Waiting for the Great Computer Rip-off

For an expert bent on crime, it seems, cracking a computer system's defenses is about as difficult as doing a hard Sunday crossword puzzle.

by Tom Alexander

One morning last September, a computer operator on duty at Honeywell Information Systems Inc. in Phoenix was startled to see the output printer on his console start up all by itself. Out rattled a message referring derisively to a recent Honeywell press release about the company's vaunted new computer system, called "Multics." When it was done sniping at Multics, the mysterious message signed off with the words "ZARF is with you again."

ZARF is the code designation for part of a joint project of the U.S. Air Force and MITRE Corp., a defense-research outfit. The project is concerned with computer security, and a favorite pastime of people involved in it is cracking "uncrackable" computers. The day before the Honeywell computer acted up, two ZARF men, Air Force Major Roger Schell and Steven Lipner of MITRE, visited Honeywell to look over the security features of prospective systems for classified Air Force computing chores. After seeing the press release about Multics, Lipner quietly placed a long-distance call to a ZARF colleague, Lieutenant Paul Karger, in Massachusetts, nearly 3,000 miles away. Karger, in turn, sat down at his teletypewriter computer terminal, dialed into Honeywell's private Multics system, and typed in a few subtle instructions that subverted every one of the system's safeguards, giving Karger effective control.

The ZARF prank was particularly embarrassing because Multics is designed with security as an uppermost consideration. Of all large commercial computers on the market, Multics probably incorporates the most elaborate safeguards against unauthorized tampering.

A stirring of fear

The kind of vulnerability indicated by ZARF's little joke is beginning to disturb the keepers of modern electronic-data-processing systems. Most EDP systems consist of one or more large, multipurpose computers and banks of stored data, usually accessible via telephone circuits from individual terminals such as the teletypewriter that Lieutenant Karger used. Until not long ago, computer manufacturers and users saw little reason to fear that an unscrupulous person at one terminal would be able to read, alter, or delete another user's data, or tamper with the intricate programs that manipulate this data.

But in the past year or two, even the manufacturers have more or less come to acknowledge that it is not really very difficult for someone with a lot of skill to do things like that, even with the most secure systems now in existence. According to one expert, indeed, it's about as difficult "as solving a hard Sunday crossword puzzle."

How to make a president blanch

Computers, of course, have come to be deeply and pervasively involved in basic functions of our society. Top executives might die off, factories blow up, foreign subsidiaries get nationalized, but if you really want to see a company president blanch, ask him what he would do if the magnetic tapes with his accounts receivable got erased.

Electronic and magnetic data have not only replaced manually kept books, but have also gone a long way toward replacing tangible assets, including money itself. Today's credit-card system, for example, is an offspring of computerization. In the words of Richard Mills, formerly a top computer expert at M.I.T., and now a vice president of First National City Bank, "The base form of an asset is no longer necessarily a 400-ounce gold bar; now assets are often simply magnetic wiggles on a disk."

But gold bars in vaults, notations in a ledger, or, for that matter, written reports from a corporate research project are immutable and immovable things compared to magnetic wiggles, which can be read, altered, or destroyed at the touch of a teletypewriter key. For criminal purposes, funds can be fraudulently credited to an account, a bank balance can be programmed never to fail, or the record of ownership of very large sums can be changed.

This is not to say that computer crime is an overwhelming source of loss as yet. Robert Courtney, who is the man responsible for the safeguards that go into I.B.M. equipment—and who is

Research associate: Caroline Parker Young

Many of these errors in concept or execution must be located and corrected before the system will work at all, but some remain hidden, or annoyingly evident, for years.

Under certain circumstances, these errors will let data leak from one user's domain to another's, or even open a way into the supposedly inviolate territory of the operating system itself. Many a subscriber to a commercial timesharing service, having accidentally pressed a certain combination of keys, has found someone else's data rattling out unbidden. By now, a lot of people have learned how to exploit software errors deliberately—not only to read data stored in the machine, but also to type in changes in access-control safeguards, data, and programs.

Attacks by tiger teams

The first delighted exploiters of these software quirks were the "systems hackers"—students at universities where some of the first time-sharing systems were installed as far back as the middle Sixties. Among other things, faculty members stored grades and examinations on some of these systems, and systems hackers became adept at changing their own grades or reading upcoming exam questions.

By the late Sixties, computer experts at Rand Corp. were warning their government patrons that all the multi-access systems on the market were vulnerable. Over the years since then, under contracts with the Defense Department, Rand and a number of other organizations have been seeking methods to improve operating-system security, as well as methods to ascertain whether any system is really secure. The most glamorous phase of this activity is the work of the "tiger teams," who actually try to penetrate systems being considered for defense uses. So far, no major system has withstood a dedicated attack by a tiger team.

The disturbing implications of all this for civilian computer operations are only now coming to be widely recognized. In principle, the ability to take over a computer's operating system implies having access to all data and all programs on the machine, together with the ability to distort them at will. Properly done, such subversion is likely to go undetected. For criminal purposes, such control would be something like having a small army of corrupt bookkeepers at one's command, but without all the risks of exposure that relying on the cooperation of human beings entails.

With the increasing use of these systems as repositories and conveyors of valuable assets and private and proprietary data of incalculable worth, a number of computer professionals have begun speculating about the grave potentialities for criminal manipulation of computer systems. Among them is Clark Weissman, a manager of computer-security research with System Development Corp. Weissman believes that a lot of criminal activity could already be going on, leaving no external evidence.

"Sherlock Holmes," he says, "can't come in and find any heel marks. There's no safe with its door blown off. Many companies wouldn't even know their data's been manipulated." As for auditing programs, "the first thing the interloper would do is corrupt the audit-trail software itself."

"The companies just eat 'em"

No one has valid statistics as to how much of this sophisticated subversion goes on, but from all indications, a lot more goes on than is ever detected. Donn Parker concludes that of nearly 175 cases of computer crime he has looked into, hardly any were uncovered through normal security precautions and accounting controls—nearly all were exposed by happenstance. One expert guesses that the ratio of undiscovered to discovered crimes may be on the order of a hundred to one.

A lot of the computer crime that *is* detected, moreover, is never publicly announced. Most security experts have collections of incidents that they have investigated but that were never reported to the police. Furthermore, some banks and companies candidly admit that when an incident is discovered, the corporate victims usually try to avoid the embarrassment and loss of confidence that publicity might bring. According to I.B.M.'s Robert Courtney, "It's generally accepted in this business that about 85 percent of detected frauds are never brought to the attention of law-enforcement people. The companies just eat 'em. Of the 15 percent that are announced, a fair number are brought in from the outside by the police."

What often happens is that the offender, once detected, is required to make restitution and then leave—sometimes even getting severance pay and letters of reference to speed him away. One consequence, no doubt, is a circulating population of unpunished, unrepentant, and unrecognized embezzlers going from company to company. Probably a more serious consequence, though, has been to suppress recognition of the extent of computer crime, and thereby to lull both makers and users of computers into minimizing it as a threat.

Ten thousand dishonest programmers

Computers appear to have magnified the potential rewards to the criminal. Parker analyzed twelve cases of computerized bank embezzlement that occurred in 1971 and found that the losses averaged $1.09 million apiece, or about ten times the average embezzlement loss. With ever larger amounts of credit and other assets moving onto EDP systems, it seems inevitable that more criminally inclined people with more elaborate resources will grab for the prizes so temptingly exposed. "There are something like a million programmers in the country right now," observes Willis Ware, a pioneer computer-security expert at Rand, "and if only 1 percent of these were inclined to be dishonest, that's ten thousand dishonest programmers."

Especially troubling is the thought of even a 1 percent incidence of dishonesty among the "systems programmers" who write the operating systems for the computer vendors or modify them to fit the needs of particular users. These programmers are the people most knowledgeable about the intricacies and weaknesses of specific systems. Jokes Robert Jacobson, a vice president of Sentor Security Group, Inc.: "Ideally, the first step in securing a system would be to shoot the programmer."

continued page 148

In a really big job, the programmer or programmers would probably have accomplices with other skills. A somber prediction along this line comes from Robert Abbott, director of an Advanced Research Projects Agency computer-security project at Lawrence Livermore Laboratory. "It's only a matter of time," he says, "until somebody mounts a team-directed approach, involving programmers, accountants, and maybe wiretappers and burglars. When it happens, it's going to be awful."

Passwords in wastebaskets

One impediment to would-be perpetrators is the difficulty of obtaining detailed knowledge about a given organization's EDP system, procedures, and accounting controls. Aside from that problem, the principal defenses against computer frauds right now are the passwords. And passwords often turn out to be a laughably weak defense, even against those without fancy programming skills. A lackadaisical attitude toward security persists in many EDP installations. For instance, it's apparent to the casual visitor that he would have little trouble walking into the offices of the average time-sharing company or service bureau —posing perhaps as a prospective customer, a delivery messenger, or even a legitimate but confused user—and proceed to scoop up proprietary tapes, printouts, or passwords.

It has also been demonstrated on more than one occasion that a persuasive liar on a telephone can entice employees of a time-sharing system into giving out passwords. In all sorts of computer installations, people bandy passwords about or write them down. Wastebaskets galore are stuffed with printouts on which passwords are visible. And often there will be some employee who will provide passwords for a bribe.

Everything else failing, a prospective intruder has technical means at his disposal. For example, he might dial up a system, plug a small computer into the line, and set it to trying out passwords.

Generally speaking, computer security is obtained only at some cost, and among the costs is inconvenience to the ordinary human beings who must use the machines. Many organizations, in seeking a proper balance, often put convenience to their harried, forgetful users ahead of airtight security. In the case of commercial time-sharing services, at least, it appears that if customers are really concerned about the privacy of certain information, they'd better keep it out of those systems.

Other defenses besides passwords have been devised. One possibility is to program the computer to identify legitimate users by asking random questions about family background, etc. "The trouble with that," says I.B.M.'s Courtney, "is that if you're running thousands of transactions a day, you don't much care to spend ten seconds or so every time arguing with the computer about who you are." I.B.M. is currently trying out, among other things, the use of magnetically striped cards that users can insert into terminals to prove their identity. Already, though, tinkerers have found that it is no great feat to counterfeit such a card, using ordinary magnetic tape. A number of companies are working on devices that will recognize personal insignia such as the shape of a hand or the unique motions an individual makes as he signs his name.

A new kind of piggybacking

Even with elaborate passwords, magnetic identity cards, and other screening procedures, along with thoroughly honest employees and guarded computer rooms and terminals, most multi-access systems have a huge sector of vulnerability: the telephone lines that stretch from one facility to another. Experts contend that it is technically a simple matter to tap into phone lines and thereby learn passwords and identifying signals, transmit false data, or penetrate an operating system. One ingenious wiretapping tactic, called "piggybacking," involves hooking onto the tapped line another computer that intercepts legitimate messages and modifies them. A piggybacker could, for example, insert additional credit transfers to accounts during a bank-to-bank transmission.

About the only defense against wiretapping is some method of scrambling or encrypting messages. It happens that this is something a computer can do quite handily. It also happens, however, that computers are very handy at *breaking* encryption and scrambling schemes, often in a matter of minutes or hours. Staying ahead of a sophisticated tapper would take both elaborate encryption schemes and provisions for changing the keys to the encryption at frequent intervals. This would impose a considerable burden in hardware costs, together with the potential for chaos if keys get lost or mixed up.

The case of the phony foreman

While ignorance of the computer system and accounting controls will probably stop the casual intruder, it's not likely to deter for long the dishonest employee or the sophisticated and highly motivated thief. As Donn Parker puts it, "The most dangerous threat is the penetrator who knows as much about the system as you do."

Such was the case in one of the more ingenious computer crimes so far, the work of a baby-faced young Californian named Jerry Schneider. Around three years ago, at the age of nineteen, Schneider spent some months learning the necessary codes and procedures of the system that Pacific Telephone & Telegraph Co. used to handle field orders for communications equipment in Los Angeles. Among other things, he posed as a magazine reporter to gather information. He also used his own computer terminal to probe the system.

Eventually Schneider learned enough to pose as a field-supply foreman and, using a pushbutton phone, tap in orders for equipment—phones, Teletypes, switchboards, etc.—to be delivered to field locations, including manholes. Then, with an old phone-company truck, Schneider or one of his employees would pick up the goods and sell them. Schneider used his entry into Pacific Telephone's computer to keep track of current inventory, and on occasion, after spotting shortages, he sold the company some of its own equipment.

One of his thirteen employees eventually turned him in after a wage dispute, but not until he had operated for nearly two years and stolen nearly a million

continued page 150

dollars' worth of equipment. After serving forty days in jail, he went into the business of advising clients on how to prevent computer rip-offs. His motto: "It takes a computer thief . . ."

Computer manufacturers are trying hard to develop systems that will be more resistant to manipulation, by either dishonest employees or outsiders. The consensus of the experts seems to be that it is possible to design penetration-proof operating systems, but that they're not likely to be commercially available in large systems in less than four years, at the earliest. When they *are* available, the problem will then be what to do about the existing systems. According to International Data Corp., an authoritative industry source, something like $17 billion has already been invested in remote-access computer hardware, and probably even more in software. Most of this stuff has ten years or more to go before the investment is amortized.

Right now, expert opinion is divided on the question of whether, even in principle, any of the existing systems can be rendered sufficiently secure to handle assets or information of very high value in the face of a sophisticated attack. Contends Steven Lipner, one of the perpetrators of that ZARF prank in Phoenix: "There are two difficulties with trying to retrofit one of these large monolithic operating systems to get better security. One, it's expensive, and two, it doesn't work."

It may take shock

Others, however, believe that security can be significantly strengthened. As one measure, some advocate the use of separate minicomputers and software as gatekeepers, to handle the chores of user identification and access control. The main purpose is to remove these sensitive functions from the intricate maze of a main operating system.

While they are showing more and more interest in these new developments, the manufacturers contend that it's fairly pointless to bring out systems capable of resisting sophisticated attack until their customers adopt better physical security measures in their own installations, as well as better screening of computer employees. And while customer interest in the problem has picked up a lot since the Equity Funding scandal bubbled up, there's still reluctance to spend much money for computer security. It may take the shock of dramatically expensive and well-publicized computer crimes to start the money flowing in any abundance.

There's talk in the trade of numerous large rip-offs. One story tells of a young swindler who arranged false credit transfers into two major banks from two other banks within a span of two weeks, and escaped with nearly $5 million. But no really big computer crimes, involving tens of millions or more, have surfaced in the public domain. A great many people in the computer-security business wonder aloud when that huge rip-off is going to happen—if it hasn't already, undetected. END

Singapore *continued from page 89*

a day—making Singapore the world's third-largest oil-processing center, after Houston and Rotterdam.

The oil-exploration rush in nearby Indonesia has been beneficial for Singapore, which now supplies much of the equipment used in offshore drilling. The government itself has three logistical bases to service wildcatters with pipe, drilling mud, and other gear. And the island serves as headquarters for dozens of contractors participating in the search. "We've had a fair amount of luck in the events around us," admits Deputy Prime Minister Goh Keng Swee. "They gave us chances, and we were ready to seize them."

The Vietnam war and its aftermath gave the corporate state another opportunity to provide products and services. Initially, the conflict brought windfall sales of patrol boats, oil, and construction materials to the U.S. military in Saigon. More recently, Lockheed has established a service base in Singapore to repair American planes for South Vietnam.

In a broader sense, American military activities have also helped stimulate plant investment. The war effort not only brought inflation to the U.S. but focused attention on Southeast Asia, where American businessmen saw opportunities outside the battle zones. As Japanese rivals grabbed business away from them, U.S. electronics companies moved production to countries with lower labor costs. Among those that flocked to Singapore were National Semiconductor, Fairchild, and Teledyne. In the last few years, fast-climbing wages in Japan have prompted such major Japanese shipbuilders as IHI, Hitachi, and Mitsubishi to make the switch, too.

Money is a major export

To realize his grand design of making Singapore an international financial center, Lee shrewdly turned to the world's most prestigious banks. His government has admitted virtually every big international bank, from New York's First National City to Moscow's Narodny, and has left them free of the numerous restraints that they face elsewhere in the Far East. So a towering new financial district is taking shape along the waterfront.

"We decided to open up the banking system to provide services that other countries don't offer," explains Michael Wong Pakshong, managing director of the government's Monetary Authority. As a start, he broke up a cartel of established British and local banks that fixed rates on all transactions. "They'd sit on their bottoms waiting for captive customers," complains Wong. "The newcomers actually went out to buy business with loan rates that were competitive. That made the others get busy fast."

Singapore's main growth in financial stature came after the government, at the urging of the Bank of America,

continued page 152

2 **Fortune's Wheel**
A review of this issue

7 **Business Roundup**
The Forecast for the Next Eighteen Months

17 **Businessmen in the News**
Miller of Textron—and others

37 **On Your Own Time**
The Down-to-Earth Values of Farming

51 **Letters to Fortune**

57 **Personal Investing**
When Book Matters, and When It Doesn't

69 **Editor's Desk**

71 **Editorial**
The Revolt Against "Full Employment"

FORTUNE

July, 1974

75 **P&G's Secret Ingredient** *by Peter Vanderwicken*

80 **The Auto Industry: What Lies Ahead Down Small Car Lane**
by Dan Cordtz

85 **Singapore, the Country Run Like a Corporation**
by Louis Kraar

90 **The Agony of the Federal Reserve** *by Sanford Rose*
(Last in a series on the new questions about the U.S. economy)

94 **Using Escalators to Help Fight Inflation** *by Milton Friedman*

98 **The Chin-Down Manager** *by John D. Arnold*

100 **Management Problems Enter the Picture at Art Museums**
by Walter McQuade

104 **First National of Chicago Banks on Art** *(A Portfolio)*

112 **The Fortune Directory of:**
114 **The Fifty Largest Commercial Banking Companies**
116 **The Fifty Largest Life-Insurance Companies**
118 **The Fifty Largest Diversified Financial Companies**
120 **The Fifty Largest Retailing Companies**
122 **The Fifty Largest Transportation Companies**
124 **The Fifty Largest Utilities**
126 **Index of Companies**

131 **How One Man Makes $120,000 a Year Selling Insurance**
by Arthur M. Louis

133 **The Old Master Makes About a Million a Year**

143 **Waiting for the Great Computer Rip-off** *by Tom Alexander*

Fortune, July, 1974, Vol. XC, No. 1. Issued monthly by Time Inc. 541 North Fairbanks Court, Chicago, Illinois 60611. Second-class postage paid at Chicago, Illinois, and at additional mailing offices. Subscriptions: U.S., U.S. possessions, and Canada: one year $12; elsewhere one year $30 to $46. Single copies $1.50. Address all subscriptions and correspondence concerning them to FORTUNE, 541 North Fairbanks Court, Chicago, Illinois 60611. Principal offices: Time & Life Building, Rockefeller Center, New York, N.Y. 10020. James R. Shepley, President, Clifford J. Grum, Treasurer, Charles B. Bear, Secretary. Authorized as second-class mail by the Post Office Department, Ottawa, Canada, and for payment of postage in cash. Member, Audit Bureau of Circulation.

Picture credits page 190