Chapter 13
Trends in Computer Technology

Contents

Page

Introduction 123

Conclusions 123
- Hardware 123
- Software 124
- Human-Computer Interface 126
- Communication 127

Processors 127

Information Storage 130
- Fast Memory Storage 131
- Intermediate Memory Storage 131
- Mass Memory Storage. 132
- Inexpensive Mass Storage 132

Software 132
- Limits 133
- Data Base Systems 133
- Languages 134
- Software Engineering 134

Input-Output Technology. 135
- Graphics 135
- Voice Communication 136
- Image Recognition. 136

Data Communication 137
- Digital Communication Technology. 137
- Digital Communication as Part of the System 138

Security Capabilities. 138
- Classifications of Computer Security 138
- Specific Techniques of Security 139
- Encryption 141
- Authorization 141
- Logging 142
- Operating Systems 142
- Data Base Security 142

LIST OF FIGURES

Figure No. *Page*

8. Projections of Logic Cost per Gate. 128
9. Increase in Capability of Semiconductor Chips From 1956 to 1980. . . . 128
10. Drop in Average Computer System Cost per 100,000 Calculations From 1952 to 1980. 128
11. Cost and Access Time of Memory Technologies 130
12. Projections for Memory Cost per Character 131

Chapter 13
Trends in Computer Technology

Introduction

Computer technology is advancing rapidly, even explosively. To assess the impacts of information systems, the current state of this technology and where it is heading must be understood. The capability that information technology puts in the hands of the computer user determines the nature of the applications that are developed.

Developmental trends are already shaping the nature of the information-based services that will be provided in the coming decade. New services that make use of the growing integration of telecommunication and information technology are being designed and implemented; and both industry and Government are looking at a wide range of innovative products and services that will be used by the in-home information system of the future.

The nature of the technology as it evolves will also influence the structure of the industry associated with it. Companies that specialized only in components are beginning to market computer systems; companies that sold only general purpose computer systems are beginning to market consumer products that incorporate these systems.

For the purposes of this study, emphasis has been placed on what information systems can do rather than on the fundamental nature of electronic technology. Many interesting developments now in the laboratory, such as Josephson junctions, * may not fundamentally change either the nature of the systems that are designed or the purposes to which they will be put, particularly over the next 10 years. Other developments, such as the microprocessor, are today revolutionizing the ways in which computers are used as well as the thinking about their potential social impacts. Overall, the anticipated changes from laboratory developments over the next several years will be more of degree than of form.

*A Josephson junction is a microscopic-size electronic logic device that operates at the temperature of liquid helium. I t is very fast and uses very little power.

Conclusions

Several conclusions can be drawn from OTA's analysis of the trends in the development of computer technology over the next 10 or 15 years. Spurred by both industrial and Government research and development (R&D) programs, information systems are undergoing a revolution that will be manifested-by a proliferation of new products and services affecting all sectors of American society.

Hardware

- Computer electronics are experiencing an extraordinary drop in price, increase in power, and reduction in size.

In *1977,* the Privacy Protection Study Commission estimated that the cost of computing would drop by a factor of more than 100 during the 20-year period from *1970* to

1990. This means that the million dollar computer of the 1960's will cost less than a thousand dollars in the late 1980's.

Concomitantly, during this same period calculating speed is expected to increase a hundredfold. In 1970, the largest processors performed 10 million operations per second, today they perform 100 million, and by 1990 there will be a processor that will perform 1 billion. In addition to greater speed, new designs can also greatly increase the power of future computer systems.

The large computer that occupied one or several rooms in the late 1960's will fit in a desk drawer by the late 1990's, and a medium-size computer will fit in a briefcase or even a coat pocket. These trends do not necessarily mean that in all cases the costs of purchasing, programing, and operating a large computer application system will decrease. Rather, more work will be done for the equivalent number of dollars.

- There will be a great expansion in the number of computers being used in business, education, and the home.

This effect is already being seen. The home computer boom, which was the first big stimulus for the computer retailing stores, has fallen off slightly, only to give way to a new marketing thrust aimed **at** small businesses. The hand calculator, which has become a ubiquitous tool, is already being supplanted. A small hand-held computer is now available in the consumer market, and electronic calculators are being built into wristwatches. Computers are also being used as part of office automation.

- Computers will be used as components in a wide range of consumer products.

With the advent of an integrated circuit microprocessor that will sell in mass quantities for $1 or less, the use of the computer for controlling everyday devices in the home and at work will become commonplace. Computers are already being used or designed to control such devices as clothes washers, sewing machines, home thermostats, automobile engines, sprinkler systems, typewriters, filing systems, electric lights, and cash registers.

While many applications will involve simply substituting electronic for mechanical control, the increased "intelligence" incorporated in the products will be used to provide such additional features as energy conservation or self-diagnosis of errors, and to give more flexible control to the user.

- New products and services based on computer and telecommunication technology will become available.

In addition to adding computer control to familiar products, the new computer technology will be used to provide a new range of products and services for the home and business. The video game and home computer are just the first of a long line of computer-based information products and services that will appear. (Electronic funds transfer and electronic mail, two examples of information services, are examined in separate OTA reports.)

- There will be a continuing, rapid increase in the power of very large computer systems.

Advances in speed, efficiency, and microelectronics coupled with new design concepts will produce computers in the 1980's that are far more powerful than the biggest ones now available. This type of power is useful for a limited but important set of computational applications, e.g., improved systems for weather prediction. Furthermore, systems that manage very large data bases require very powerful computer processors, particularly when sophisticated searches and analyses must be made.

Software

- Software technology is expanding steadily, although not as rapidly as the hardware.

Computer programs are sets of basic instructions that tell the computer the steps to

take in doing a task. Programs can contain millions of instructions, and their design is as varied as the number of ways computers are used. While computer scientists have been successful in developing theoretical models of computer hardware logic, efforts to build an equivalent theory of programs have not been rewarding to date. Thus, developing systematic techniques for creating, testing, and monitoring computer software has been a slow and tedious process. Some experts maintain that programing is still more of an art than a science.

The continuing R&D on programing languages and software engineering will provide a flow of improved techniques and software tools, but the rate of improvement will not match the explosive growth in hardware capability.

- New software techniques will allow computers to process a wider variety of data.

Traditionally, computers have processed either numerical or alphabetic data structured in very rigid formats. However, software for processing text, graphic images, and digitized voice is developing rapidly in addition to software for processing data alone. The result will be new families of products and services affecting Government, industry, and the citizen at home.

- Software technology is the limiting factor in controlling the rate at which new applications appear.

The use of the new specialized hardware that is being designed is confined to very restricted purposes, or is merely putting existing software ideas into hardware form for increased efficiency. The software basis for most new computer applications in the 1980's exists now. There does not appear to be much likelihood that a new concept of computer design will change the way computers are used in the next decade. Rather, the changes will be in the scale of their use and in who will be using them.

- The predominant cost of information systems will be for the software; the information industry will become increasingly labor intensive.

This conclusion follows directly from the last two statements coupled with the labor intensive nature of programing. This trend will influence the marketing practices of computer manufacturers, who will increasingly find profit in the sales of complete systems—combinations of hardware and software—rather than hardware by itself.

- Software reliability, security, and auditability will improve slowly.

Large systems, because they are complex and cumbersome, tend to suffer from the kinds of reliability problems that are not solved by building more reliable hardware. The problems of assuring that a system is actually performing as intended and cannot be compromised, accidentally or deliberately, are inherent in the complexity of software design.

Furthermore, although computer software experts are improving their understanding of how to increase the reliability of programs, they are unable to keep pace with the growth in the size and complexity of the systems being designed. Recently, system designers have become more aware of the need to design secure and auditable applications, and users have become aware that they can demand such capabilities from the producers. Thus, although some improvement is taking place, substantial progress will depend on more R&D.

- New data base techniques will allow massive data banks that serve multiple uses.

Data bases will grow; some will contain trillions of units of information. At the same time, people will want to work with the data in more varied ways. Today, sophisticated programing is often required in order to handle efficiently each different type of query a user might want to make of the data base.

However, researchers are developing methods to improve the efficient use of large

data bases and to make them serve multiple needs. This is being done through the development of more powerful query languages, new ways of organizing the data within the machine, and new hardware designs.

Human-Computer Interface

People communicate with computers for three basic reasons: to describe the task to be done, to enter data for processing, and to derive results. Improvements in this technology will result not only in less costly systems, but also in a vast expansion of information systems capabilities and in their more efficient use.

- There will be an increase in the direct use of computers by nonexperts.

Improvements in programing languages will allow users to communicate more easily with the computer. Historically, programing and system control languages have been complicated and time-consuming to learn. They often require understanding how a computer operates. New, easy-to-learn but powerful languages will increase the number of people who will use computers directly without recourse to an intermediary expert. In addition, the proliferation of computer introductory courses in high schools will increase the number of people who have a basic knowledge of computer systems.

This trend will allow many more simple applications to be developed by users individually or in modest organizational settings. However, in larger organizations, or for applications that require integration with other systems, it will mean that much of the programing for modern small systems will be done by end users in industry and in the home who are not subject to control by central data processing management. This may lead to such problems as misuse, poorly functioning systems, or incompatibility.

- More data will be captured by computers and stored in machine-readable form.

The distribution of computing power through the use of microprocessors linked together over communication lines will increase the amount of data captured at the source and stored in computer-readable form. Some types of information are captured deliberately, as in the case of the computerized register in a retail store. Other types, which are captured only as a byproduct of automation, may be found to be useful enough to keep. For example, the system data collected by word processing systems may be considered useful by managers in monitoring secretarial efficiency. The proliferation of capturing such data may raise serious policy issues.

- Output will be organized to present information that is more directly useful to the user.

It has been known from the earliest days of computing that the form in which the results of computations are presented can determine, in great part, whether it is actually used or whether the answer being sought is found. Advances in both the hardware and programing for image display and speech are being brought out of the laboratory and into the commercial market.

Research in information display is discovering how to filter significant information from insignificant data and present it to the user in the most efficient way. There is now a new, burgeoning interest in the use of color graphics display, a technology long considered the domain of the computer research laboratory, but too expensive for general use.

- There will be increased interface with information systems by consumers in their homes and employees in their offices.

Many systems designed for entertainment, education, information retrieval, and computational services are beginning to be offered through a combination of evolving television sets and telephone instruments because of easy-to-use software, data banks, and the distribution medium provided by cable television (CATV). As a result, there is a possibility that society as a whole will be

substantially affected, but to what extent is presently unknown.

Communication

The rapidly increasing availability of inexpensive digital data communication through specialized networks such as Telenet and Tymnet, coupled with the trend of manufacturers to design systems with elaborate communication hardware and software built in, are motivating growth in the use of distributed, communication-based systems. New satellite-based data communication services will further stimulate this trend.

- The use of distributed data bases and distributed processing will grow rapidly.

Rather than centralizing data collection and processing as in the past, the most efficient procedure in the future will be to localize these functions at the point where the data are originally captured. Organizations will have computational capacity distributed among all of their offices. All computer-based devices, even word processors, will be linked into the central system.

The problems in managing such a distributed system will be a major concern of large organizations. In particular, procedures for controlling access and for ensuring data quality will be more difficult in a distributed environment. However, dealing with them effectively will be crucial to the successful operation of communication-based systems.

- There will be increased availability of computer services to the home and business over communication lines.

Many homes will have small computers or computer terminals, and those that do not will likely contain telephones and television sets that have been equipped with computer control. All of these devices will provide links from the home and office to a multitude of information services provided over a variety of communication channels such as television broadcast, telephone, or cable lines.

Processors

The 1970's have seen continual dramatic improvements in the characteristics of the components from which computers are made. It is expected that this trend will continue through the 1980's, with computing hardware becoming remarkably inexpensive and efficient.

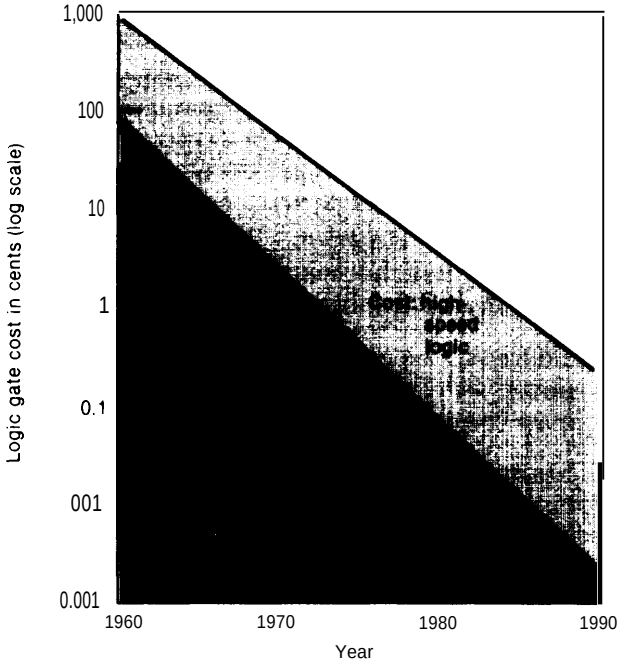
The decline in cost per logic function from 1960 projected to 1990 is shown in figure 8. In 1960, the price of a logic gate ranged from $1 to $10 per unit, depending on speed. By 1990, that price is expected to range from a few thousandths of a cent to a few tenths of a cent per gate. This continuing decline is based in large part on the dramatic increase in capability of semiconductor chips, as illustrated in figure 9.

There has been a parallel increase in the speed of processing. In 1960, the fastest machine executed about 1 million instructions per second. By 1990, there probably will be computers that will execute a billion or more instructions per second, a thousandfold increase in speed.

This combination of increased speed and decreased cost for logic components results in a steady decline in the cost of computation. The drop in the costs of computing on IBM systems that are roughly equivalent, over the period 1952 through 1980, is shown in figure 10.

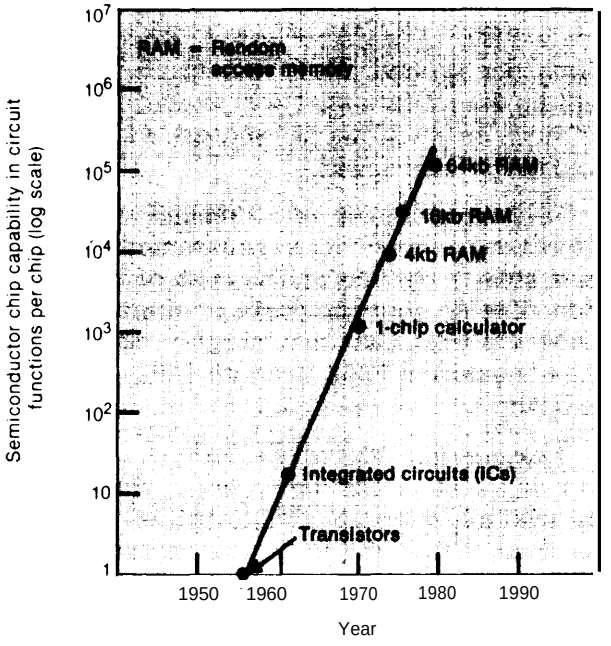
These gains have all been due to progress in integrated circuit technology, the process by which electronic components are printed on small chips of silicon. Using these chips as components has resulted in a steady shrinkage of the size of computers from assemblages that filled several rooms to the current desk-top versions. Mass production techniques have replaced the hand-wiring of

Figure 8.— Projections of Logic Cost per Gate



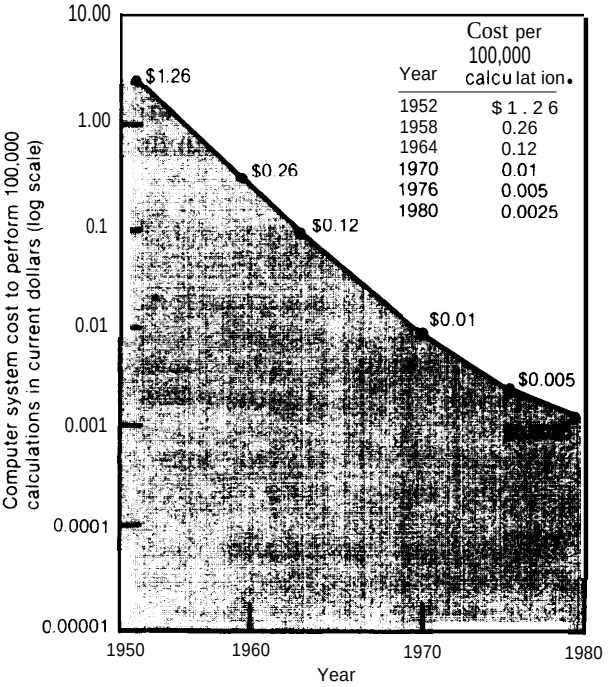
SOURCE Office of Technology Assessment and Privacy Protection Study Commission

Figure 9.— Increase in Capability of Semiconductor Chips From 1956 to 1980



SOURCE Institute of Electrical and Electronic Engineers *IEEE Spectrum* VOI 17 June 1980 p 48 U S Manufactures of semiconductor chips in cl ude f irms such as Intel Motorola Texas Inst rum en Is Rockwel 1, Na tional Semiconductor and Zilog

Figure 10.— Drop in Average Computer System Cost per 100,000 Calculations From 1952 to 1980



"Cost per 100,000 calculation is based on data for the following IBM computer systems (with year in parentheses) 701 (1952), 7090 (1058), 360/50 (1964), 370/168 (1970), 3033 (1976), 4300 (1980)

SOURCE Office of Technology Assessment and President's Reorganization Project, *Federal Data Processing Reorganization Study Basic Report of the Science* and Technology Team, Washington, D C June 1978, pp 2930

a decade ago, speeding up the manufacturing phase. Energy consumption, both to operate the computer system directly and for the necessary system cooling, has dropped enormously.

The financial implications of these latter trends are significant in that they are stimulating a rapid growth in computer applications that will accelerate beyond their current high rate in the 1980's. Facility costs have historically been a major expense to users installing computers. Now, many systems take up only a desk top, require no specialized environment control, and plug into a normal electrical wall socket. This flexibility means that many computer systems can be installed at any site, from the home to the business, with little or no added cost for preparing the physical site.

Inexpensive very large-scale integration (VLSI) based computer hardware will also lead to lower maintenance costs in the 1980's. Maintenance currently is estimated to cost about 5 percent of the computer's purchase price per year for medium-size computers. The figure is higher for smaller machines. A reduction in these costs will result from lower failure rates, easier maintenance by replacing larger modular units of the system, and built-in hardware redundancy and fault diagnosis.

Implications: These trends have several implications for computer hardware. In the first place, as illustrated in figure 10, there has been and will continue to be a steady drop in the cost of computing on general purpose, medium- to large-scale computing systems.

Second, small inexpensive, personal desktop computers have appeared on the market in the last few years. These "microcomputers, while modest by present standards, are quite powerful relative to the standards of only a decade or two ago. The price of these systems will drop rapidly, and their capacity will grow over the next decade. These small systems will likely drive the development of a true mass market for computers, a market analogous to the current one for hand calculators.

In addition to making the microcomputer possible, the ability to mass-produce chips and to custom design them at the same time, using the automated production machines, means that there will be a proliferation of special-purpose computers that are custom-made for specific applications. One of the motivations for the development of the so-called "general purpose" computer was that a computer system was expensive and difficult to design and build. Thus, many different user markets had to be identified for a single design in order to provide a sufficient customer base to justify its production.

This view of the manufacturers was reproduced in miniature within each computer center, which accumulated as many different types of applications as possible in order to justify acquiring a large computing machine, and thereby benefit from economies of scale.

These days, however, it is feasible to build special-purpose machines, because the specialized markets have grown and because the cost of designing and marketing custom tailored systems has dropped. As an example, a variety of firms (some quite small) are marketing so-called "array processors, " computers designed to calculate the solutions to systems of mathematical equations that display certain special characteristics. These processors are designed to be connected to a general purpose computer, and to be called on only for the specific calculations at which they excel. In the jobs for which they are intended, these array processors, which cost about as much as a large computer, are hundreds of times more powerful than the biggest computers available. The market for this machine exemplifies the increasing ability of small firms to enter the computer hardware business and carve out a niche for themselves.

Basic R&D in hardware design is picking up again after a hiatus. It moved out of the academic and pure research laboratory in the 1960's due to the high costs of building hardware and the lack of enthusiasm for new design concepts on the part of manufacturers. Now, the costs and feasibility of experimental research have improved dramatically. The result should be a proliferation in the 1980's of small specialized computers, tailored to particular needs. This trend will reduce computing costs even more than would result from the drop in component costs alone.

In general, experts expect that a continuing trend will be seen toward modular computer architecture. Logical functions will be distributed over the entire system. The central processor will be a traffic director controlling the flow of work among the various units. There will be specialized computation units like the array processor discussed above, file management processors for han-

dling data bases, communications control units, specialized language processors, and others. Because of widespread high-speed digital communications, these various components will not need to be in the same room or even the same city to be part of the system.

Information Storage

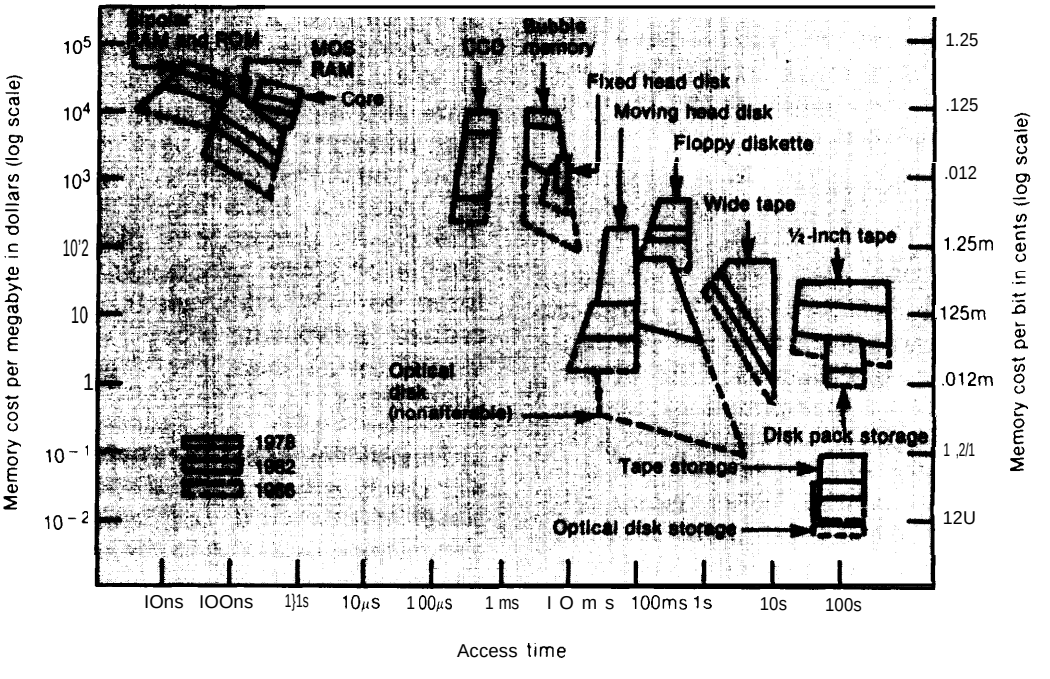
A computer memory comes in a wide variety of sizes, speeds, and types. Any particular system uses an assortment of memories to support its operation. Its most significant design characteristics are *retrieval time* and *capacity.*

Retrieval time is the time it takes to get a segment of information from the memory. The technology currently available provides a range of times from 1 nanosecond (1 billionth of a second) to a minute or more. Retrieval time includes the time both to find and to read the information.

Capacity is the amount of information that can be stored conveniently and economically. It is measured in *bits* (the smallest fundamental unit of information), or *bytes,* an 8-bit grouping roughly equivalent in information content to a single alphabetic character or two numerical digits.

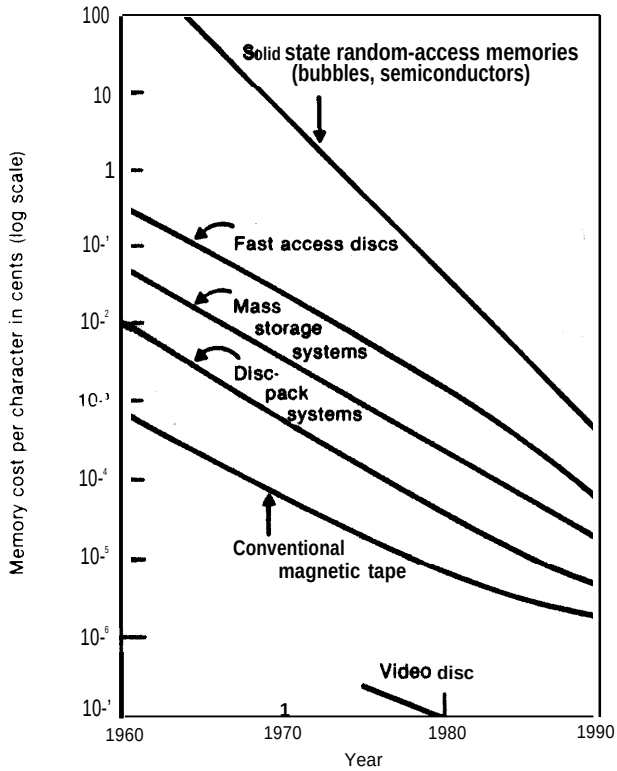
There is a distinct tradeoff between speed and capacity. Therefore, in connecting a computer that performs millions of instructions in a second with a world that operates in a much slower timeframe, a hierarchy of memory types is used. The current selection of memory technology available to system designers is shown in figure 11, and the projected drop in cost for information storage through 1990 is shown in figure 12.

Figure 11.—Cost and Access Time of Memory Technologies



SOURCE Institute of Electrical and Electronic Engineers, *IEEE Spectrum* vol 18 March 1981 p 41

Figure 12.—Projections for Memory Cost per Character



SOURCE: Off Ice of Technology Assessment and Privacy Protect Ion Study Commission

There are two other important characteristics of various memory systems that affect their use in particular applications. These are *volatility* and *writability.*

Volatility refers to the long-term stability of the memory. Many storage systems lose the information they contain when the power source is removed or interrupted. Others keep the information indefinitely until it is changed.

Writability refers to the ability to insert information in the memory. Memory is classified as read/write or read only, depending on whether or not the computer can copy new data back into the storage in about the same time scale as information can be read. Read only memories are written once and the recording is permanent. In this discussion, memory is roughly categorized as *fast, intermediate,* and *mass storage.*

Fast Memory Storage

Fast memory storage constitutes the upper left-hand group in figure 11. It is the most closely connected to the processor, and hence its speed must be consistent with that of the computer hardware. Because of the relatively high cost of fast memory, it is usually the smallest memory in the system.

For many years, core memories based on the magnetic properties of an iron compound were the principal technology used for fast memory storage. However, this technology seems to have reached its limit in cost, speed, and size. Most new memories now are designed around VLSI semiconductor technology.

Intermediate Memory Storage

Intermediate memory storage, which is reasonably fast but inexpensive enough to be used in large quantities, serves as a buffer between the high-speed semiconductor memory and the very slow mass storage devices. In the long term, *bubble memory* may develop into the technology of choice for intermediate memory storage. Information is stored as tiny magnetic domains that circulate along a printed track in a semiconductor medium. Some bubble memory products are already on the market, and new improved ones are being announced continually.

One of the advantages of bubble memories is that the domains are stable. Therefore, when a bubble memory is used in a terminal, for example, data can be entered and stored in it for later transmission without needing to keep the terminal hooked up continuously to a power supply. The technology of bubble memories is progressing rapidly. One manufacturer has already announced plans to market a million-bit chip that will cost around $2,000 in small quantities.

High-speed magnetic disks are still widely used for intermediate memory, and will continue to be the most important technology for this decade. Steady improvements will be announced throughout the 1980's. Some ex-

perts predict that disks will eventually be used in a more finely stratified memory hierarchy, rather than being replaced by bubble memories. This may depend on whether progress in expanding the capacity of bubble memories continues as rapidly as it has.

Mass Memory Storage

Progress seems to be slower in the area of very large storage devices. No radically new technology has appeared that seems to promise any breakthroughs. Magnetic tape will continue to be used heavily over the next decade.

Many new mass storage technologies– e.g., video disk—are difficult and expensive to write, but very cheap and easy to reproduce and read. Erasing and rewriting are often impossible. Costs per bit of storage for archival applications are low enough to be competitive with paper storage. Incremental improvements over the next decade should strengthen this advantage and stimulate a trend toward permanent document storage in electronic form.

Inexpensive Mass Storage

The rising market for small inexpensive computer systems is producing a demand for small, very cheap, bulk storage technology. The technology is different from that provided for large systems. The size of bulk storage needed is less, and there is more tolerance for slow search times. Currently, personal computers are supported by two types of bulk storage, magnetic tape cassettes and “floppy” disks.

Tape readers are very cheap, as is the tape itself. However, read time is quite slow, even by personal computer standards. Floppy disk hardware is more expensive, although still within the requisite price range. The disks themselves are cheap and easily stored.

Some manufacturers, particularly those marketing computer games, sell programs permanently written on solid-state read only memories (ROM). While relatively expensive as a medium, ROM has the advantage of being difficult to copy, thus discouraging the pirating of software. The ROM approach has not been well accepted by the marketplace, however.

Software

Computer software is also a form of technology. Although it is not a tangible product like a piece of hardware, software shares many of the same characteristics. Much R&D carried out by computer scientists concern software problems. It often results in new concepts and basic techniques for organizing data and sequencing instructions to enable a computer to accomplish a particular task.

Very large programs are harder to analyze, design, and produce than are equally large machines that run them. Consequently, the state-of-the-art in software lags behind that of hardware.

Occasionally, a major breakthrough in programing can motivate new machine designs. For example, a wave of new small processors has appeared on the market to support signal processing applications. These processors are based on the “fast Fourier transform” algorithm, an important discovery made a few years ago that allowed the solutions to certain types of mathematical computations to be calculated 10 times faster than previously.* Even greater speeds

*The Fourier transform itself is a pre-20th century mathematical technique. The advance was a new way to perform the numerous and tedious computations the technique requires.

have been achieved by using special processors to take advantage of this algorithm.

Limits

One area of research that will affect software development in the 1980's is fundamental research in computational complexity. Until recently, fundamental theory in computer science was concerned with computability–whether a computer could calculate an answer to a problem. However, the class of problems that the computer could theoretically solve was enormous. More recently, researchers have been exploring the more practical questions of how easily a problem may be solved, how fast, and how much computer power would be required. The answers have been surprising. Many categories of problems have been found to be almost impossible to solve, that is, the best program possible on the fastest computer available would take many years, even millions of years, to calculate an answer. Such results have already had practical application. For example, they have led to the development of new types of cryptographic codes with interesting new properties. Future research may lead to the ability to calculate theoretically the breakability of a code.

Over the next decade of ever increasing computer power, some types of problems are likely to remain intractable. Complexity theory will help improve the understanding of these limits of computers as they are now designed. Furthermore, it may possibly motivate some radical new concepts in computer design.

Data Base Systems

There is a trend toward the use of large integrated data base systems that support multiple applications. Researchers have been developing methods for organizing data so that it can be accessed in many ways, not all of which may be predicted when the system is designed. Some of the most general data structures, such as relational data bases, are not as yet efficient for very large data bases, but are appearing in commercial products for use with medium-sized systems. New developments in data handling algorithms, and new hardware designs specifically tailored to the support of data access systems, should provide continually improving capabilities during the 1980's.

Improved query languages will allow the information user to interact directly with the computer to obtain the needed data. The integration of better report generators* with the data base system will allow the output to be produced in a more directly usable form. These advances will provide the system user with access to the data base which is much more direct than is now the case. Currently, the normal practice is to work through an intermediary, both to frame the initial inquiry and to interpret the results.

The capability to transfer information between data bases over communication networks will also be improved. This capability, already well-developed in some specific systems, will allow more general exchange among systems connected to commercial data networks. Standard protocols and forms will be agreed on. True distributed data bases are systems in which the location of any particular item of information in the data base may be anywhere in a national or even international network, and in which access to that data is handled totally by the system. These should start to appear commercially in the 1980's,

The increasing size of data bases, the multiplicity of their uses, the wider remote access to them, and their integration over telecommunication lines will all present problems in preserving the security and integrity of the information. It will be more challenging to protect the privacy of personal data or the security of economically valuable information on such distributed systems.

* Report generators retrieve information needed by a manager, perform moderate calculations on it, and organize it in a readable and usable form.

Languages

Languages are the means by which users describe to the computer the kinds of operations they want performed by the system. *Machine language* is the set of instructions that is wired into the computer. Although some machine language programing is still done, it is very difficult and inefficient to use due to the size and complexity of most applications. Modern systems on a medium-sized computer may contain more than a million machine language instructions.

Faced with these difficulties, programmers turn to a *higher level language* to write most software. As computers have grown larger and more complex, and as the tasks demanded of them become more complicated, there has been a continual trend toward the use of languages designed to be more representative of the way humans express problem-solving procedures.

In addition to increasing programing efficiency, developers of higher level languages have other goals. Some special languages are tailored to produce efficient codes for particular classes of applications. Others have been developed based on the perception that programing a computer is a form of mental problem-solving, and that the language as the vehicle for that effort is an intellectual tool that can directly help thought processes. Finally, there has been a trend to develop languages that integrate users more closely with the system, thus lowering the degree of expertise required to program the computer. By programing in these user oriented languages, persons who are not computer specialists can interact directly with a system rather than through a professional programer intermediary.

The rapid expansion in the use of large data base systems that serve many users over communication networks is driving a major development effort in *query languages.* They are the means by which a user gains access to a data base, describes the desired information and specifies the format in which it is to be presented.

A principal driving force toward further language development is economics. Hardware costs are decreasing while labor costs are increasing. Developing languages that will increase the productivity of programmers has become a high priority. Ultimately, some researchers envision automatic programing in which users specify the problem to be solved in a language close to that used in their environment—engineering, law, medicine, and so on. The computer, using this problem statement, would write its own program.

Full development of such automatic programing systems is far in the future, although simple systems for preparing management reports and models derived from data bases are already in use. More short-term effort is being concentrated on developing tools that help the programer use the computer as an active agent assisting in the creation of a system.

Progress is expected to be slow. It will be impeded by the sheer difficulty of matching the essential ambiguity of human thought and language with the absolute rigidity of computer language. It is also economically difficult to implement radical new languages that require substantial retraining of programmers. Finally, there is a reluctance to write programs in languages that are not widely used and known, for the usefulness of a program so written may be unnecessarily restricted.

Software Engineering

For most of the history of computers, programing has been considered an art rather than a form of controlled design. Emphasis was on the ingenuity and elegance of the product, rather than on more mundane measures of utility. Creativity will always have a place in good programing, but its emphasis conflicts with managerial imperatives for economy, control, and predictability. In particular, when the development of a major system requires the coordination of hundreds of programmers writing millions of lines

of code, the project must be managed in such a way as to guarantee a usable product, on time, and at a reasonable cost.

The relatively new discipline of software engineering has been attempting the difficult task of developing techniques both for programing and for managing the programing of large software systems. The operating system and support software of a large multiprocessor computer system is extraordinarily complex. However, the economic imperative will force work in this area and assure the quick adoption of new results.

Until the present time, efforts have been geared to developing both techniques for breaking a large proposed system into successively smaller logical subunits that can be assigned to programing teams, and ways in which to manage the work of the programmers and the communications among them. These and related techniques will gradually become commonplace over the next 5 to 10 years as they are learned by the next generation of programing professionals and managers.

Input-Output Technology

The principal means of communication with a computer has traditionally been through a form of typed input and alphanumeric printed output. Although this type of communication will continue to dominate in the near future, it is inadequate for many new applications. Advances in technology for human-computer interaction will change the way in which computers are used by many people.

Graphics

Graphical display of information is becoming more economically viable, and the technology, both hardware and software, is improving in its capability. In the last few years, researchers have developed efficient techniques for removing hidden lines in order to display solid objects and for combining half-tone, shaded image production with color. Some current research is focused on developing techniques that model various surface reflectivities and textures with respect to different types of light sources.

While work is proceeding on improving the speed of graphical computations to allow the terminal to display very high resolution pictures fast enough to depict motion, such a capability may remain very expensive over the next few years for any but the most simple types of pictures.

Sharp cost breaks are expected for displays with lower image quality. The use of bit-mapped frame buffers, which store slow computer graphics output and play it back at normal speed over a display terminal, will grow as the costs of memories drop.

Some research is being pursued on holographic output of three-dimensional images. However, holographic display is not expected to become widely used in the next decade.

Computer graphics technology is already finding widespread commercial use for creating animated films. It competes favorably with traditional manual techniques. The uses range from pure and commercial art to the production of educational films. Computer languages and graphics software have been developed to allow artists and designers to interact directly with the computer, generally through the display screen, to create their images.

In computer-aided design, the user is interactively coupled to a display screen with a graphical data base and analytical programs stored on a computer. Designers use the computer and the display to develop their

designs on a screen. For example, an architect designing a building on the graphics display can have an instantaneous computation of cost, and a civil engineer can do stress calculations while designing a bridge. Computer-aided design has emerged from its infancy. Steady improvements in software and decreasing computing costs will likely make it the methodology of choice for most engineering design in the 1980's. Even today, integrated circuits and printed circuit boards are preferentially designed by these techniques.

Graphical output of computer data can transmit information that is difficult or even impossible to derive from a printout list of numbers. Whether calculating stresses in an airplane wing, the water flow in a flood plain, or the molecular structure of an enzyme, the numerical output of the computer calculations must be translated into a picture before any sense can be made from the results.

Voice Communication

Voice communication with computers is on the verge of becoming commercially successful. The advances have been both in developing better and cheaper computational techniques for generating and recognizing speech and in learning more about the ways in which such systems could be used. This new understanding has lowered the estimates of what would constitute a commercially useful level of performance. Capabilities far short of a human level of performance can markedly enhance communication between human and computer. Some experts even expect a voice-driven typewriter to be on the market before the end of the decade.

There are two basic problems in speech synthesis—first, creating a voice tone carrying a phoneme (a fundamental linguistic element of speech), and second, stringing these phonemes together to make a sentence or phrase. Although neither problem has been solved to the ultimate point of producing natural human-sounding sentences, the technology is improving rapidly. It has already reached the point of commercial utility.

Several companies sell chips in the $10 range to synthesize speech sounds. Texas Instruments offers a mass-produced electronic toy, Speak and Spell® , to help children learn to spell.

One important application of speech is a reader for use by the blind that converts typed text into spoken words. While currently very expensive, these devices should become more economical in the near future.

Speech recognition is a more difficult problem, since the system must deal with an input having great variability. The voice and style of speech varies widely among individuals; the computer recognize is potentially confronted by a wider array of potential vocabulary to identify; and it must analyze a multiplicity of grammatical structures. Again, entrepreneurs have found that even the very limited capabilities now possible are marketable.

So-called "continuous speech" recognition, understanding natural speech, is still in the research laboratory. While large-scale commercial systems are not expected in the short term, the strong market already developing for limited range speech recognition systems will motivate R&D and encourage the rapid commercialization of research results as they appear.

The best performance to date in a research laboratory environment has been shown by a system that can recognize sentences 91 percent of the time from multiple speakers using a vocabulary of 1,011 words. Major research efforts are proceeding at IBM and at a few university laboratories. Commercial devices with small vocabularies are now being marketed.

Image Recognition

Image recognition presents another form of the problem of recognizing patterns of data. The state-of-the-art is at a similar

point. Simple self-contained patterns not in a confusing context can be recognized. Devices on the market read standard typewriter and even handprinted characters. Point-of-sale scanners in stores read and recognize the universal product code on packages drawn across the unit at various speeds and orientations. However, analyzing a more general picture for a variety of elements is a more complicated task, one which, like speech, may depend upon some "understanding" of the context of the pattern.

Slow but steady advances in pattern recognition technology are occurring. The sharp drop in cost for the requisite technology is increasing the range of potential applications.

Data Communication

The ability to move data quickly over long distances through the use of new digital communication technology has had a significant impact on the design and use of information processing systems. Designers now have the opportunity to build systems with greater power than was previously possible, enhancing their ability to process information and provide it to the user in a timely manner. More importantly, however, telecommunication has brought the user closer to the computer by allowing direct interaction with the processing system. As a result, the use of information processing technology has become an integral part of the day-to-day work of many organizations whose operations have become totally dependent on a computer system.

only technology that relates directly to the development of computer-based information systems is discussed here. (For a detailed analysis of communication technology, see the OTA assessment report entitled, *An Assessment of Telecommunication Technology and Public Policy.*

Digital Communication Technology

The steady improvement of telecommunication service over the last quarter century has benefited the design of computer systems by decreasing their cost and improving their reliability. Significant applications using communications date back to the early 1960's. However, the cost and complexity of putting together a communication-based computer system restricted its use to applications, such as reservation systems, that had an inherent need for remote data entry and display.

Existing communication carriers and new enterprises are beginning to offer new data communication services. These services are designed to provide inexpensive high-speed communication capacity specifically designed for use by computer systems. With these new services available, a host of new communication-based applications will appear over the next decade.

Traditional communication systems have been tailored to carrying voice. The characteristics of voice communication are quite different from those of data communication between computers or between computers and people. The voice telephone network, through switching, provides a temporary line connecting two users. The charges are based on the length of the line provided and the length of time it is made available.

Data communication tends to come in very high-speed bursts, with long periods of silence between transmissions. To perform this type of communication on a traditional telephone network is inefficient, as the line is unused for most of the time. One approach has been to design a network with multiple path connections. Packets of information, along with a destination address, are sent over any instantaneously available path, and the user is charged for the quantity of in-

formation transmitted and for the connection with the network. One payoff in sharing traffic from a larger community to obtain better line usage is lower user costs. Secondary benefits include error-free performance and higher reliability. This type of communication facility is called packet switching, and is available as a commercial service. Thus, a librarian in Washington, D. C., with a terminal can dial a local number to access the Washington entry to a national data communication network. Through that network, the librarian can access a bibliographic data base in Los Angeles, and do so at a low cost.

Digital Communication as Part of the System

Viewed in the context of computer system operations, data communications are no different from any other application. However, they do introduce new capabilities and problems to the design, implementation, and operation of information systems.

Early implementations of the data communication programs were designed to take advantage of processor cycles that could not be used productively by other applications. However, the growth in the communication workload, combined with other new tasks that may have been loaded onto the processor, can saturate it and create a need to move the communication management from the central computer to a peripheral processor.

Fully programmable front-end processors support the trend of moving communication processing away from the central computer, In some cases these devices have been specifically designed for communication processing. In other cases, general purpose minicomputers are being used as front ends. Either way, the availability of inexpensive logic and memory components has contributed to the further distribution of the communication function away from the central processor.

Security Capabilities

Computers have handled sensitive data and programs for many years; however, it is only recently that the need to secure them has become a serious concern to system designers and operators. During the social unrest of the 1960's, concern arose over the physical security of computer systems. They were expensive and visible symbols and, consequently, attractive targets for sabotage. Later, concerns over privacy and an awareness of increasing incidents of financial computer crime motivated the managers to take a more sophisticated look at protecting their systems and data.

Classifications of Computer Security

Security experts distinguish between three types of security: *physical, procedural* and *technical.*

Physical security refers to techniques that physically isolate a computer system from access by unauthorized persons. It also includes protection of the facility from external dangers such as earthquake, fire, flood, or power failure.

Procedural security is the set of rules by which a system operator manages the system personnel and the flow of work in the organization. It can include such measures as preemployment screening of staff, work assignments that minimize opportunities to act in inappropriate ways, auditing procedures, and controls on the flow of work through the system.

Technical security refers to the software and hardware controls set up within the system itself. Techniques used to provide security may include cryptographic encoding of data, complicated access and iden-

tification procedures, and hardware which is dedicated to the auditing function.

Some security experts claim that too much attention on technological fixes has distracted system operators from more traditional but effective measures they could be instituting. However, the increased proliferation of small systems and the trend toward communication-based systems are making technical security more important. The techniques of physical and procedural security are well-understood and translate relatively easily from the noncomputer world into that of the system operator. Technical security, a newer area of research, is less understood, but is related directly to the problems of system design.

Computer scientists have proved that it is theoretically impossible to achieve perfect security inside the program itself. That is, it cannot be demonstrated that any particular combination of hardware and programing is proof against some new unexpected type of attack. Improving the security of a computer system involves balancing the costs of protection against the expectation of loss resulting from the threats and vulnerabilities. While it cannot provide a final answer, R&D in the field of computer security can substantially decrease protection costs.

Risk analysis, the process of weighing all these factors in a decision model, is a difficult job. The precise factors are unknown, and it is difficult to determine whether all possible alternatives have been covered. Research can develop techniques for performing risk analyses with greater precision, and the Government has new research and standards activities in this area. While the standards are directed at Federal systems, they will provide useful guidance to the private sector.

Technological instruments for security fall into three categories, according to the intent of the designer: *prevention, detection* and *auditing. Prevention* means keeping unauthorized persons from having access to the system, and keeping authorized persons from using the system wrongly. *Detection* means catching an unauthorized procedure when it is attempted and preventing its completion. *Auditing* means the determination of whether unauthorized acts have occurred. A particular security technique is usually directed toward one of these goals.

Specific Techniques of Security

Authentication: The first objective of security is to assure that only authorized personnel can access the system. *Identification* is the process of establishing a claim of identity to the system, either with a name or an account number. *Authentication* is the process of verifying the claim.

The simplest and oldest procedure is to use a password or number that is known only to the individual authorized to use the system. The *personal identification numbers* assigned to bank customers for use on ATMs are examples of such codes.

The security provided by password schemes is limited, although more elaborate versions offering some improvements have been developed. However, the security of any password scheme depends fundamentally on the ability and willingness of the user to keep the code secret.

Physical identification techniques, which depend on measuring certain personal physical characteristics, are being developed for use as authenticators in computer system access. To be useful, any such system must be able to discriminate between persons, but at the same time be insensitive to changes in the characteristics of a particular individual over time.

The system operator, when selecting an authenticating technology, has to make a choice in balancing two types of errors—classifying a fraudulent identity as correct (type I) and classifying a proper user as fraudulent (type II). These two types of errors have costs associated with them, and are usually at opposite ends of a tradeoff

curve for any specific technology. The type I error can be minimized only at the cost of maximizing the type I I error, and vice versa.

Fingerprints: The technology exists for reading and encoding fingerprints with minimum delay, but the devices are expensive (over $50,000). Although the pattern is complex, fingerprints can be encoded in a computer using less than 100 characters by storing only certain key data points. This storage efficiency means that a complete set of fingerprints for every person in the United States could be stored easily in a commercially available bulk memory.

The cost of directly reading fingerprints, however, seems to suggest that it will not become a widely used method of authentication, at least in the near future. Its use will be restricted to very high security requirements, and to applications where fingerprints themselves represent significant data, such as in police work.

Hand Geometry: A new and surprisingly effective form of physical identification is the geometry of the hand. Individual finger lengths vary from one person to another. This variance is sufficiently significant and unique to be the basis for a relatively inexpensive (around $3,000) identification device. It is based on the use of a high intensity light shining on a pattern of photocells. It is sensitive both to external geometry and to the translucence of the flesh near the fingertips. Thus, it is quite difficult to deceive it with any artificial device.

Voice Recognition: Research on the techniques for voice analysis and voice synthesis has resulted in methods for distinguishing individuals by their speech. In these systems, a random list of words is shown to the individual, who then speaks them into a microphone. By having the computer generate a new list each time, the system makes it impossible for an imposter to use a tape recorder to fool the system.

The system has high interpersonal discrimination, but seems to be weaker on intrapersonal differences. It may reject authorized persons suffering from colds, hoarseness, or even emotional tension.

Voice recognition systems are not yet commercially available, although at least one firm, Texas Instruments, has installed a home-developed system for use in their facilities.

Since information collection is relatively cheap, requiring only a standard microphone, amplification, and signal conversion hardware, the limitations of the technology seem to be in the computational techniques. As software improves, and as the cost of computer hardware drops, voice recognition could become a popular low-cost authentication technique.

Signature Verification: Passive signature verification uses pattern-recognition techniques to analyze and encode a signature on a check or form. It is a difficult task, because a signature can vary depending on an individual's mental and physical state, the type of writing implement used, and because forgers can be quite skillful. One company has announced a product for providing passive signature verification for bulk application, particularly the processing of checks. It is not clear whether such technology is operationally effective in identifying forgeries, and whether it could be reduced in cost sufficiently to be used at the point of sale.

Dynamic signature verification systems track the actual path of the pen point as the individual creates a signature. Sensitive instruments measure variables such as the pen's speed and acceleration, the amount of time the point remains on the paper, and the changing pressure on the point. Several organizations, including IBM, are working on dynamic identification; however, no products are as yet commercially available. Some experts judge this to be a promising technology.

Much R&D is aimed at finding a more reliable substitute for the currently used magnetic cards and passwords to identify and authenticate individuals. To date only a

few products have come on the market, and those have been designed for use in applications with very high security requirements. The cost limitation seems to depend on the characteristics of the sensor, since the microprocessor costs have dropped so low. No doubt a growing demand could motivate a flurry of new products in the early 1980's.

The amount of data required to store computer representation of the pattern for any of these candidate technologies is relatively small—a few hundred characters. Thus any of them, if they become widely implemented, could become the basis for a quasi-universal identification code used by all private and Government organizations.

Encryption

In the past, cryptography was principally a tool for military and diplomatic communication. Now, however, modern data communication systems increasingly are transmitting private information of high value, and the need to protect these communications from interception and manipulation has prompted an explosion of interest in civilian encryption.

A standard for encryption technology, the Data Encryption Standard (DES), has been established by the National Bureau of Standards for Federal use. It is apparently also being widely adopted in the private sector, since several commercial manufacturers are producing devices based on it. While some experts have questioned the robustness of DES, it seems to have been accepted generally as an inexpensive technology that is at least effective for low- or middle-level security needs.

Another set of techniques that has received some attention lately has been labeled "public key" encryption. The idea behind these codes arose from basic research in computational complexity, a field of computer science dealing with possible theoretical limits on the ability of even the most powerful computers to compute certain mathematical solutions. A public key code uses one key to encrypt and another to decrypt a message. Knowledge of the encryption key is no help in deriving the decryption key, even though their mathematical relationship is known. Thus, the security of the code does not depend on the security of either the encoding key or of the secrecy of the mathematical relationships. Since one of the major problems in the use of cryptography is control of the key itself, a system in which the decoding key need not be known even to the data sender is promising for many applications.

Public key codes also promise to be useful in electronic message systems, since they can be used for authenticating messages in the absence of signatures. Several applications of this sort have been proposed. However, public key codes are in their infancy, and it is not known with certainty whether unanticipated problems will arise as they are used.

Encryption has uses other than merely securing communications. Used internally in a computer system, it can isolate sets of data from unauthorized users. It can also allow users to enter data but not to read it, or to read but not modify data. It can even separate the activities of various connected computer processors.

Authorization

Most large-scale information systems are designed to serve several users simultaneously. The data bases in the machine often contain clusters of information that serve multiple needs. It is necessary, then, to control the access of users who are authorized to be on the machine, but may not be authorized to have access to specific parts of the data.

For each user, the system must keep track of which parts of the file can be accessed and manipulated, and what forms of access are held (read the data, enter new data, and so on). The system also must control the giving of permissions. Can one user, who is authorized to see a file, give access permission

to another user? There are many situations in which this is a legitimate and even necessary procedure, yet it complicates enormously the problems of access control. Researchers are developing ways to model these assignments mathematically and avoid unexpected loopholes in system access control.

The continued growth in the size of information systems and in the numbers of people allowed to access them will continue to put pressure on system designers by complicating the authorization process.

Logging

Logging is the process of auditing the accesses made to a data base by all users. Systems for keeping a complete or partial record of all access to the data have received more attention since privacy has become an issue. The system operator needs to account for all accesses made to files of personal data. Since the log itself is a file that contains potentially sensitive personal information, the need to protect it may be even greater than that for the original data base. For this reason, some experts suggest the use of a separate small machine to monitor accesses to the data base.

The system operator can then examine the log for unusual patterns of file access or other significant actions of the users that may indicate that unauthorized use is being made of the system. When it is possible to code certain unusual patterns of use, the logging system itself can be programed to watch for those events. It will then either send a warning to the system operator, or call on a special security surveillance program that collects as much detailed information as possible about the transaction.

Operating Systems

The operating system of a computer, the set of programs that control its work, is the fundamental piece of software on which all other application programs depend. Consequently, the integrity of the operating system is a necessary prerequisite for any other software security. Although no system can be designed to be perfectly secure, there is much that can be done to construct highly secure systems.

R&D is ongoing in this area, and results will be slowly incorporated into existing systems. However, progress will be hindered by the difficulty in adapting current operating system programs. These contain millions of instructions, and have been modified and expanded over several years by many programmers. The systems are difficult to change, as are the habits of their users.

Some computer installations still use operating systems written nearly 20 years ago. Computer operators fear that disruption and trauma would result from adopting radically different operating systems, and manufacturers resist compromising investments amounting to billions of dollars that they have made in existing programs. Thus, the most acceptable new techniques over the short term will be those that can be adapted to existing systems. However, it is the very size, complexity, and growth history of these current systems that create their greatest weaknesses—the logical holes and flaws through which a determined outsider can gain access.

Data Base Security

As data bases grow larger and are designed to serve multiple purposes, the likelihood increases that system operators will want to grant selective access. The problem is difficult. In an employee data base, for example, it may be desired to allow the personnel department access to some records, the finance department to others, and the medical department to still others.

One of the major problems is that of authorization determining which user can do what. Another related issue is how to structure the data base to allow such authorizations to be enforced. The question of which controls are even possible is, in itself, a complicated one. Research in data structures is

developing new techniques which will probably come into use rapidly as new data base systems come on the market.

Encryption is one technique that will be used increasingly in cases where different groups of data and their users can be easily partitioned in terms of access control. It will be less useful when the data are highly integrated, and when it is not known during the design stage where boundaries will eventually be drawn.

Years ago, some hope was placed in the use of so-called "aggregated files, " particularly when used for research with sensitive personal data. These files supposedly eliminate problems associated with maintaining personally identifiable data by stripping off identifiers and lumping them together in statistical clusters. It has been shown, however, that aggregating data statistically does not always assure that a clever inquirer cannot reverse the process and derive substantial personal information. In the same way, merely stripping identifiers off records of personal information may not preserve the integrity of the information, for a surprisingly small amount of descriptive information can serve to identify an individual uniquely. R&D is being conducted on ways to transform data bases collected for social research purposes so that the individual information is completely obscured, but statistically relevant calculations can still be done.