crime prevention review

Volume 6 July 1979 Number 4

Published by the
ATTORNEY GENERAL'S OFFICE
State of California

CRIME PREVENTION REVIEW

Published Quarterly by the Office of the Attorney General—
State of California

GEORGE DEUKMEJIAN, *Attorney General*

Crime Prevention Unit
3580 Wilshire Blvd., 9th Floor
Los Angeles, California 90010

MRS. JUNE SHERWOOD, *Director*

A. KEN MORALES, *Coordinator*

MELANIE C. INGRAM, *Assistant Coordinator*

Contents

Vol. 6 July 1979 No. 4

crime prevention review

Vol. 6 July 1979 No. 4

Understanding Computer Related Crime

Lyle A. Cox, Jr. and Roger R. Schell

Both Lyle Cox and Roger Schell are members of the faculty in the Computer Science Department at the Naval Postgraduate School in Monterey, California.

Professor Cox has extensive computer design and applications experience, including the design and implementation of systems for the National Security Agency, the U.S. Department of Defense, the U.S. Department of Energy, and several California law enforcement agencies. He has a Ph.D. in Computer Science in addition to his L.L.B. Degree.

Professor Schell is a Lieutenant Colonel in the United States Air Force who has served extensively in the development of computer based military systems. For several years he was technologist and program manager for the Air Force's $9 million Automatic Data Processing System Security Program. Professor Schell received his Ph.D. from M.I.T. in Computer Science.

INTRODUCTION

Al Capone's bookkeeper is reported to have said: "I can steal more with a pencil than ten men with machine guns." That was probably a conservative estimate. Regardless of the bookkeeper's actual capabilities, his chances of escaping detection and apprehension by law enforcement authorities would have been significantly better than those of a gang of gunslinging outlaws. If we can replace a hundred or a thousand bookkeepers with a single computer, consider the possibilities. The threat to our society posed by the misuse of computers cannot be ignored. The magnitude of the possible damages, and the difficulty of detecting and investigating computer related crimes constitutes a serious problem.

What is the magnitude of the problem? A federal study reported: "inquiry revealed that computer fraud is a growing problem in both the Government

and private sector and that, in many instances—no one knows how many—it is impossible to detect."[1] As a follow-up, a study of such crimes in the private sector was performed by the Stanford Research Institute. This study reported that the average loss per incident in private business was $450,000, a number which has probably increased in the years since these studies.

Computers, and hence this situation, did not exist thirty years ago. If technology created this problem, can it create the solution? Optimists in the field are hopeful that research will, in time, resolve many of the problems. Until that day arrives we will have to rely upon more conventional crime prevention techniques (as intelligently applied by well informed members of the judicial and law enforcement communities) to minimize the disruption to our society.

In the remainder of this article we will review the nature of computer related crime, including the most common threats. We will historically examine the evolution of computer technology which partially explains our current situation. We will briefly introduce those new techniques which promise to alleviate (eventually) some of the problems of misuse of computers. Along the way we will mention some of the practical (stopgap) preventative measures which can be used until more permanent solutions are developed.

THE COMPUTER THREAT

Gradually we have seen the implementation of myriads of computer systems of all sizes. These systems may be thought of as consisting of three components: "hardware," "software," and data. The physical devices are generally termed "hardware," as contrasted with "software" which includes all of the programs. For most purposes we may consider software to consist of two types of programs: those that "operate" the hardware (in a supervisory sense) and those which use the hardware and supervisory software to solve problems or to perform certain desirable functions. Since most of the non-scientific computer applications involve information processing, the final component of computing is the data base. This is the compiled, formatted body of information to be operated upon by our computer hardware and software. These components are all present—to varying degrees—in our common computer systems: credit data, justice information, computer vote tabulation, consumer billing, health data, insurance data and management, and computer communications, to name a few.

Computer related crimes can directly involve any or all of these three components. In general, computer threats can be categorized into four broad areas: 1. theft of computational resources, 2. disruption of computational services, 3. unauthorized information access, and 4. unauthorized information modification.

This categorization implicitly rules out two fundamental problems. First, unintentional acts are not considered, since they are generally not criminal in nature and they more properly fall into the areas of computer system reliability and human engineering. Second, the employment of the computer as a tool in the commission of a crime will not be considered. Almost any tool can be used by unethical parties for achieving socially undesirable ends, and the computer is not an exception.

[1] "Computer Related Crimes in Federal Programs", Government Accounting Office Study, April 28, 1976.

Of the various types of computer related crimes perhaps the most common form is the theft of computational resources. Much as some people connect into electric utility lines and divert power for their use without payment, computer resources can be diverted. This category includes both malicious and benign computer uses. For example, the use of systems by authorized users for unauthorized purposes (game playing, printing of pictures, calendars, etc.) represents a drain upon any computer system. Furthermore, the systematic use of a processing system on a larger scale by unauthorized users can have both economic and production impacts.

Unauthorized programs which extensively use the hardware and the supervisory software can consume many thousands of dollars of computer services and compete with authorized programs. In addition to lost time, hardware subsystems—storage for example—may be filled by the unauthorized programs to the exclusion of valid data, causing failure or delay of authorized programs.

If measures are taken to exclude unauthorized users or programs, the persons responsible may misrepresent themselves or their programs, claiming to be valid users or jobs. In this way, they can continue to run their programs and charge any expenses to some legitimate user. Strict accounting (as a countermeasure) can be expensive in itself.

The second category of computer related crime is the disruption of computational services. Consider the situation of two companies competing for a contract. Company "A" has an automated cost/schedule system while Company "B" does not. In the last several days before bidding closes, Company "A" 's computer (upon which its management relies) is unavailable due to a series of failures. Company "A" is forced to develop its bid without benefit of its system and thus proposes a contract with a cost 5% higher than the more accurate, computerized figures would have suggested. Company "A" loses in its bid on the basis of cost. The computer failures were caused by saboteurs from Company "B".

Such disruptions of service can be extremely expensive if the timing is correct. Interruptions can be caused by attacks upon any of the components: hardware, software or data base. Physical damage to the hardware, confusing or modifying the supervisory software, subtle changes in the applications software, or modifications to the data interface can all cause such problems. This process does not necessarily use significant amounts of computer time, nor does it require either the access or modification of data. Nevertheless, access to the system by authorized users can be denied thru these subtle attacks.

In such situations the crime usually goes undetected. Often the failures are blamed on "bad luck" or on inadequate preventative maintenance. Since resources accessed are minimal, proof of criminal acts or intent are often difficult to obtain. Identification of the perpetrators is even more difficult.

The third type of computer related crime is more familiar: the unauthorized access to data stored in the computer. This type of act, much akin to our popular view of espionage, is well understood when we speak of unau-

thorized access to conventional data files stored on paper in filing cabinets.

Computers add a new dimension to this problem. The enormous storage capability and the fast access times make abuses more costly. A criminal might normally have to search an office for hours to find the data he wanted (if he finds it at all). The long periods required for such nefarious searches greatly increase the chances of being "caught in the act". Using a computer, the criminal can search data bases equivalent to several office's filing systems in a matter of seconds. The fact that computer data systems often store data used for critical decision making processes (such as the hypothetical situation of Company "A" above) usually implies that the data is entered in a more timely manner than paper based systems. The complete and up to date information in a computer system makes it a tempting target. "Outsiders" with full access to "inside" information pose significant threat to business and society. Like other forms of abuse, unauthorized accesses are difficult to detect.

The difference between unauthorized access and the remaining fourth type of computer related crime is the action of modification of the data. We have mentioned the advantage of knowing the facts upon which a competitor is basing his decisions, and of knowing the decisions as soon as they are made. Of far greater use would be the ability to "feed" data (erroneous or misleading or incomplete) into the competing system and thus control or influence the decisions to your benefit. One could virtually "change the facts" to suit the situation.

The classical cases of a computer operator modifying his credit rating, or of erasing the records of his outstanding debts are small examples of this type of crime. Also included in this category of crime are modifications made to programs. For example, modification of accounting routines to prevent charges to one's credit card from being billed to one's account is another example. In view of our increasing dependence upon computerized systems in banking and commerce, the potential for large scale disruptions are enormous.

We have placed our trust in our computer systems and, by and large, they have proven to be fast, efficient and reliable. We have not, however, placed any great priority on the development of protection methods for our investments. In the following section we will review the evolution of computer systems as insecure entities, and mention some common areas of attack which can be partially protected.

EVOLUTION OF COMPUTER SYSTEMS AND SECURITY

To better understand how computer related crimes can occur, let us first look at how our evolving use of computers has brought with it computer security problems. This tutorial introduction will, hopefully, help us understand what we can do—and cannot do—to correct the problems we identify. We will then examine solution alternatives in more detail.

Single User, Dedicated Computers

Prior to the mid-1950s computers were commonly dedicated to a single user at a time and security was a minor concern. He used the machine either

on his own behalf or as a programmer for someone else. The computer power was limited, and with reasonable planning the user kept the machine busy for his period of use. The jobs were typically processing of numerical data, i.e., "number crunching". This sort of data processing requires only a limited amount of software and data.

The user brought with him (e.g., as a card deck) all the needed data, and security was little problem. No one else could affect the machine while he used it. If he had sensitive data he could, when done, easily purge the small amount of data that was stored in the machine, and take his data and results with him. With no sharing of the machine resources and no sharing of his data, the user was largely in control of his own security.

Shared Resource Computers

In the mid-1950s to mid-1960s computers became more powerful and were too expensive to dedicate to a single use; the human was just too slow to efficiently employ the machine. In the same time frame, processing became oriented more towards symbols rather than numbers; that is, information processing began to supplant data processing. During this era computers were typically shared by a number of users in one of several ways. Software packages evolved, called "operating systems" or "monitors" (the "supervisory software" mentioned above), controlling the shared use of the machines. In this mode the machine was under the physical control of a computer operator, not the user. In a simple case users may submit their job and the operating system will merely select which job of all those submitted to run. More common and useful operating systems will dynamically share the machine so that several jobs are running at the same time—through a technique called "multiprogramming." Even more sophisticated operating systems use a technique called "time sharing" to simultaneously connect many users with remote terminals to the computer—giving each user the illusion that he is connected to a dedicated computer. But regardless of the operating system particulars, the computer itself (via the operating system) controls the sharing of its resources.

In this shared resource environment, the nature of the computer security problem becomes quite clear. The operating system software is necessarily more privileged in some sense than the user jobs. In fact it can affect the processing of and access to the information of any user, yet this seems to be no problem as long as the operating system is friendly. Unfortunately, it was quickly discovered that a malicious user could easily penetrate the operating system and induce it to share its privileges; that is, any user could through deliberate effort access the jobs of other users. Furthermore, for even simple operating systems it is impossible to test or evaluate the myriad of possible ways it can be so subverted.

The obvious answer to this problem of the unreliable internal security controls is to eliminate any user who is not authorized all access to all the information—just as you would not give your house key to a known burglar. Observe that this is essentially reducing the problem to the previous case of a dedicated computer—but with a group of friendly users rather than a single user. This brute force solution, however, has two disadvantages. It can be quite expensive since it reduces the sharing of the computer re-

sources. It can also encourage imprudent risks because of the temptation to increase sharing by treating users as friendly when they may in fact be hostile or negligent. The distinctive characteristic of the shared resource computer (with no sharing of information) is that security can be provided by isolating the users into compatible groups that share machine resources.

Information Sharing Computers

Since the mid-1960s, computers have been increasingly used for information processing. The principal capability of these systems is access to information (not processing of data), and the access to computerized information must be controlled. These controls can be as simple as distinguishing whether a user can read or both read and write a data base, but they can range to more complex controls over access—such as those implicit in the Federal Privacy Act of 1974 and similar state statutes.

These information systems are still expanding into numerous areas of our society—banking, securities, medicine, law enforcement and judiciary, to name but a few. At the same time that the dependency on these systems is growing, the opportunity for computer related crime is growing. Yet the isolation technique previously used is totally unworkable—since the very purpose of these systems is to provide controlled (shared) access to information. This means that for security we have no choice but to use the internal controls of the computer itself—that is the operating system controls. Unfortunately, for nearly all contemporary systems these controls are totally inadequate. This leaves us in somewhat of a quandry as to how to proceed.

RESPONDING TO THE THREAT

We have already reviewed the threat including the motivation and potential damages. From our historical review we see that there are basically two kinds of responses: (1) we can limit the opportunity to do harm and, in doing so, we reduce the means, viz., reduce the vulnerabilities. (2) Although the internal computer vulnerabilities are widely reported and deep seated, adequate technology is emerging and there are a number of stopgap measures and ways we can currently posture ourselves to accelerate and exploit this technology in the future.[2]

First a somber warning is in order: there is today a plethora of computer security gimmicks (hardware, software, books, courses, checklists, etc.) that fail to address the real underlying problems. Not only are these mostly ineffective and wasteful, but frequently they are actually counterproductive. The "work ethic" simply does not apply: just spending time and money on security is not likely to be very beneficial. The key is to clearly understand what problem is—and is not—being addressed by any proposed countermeasure. Now for a look at some specific countermeasures that can be effective.

External Controls of Physical Access

Regardless of how it is used, a computer must be protected from physical

[2] Schell, R. R. "Computer Security, the Achilles' Heel of the Electronic Air Force" *Air University Review*, Vol. 30, No. 2, January–February 1979.

access by the criminal. The computer and all its users can be within a security perimeter established by guards, dogs, fences, or less dramatic methods—consistent with the value of what is being protected. Little more will be said since these security controls are not really unique to computers. For example, approaches to building security are just as applicable to buildings that contain computers as to those that do not.[3]

With a computer in the dedicated mode—for either a single user or a compatible group—note that these external controls alone are sufficient to maintain the security of the system. In this mode, use of the computer is restricted so that all users are authorized access to all the computerized information. A potential attacker must overcome the external controls and penetrate the inner sanctum of authorized users. No failure or submission of the computer itself can compromise security because of the protected environment. In fact the real attractiveness of the dedicated mode is that it reduces the computer security problem to the much more well understood problem of physical security.

External Controls of Logical Access

For shared resource computers in particular, it is quite common to operate in what is logically a dedicated mode, even though physically there is not a machine dedicated to a single group of users within a single security perimeter. There are several techniques to ameliorate the limitations of the dedicated mode without seriously jeopardizing security. However, note with care that, contrary to common implications, none of these reduce the vulnerabilities of the internal controls.

Communications Cryptography—Remote and interactive access to a computer is a popular and most useful capability. Yet if the associated electrical communication paths are outside the security perimeter, "tapping" of the communication is an easy technique for any of the four threat categories we identified earlier. Cryptography devices, however, can "scramble" the information while it is being transmitted, making it logically within the security perimeter. By making the information unintelligible we can counter all the threats categories except disruption of the communications. Fortunately the National Bureau of Standards has established a Digital Encryption Standard (DES) that is becoming widely available. Cryptography is surely one of the most important techniques for controlling logical access.

Periods Processing—It is often satisfactory to dedicate a computer to a group of users for a period of time rather than continuously. Recall that this was common for the single user, dedicated computer. This requires an orderly completion of work at the end of each period, followed by a purging of all information stored on the machine and its peripherals. This is typically a tedious, error-prone manual procedure that can waste valuable machine resources. Although adequate, careful design is necessary to insure that all information is in fact physically obliterated between periods of use. This technique is, of course, not satisfactory for on-line systems where more than

[3] California Crime Technological Research Foundation report: "A Technological Approach to Building Security", *Crime Prevention Review*, Vol. 5, No. 3, April 1978.

one user group requires access at the same time—only separate physical machines can meet this need.

Authentication—It may well be difficult to physically control all access to the computer, particularly when this includes control of numerous remote terminals with a variety of legitimate users. Authentication techniques can be used to logically control access to the shared resources computer. There are numerous sophisticated authentication devices such as fingerprint and signature analyzers. On balance, however, these tend to be expensive and troublesome gimmicks with little advantage over a good secret password system. The password serves essentially a "combination" to a "lock" allowing access to the system. It is desirable that an easily remembered (but pronounceable) password be generated for the user—to avoid his choosing one that is easily guessed. The system should notify users of attempts to use invalid passwords, and passwords should be forced to change periodically, with more frequent changes upon user request. For those limited cases needing added protection against compromised passwords, this can be augmented with a "one time" password, e.g., on a magnetic strip badge. One final pitfall is noted: although passwords may effectively permit or prevent access to the machine, this authentication cannot be depended on to distinguish between the various permitted users —since this again relies on the weak internal controls of the computer itself.

Deliberate Overprotection—A dedicated group of highly privileged users may require access to information that is much less sensitive than their most protected information. This less sensitive information can clearly be input into their system and made available to them with no problem. However, all output (physical media or electrical) from the system must be protected as if it contained the most sensitive information. This is because, again, only the (unreliable) internal controls can prevent contamination of the nominally less sensitive data. This can lead to a serious proliferation of (potentially) sensitive information and a corresponding disregard for the protection needs of the truly sensitive information.

These few techniques (and not many others) are reasonable stopgap measures. They leave unanswered, however, the most serious problems of the information sharing computers. These problems relate to the internal controls of the computer itself.

Explicit Policy for Controls

A most important and fundamental step is defining what we mean by "secure"—and fortunately this step can be taken in spite of the technical weakness of today's computers. A clear, well-formed, precise policy is essential to establishing a secure computer system. The computer must be told exactly what policy it must enforce so that it can ensure that only authorized people can read or change information or instructions in the computer. The computer cannot make a judgment as to whether the user who is asking should have access to stored information. It can only grant or deny access based on the authorizations that it has been given. Thus, what is needed as the basis for any secure computer is to have policy that gives people well-defined authorizations to information.

Realistic Labeling—To support a meaningful policy it is essential that all

information be "labeled" as to its need for protection and that all users be "labeled" as to their authorization for access. In the past few years research has shown that nearly all practical policies can be implemented using a simple two-part label. The first part represents a hierarchical sensitivity level—such as the confidential, secret, and top secret labels used by the Department of Defense. The second part represents isolated compartments of access—for example, for privacy information, criminal history and medical information might be in separate compartments. Such a two-part label for information represents its "classification" and for a user represents his "clearance."

Enforced Access Control—If a computer (operating system) maintains these labels internally, then it can assume its "rightful" responsibility for enforcing the policy—viz., permit only properly "cleared" users to access "classified" information. Even if a user deliberately or accidentally attempts to violate the policy, the system can detect and rebuff the attempt.

These sort of explicit policy controls are the cornerstone of any meaningfully secure computer system, and the required technology is well in hand—complete with mathematical models and formal specifications. For the dedicated mode, such an explicit policy is needed in order to properly segregate —albeit with external controls—the users into compatible groups with their data. Unfortunately, most vendors have not actively marketed such explicit controls, although a few good products are now beginning to appear for information sharing computers. For example, both military and automobile industry users have for several years successfully used the Access Isolation Mechanism (AIM) offered by Honeywell as part of their large scale Multics operating system.

Effective Internal Controls

Although such an explicit policy is necessary it is not sufficient—the nub of the problem remains the efficacy of the internal (operating system) controls for information sharing computers. Today there is only one technology—known as the security kernel—that can provide truly penetration-proof internal controls. A security kernel is essentially a small subset of an operating system and its associated hardware: a subset that is provably sufficient to guarantee internal enforcement of an explicit label policy, regardless of the rest of the operating system or user programs.

The security kernel is a technical breakthrough that has transformed the designer's game of wits with penetrators into a methodical design process. One of the authors first introduced this technology in 1972 and, since then, research and development have demonstrated its feasibility, broad functionality, security certifiability, and supportability. Although the technology is available in the public domain, no major vendor today offers a kernel-based operating system; however, several are currently under development with government sponsorship. The problem is now one of industry assimilation of this technology.

CONCLUSIONS AND RECOMMENDATIONS

Computer technology has brought with it a serious problem of computer related crime, but the judicial and law enforcement communities can serve an important role in minimizing its impact.

First, you must recognize the problem for what it is—some parts easy and some hard. The key element of the threat is the malicious user. The internal security controls of contemporary computers are totally undependable in the face of a deliberate (malicious) effort to circumvent these controls. A dedicated mode of operation eliminates dependence on these weak security controls, but with a serious loss of information sharing capabilities. Stopgap measures can be used to increase the utility of the dedicated mode.

Second, you must formulate an explicit, label-based policy for specifying the permitted accesses in a computer information system. This issue of policy is fundamentally not a technical problem. In fact, an adequate policy is essential before effective use can be made of technical solutions.

Finally, computer system designers must apply the security kernel technology in order to provide badly needed information sharing computers that are secure. It appears that computer technology can indeed create the solution to the underlying problems it has created—the woefully inadequate internal (to the computer) security controls. You can have a very significant role in the solution by first insisting on controls to directly support the explicit policy and then stimulating use of the security kernel to make these controls dependable.

In summary, the problem of computer related crime is serious, and it is beginning to be understood; this article is intended to contribute to that understanding. Just as the problem has evolved, the solution can evolve with suitable stimulation and encouragement from those who understand the problem—and hopefully the reader will do his part.

END