Anatomy of a computer crime*

by SUSAN HUBBELL NYCUM
Chickering & Gregory
San Francisco, California

INTRODUCTION

This paper describes the process of an investigation** into the technical and legal aspects of a computer abuse of alleged theft of programs stored in a computer. The goals of such investigation are to provide information to help make computers and computer systems more secure, to provide computer technologists and managers with data as to the potential exposure for a particular activity, and to provide law enforcement officers and prosecutors knowledge of whether and to what extent existing laws may apply to the case.

There is no wish on the part of the investigators to sensationalize a case or bring to the victims and perpetrators more notoriety or exposure than already exists from public documents and proceedings or prior press coverage. Therefore, the paper will not use actual names and will where possible, generalize rather than particularize places and organizations.

Methodology of investigation

To date the investigators have knowledge of over 500 reported cases of computer abuse. To investigate each of these is beyond the existing level of resources. The cases that are selected for field study are those which offer one or more of the following:

(1) a plethora of available detail;
(2) an interesting, yet typical rather than wildly bizarre modus operandi;
(3) a suspected or demonstrated significant gain to the perpetrator or similar loss or exposure to the victim;
(4) a nontrivial legal question as to what crime or legal wrong has been committed; and
(5) a nontrivial investigative question for the law enforcement agency.

These five topics are more fully developed as follows:

(1) The incident must be available for research. The project prefers to investigate an incident at the postresolution stage. This qualification more readily assures that the parties will candidly share their experiences. While individuals tend to rationalize their actions at all stages of an incident, post-conviction interviews with perpetrators are more candid than pretrial or presentencing interviews. Similarly prosecutors and law enforcement personnel are understandably constrained from discussing a case before conclusion. Victims considering or in the course of civil litigation are normally uncommunicative.*

All aspects of the incident must be open to research to avoid the three common barriers to objectivity: bias, prejudice and interest of the parties thereto. In addition, each person involved sees the incident from a different perspective. As with the old anecdote about the blindfolded group asked to describe an elephant by touch, one at the trunk, one at the tail, one at the feet, each party to an incident “sees” the case somewhat differently and extrapolates the whole from his own experience. The investigator needs to put those various viewpoints together and can best do so from a wide variety of interviews.

(2) There are always unique approaches to the perpetration of computer abuses and there are always “old friends” of tried and true approaches. Since the project has six years of experience, many of the typical approaches have previously been identified, investigated and catalogued. If an incident looks like a good example of a known modus operandi, there is low utility, absent extenuating circumstances, in investigating that type again. At the same time a “far out” approach, dependent on a set of unique circumstances has lower utility than an abuse which could happen repeatedly to a larger set of victims, e.g., point of sale terminal users. This is not to say that new twists to old abuses or sophisticated efforts which thwart existing security are ignored. These may be the most critical cases from which to learn improved security techniques.

(3) The project does not chase the illicit makers of a

* The preparation of this paper was supported, in part, by the National Science Foundation Grant #MCS76-01242. However, any views or conclusions in this paper should not be interpreted as representing the official position or policy of the sponsor or Chickering & Gregory.
** As performed by Susan Nycum and Donn Parker pursuant to the above National Science Foundation Grant.
snappy calendar* any more than a traditional investigator is concerned with the typical business practice of taking pencils from the office for home use. The project prefers to spend time where the results of the study will help minimize exposure to nontrivial risks.

(4) From the standpoint of legal research, abuses to software and services are of greater significance than those to hardware. This is because hardware, however complex, is visible, touchable material, the generic equivalent of other materials the abuses to which the law has coped with for centuries. Software and computer services, e.g., computer time, are new forms of intangible property and less amenable to traditional legal treatment.

(5) How does one find out in what way the abuse happened, how does one prove what happened for the purpose of prosecuting the act and later implementing security against similar occurrences and implementing proper audit trails. This criteria can be evaluated with respect to inventiveness of the modus operandi or with respect to the rules related to evidence gathering, e.g., telephone traces.

Once an incident is selected for investigation, the project contacts the cognizant persons, the victim, perpetrator(s), law enforcement persons: prosecutors, and judicial personnel and sets up personal appointments with these people as nearly contiguous in time as possible at the interviewee’s office or residence (including jail cells where applicable). (This helps to preserve the continuity of the investigation and to assure that similar questions and similar weighting techniques as to response are used.)

At an interview the researcher explains the project goal and invites a description of the event in the interviewee’s own words. The approach is one of openness and professional interest. There is no attempt to intimidate or lead the interviewee. There is also a minimum level of sympathy or support for action taken. Experience indicates that rapport can be established with the interviewees without compromise to the interview—the project is not on one side or the other. New points that arise in a later interview are checked for comment by earlier interviewees on a call back basis. There are patterns to interviews but these vary with the type of abuse and the class of interviewee, e.g. victim, prosecutor, perpetrator. Notes of interviews are transcribed as soon as possible after the fact and details of the investigation rechecked and gaps filled in and authorities explained by subsequent contacts.

Results of case studies are added to an aggregate of data on several issues, project findings are never based on one incident.

Selection of the Brown** case for investigation

The Brown case was a theft of proprietary software from a private installation over telephone lines. It was investiga-
Prosecution

As the telephone access was across state lines, the FBI investigated the incident and the cognizant U.S. attorney prosecuted the perpetrator for violation of federal law, Section 1343 of Title 18 of the United States Code (wire fraud).* The indictment was summarized by the judge as follows:

"That the defendant, [Brown], obtained the unpublished telephone access number to the computer systems operated at and by [Company] exclusively for [Government];

That the defendant unlawfully and without authority obtained account numbers, user identification numbers, and other information which was necessary in order for him to access the said computer and computer systems;

That the defendant, through the use of said information, gained access to the computer systems operated by [Company] for the exclusive use of [Government], including the system known as [X];

That the defendant without authorization used said identification numbers and account numbers, and without authorization obtained information, including print-outs, from the computers and computer systems, then knowing that he did not have authorization to gain such access and to retrieve such information.

. . . It is further alleged in each of Count I and II that for the purpose of executing said scheme to defraud, the defendant caused to be transmitted in interstate commerce by means of a wire communication, namely a telephone communication between the defendant in [Y State] and [Company in Z State], certain signs, signals and sounds. Count I alleges a transmission on our about __________, 1975 and Count II alleges a transmission on or about ________, 1975.

In summary, then, the defendant is charged with devising a scheme to defraud and with using a wire transmission in furtherance of that scheme. The same scheme is involved in each count, although different transmission have been alleged.**

A third count which alleged receipt of stolen property, was dismissed by the judge who ruled that the electronic impulses transmitted by telephone line across state lines could not constitute stolen goods because they were not tangible items.

The defendant admitted the act of copying the system but argued first that the system was in the public domain and thus he hadn’t taken anything proprietary from an owner and second that his intention was not to use the system for his own interests but to show the vulnerability of the company’s systems security.

After a two and one-half hour deliberation, the jury found the defendant guilty on both counts.

Similarity to other cases

The fact pattern of this incident was close to that of an abuse which took place in California several years earlier. In the former case a programmer pled guilty to theft of trade secrets. These trade secrets consisted of a proprietary application program the perpetrator had copied over remote telephone lines to his employer’s computer and then printed out a hard copy thereof on his employer’s printer. The perpetrator in that case admitted that he intended to use the program for competition on behalf of his employer against the victim.

The contention of the perpetrator in the Brown case that his intention when he copied the program was to show the Company that its systems security was inadequate. This is most reminiscent of a 1974 Oregon case of computer abuse in which a student notified the console operator that he had taken control of the computer operating system from a terminal and had done so for the purpose of pointing out the security vulnerability of the system. The system in the Oregon case stored motor vehicle registration data including personal information. The system in the Brown case was targeted to contain government data classified "secret."

UTILITY OF THE CASE TO THE STUDY

The case was of great utility to the study of computer abuse from several aspects.

Security implications

The victim company described its systems access controls as a three part key number access: account number, associated user identification and password all of which had to be provided by the user and verified by the system before computer time could be used and files could be accessed. In their interview with the study the spokesmen were candid about their concern for the security breach but indicated the level of existing security was adequate to protect from external intrusion. Another employee of the company stated in a separate interview that steps had been taken after the incident to tighten the level of security. Testimony at trial indicated a security weakness in that passwords were infrequently changed:

Q. How often are the passwords changed?
A. Right now, they are changing once a week.
Q. Well, up until the time of this little problem, how often were they being changed?
A. At that particular time, I couldn’t tell you, but it was not very often.
Q. Well, I guess the next question obviously is, has the password been changed periodically as a result of this incident?
A. They were supposed to be changed periodically before the incident.

* §1343. Fraud by wire, radio, or television. Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined not more than $1,000 or imprisoned not more than five years, or both. Added July 16, 1952, c. 879, §18(a), 66 Stat. 722, and amended July 11, 1956, c. 561, 70 Stat. 523.
** Transcript pp. 832-833.
Q. Well, I think that's clear, but I mean did this incident bring on a policy of changing those passwords?
A. No, the policy was there prior to that.
Q. Did this incident bring on an implementation of the policy of changing passwords?
A. Yes, it did change the password, yes.
Q. Okay, because they found that to be a weakness in the system, isn't that fair to say?
A. That's correct.
Q. And how about the identification numbers now, are they being changed more frequently?
A. The systems people's identifications are being changed more frequently.
Q. Are they becoming more complex?
A. The format remains the same.*

The prosecutor

The prosecutor stated that this had been the first exposure of that office to computer abuse and they felt hampered by the lack of adequate federal law applicable to the case and by their own unfamiliarity with the type of activity. (The FBI could not be interviewed without a many months' delay because of backlog of requests under the Freedom of Information Act. Their reports, however, had been used by the U.S. attorney who did share his experience on the case with the study.)

Impact on programmers

From the standpoint of programmers involved with programs developed other than by themselves entirely with their own resources, the case points out two critical matters.

Most programs are owned by someone; very, very few are actually in the public domain. Indeed, another paper by the study is directed to a discussion of the ownership of programs whose development was sponsored in whole or in part by government funds. If the perpetrator Brown thought himself innocent of any wrongdoing when he took a copy of the company program, he was woefully mistaken. That assumption, which is unfortunately widespread, is wrong. Programmers must assume, unless assured otherwise by the persons responsible for the program, that it belongs to someone and permission to copy or use the program must be obtained in advance of such use.

System security is a legitimate concern of all those involved with computer installations and programs running thereon. If Brown was truthful, his efforts to convince the company during his employment of its lack of systems security through memo and meetings were unsuccessful. His testimony was that having failed to achieve better security while an employee of the company, Brown intended to copy the entire program after termination and present the company with the evidence of a series of perpetrations and the significant results of such accesses. (In fact he accessed the system approximately 60 times without authority.)* The jury disbelieved Brown. His case might have been stronger had those noble intentions been documented or had he in any way enunciated his concerns to users of the facility or to law enforcement personnel. Computer people whose personal ethics require action similar to Brown must realize and acknowledge that the action carries with it the possibility of conviction of a crime.

Legal aspects of the case

The case was interesting from a legal standpoint for several reasons.

The Judge’s dismissal of the count of receipt of stolen property was the second time a jurist had been faced with the unauthorized transfer of a copy of a computer program in the form of electronic impulses over telephone lines. In both cases the judges found this act to be outside the purview of the penal laws affecting asportation (carrying away) of personal property.

The prosecutors felt hampered in their conduct of the case by the lack of directly applicable law. They were fortunate that the alleged theft had been interstate and thereby subject to federal jurisdiction and the federal wire fraud statute. Had the incident occurred entirely intrastate, the laws of the particular state involved might not have provided the source of a prosecutable offense.

The character of the property involved, software, exposed the prosecution and the defense to the complicated and confusing issue of identification and protection of proprietary interests in software. This issue, as discussed above, was also a source of stated misunderstanding by Brown.

From a security standpoint, the methods of perpetration and detection were of value in determining how to make computer systems more secure, both technically and operationally.

CONCLUSIONS

Conclusions reached from a study of this incident include:

1. There is a need to educate prosecutors and defense attorneys about computer abuse. This was not the first or only instance of compromise of a computer system and a theft of a program and it was not the only instance of such a compromise being made purportedly not for gain. It would have been helpful to each side to have known of other occurrences.
2. Prosecutors and law enforcement officers need information about the environment and terminology of computer installations so that investigation and case preparation can proceed more independently of the victim’s guidance.
3. Computer organizations need to know how to protect proprietary software, legally and physically.

* Official Transcript, pp. 88-89.

* Transcript p. 749.
4. Computer professionals need to be aware of their legal exposure for appropriation for their own purposes of software not owned solely by themselves.
5. Computer organizations need to realize that security precautions are an ongoing concern and that procedures must be kept current to remain effective, particularly vis-a-vis current and former employees who know the system.

GENERAL REFERENCES