could steal the NCSS directory from the bank's system, according to a bank technician interviewed early this year.

''Every timesharing firm in the world has these skeletons in the closet,'' laughed Mr. Smith, the former NCSS manager. ''Get the heads of technicial development from these companies together,'' he said, and when they start swapping stories ''they'll probably be in hysterics.''

Obviously, however, not all raids on the system are criminal in intent. ''Whenever security is breached, there is a threat,'' said Mr. Morley of the Guild. But, he added, ''in this specific case, whoever did it, probably did it as programmers do things, to play -rather than with any serious intentions of offering them for sale or doing anything with them themselves.''

Indeed, because of its very importance, the password directory is the traditional target for what the computer industry calls ''hackers.''

Hackers are technical experts; skilled, often young, computer programmers, who almost whimsically probe the defenses of a computer system, searching out the limits and the possibilities of the machine. Despite their seemingly subversive role, hackers are a recognized asset in the computer indutry, often highly prized.

Security was never a ''major factor'' in the original design of today's timesharing systems, explained Mr. Feinleib - and original design has been constantly extended to cover new applications, carry new responsibilities. So much of what passes for security, noted Mr. Jesserum, evolved as designers patched loopholes discovered by hackers.

But the potential for harm is definitely there. Which may be why D.& B.'s reaction to the discovery of the directory theft was far more forceful than

many at NCSS felt necessary.

''I think it was a total over-reaction,'' said John Pryor, who recently resigned as NCSS vice president for sales, reflecting the general NCSS view that hackers were at work.

Corporate D.& B., however, moved in quickly to directly manage the crisis. Senior NCSS officials claim that even the very guarded NCSS alert, signed by NCSS president David Fehr, was actually written by D.& B. chairman Hamilton Drake. (Again, D.& B. refused comment.)

''It has come to our attention that a former employee may have obtained information which could potentially compromise system access security,'' read the terse Nov. 20 memo. ''Although a breach of any customer's data security is highly unlikely, in line with our total commitment to maintain absolute security, we strongly urge that you immediately change all passwords by which you access the National CSS' systems.'' The message ended with regrets, but no further details.

For at least one customer, the auditing firm Coopers & Lybrand, an NCSS customer as well as D.& B.'s corporate auditor, it wasn't enough by half.

A week before the alert, Frank Logrippo, Coopers' manager of internal financial reporting, had received a call from Gretchen Mitchell, a senior NCSS customer liaison. She told him that the directories had just been found in California. He immediately began changing the hundreds of passwords his company used on NCSS. When Mr. Fehr's bulletin reached him, he said, he saw NCSS dissembling.

''If the passwords were found at someone else's site,'' Mr. Logrippo said, ''it's not 'may be compromised' - it's compromised!'' Whatever the outcome of the NCSS case, the F.B.I. investigation may, in passing, have uncovered a clear case of industrial espionage. Several years ago, according to two former

NCSS executives, NCSS was offered the password directory of its largest direct competitor - the Service Bureau Corporation, now a $300 million subsidiary of the Control Data Corporation - by a programmer at a New Jersey pharmaceutical company that was then a client on the S.B.C. network.

The S.B.C. directory, covering some 10,000 clients, was on the block for $5,000 cash, according to Michael Pomerantz, former NCSS district sales manager for New England, who said he received the initial offer. Mr. Pomerantz said NCSS had rejected the offer and notified S.B.C. In the typically murky style of the industry, senior officials at S.B.C. say they can find no record of the incident. ---------- Vin McLellan is a Boston-based writer specializing in technology and politics. He resigned as a reporter for Datamation magazine in February. A PROGRAM CALLEDPILFER

Three years ago, very much in the industry tradition, a group of National CSS field representatives were found to have developed several elaborate systems to penetrate NCSS security. It was a classic instance of the mischievous but perversely positive ''hacker'' tradition among computer programmers.

As the handful of those directly involved described it, the group discovered two loopholes. One was a technical weakness in the system. Another simply exploited a high-priority password a Detroit businessman had seen taped to a wall when he was given a tour of the NCSS data center.

For over a year, NCSS's Detroit-based technical ''reps'' had regularly consulted and used the directory. They were even able to set up an electronic ''trap'' in the computer to catch new passwords - and changes in key passwords.

Arthur Bolder, a former NCSS account representative who is now a consultant in Ann Arbor, Mich., became something of a folk hero at NCSS when he voluntarily came forward, after another tech rep was caught, to reveal the full

scope of the group's capabilities.

Mr. Bolder had written a little program called Pilfer. As he explained it, he simply had to type in the name of an NCSS client or an NCSS executive, and the program would automatically break system security, get the user's password, and deliver to Mr. Bolder an open line to whatever was stored in the computer under that account.

Mr. Bolder said he was threatened with immediate discharge if he ever told anyone how Pilfer worked. Yet even his 1979 letter of reprimand - from Robert Weisman, now NCSS chairman and president of the Association of Data Processing Service Organizations, the industry trade association - acknowledged the hacker tradition.

''The Company realizes the benefit to NCSS and in fact encourages the efforts of employees to identify security weaknesses to the VP, the directory, and other sensitive software in files,'' Mr. Weisman wrote. Mr. Bolder had erred not in beating the system but in failing to report his success.