CYBERNETICS

Computers and Security

National Data Bank proposal and shared time facilities bring danger of information leaks.

by Carl Behrens

Computer engineers are realizing that their tremendous success in building fantastically able machines is bringing them attention from non-technical people—and with it the prospect of Federal control of their operations.

Their awareness was evident at the recent Spring Joint Computer Conference in Atlantic City, where the problem of security in computer operations took star billing. The feeling was evident that if the industry doesn't solve the problem, Congress will step in.

Two developments have brought computers into sudden focus for lawmakers and the general public.

One is the proposal by a segment of Washington bureaucracy that the vast amount of information collected by various government agencies be pooled in a single National Data Bank, where it would be conveniently available to economists, sociologists and planners whose decisions are based on what the public has, does and wants.

The other development is the increasing popularity of time-shared computers, in which a large, expensive facility is tapped by numerous small-scale operators at remote consoles.

Both developments are aimed at using expensive, bulky machinery more efficiently. And both carry the problem of making sure information stored in the central facility does not get into the wrong hands.

The National Data Bank has run into a Congressional stone wall because there is no assurance that personal information from one agency—say the Census Bureau—wouldn't get into the hands of another, such as the Internal Revenue Service.

The Data Bank may be dead or dormant, but time-sharing of computers by several competing companies is very much alive, and active, although still in its infancy. When the practice becomes more widespread, the chances of both deliberate and accidental spilling of information will increase.

Even prototype systems have had their security problems. At the Massachusetts Institute of Technology, Project MAC—for Machine-Aided Cognition—ran into trouble when students invaded the computer room and tampered with the machine's program.

Project MAC's director, Dr. Robert M. Fano, says protective measures are being designed for the Project MAC system, which should begin full operation this fall. Hundreds of scientists, engineers and students will have simultaneous access to the system through remote installations at Cambridge and at the Bell Telephone Laboratories in Murray Hill, N.J.

The effort to use more efficiently the computer's great speed in calculating—by letting a number of customers use the machine almost simultaneously—puts a further strain on areas where the computer is least efficient. These are the input and output sections, where instructions and data are inserted and answers extracted; the control section and the memory section, where information is stored for later use.

These strains will increase as security needs make identification procedures more stringent. One time-share specialist estimates that eventually 10 to 20 percent of a computer's memory will be taken up with routines to identify users requesting information, to insure against unauthorized access to the memory. And the more identification is required, the longer it will take to get on the computer's line and get answered.

The difficulties emerge because the computer can only recognize information in a very simple form. All of the computer's complicated logic and memory circuits consist of electronic switches which at any moment are either on or off.

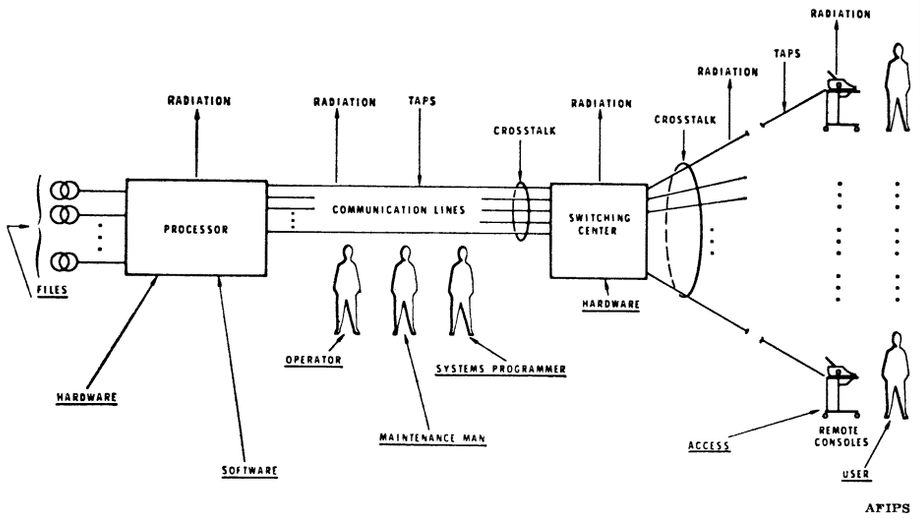
Numbers are represented by two digits: "1" when the switch is on and "0" when it is off. Each number has to have a tag so it can be drawn out of storage at the proper time. The tags also are in the form of "0's" and "1's."

In order to operate on the information it has, the computer must have a control section—a series of circuits that translate orders such as "add" and "multiply" and "take the sine of" into computer language. To do this, the numbers are led through a complex series of circuits called gates, which operate only when two or more numbers arrive at the same instant.

Three types of gates are common in computers: "and," "or," and "not" gates.

To add "1" and "1," the computer needs three "and" gates, two "not" gates and an "or" gate, each gate consisting of two or more transistors and many other electronic components.

tions can be given to the computer to open certain sections of the memory only to qualified users, but an efficient machine has to be flexible enough to change those instructions as customers



Time-share computers: many information leak points, human and hardware.

To take the sine of a number, an unconscionable number of additions has to be made.

The computer makes this operation more efficient than looking in a sine table because of two factors:

- The additions can be made at a rate of millions per second;
- Engineers have found a way to store in the computer's memory—still in the form of "0's" and "1's"—complex instructions to be followed so that the machine will make the right additions in the right sequence. These instructions can be triggered by a simple command by the machine operator.

Additional commands can be wired into a computer so that data put into one section of the memory will be available only to customers that have the key—a code word, for instance, or a restricted quantity of remote consoles. These procedures are necessary merely to keep data concerned with one problem from interfering with another one.

To thwart deliberate attempts at stealing data, the security measures have to be increasingly complicated and use more and more of the computer's capacity. A code word—in simple-minded computer language—has to be fairly long to contain enough digits to make deciphering it more than a simple exercise.

Another weak link in the security system is the transmission line between the central facility and the remote consoles. Public wires are used to carry both passwords and information, and wires can be tapped with dismaying ease.

The control section of the computer is also potentially a leak-point. Instruc-change. An unscrupulous programmer could change those instruction to obtain unauthorized data for someone else.

In order to restrict unauthorized changing of instructions, some time-share computers allow the remote consoles to operate only in what is called the "read-only mode," which means that instructions cannot be changed except at the central facility. But this does not eliminate the possibility of leaks at the main station.

In fact, the personnel problem appears to be the weakest point in the security of time-shared computers—at least where deliberate espionage is concerned.

Engineers are confident they can make their machinery leakproof, if they design security into the machines as they are developed. The analogy to telephone equipment is often drawn. Precautions could have been taken to make wiretapping very difficult, they say, but once the expensive equipment was installed without those precautions, it was economically infeasible to rework the whole system.

Some computer experts suggest government inspection and certification of time-share computers to guarantee that industry puts in the necessary hardware.

But personnel leaks will still remain. Industrial espionage is a booming business at present, but information is scattered and difficult for a thief to assemble. In a large computer, each memory bank is a hoard of information, and computer users wonder how it is going to be guarded—and by whom.