POSITIVE ALTERNATIVES TO COMPUTER MISUSE: A REPORT OF THE PROCEEDINGS OF AN ACM PANEL ON HACKING

by

J.A.N. Lee, Vice President
Roz Steier, Managing Editor, CACM
Gerald Segal, Education Manager

April 1986

TR-86-9

K.4.1 Computers and Society
K.5.1 Legal Aspects of Computing

POSITIVE ALTERNATIVES TO COMPUTER MISUSE

A REPORT OF THE PROCEEDINGS
OF AN
ACM PANEL ON HACKING

1986 January 08

J.A.N. Lee, Vice-President
Roz Steier, Managing Editor CACM
Gerald Segal, Education Manager

Association for Computing Machinery
New York NY 10036
(212) 869-7440

CR Categories and Subject Descriptors: K.4.1 [**Computers and Society**]: Public Policy Issues—*regulation*; K.4.2 [**Computers and Society**]: Social Issues—*abuse and crime involving computers*; K.5.1 [**Legal Aspects of Computing**]: Software Protection—*proprietary rights*; K.6.m [**Management of Computing and Information Systems**]: Miscellaneous—*security*; K.7.m [**The Computing Profession**]: Miscellaneous—*codes of good practice, ethics*

General Terms: Security

Additional Key Words and Phrases: hacking

1. INTRODUCTION

If one believes press reports, the misuse of computers is rampant. At the same time many other misuses have gone unreported as a result of the embarrassment and loss of image integrity of those affected (as victims) and the belief that to expose such misuses will lead to further problems and expense, as well as encourage copy-cat crimes. Much of the press coverage of computer misuse has centered on the younger members of the computing community using inexpensive personal computer systems. The placement of powerful tools into the hands of adolescents without imposing the appropriate controls would appear to be a contributing factor to their unfettered use of computers and communications systems. Such usage ranges from benign exploration of the powers of computational and communication systems, through the malicious use of those devices for personal aggrandizement, to the use of computers for distinctly criminal activities. At present there are no technological or ethical barriers that separate the explorer from the criminal; possibly the prospect of being able to perform more and more complex projects can innocently lead the benign user into improper activities. Conversely the blame for breaches of security and the infiltration of personal, private systems, is sometimes placed on the backs of the owners of those systems for maintaining an attractive nuisance.[1]Concern must also be expressed about the community-developed attractive nuisances of bulletin boards (BBS's), many of which are benign, but too many of which are used to extend the fringe areas of illegality in exchanging pirated software, providing message systems for immoral or illegal purposes, [2] and revealing cracks in governmental and commercial security.

To grapple with these and related questions, the Association for Computing Machinery hosted a Panel on Hacking during April 3-4, 1985 in Menlo Park, California. The invited participants included government and corporate security specialists, educators, and hackers. The Panel resolved that, while aiding legal developments by other agencies is important, it would be more appropriate for ACM to investigate positive alternatives to computer misuse as a primary goal to deter the young explorer from potential criminal activity.

The initial task of the Panel was to clarify the term "hacker." Unfortunately, the news media have used hacker pejoratively for these computer users who have turned exploring into trespassing. While the term has honorable origins, [3] many of the more

[1] An example of an attractive nuisance is an unsecured swimming pool in a community of young children who find its use irresistible. The owner is then liable if, during the unauthorized use of the pool by one of these children, an accident occurs.

[2] "Officials Find D.C. Systems Providing Child Porno Info", Gov. Comp. News, 1985 Nov. 8, p.17.

[3] See: Levy, Stephen, HACKERS: Heroes of the Computer Revolution, Anchor Press/Doubleday, Garden City, New York, 1984.

notorious activities of some early hackers, especially Phone Phreaking must be regarded as having been criminal.

In the 1960's the word connoted dedicated, innovative computer programmers whose goal was to liberate computer technology from the province of a technocrat priesthood. There were famous names among them: Lee Felsenstein, originator of the Osbourne computer, Steven Wozniak, designer of the Apple computer, and John Draper (Cap'n Crunch) one of the developers of the Phone Phreaking Blue Box. The word fell into disrepute when it was picked up by the news media to describe teenagers and others who misuse computers, either as pranksters or criminals. Hacking has provided much of the innovation in personal computing, and the new breed of user-friendly software systems is often either an emulation of hacker products or commercially developed (and marketed) by hackers. Today, the term hacker is regarded as variously referring to a person obsessed with using and exploring computers and communications and to a person who utilizes computing talent to gain unauthorized access to software, systems, and databases. This current usage is embedded in the public consciousness and cannot be easily altered. Hacking then, must be regarded as covering a spectrum of usage ranging from the benign to extreme criminal activity. [4]

In this context the problem of controlling misuse is two-sided. Means must be found to deal more effectively with the career criminal through the legal system, while channeling unbounded inquisitiveness of the teenage hacker into constructive learning and use. This broad spectrum presents a challenge to every sector of society, from families and educational institutions, to government and industry: How can society nurture computer talent and appropriately deal with the computer criminal?

[4] In this report we have attempted not to use the term Hacker except where specifically relevant to the topic and where there is no intended connotation of good or evil.

2. THE MOTIVATION AND EXTENT OF EXPLORATION

Few people approach a field of technology with a complete knowledge of the capabilities and potentials for using that technology. Initially sufficient information is provided in order for the participant to fit comfortably into the domain without having to rely on continuous assistance, much as one learns about the language and customs of a foreign country before visiting. This educational development process is generally supported by:

- A knowledgeable mentor with sufficient experience to guide the neophyte through the adventures and pitfalls of further exploration,
- An experimental methodology which is proven to provide a safe passage through unexplored aspects of the technological environment, and
- A reward (and punishment) system which provides a metric for judging the efficacy of exploration, and encouragement for further exploration.

These factors often do not exist in the learning environment within which many of our young people come to understand the computer and thus learning becomes a matter of trial and error and some topics are overlooked in the rush to knowledge acquisition.

Computers do not strike back, and once over the initial fear that something might go wrong and the user will be liable for some unknown tragedy, users have little hesitation in trying to explore the unknown without fear of retribution. All too often using someone else's user-id and password to gain access to a system is not regarded as any more inappropriate than using someone else's copy of a (copyright) protected software package is wrongful. The intent and motivation of exploring ranges from the natural curiosity of the human mind, to the desires to locate new capabilities which can be demonstrated to others, thus to achieve advantageous social interaction and status. The Panel identified the Robin Hood Syndrome in which social status can be obtained through the sharing of knowledge, even though the recipients may not be aware that they are receiving stolen goods. The adolescent syndrome also finds in the computer a potential tool in the rites of passage and rebellion, and as an escape from the boredom of schooling and parental control. In the domain of these usages of the computer, a broad extent of activities can be identified, ranging from simple (benign) browsing of files, through obtaining, withholding, restricting and publication of private information, to contamination and destruction of that data. In each of these cases legitimate tools are used for illegitimate purposes – to obtain and manipulate information which is not normally available. It is reasonable to ask "What is the problem?" and "What are the activities to which we object?" While the list may be very long, the primary objectionable activities are:

- Infiltration of governmental and commercial systems,

- The unauthorized publication of private or propriety information, and
- The theft of services – ranging from computer time to communications access.

But what damage do we perceive accrues to the system owners from these activities and is it truly necessary to impose inconvenient restrictions on legitimate users merely to entrap and punish the minority? Are there benefits to be gained from these misuses? Can these currently unacceptable activities be turned to the good of the community? The Panel had mixed reactions to these questions. On the one hand corporate representatives felt the need for the protection of their products and, where they maintained information about individuals, they felt the need to live up to the trust expected of them both morally and legally by those individuals. To repeat the question asked previously: How can society nurture computer talent and appropriately deal with the computer criminal? Or put another way, how can the honest be kept honest while not imposing such stringent requirements so as to protect systems from the dishonest, without losing the friendliness and usefulness of those systems? The Panel struggled with these extremes and attempted to recommend solutions that would provide security without stifling legitimate curiosity.

The computer/telephone environment provides computer-mediated person-to-person communication with the potential for mixed results. The anonymity of communication can encourage the otherwise shy or retiring adolescent to make friends and to create a peer group without ever physically encountering the other members. Anonymity spawns courage that can be used positively; it also provides the malicious hacker or the potential criminal with a cover to conduct nefarious business. Anonymity also can spawn irresponsibility where communication can amount to slanderous and libelous statements. [5] Such communication is a potential for the development of peer groupings in which an ethical sense of social interaction can be developed, provided such ethical nuances exist somewhere initially and at least one participant who will stand up for those concepts. Peer groups can provide the means by which learning (as contrasted with purposeful teaching) is achieved through the sharing of experiences and tools. The sharing of tools which are either developed or extended by a member of the group, or developed as a group activity in the tradition of early hacking methodologies, can be a positive alternative which should be encouraged.

Similarly, access to information through BBS's operated by peer groups, can provide news of computer and communication developments, without which the peer group can become too insulated from the outside world. ACM (and other sister organizations)

[5] Members of the Panel noted differences between attitudes in their own colleagues when in person-to-person physical contact and when communicating through a computer network, and recognized the psychological changes which occur in such an environment. See also: Shapiro, N.Z., & Anderson, R.H., Towards an Ethics and Etiquette for Electronic Mail, Report R-3283-NSF/RC, The Rand Corp., 1985.

need to provide the means for this infusion of technology, in a form which will be easily accessible and acceptable to the young adolescent. Challenges such as those included in the COMMUNICATIONS OF THE ACM regular articles titled "Programming Pearls" could readily be used as a vehicle for this technical empowerment of young users. At the same time, the openness of such communication will have the potential for making it easier for the criminal element to extend their capabilities.

One of the major ethical claims of the hacker community is to the right to access information; in the world of today (regrettably) the ability to have open informational systems has gone the same way as the unlocked automobile and the open household front door. Conversely, it appears that the openness of information systems is proposed by the hacker community for the explicit intention of browsing – an activity which is regarded as being tantamount to trespass by most owners. So long as there is the potential for illegitimate use of information (private files or proprietary software) owners have the right and responsibility not only to protect their files but also to charge their legitimate customers for the additional costs of that protection.

At the MIT AI Laboratory in the late 1950's and early 1960's, the hacker ethic provided an environment in which there were no private files and even system software was open to both inspection and modification. In this environment everyone was free to improve on each other's files by changing the way things worked and by improving systems to meet the current standards of the state-of-the-art. Levy [6] reports that this did not create the chaos which is envisioned by random development. Hackers in that environment expected help from their neighbors and freely gave it back. Since the system was public property even private copies of software could be updated/replaced by other hackers. That environment does not exist any longer and is unlikely to be replicated in today's commercial environments. The hacker is still searching for such an environment and emulates it in accessing other environments. Customization may enhance a system for one's own purposes but may obscure other user's legitimate uses. For example, UNIX † provides a shell which, of itself, is somewhat pristine and curt. Personal customization is comparatively straightforward and can easily develop command systems which are natural for one user while being totally obscure to another. This can be achieved without modifying the shell; changes to the system which affect all users are unacceptable and destroy the maintainability of the system. The intruder's feelings of contribution by revealing the insecurity of a system or by correcting someone else's files, supersedes the feelings of mere intrusion and trespass. The owner of the files regards such contributions as contaminations of the system and is fearful of other changes which may have serious effects. The fact that only an inquisitive explorer has infiltrated a system is no consolation to a system owner who must now expect that the malicious intruder will follow in hot pursuit.

[6] Ibid.

† UNIX is a trademark of AT&T Bell Laboratories.

There must be some feelings of deja vu amongst observers of the hacker environment who were themselves active in the days of the SDA (Students for Democratic Action) and the Weatherman Underground. The distribution of power by making information open and free is often abrogated by putting that power into the hands of only those who have the tools to access that information – a clear reversal of the intention of informational freedom. One response to the problem of illegitimate access is to increase the number of technological "locks and keys" on the system. However, this solution has the additional effect of harassing legitimate access. User-friendliness, especially in the log-in process, innocently encourages intrusion, and when coupled with the ability to side-step into other accounts, leaves an open door to trespassers.

The attraction of the computer discipline to young people who do not have the appropriate technological educational preparations can lead only to the undisciplined exploration of the field and the eventual haphazard approach to learning and self-education. The uncontrolled introduction of juveniles into the field equipped with systems beyond their understanding or capabilities must only increase the need for security consciousness.

3. PROBLEMS WITH CURRENT TREATMENT

Parker and Maxfield [7]suggest that there are four solutions, each to be applied in varying degrees across the spectrum of hacker types:

1. changing services to be more resistant;
2. (developing and applying) appropriate criminal statutes with vigorous prosecution;
3. changing (moral and ethical) values especially among young entrants to the computer field; and
4. (building) technical safeguards ... into the hardware and software of computer systems.

Current attacks on the problem of intrusion, software piracy and other forms of activity which come under the current heading of HACKING encompass mainly item (2) above – solving the problem by the development of new laws. There exist projects which expect to result in, at least partial, solutions to (1) – improving system resistance – and (4) – installing technically sound safeguards. We suspect that there are those who believe that approach (3) – changing attitudes – will result in part automatically from (2) – legal reinforcements.

The Panel reviewed the approaches to the problem by several segments of our community though it should be observed that not each community views the problem in the same light, nor has the same goals.

3.1. THE LEGAL SYSTEM

It is certainly a truism that any approach taken by the legal community (ranging from legislators writing laws, through law enforcement agencies to prosecutors and defenders) occurs only after improper acts have taken place. Government Computer News, [8] discussing the Bills in Congress which have stagnated over the past two years, suggests 'Industry representatives ... worry (that) Congress are simply reacting to well-publicized hacker stories and will avoid most of the real, tough decisions surrounding the issue.'

[7] Parker, D.B., & Maxfield, J.F., The Nature and Extent of Electronic Computer Intrusion, NSF Workshop on the Protection of Computer Systems and Software, October 1984, (to be published).

[8] "Computer Crime Debate Resurgent", Gov. Comp. News, 1985 July 7, p.1.

Nycum and Appelman [9] have pointed out that the current legal systems which might be applicable to the perceived inappropriate elements of hacking (system intrusion in particular) are generally based on the concepts of physical theft and trespass and thus are difficult to use effectively. Moreover the differences between State laws and the almost inherent interstate nature of computer crime cause problems in determining jurisdiction, and the lack of a Federal law provides confusion which can be used by the defendants to avoid effective prosecution. Attempting to use existing laws which are couched in terms of tangible items leaves open the notion of what has been stolen. In at least one early case prosecuted in Virginia, a conviction for the theft of computer services was overturned by the State Supreme Court on the grounds that it was not possible to steal time! In other cases the lack of documented crime (and hence legal action) leaves the courts with no precedents with which to guide prosecution and against which to measure the public attitude towards such activities.

While the FBI does train agents, a three week course is not enough to provide the level of expertise needed. Vigorous prosecution will require agents who are as knowledgeable in the field as those they are watching. Other law enforcement agencies have similar problems; it is unlikely that the one-man criminal investigation unit of a small college town (where the student population quadruples the town size effectively) can deal with the sophistication of the computer intelligentsia! Cooperative use of specialists is imperative in these situations.

While some offenders are treated as technological heroes who strayed a little too far in their electronic exploration, others have their equipment confiscated and are labelled as juvenile offenders on probation. Where the jurisdiction is not in the courtroom, but is (say) within a university or college, other actions may be taken. These include internal administrative hearings without the benefit of legal counsel and can result in lost grades, academic probation, or even expulsion.

3.2. THE PRESS AND OTHER MEDIA

The Panel included several working journalists who were the target of outspoken criticism during the meeting. Not to be outdone they in turn criticized participants who represented the several sides of the issue. There is the side of people like Stephen Wozniak and John Draper, who have been reported to endorse (some or all of) the activities which are objected to by most of us; [10] there is the side of the security consultants who see everyone who breaks a rule as the enemy; there is the side of the educators who want to distinguish between irresponsible acts and the actors who commit them, and who want to nurture the latter; there is the side of those whose main

[9] Nycum, S.H., & Appelman, D.L., Legal and Managerial Approaches to Intrusion Protection, NSF Workshop on the Protection of Computer Systems and Software, October 1984, (to be published).

[10] "Wozniak: Hacking is creative venture," Associated Press, 1985 February 19.

concern is protecting the reputation of what they consider a strongly positive activity called hacking, different from the activity of breaking into computers.

On one side the journalists expressed concerns (reported previously in this report) about the cover-up of crime by corporations and institutions, and the lack of technological knowledge of the public relations contacts who were unable to explain problems of intrusion and trespass to reporters in technical terms. On the other side they had sympathy for the hacker's demands for openness of information, but were strongly supportive of the muting of such openness by the needs for privacy and confidentiality of individuals. It was noted that the malicious hacker community has been less than appreciative of the reporting of computer crime and the exposure of unsavory activities.

The Panel was concerned about the propensity of the press to overly simplify computer-related problems and thus to overlook the technological ingenuity of system intruders [11] and the lack of preparedness and reliability of commercial systems. The media does take a positive role in other areas to lift restrictions on, and to distribute information, but the public has little cognizance of this contribution.

While not exactly falling under the heading of Press and News Media, it is also interesting to note the characterization of hackers as nerds by the writers of TV productions and other authors. Levy tends to confirm this view! Except perhaps in the film "War Games" this epitomization of computer aficionados does nothing to improve their self-esteem and may in fact be an instigator of their own form of electronic rebellion.

3.3. PARENTS

Much of the publicity surrounding the exposure of young intruders into computer systems has left the impression that their parents were totally unaware of the activities of their offspring. They had provided their children with the necessary computer and communications equipment (sometimes extended by the acquisition of hardware and software through BBS participation) and had been highly pleased that the young people were spending their evenings in their rooms rather than cruising the streets! Actually in some cases the parents were themselves computer professionals at least capable of understanding the capabilities of the tools their adolescents had acquired or built, but they had failed to monitor the uses of the equipment. For them also, it was a surprise when the FBI knocked on their door! In many other situations, it must be true that the students are far more knowledgeable of the capabilities of computer/communication systems than their parents. In fact, though personal computers may have been purchased originally as family entertainment devices, the control has been taken over by the family expert. To the majority of the family the glamour of

[11] This technological ingenuity is hardly overlooked by the follow recipes taught them by someone else. The media err in the opposite direction, making them out to be geniuses when they are not.

game playing has worn off, the complexity of programming anything beyond simple, trivial problems is overwhelming, and the cost of sophisticated software packages will almost outstrip the original cost of the computer! Like the surge of interest in the Citizens Band radios of the late 1970's and the subsequent settling down of their usage to the enthusiasts (hackers) and truck drivers, the personal computer is entering a phase of more legitimate usage as an educational and professional tool.

The responsibility for violations of the law by juveniles and the subsequent liability for damage may rest with parents in some jurisdictions. As in the case of dealing with adult crime, the legal system is in a period of catch-up; like other crime, the youthful offenders are generally given the benefit of the doubt and released unscathed since:

1. They are juveniles,
2. It is their first offense,
3. The prosecution does not understand the severity of the crime, any more than the perpetrator realizes the errors in intruding into private systems, and
4. The victim does not want to expose all of their shortcomings in security to the light of a trial (though most juvenile cases are heard in private). [12]

3.4. EDUCATORS

Several States have recently enacted requirements for students graduating from high schools (and for a limited time from colleges) to include computer literacy in their curriculum. ACM has itself in the past year published a set of guidelines for high school curriculum and for the certification of high school teachers. [13] The Panel supported these innovations especially since the high school curriculum clearly promulgated a broad educational approach to computers rather than merely courses in programming languages. However the Panel noted the lack of emphasis on the ethics of computer usage in this curriculum; it is not expected that there should be specific presentations on ethics but instead that ethics should be a continuing theme throughout other presentations and activities.

There was serious concern for the lack of funding for:

1. Teacher training, and
2. Adequate equipment

[12] On the other hand some hackers are repeat juvenile delinquents with conviction records for many other offenses unrelated to hacking – D.B. Parker.

[13] "Computer Science for Secondary Schools: Curriculum and Teacher Certification," CACM, Vol.28, No.3, March 1985, pp.269-279.

and the propensity for school systems to assume that the learning of computational techniques, and the understanding of the wide applicability of the computer, can be achieved informally in teacher's spare time.

As has been noted in many university and college settings, where the advent of the computer as an academic tool was quickly followed by intrusions into administrative systems, a similar phenomenon is occurring in the school systems especially where a mainframe system is employed rather than a collection of personal computers. This has two deleterious effects: (1) when student record information is maintained on-line then the system can no longer be open with minimum security, and (2) student usage is forced to take a lower priority than administrative uses. In at least one State it was recommended that computational facilities be separated for these same reasons.

In all areas of school systems there is a need for education regarding computer technology and usage. Too often, we believe, computers are expected to be educators and the mere presence of a computer in a classroom solves all the problems of computer literacy. This is little different than expecting that placing a piano in an auditorium will lead to the development of a music program.

3.5. BBS OPERATORS

Bulletin Board Systems (BBS's) operated by computer, accessible through telephone systems, exist in most parts of the U.S. Most of them are perfectly legitimate and are used as a means of communication which obviates the need for direct and immediate contact and without the expense of a true computer network. Moreover BBS's permit the establishment of contacts between persons who would not otherwise meet each other. This is achieved by having those who are anxious for help or assistance posting notices in generally accessible files and then waiting for response from other browsers. Some BBS's concentrate on specific subjects while others serve a geographical area.

Many BBS's are operated by young computer users, typically consisting of a system costing as little as $2000 supported by a telephone auto-answering modem, a file system (probably on diskettes, but preferably a hard-disk) and the necessary software to provide the browsing and message posting facilities. Maxfield points out that generally the use of a computer [14] as a full-time BBS does not permit its use in other ways. Bulletin Board operators thus will often possess more than one system, using the BBS mainly as a source of information for themselves as contrasted with its use as a service to others. While most BBS have a facility for private communication between individuals, the BBS operator probably has open access to these files which may serve as an important source of information.

[14] Maxfield, J. F., Computer Bulletin Boards and The Hacker Problem, Boardscan, Detroit MI, 1984, 10 pp.

From the operator's point of view the cost of operation is small compared to the potential benefits of accumulating software and information. Underground BBS's (that is, systems used to disseminate information for criminal purposes) are often repositories for:

- Telephone customer billing codes and common-carrier access numbers,
- Access numbers of mainframe computer systems and networks,
- Procedures for wiretapping and phone tapping,
- Credit-card numbers,
- Lock picking instructions, and
- Recipes for bombs and immobilizing sprays (mace).

The cost of using a BBS varies from a direct exchange of money and a background check (to ensure that the potential user is not associated with a law enforcement agency), to the provision of a credit card number (supposedly against which to charge the cost of the service) or a copy of a piece of protected software. Young users can be easily deceived into providing the latter items without realizing the consequences. On some BBS's it is possible to obtain additional hardware for your own system in exchange for credit card numbers or software. As the amount of information and data on a BBS accumulates, there is a greater attraction for other users and a greater propensity for demanding larger entry fees.

The illegal uses of computers and communications systems and ingenious use of the technology has outstripped the legal system's ability to keep up. As in other cases, it is necessary that the innate ethical and moral values of the users provide a natural stability against the potential for misuse. Recognizing the potential for misuse, many BBS operators provide a warning that they cannot be held responsible for information in the system:

> The operators take no responsibility for any messages, files, or other incriminating info on the boards, or in the General section, because those files were uploaded by anonymous users.

It is doubtful if any such caveat would prevent the operator from prosecution if such systems were used to conspire to commit a crime. But do telephone companies get prosecuted when a telephone is used as a tool of criminal conspiracy?

A lack of established guidelines for the operation and use of BBS's leaves open a tremendous capability for misuse; as in so much of what is covered here, it is probably the few who are defacing the boards of the legitimate users. Associations such as ACM operate boards of their own; while one can expect that members will use them in accordance with good professional practices and in conformance with the Code of Ethics of the Association, it may be unreasonable to expect the owners to monitor each and every communication to ensure the appropriateness of usage.

BBS's provide a community of users within which there is the potential for the growth of social interaction and self-control. As a means of communication without fear it can be used to overcome the isolationism of the technically motivated user who has not infiltrated the clique world of the school system. On the other hand, the access to a BBS often requires the use of long distance telephone lines for comparatively long periods at a cost which is not supportable on student allowances. This supports the potential for the misuse of credit cards and other forms of toll fraud.

3.6. EMPLOYERS

The criminal use of computers by authorized users who can hide their deeds from their employers for long periods is inestimable. Parker [15] has reported such crimes over the years and it is vehemently believed by several of the Panel participants that the amount of reported white-collar crime is small relative to the true losses. As in other aspects of this problem, it is due to the lack of understanding on the part of the management that the employee is able to outwit them – and continue this practice for considerable periods. After all, these employees are the experts and have control over the lifeblood of their employers' organizations, and their financial and technical data.

These same organizations, when hiring a Comptroller would run extensive background checks to ensure the security of their financial information; such persons would also be bonded at the expense of the company. Yet the persons who have intimate control over that same data and who provide that data to the Comptroller are often neither subjected to background checks nor bonded. The embarrassment of having placed one's confidence (and confidential data) in the hands of unqualified employees is a stigma which leads to the cover-up of their crimes. Many instances of the re-assignment, or even apparent promotion, of individuals have been the rewards for being caught! Moreover, the lack of management expertise causes a ripple of problems such as:

- the inadequacy of the security of the systems they maintain and

- the hiring of subordinates who are no more qualified than their managers.

According to a recent survey of Data Processing Management Association members, [16] only two percent of offenses occurring in their workplace during the past three years were committed by outsiders. Misuse of computer services was cited by 49 percent of the respondents as the largest category of computer abuse, followed by program

[15] Parker, D.B., Crimes by Computer. Charles Scribner's Sons New York, 1985.

[16] COMP-U-FAX ® Survey, Park Ridge, IL., May, 1985.

abuse (24 percent), data abuse (22 percent) and hardware abuse (5 percent). Computer service violations were two types: unauthorized use (42 percent) and disruption of services (7 percent). According to DP executives responding, much of the unauthorized use arises from employees who use the corporate information resource as if it is their own personal property – often in direct violation of written or verbal policy.

3.7. COMMUNICATIONS SUPPLIERS

The lowered cost of computing has not been accompanied by lowered costs of communications. The computer industry has provided an inexpensive and highly powerful communicator and then failed to provide the concomitant economic means to communicate. No wonder Phone Phreaks choose to infiltrate telephone systems instead of paying the costs. The Panel felt strongly that given the appropriate safeguards to prevent side-stepping into other more sensitive systems and nets, a means ought to be able to be established for inexpensive communications system for young, would-be explorers.

3.8. SOFTWARE DEVELOPERS

In the beginning, software was developed by vendors and users for free distribution and for use in their own promotion. Howard Aiken (in an interview with Henry Tropp in 1972) [17] predicted that by the year 2000 computers would be given away freely in order to sell their applicable software. It would appear we are in the middle of that transition today, with hardware costs decreasing at a greater rate than Grosch's Law. Software acquisition costs, even for standard packages such as language compilers, are spiralling upwards as their user-friendliness improves. At the same time software vendors have taken steps to protect their products either by copyrighting them or by applying copy protection (prevention) techniques to the copies.

Coming from an environment in which information and data are free, the hacker community finds these restrictions appalling and actively rebels against them. In some of the current vendors organizations are previous hackers who found that they must support themselves by this protection. Legitimate copies of some software can be obtained at costs amounting to 10-20 percent of the advertised cost. Some software companies have chosen to substantially discount versions of software when updates have become available, but still permit owners to upgrade to later versions at comparatively little cost.

[17] Archived in the Mathematics Section, National Museum of American History, Smithsonian Institution, Washington DC.

3.9. THE ENFORCEMENT OF LAWS

Panel members were concerned that the law will be impeded in its prosecution unless there is dedication to report computer-related crime and to apply the penalties. The system of law under which we operate depends heavily on legal precedents and the collection of appropriate evidence. The former can be developed only as the laws are vigorously enforced and prosecuted by knowledgeable prosecutors and judges; the latter may require the use of the technology. In the same manner as the definition of electronic property is somewhat at question, electronic evidence may be as suspect, and thus require special definition. The legal equivalency of tangible and electronic evidence needs to be established and guidelines for the collection of such evidence be developed as other forensic systems.

The Association can assist in this endeavor by establishing the legal definition of terms as computer, communications software and equipment. Also, it can provide expert witnesses to the appropriate legislative committees and hearings. ACM and other associations might be of help in:

- determining agreed legal definitions of such terms as computer abuse, access, user, networks, and programs.

- establishing what constitutes computer trespassing as opposed to physical trespassing;

- establishing the interpretation and handling of evidental materials in computer crime cases;

- helping to define where the responsibility lies in certification of computer systems and products – especially the extent of liability of security products not providing adequate protection.

The problems related to the application of law to the abuse and misuse of computers can be expected to result in laws which spill over into other areas. The liability of a programmer for errors in programs and the unreliability of a supposedly secure system may be affected by laws intended to focus on the computer criminal. While there are moral responsibilities faced by programmers, no studies have been made of the protections or exposures faced by them. These may result in either criminal or civil actions which cannot be protected by current product laws. First Amendment arguments of freedom of speech may not be found to protect users and operators of BBS's. Errors and omissions which permit illegal acts must be protected from being considered as conspiracy. At the same time employers must be able to discipline their employees for malfeasance.

The Panel felt that there was a need to educate and inform the public about the risks of using computers; risks that they faced in attacks from external sources as well as the risks they faced for the improper use of that equipment. ACM should form a coalition with other societies and organizations (which are not necessarily only educational or professional, but might include trade organizations) to support the development of appropriate laws, and to encourage its membership to participate in local and State hearings as advocates of stronger, enforceable statutes.

The Panel recognized the responsibilities of ACM in these approaches to support the writing of appropriate laws and the appropriate use of the technology to secure sensitive systems. A consistency between Federal and State laws is a necessity, with the recognition that computer/communications crime is most frequently carried on across State lines. Accused violators should not be given the opportunity to hide behind the weaker laws of one State when jurisdiction over the crime and the person is at question. Consistency would resolve this problem. The Association can assist in this endeavor by defining what is a computer and communications equipment, and by providing expert witnesses to the appropriate legislative committees and hearings.

4. PANEL DISCUSSION

The Panel felt that these problems with expert treatment would lead to a series of recommendations for solutions. Some of the discussion of these topics follows.

The Panel addressed the idea of access to significant computing power for both students and their parents. Empowerment can lead to increased responsibility, as is exemplified in karate instruction. Skill in karate can be a deadly weapon. [18] Therefore karate schools begin with exercises to develop discipline and with an oath not to abuse the art. The analogy suggests that the answer is to combine ethical training with real empowerment.

The Panel discussed the need for practical programs both within and outside the school which would include proper role models and mentors. The programs themselves should provide access to the latest technology. The technology available to most young people is not a simpler version of what experts use; it is a more arcane medium. The programming languages, the file storage, and the editing tools are inadequate for challenging intellectual work. High-school teachers who are themselves qualified computer scientists need to be trained. In the short term, ACM and other societies could promote active cooperation between university computer science departments and high schools.

The problem of access to equipment is economically more difficult. Between schools a SCHOOLNET could be created. A three tiered teaching environment is envisioned. The first could be a Local Area Network within the school. At this level students would learn network protocols and establish their own operational guidelines. This can be implemented on small microcomputers the school computer or larger mainframe. The second level would be a communications network on a district or city-wide range. Students would have access to the district or Education Board's mainframe computer using modems and their school or home computers as terminals. Operational guidelines should be established, where possible, by a committee of students elected by their own local group. Finally, a nationwide network for students could be established by extending the university electronic network, CSNET, to secondary and elementary schools, or by providing space on one of the commercial electronic services e.g. EDUCOM, The Source.

The entire project provides the context for making abstract ethical issues concrete. Violations of student-created procedures affect all student users. Perpetrators are judged by their peers, who in turn have to monitor their systems. Outside of schools, government and industry should be encouraged to establish regional computing centers to provide interested users with a safe arena for ethical experimentation. Here, too mentors are important.

[18] See Appendix.

In its chapters and student chapters, ACM has mechanisms in place to make valuable contributions to these programs. In addition, ACM should consider organizing software libraries as were popular in the 1960's with contributed software available at the cost of storage and reproduction.

5. RECOMMENDATIONS

In order to promote effective legal and ethical use of the technology, the following requirements were identified:

1. A code of responsible use should be developed that can be introduced into high school classes within the ACM curriculum and that can also be used by other youth organizations as an educational tool. It is here that problematic or potentially harmful situations can be identified. Activities and methods should be developed to show how to address these moral and ethical issues in the classroom and business.

2. ACM should provide a series of case studies which can be use by teachers in classes to demonstrate the applicability of ethical concepts to computing.

3. A broad-based educational program for parents should be provided which would prepare them for interaction with their children. The program should encompass a body of information about the positive aspects of computer ownership as well as the awareness of the potentials for misuse.

4. Access to significant computing power should be established for interested users, both students and their parents.

5. Practical programs, both within and outside the schools, should be implemented. They should include the identification of role models or mentors. ACM can act to encourage commitment of computer professionals to pedagogic activities. Government and corporate employees should be given incentives to participate in such programs.

6. Regional computing centers should be established by institutions and corporations using equipment which is either recycled from unused or outmoded stock or presented new in the form of donated supplies.

7. The apprenticeship of young students within local companies either as part-time activity on a continuing basis through club or youth organization sponsorship with employees acting as individual mentors, or on a periodic basis such as permitting students to visit for a day and to work with professionals.

8. An organization analogous to the Amateur Radio Relay League (ARRL) could be created with a charter to organize contributed resources and make them available under a program of mutual education and improvement of skills.

9. Federal and State laws that are consistent and enforceable have to be passed. These should include consistency in the treatment of electronic information as

a proprietary asset, as well as in the treatment of wiretapping, EMS/EFT, and electronic records.

10. A central information resource of computer experts could be provided to the press and other news media through which they could obtain information on stories they are writing and from which they could obtain insights and opinions relating to the technological aspects of the stories.

11. A technically sophisticated magazine should be created for hobbyists beyond the level of current commercial magazines that would challenge the reader rather than give them canned routines and reports.

12. Private computer systems accessable from telephones should be designed and operated to be resistant to unauthorized access and provide due notice that they are restricted to preauthorized access. They should also be designed to be unattractive to attempted intrusion.

6. CONCLUSIONS

The recommendations of this Panel have been reported in the appropriate sections of this white paper. While the Panel was somewhat ambivalent on the solution to the perceived problem legal means (though there was a marked lack of opposition to legal activities which would lead to reasonable legal controls), it was the consensus of the whole Panel that there are positive alternatives which need attention. Concern was expressed on several occasions that other known approaches to the problem did not consider encouraging new entrants delete targeting the entry of the user into the field and the solution to the greater portion of the problem by education. It was recognized that it is a specialized form of education that is being recommended. On the other hand the cost of such efforts may be considerably less than the losses being incurred today by computer-using organizations. If only a small portion of the funds expected to be expended in improving security and reliability were to be channelled towards education, perhaps a great part of the problem could be eliminated.

ACM is encouraged to work through its institutional members, and especially those which are corporate members, to find solutions to these problems through positive alternatives.

APPENDIX A. LIST OF PARTICIPANTS AND OBSERVERS

A.1. PARTICIPANTS

John A.N. Lee, Vice President ACM, Panel Chair,

William Davis, Jr., Computer Security Specialist and Association Representative, Mt. Vernon NY,

Neil Day, High School Student, Weston MA,

Lee Felsenstein, Founding Member of the Homebrew Computer Club and originator of the Osbourne Computer, Berkeley CA,

Batya Friedman, Computer Educator, Berkeley CA,

Geoffrey Goodfellow, Computer Security Consultant, Menlo Park CA,

Joseph S. Greene, Jr., Col. USAF, Computer Security Specialist, Fort Meade MD,

Brian Harvey, "First Generation Hacker" and Educator, Berkeley CA,

Vico Henriques, Association President and Lobbyist, Washington DC,

Stuart Katzke, Government Computer Security Expert, Gaithersburg MD,

Steven Levy, Author of the book "Hackers", New York NY,

John Maxfield, Consultant, Southfield MI,

Mary Miller, Student/Teacher, Blacksburg VA,

Donn Parker, Computer Crime Specialist, Menlo Park CA,

Richard Sandza, Newsweek Journalist, San Francisco CA,

Gerald Segal, ACM Education Manager, New York NY,

Dennis Steinauer, Government Security Specialist, Gaithersburg MD, Pete Tasker, Software Security Specialist, Bedford MA,

William Tener, Corporate Computer Security Specialist, Orange CA,

Jim Warren, Founder of the West Coast Computer Faire and Editor-in-Chief, Silicon Gulch Gazette, Woodside CA.

A.2. OBSERVERS

Peter Neumann, Chairman, ACM Committee on Computers and Public Policy,

Rosalie Steier, Managing Editor, Communications of the ACM.

APPENDICES

Position Papers Submitted by Participants

Computer Bulletin Boards and the Hacker Problem -- John F. Maxfield
Computer Hacking and Ethics -- Brian Harvey
Real Hackers Don't Rob Banks -- Lee Felsenstein

COMPUTER BULLETIN BOARDS AND THE HACKER PROBLEM

by John F. Maxfield

BOARDSCAN
19815 W. McNichols
Detroit, MI 48219

Introduction

Computer hacking (i.e. malicious breaking and entering of computer systems) is an outgrowth of the phone phreaking of the 1960's and 1970's. Twenty-five years ago, if you wanted to become a phone phreak, you had to have a great deal of technical expertise and be skilled in electronics. Today, the entire picture has changed with the introduction and subsequent spread of the home computer and home modem. Phone phreaking (and computer hacking) has taken on a new dimension since the element of technical skill has been eliminated by the wide dissemination of this knowledge through underground publications and home computer bulletin boards.

History

Phone phreaking began in the late 1950's with the advent of Direct Distance Dialing. Several persons (including this author) independently developed the device which later became known as the blue box. The first blue box was captured by police in a raid on a betting parlor in Brooklyn, New York in 1961. It was so named because it was painted blue. Throughout the 1960's numerous phreaks were identified and arrested, however, little or no publicity was generated in the press. It was not until 1971, with the publication of the infamous Esquire magazine article and the arrest and conviction of Cap'n Crunch, that phone phreaking became a new national phenomenon.

In the fall of 1971, Steve Jobs and Steve Wozniak, the inventors-to-be of the Apple home computer, met John Draper, alias Cap'n Crunch, and learned how to build and use blue boxes. The two Steves supported themselves though college by manufacturing and selling hundreds of blue boxes. The relationship with John Draper continued even after Draper was arrested and convicted for a second time. By 1978 the Apple home computer was in production and Draper designed a special telephone interface board which would allow the emulation of the tones generated by a blue box, turning the Apple computer into an illegal device. Draper even considered marketing this accessory, however, the third arrest of Draper and the confiscation of his modified Apple computer abruptly put an end to these plans.

The introduction of time sharing in the late 1960's opened another door for illegal electronic activity. College students now could explore mainframe computers. In the beginning, hacking was openly encouraged as a learning tool. However, by the mid-1970's, hackers had caused so much harm and mischief that many facilities began taking steps to limit this kind of abuse. The few high schools that were advanced enough to own computers and offer programming classes soon found themselves made the victims of their own students. Until home computers appeared on the scene in the late 1970's, hacker attacks were somewhat limited by the scarcity of portable terminals.

In 1978 the first computer hobbyist bulletin boards began to appear. These early systems usually ran on borrowed mainframes and the users were limited to easily acquired teletypewriter terminals since the early home computers lacked sufficient capability to be used as terminals. This author took over the management of one of these pioneer systems in 1979. This system is still in operation today but due to hacker attacks suffered in 1979 and 1980 has been changed from an open access system to one with a highly evolved password controlled environment that is virtually hacker proof.

Finally, in 1980, the first true home computer bulletin boards began to appear in Los Angeles and New York City. From the very beginning, many of these BBS's were used for the dissemination of illicit information. The Starcom BBS and another called MOMS in L. A. and the OSUNY BBS in N. Y. C. were the forerunners of today's underground network. By the end of 1982 there were over 500 BBS's in operation nationwide. As of September 1984 there are an estimated 2,000 systems with more coming on line each day.

When MCI cracked AT&T's long-distance service monopoly in 1980, the phone phreaks were ready. Using a technique pioneered by Cap'n Crunch and his blue computer, software was developed for the purpose of scanning out the private customer billing codes used by the fledgling alternate long-distance companies. These new common carriers were forced to use these billing codes as caller line identification (ANI) used to bill AT&T long-distance calls was denied these new carriers. In effect, the monopolistic attitude of AT&T and the weakness of this billing scheme promoted the growth of phone phreaking and the spread of BBS's, since it was now extremely easy to place fraudulent toll calls. The sale of home computers and modems began to boom as thousands of persons learned about the underground BBS's and the free pirated software that could be downloaded from them.

Time-sharing packet-switched networks appeared on the scene, such as ARPANET, TELENET, and others. With local access numbers in most major cities, hackers could now freely explore new territory. By 1982 ARPANET and TELENET had been thoroughly penetrated and taken over by uncontrolled hackers. Malicious hacker clubs such as the 414's and the Inner Circle sprang into being. Today, there is virtually no system or network, either telcommunications or mainframe computer, that has not been compromised. Tens of thousands of juveniles, equipped with home computers and modems, regularly make attacks on systems. Hundreds of adults, motivated by the potential for financial gain, openly aid and abet the hackers. A new breed of criminal is emerging and unfortunately appears to be here to stay.

```
**************************************************************
*  THEY ARE OUT THERE RIGHT NOW TRYING TO CRACK YOUR SYSTEM  *
**************************************************************
```

What is a BBS?

A Bulletin Board System exists for the purpose of allowing home computer users to communicate and exchange information. This communication may consist of private messages, public messages such as requests for help or equipment for sale, computer programs or just about anything that can be transferred via a telephone line and modem. Many computer clubs have set up BBS's for the benefit of their members. A club member can ask for and receive help with a computer related problem and can download public-domain software. There are BBS's that cater exclusively to those looking for sexual partners. Many of these on-line dating services cater to homosexuals. Unfortunately, there are always those who try to take advantage of a good thing. If you can download public-domain software, you can also download copyrighted software. At least half of all BBS's fall into the category of pirate systems who stock the latest game and business software and allow it to be freely exchanged and traded. Still other BBS's cater to those who desire to break the law. These boards account for about 10% of the total. On one of these phreaker boards, you can find out how to avoid paying long-distance call charges, how to steal services from time-sharing companies, and how to engage in a wide range of criminal activities.

For various reasons, many boards are private access. A computer club might wish to restrict access to members only. Similarly, a hacker gang would certainly wish to block access by law-enforcement. There is a special type of pirate BBS that is called an AE PRO line. AE PRO is an abbreviation of the name of a popular program for the Apple computer called Ascii Express, The Professional. AE PRO is a modem to modem direct file transfer program that allows for uploading and downloading of programs or text files from one Apple computer to another over the phone lines. AE lines as these BBS's are called, require a secret password (part of the AE PRO program) for access. If you know the password, you can transfer cracked copyrighted programs to your computer. There is a semi-organized network of these AE lines all across the U. S. that exist solely to distribute pirated software.

```
******************************************************************
*  BULLETIN BOARD SYSTEMS BECAME UNDERGROUND EDUCATION CENTERS  *
******************************************************************
```

A BBS consists of a home computer such as a TRS-80, an Apple II, a Commodore C-64 or the like. Connected to the computer will be several floppy disc drives, a modem and, perhaps, a printer. A hard disc drive may be substituted for one or all of the floppy disc drives. Since information storage and retrieval is the main purpose of the system, the more disc drives and the larger the capacity of them, the more information (i.e. messages, programs, etc.) that can be stored for retrieval by on-line callers.

A typical minimum system would consist of an Apple II+ with two disc drives and a modem. Cost of such a system would be about $2,000.00. At the other end of the spectrum would be a system with multi-user capabilities and multiple phone modems and lines. One such system in the Midwest has 8 phone lines and two 40-megabyte hard disc drives and runs on an Altos 68000 UNIX computer. Value of this home hobbyist system is about $25,000.00.

It is very easy to become addicted to BBS's and the strange electronic underground that is associated with them. While a BBS is not inherently an evil thing, it does tend to contribute significantly to electronic crime. If a person becomes deeply involved in the BBS scene, one of their first problems is the size of the telephone bill. It is just too easy to obtain and use a billing code belonging to a customer of one of the alternate long-distance services such as SPRINT or MCI. Calls placed in this manner, where Equal-Access is not in effect, cannot be billed properly, nor can the originator be identified. If the long-distance service company tries to call the recipient of the fraudulent call, they will be answered by a modem and home computer. Even if the BBS operator is cooperative, learning the identity of the BBS caller is difficult since most fraudulent callers use a handle instead of their real name.

Fraudulent calling is not limited to the users of the underground systems, but is common to all BBS's. Large numbers of phreaked phone calls are placed to sexually oriented BBS's. BBS's by their very nature have to be classed as attractive nuisances if they are not policed or regulated. It would appear that laws regulating BBS's are needed. An analogy would be the laws governing the height and type of fencing to be used around a home swimming pool area. Unfortunately the large majority of BBS operators are juveniles which contributes significantly to the problem. Sadly, most parents haven't the slightest idea what their son or daughter is doing with the home computer!

Any successful BBS almost always has a problem with a lack of sufficient disc storage space. Given the widespread use of credit cards and the availability of telephone order houses that carry computer equipment, it was inevitable that credit card fraud would enter the BBS scene. Credit card numbers are widely traded and posted via the underground BBS's. Prime targets are the high credit limit cards that will allow the fraudulent purchase of a hard disc drive ($3,000 - $5,000). There are many underground BBS's that openly brag about the new hard disc drive that was acquired for the system in this manner. It is hard to understand how a 14-year old boy could afford a $10,000 home computer system, yet BBS's with this much equipment owned by juveniles are quite commonplace.

Hardware alone does not constitute a BBS. There must be software also. Mention has already been made of the Ascii Express software for the pirate download systems. A normal BBS can use a wide variety of BBS software, either commercially produced or homemade. The various program types are not germane to this discussion, however, some of the more popular BBS programs are Networks and T-Net (and their pirated equivalents) for the Apple computer. All normal BBS software has most or all of these features: message base or bulletin section, text and data files, E-mail or private message section, program download/upload section, user listing.

The message base may consist of one or more sections dividing the messages into various categories. Typical categories are General, For Sale, Help, Meeting Announcements, etc. These sections are accessed from a menu of choices and the user may view the message titles, read any or all of the messages, post a new message, or delete a previously posted message. To limit objectionable messages, most systems will not allow posting until you have either been validated by the operator or have called the BBS several times.

In addition to the message base there are usually special files that may be viewed by the user but can only be placed there by the system operator. Examples of such files would be lists of other BBS systems, instructions for use of the system, news items, etc. Sometimes these files are combined with the program download section and may contain the documentation for the available programs.

The E-mail (electronic mail) section allows private communications between users. E-mail can only be read by the intended recipient or the system operator. On the underground boards the E-mail section is where much of the illegal information is exchanged, such as credit card numbers. E-mail will account for about half of the storage space on a typical system.

Most BBS's make a listing of the other users available to facilitate using the E-mail section. Obviously you cannot send mail to someone who does not use that particular BBS. Sometimes the user list will give the user's telephone number or address, but most often will merely list only the names or handles used by the various users.

Interestingly enough, BBS's are often the victims of the very hacker community they support. Crashing a regular BBS or even a rival gang's BBS is common. Due to the hacker problem and the anonymity of the user, most BBS's will assign a private password to each user and will only allow access to post messages if the new user gives his or her real name and telephone number to the system operator in a private message. Validation of the user typically takes 24 to 48 hours or more depending on the responsiveness of the system operator. Validation may also involve the raising of a user's security level so as to access parts of the BBS that otherwise would be off limits.

Why does a person set up a BBS?

Why would a private individual go to the expense of setting up a BBS? One major expense is the computer itself, which cannot be used for any other purpose while the BBS software is running. Some BBS operators have two or more computers so as to be able to perform other tasks without disturbing the operation of the BBS. Another expense is the telephone line, although this is minimal in comparison to the cost of the computer. Unless there is a computer club or some sort of commercial sponsor, all this cost has to be borne by the system operator. Some BBS's charge a nominal fee, say $5.00, in order to be validated, however these systems are not well patronized and are in the minority. There are a few underground BBS systems which charge a fee to access the program download section or the illegal information sections.

The operator of a popular BBS system is in a position to make lots of friends and acquaintances with mutual interests because he or she must communicate with the new users in order to screen them for subsequent validation. The operator of a dating service BBS obviously will have first pick of any newcomers.

A system operator can read any of the private mail messages on the system since he alone has full access to the contents of the disc drives. Even if the operator of a sexually oriented BBS did not directly participate in a communication with a user, he can certainly act as the electronic equivalent of a voyeur by reading the supposedly private correspondence between the users. If the system operator is discreet, the users will be completely unaware of any intrusion.

(This author ran an underground BBS for a while and found the E-mail to be an excellent source of intelligence.)

The operator of a pirate BBS will acquire a tremendous collection of free software from the users. Many of the early pirate boards would allow a user to download 4 or 5 programs only if they first uploaded one new program. This strategy ensured the system operator would always acquire the newest programs as they became available on the underground market. Software collections of over 1,000 programs are not uncommon. Most of the juveniles who set up BBS's do so for this reason alone. There are unscrupulous adults who obtain commercial and business software in this manner which they then resell to unsuspecting clients.

Most underground BBS's require a new user to prove that they too are a member of the underground by providing the BBS operator with some sort of illegal information, whether it be an MCI customer code, a credit card number, or something of similar nature, before granting full access to the BBS. The BBS operator is the one person most likely to benefit by permitting underground activity on the BBS.

Underground BBS's

How do you find an underground BBS? As a starting point, just attend a meeting of a local computer club and ask about BBS's. A few minutes conversation will usually suffice to come up with the names and numbers of several pirate systems in the local area. All BBS's must advertise their presence in order to attract users and new information. Once you get validated on one system, you will usually be able to download a list of other systems from which you can get lists of more systems, ad infinitum. Most underground systems have obvious names such as Applecrackers, Twilight Phone, Forbidden Zone, Securityland, etc. There are a few which masquerade as normal legitimate systems or have non-descript names. If a BBS has menu selections which list special message bases such as Underground, Special Access, Phone Phreak, Hacking, Technical, Restricted, etc., you have probably found an underground system. Some BBS operators try to hide these illicit sections by making them invisible to a user who does not have the necessary security clearance. However, most users tend to be careless and if there is a hidden section, you will usually find reference to it in a message posted in another section. Another excellent way to tell if the BBS caters to the illegal, is to note whether or not the BBS operator has posted a disclaimer claiming freedom of speech and absolving the operator from any liability due to message content. The tougher the wording of this disclaimer, the greater the illegality of the information stored in the BBS undoubtedly will be.

Here are a couple of disclaimers which I found to be rather comical:

> The sysops take no responsibility for any messages, files, or
> other incriminating info on the boards, or in the General section,
> because those files were all uploaded by anonymous users.

> DO YOU WORK FOR OR ARE YOU AFFILIATED WITH ANY GOVERNMENT,
> DETECTIVE, OR POLICE AGENCY, PUBLIC OR PRIVATE, OR WOULD YOU EVER
> REVEAL ANY INFORMATION GAINED FROM THIS BBS TO ANY OF THE ABOVE,
> OR DO YOU WORK FOR ANY TYPE OF LONG DISTANCE COMPANY, PUBLIC OR
> PRIVATE, AND/OR WOULD YOU RELEASE ANY INFORMATION GAINED FROM THIS
> BBS TO ANY SUCH LONG DISTANCE SERVICE OR ITS AFFILIATES?
>
> PLEASE ANSWER YES OR NO >>
>
> (If you answered YES, the computer would abruptly hang up.)

As mentioned previously, access to an underground BBS will usually involve giving the system operator proof that you too are a criminal. Also, the system operator will usually be more careful in screening and will almost always call you back at the phone number given to verify that you are really who you say you are. More than one telephone security person ran afoul of this when a secretary answered the phone! Some system operators will make use of the telephone company's CNA (Customer Name Address) bureau to verify whether you are using your home phone and to get your address. If you give the number of an unlisted residential phone, the CNA bureau will not give out any information other than to say that the number is unlisted. Another way to get validated with few problems is to have someone who is already established in the underground vouch for you. If you are the operator of an underground BBS, you will be validated instantly in exchange for similar privileges on your BBS.

Some of the nastier underground boards are limited to access by invitation only. If you are not a member of that particular hacker gang, you will not be allowed access. In most cases of this type, the BBS will not even permit a non-validated user to sign on. The only recourse here is to either become a member of the gang or to work through an informant who is a member. This is a tedious business at best and is the sort of thing better left up to experienced operatives. In the course of my work, I have gained access to private BBS's with as few as a dozen select hackers. Luckily, these private boards are in the minority and by their exclusiveness make themselves a highly visible target. Another factor which tends to work against this sort of BBS is that the amount of information, while it is usually of an extremely sensitive nature, is not widely disseminated, thus minimising the potential for serious harm.

(In a few cases, this author found it harder to access a phreaker BBS than to access a high security government computer system!)

All sorts of illegal information can be found on these underground systems, such as:

Lists of customer billing codes and common carrier access numbers.

Plans and instructions for phone phreak blue, red, black, and silver boxes.

Access numbers, passwords, and logon procedures for mainframe computer systems.

Procedures for wiretapping and phone bugging.

Instructions on how to pass oneself off as a computer or telephone repairman or other employee so as to gain information or access to be used for fraud.

Plans and instructions in the art of lockpicking.

Do-it-yourself instructions for the home manufacture of explosives, poisons, and incendiary devices.

Lists of phone numbers of famous people, government installations, computer systems, and telephone operator call routing codes.

Lists of credit card numbers (i.e. VISA and MASTERCARD) to be used to order merchandise over the phone for resale or trade.

How to invade the privacy of anyone through access to their computerized credit and financial records.

Ways to harrass and/or harm anyone you don't like either over the phone or by other means.

Programs for downloading to convert your home computer into a blue box or to use for scanning for modem numbers or customer billing codes.

```
**************************************************
*    Don't worry about Orwell's Big Brother,     *
*  the problem in 1984 is with little brother!   *
**************************************************
```

Some of these BBS's have to be seen to be believed. As time passes and the BBS operators experience little or no control of their activities by law enforcement, they become more and more egregious. Some BBS's contain information of great use to both organized crime and enemy foreign powers.

Sources of illicit information

Many of the hacker gangs (who will be described later) set up group excursions to industrial parks or office complexes for the purpose of scavenging information and equipment from the trash dumpsters behind the buildings. Dumpster diving is a major source of passwords, system documentation, and other information. Credit card numbers are also obtained in this manner by salvaging and piecing together the carbons from the charge slips. Computer and electronic store garbage cans are a favorite hunting ground. Other major targets are telephone company switching centers and vehicle garages.

All too often, unscrupulous or careless employees of major corporations pass on details of computer operations to friendly hackers. In some cases the hacker, himself, has legal access to the computer center as, for example, an equipment repairman or delivery person. Hackers often pose as customers or employees and try to obtain information over the telephone about system access and passwords. Many times, this human engineering succeeds where other methods have failed.

As a last resort, physical theft is often attempted. A common ploy is the interception of mail containing customer account codes or passwords. Occasionally break-ins and theft of documentation, terminals or other equipment are a preliminary to a major hacker attack on a computer system.

Programmable smart modems which allow computer controlled phone number dialing and special software are used to find computer access numbers or customer billing codes. Numerous programs exist for almost any combination of home computer and modem that perform sequential or random dialing of trial numbers until a modem is located or a billing code is compromised. Some of these programs will test upwards of 1,000 numbers an hour. The recent movie Wargames showed in great detail the operation of one of these scanner programs.

Some hackers specialize in scanning and publish tremendous lists of codes and telephone numbers. Legislation is needed to control telephone scanning.

All of this information eventually winds up on an underground BBS. Once posted there, the information will be picked up and reposted everywhere. Some of the juveniles, in an effort to impress their peers, will gather up every little tidbit and repost it on all the boards that they call. Much of the information that is posted in this manner is old or useless because it has passed through so many hands. Any information of a sensitive nature or of extreme usefulness will not be publicly posted right away. Most of the hacker gangs will not post fresh information unless it is the gang's own BBS.

This author posted a test message one time on a California BBS. Only one hour and twenty minutes later, I discovered that the same message was now posted on a New York BBS. Within one week the message had been reposted on dozens of BBS's nationwide. It is useful to plant false or erroneous information in this manner so as to confuse the inexperienced hackers.

```
****************************************
*  YOUR GARBAGE IS A HACKER'S GOLD  *
****************************************
```

Hacker gangs

The early computer hackers tended to be of college age, as the exposure to computers occurred mainly at that educational level. With the advent of home computers and the teaching of computer basics in the lower grades, the average age of the beginning hacker has steadily dropped to a current level of only 14! The overwhelming majority of BBS owners and users are teenagers. Teens tend to form cliques and peer groups, so the formation of phone phreak and hacker gangs was inevitable. The parents of these bright teens usually do not, themselves, understand or comprehend the power of the computer. This means that the teens are not subject to the same parental restrictions that would govern their going out, the use of the family car, dates, etc. Many parents view the home computer as an excellent babysitting device. If their son or daughter spends the evening quietly in their room with the computer in lieu of a visit to the local pool hall or video parlor, the parents feel reassured that their offspring is not getting into trouble. In reality, these teens may be engaging in electronic gang activities that have serious implications. The losses to the software industry, alone, are staggering.

Unfortunately, many of the gang leaders are older more experienced teens, perhaps college students, who are interested in hacking, not for the intellectual challenge, but for the financial rewards. A few gang leaders are adults who are politically or financially motivated. There are several adults who are major figures behind the cracking and distribution of pirated software for resale to the public. One adult gang leader openly solicited credit card numbers from the juvenile members in exchanne for hard disc drives and other equipment that the adult would order fraudulently. Some of the teenage leaders bask in the tremendous notoriety and acclaim from their peers and strive to be the biggest phreaker or to have broken into the greatest number of computer systems.

The gangs may be local in nature such as the infamous Milwaukee 414 gang, or they may be national in nature such as the Inner Circle gang, or even international such as CHAOS, a Commodore C-64 cracking and pirating club, with headquarters in West Germany and the United States. In all cases, these gangs had a BBS that was their main base of operations and served as a (supposedly) secure communications center. The 414's had a private BBS that was so secret it didn't even have a name. The Inner Circle had the Securityland BBS and also illegitimately gotten accounts on GTE's TELEMAIL network. CHAOS operates on a variety of BBS's in both the U. S. and W. Germany. (I have had access to all of these BBS's and a large number of others.)

```
*******************************************************
*  WHEN MODEMS ARE OUTLAWED ONLY OUTLAWS WILL HAVE MODEMS  *
*******************************************************
```

Organized crime and the BBS

Naturally the underground BBS would have its uses in organized crime in much the same manner as the teen hacker gangs would use one. This author has good reason to believe that organized crime is controlling a number of BBS systems in the Midwest, the New York City area and in Florida. One informant knows of a BBS that is located in an off-track betting parlor. The teens are easily recruited to act as information gatherers, who will work for little or nothing and in most cases don't even know they are being so used. This author and other adult hackers have been approached and offered large sums of money to tamper with banking and credit data computers. Organized crime is swiftly moving into this new and relatively untapped area of crime. There is a very real and present danger here if the BBS's are allowed to operate unchecked.

Private underground BBS's

As law enforcement becomes more involved in prosecutions of hackers and phone phreaks, the illegal BBS operators become more paranoid. There is a slow trend toward all underground BBS's going to private invitation-only operations.

You will not learn of a private underground BBS from the normal sources mentioned earlier because the users are usaully sworn to secrecy. Inevitably, there will be a leak, either an indiscreet message posted on an open system or from the apprehension of a suspected hacker who turns informant. Once entree has been established on a private board, it will usually be possible to find out about and gain access to the other private boards. The one downfall to the entire underground BBS network is that the systems must have users and the only way to get them is to pass the word around.

This author participated in several sting operations where informants posing as hackers joined (or were invited to join) several gangs. In another sting, a completely bogus gang was created which took over several smaller real gangs. The true identities of the gang members became known to the leaders of the bogus gang, of course. Mop up was then easy with the dissolution of the bogus gang.

The private BBS's use a variety of means to block access by unauthorized users. These methods are familiar to anyone who deals with mainframe system security and are borrowed from that technology. Special preliminary passwords changed at regular intervals, hidden sections within an otherwise normal appearing system, and even, in the case of one BBS, a primitive dialback system, are used. As time goes on, more sophistication will emerge, however, nothing beats an informant who is in possession of all the secret passwords and phone numbers. The teens are the mainstay of the underground but they are also its weakest link.

Controls

There are various legal remedies available, both civil and criminal. However, there is no uniform code of law from one State to the next. The Federal justice system lacks a central clearing house for computer and telecommunications crime control, and also cannot deal well with juveniles. Computer hacker attacks tend to be multi-jurisdictional nightmares that traditional law-enforcement does not handle very well. When the 414's were breaking into computers in New York, California, and New Mexico from their homes in Milwaukee, they were only caught through an intensive call tracing effort that took many hours and only after they had successfully penetrated some computer systems for months. As it turned out, the FBI in Detroit was in possession of the solution to the identity of the hackers, but neither Detroit nor Milwaukee were in communication with each other until the arrest of the hackers made nationwide newspaper headlines. Steps are being taken to prevent this unfortunate situation from recurring.

The BBS operator controls access to the system through the user validation process, is responsible for the format of the system, and decides what the various message base topics are to be. In the case of an underground board, the system operator is the person who made his BBS available for illegal information, not the users. If the system operator has to validate a user for special access to an underground section, it is clearly the operator who is a party to any wrongdoing, regardless of posted disclaimers.

The issue of freedom of speech is a sensitive one, however. Perhaps a licensing arrangement such as is used for ham radio operators and those who use Citizens Band radios is in order. Possession of an unlicensed BBS could be dealt with in a manner similar to that of possession of an unlicensed radio transmitter.

For a time, the State of Oklahoma had telephone tariff restrictions that charged an extra $50.00 for the connection of a modem to the telephone lines. This charge was subsequently dropped under protest by home computer owners. If this sort of charge were applied to lines used by a BBS, it would eliminate all but the few who were willing to pay extra for the privilege of owning a BBS. The telephone line connected to a successful BBS is always busy. Thus an extra tariff could be justified on the grounds that more than the normal amount of circuit time was being used up.

Finally, public awareness of the problem and the voluntary reporting of suspicious BBS's to the authorities and the closing down of teenage systems by concerned parents would go a long way toward controlling the problem. Several nasty BBS's were shut down last year when the leader of the 414's bragged about them on a network TV show. Only then did the father of one of the BBS operators find out what his son was really doing with the home computer.

Defeating a mainframe hacker attack

Access attempts should be limited to only two or three tries per call. If someone is attempting to guess a password, this will slow them down considerably. A log must be kept of all attempts and an operator notified if the number of invalid logons exceeds a certain number in a given time period. Logs prove to be invaluable in tracking hacker activity since they may contain clues to the identity of the hacker or their location.

Backdoors into the system must be eliminated or fixed. Typically, juvenile hackers succeed only because common maintenance passwords or preset factory defaults are still present in the system.

If certain ID's are only used during certain hours, hacking can be curtailed by placing time restrictions on as many accounts as possible. Hackers typically are most active at night, on weekends or during school holidays. If the system is not normally accessed by the legitimate users during these times, it is best to block access entirely.

Naturally all standard precautions should be taken with passwords. However, sometimes management takes the view that the system should be easy to access. This is a serious mistake! A user friendly system is also hacker friendly. Do not prompt users at logon or give any clues as to the correct procedure until after the entire logon has been entered. HELP files should not be available unless a logon is successful. User friendliness is best left until after a logon has been validated.

Dialback systems will stop the average hacker cold. (The so-called Wizard of the Arpanet was completely frustrated in an attempt to crack a telephone company computer protected by a dialback system.) Dialback can be cracked, but the level of skill and equipment required is beyond that of the normal hacker. Dialback is extremely inconvenient to use, however.

The best way to catch a hacker is to set a trap. The 414's were caught only after their leader found a Star Trek game on a bank computer and played it for over 2 hours while the FBI traced the call. This author set a similar trap that resulted in the apprehension of a hacker in 1981. Suggestions for possible boobytraps are exotic games, a logon simulator that shunts the hacker off into a special compartment, a simulated operating system with dummy command menus and the like. Naturally, there should be suitable alarms given when the trap is sprung. It is high time that systems started fighting back!

```
*********************************************
*  TO CATCH A HACKER, SET A COMPUTER....    *
*********************************************
```

Recommended reading

Donn B. Parker, Fighting Computer Crime, New York: Charles Scribner's Sons, 1983
(All about the modern computer criminal and his methods.)

Timothy Orr Knight, The World Connection, Indianapolis: Howard W. Sams & Co., Inc., 1983
(Good discussion of BBS's and how to use them. One chapter mentions hackers and phreaks.)

Allan Lundell and Geneen Marie Haugen, "Merry Pranksters", Digital Deli, Editor Steve Dillea. New York: Workman Publishing, 1984
(Blue boxing in the late 1970's.)

Ron Rosenbaum, "Secrets of the Little Blue Box", Esquire Magazine, (October 1971), reprinted as "The First Computer Freaks", Esquire Magazine, (June 1983): pp. 376-391
(Blue boxing in the late 1960's and early 1970's.)

"Computers: X-Rated, The Joys of Compusex", Time Magazine, May 14, 1984: p. E5
(Discussion of sexually oriented BBS's.)

Tom Shea, "The FBI Goes After Hackers", InfoWorld Magazine, March 26, 1984: pp. 38-44
(The undercover adventures of John Maxfield, alias Gerald Schmidt.)

Richard Sandza, "The Night of the Hackers", Newsweek Magazine, November 12, 1984: pp. 17-18
(Discussion of underground BBS's.)

John F. Maxfield and Pam Javazon, "Phreaks Hack at Telecommunications", Telephone Engineer & Management Magazine, November 15, 1984: pp. 102-104
(How home computers are used for electronic telephone fraud.)

Underground publications

TAP magazine is not publishing at this time and its future remains unclear as one of its publishers has been indicted on fraud charges.

2600 magazine began publication in 1984 and has been publishing on a monthly schedule. While it is not our recommendation to support the efforts of these underground hackers, it might be wise to subscribe in order to know what these people are up to.... The address of 2600 is:

2600 Enterprises Inc.
Post Office Box 752
Middle Island, NY 11953

Annual subscription is $10.00

- End -

Computer Hacking and Ethics

Proposal for an ACM White Paper
Brian Harvey

> [Neal Patrick] said he and his friends, who named themselves the "414s" after the Milwaukee area code, did not intend to do any damage and did not realize they were doing anything unethical or illegal. In fact, when asked [at a Congressional subcommittee hearing] at what point he questioned the ethics of his actions, he answered, "Once the FBI knocked on the door."
>
> -- "'Common Sense' Urged on Computer Break-Ins," 26 Sept 83; (C) 1983 New York Times News Service

It's no secret that a mature sense of ethics is something a person develops over time. Parents are supposed to exercise authority over their children because the children are not expected to know how to make certain decisions for themselves. We have a juvenile court system separate from the adult criminal court system because we believe that a young person is not capable of crime in the same sense that an adult is capable of it.

Within this century, the obvious idea that the ethical sense of an adolescent isn't the same as that of an adult has become the focus of scientific research. Psychologists have entered a field once left to philosophers: moral development. The best-known attempt to formalize this development is probably the six-stage theory of Harvard psychologist Lawrence Kohlberg. Here is his description of Stage 3, the Interpersonal Concordance or "Good Boy-Nice Girl" Orientation:

> Good behavior is that which pleases or helps others and is approved by them. There is much conformity to stereotypical images of what is majority or "natural" behavior. Behavior is frequently judged by intention--the judgment "he means well" becomes important for the first time. One earns approval by being "nice." [Kohlberg, p. 18]

Is Neal Patrick at this third stage of moral development? He seems to judge his own actions in terms of intention. From the perspective of the stage theory, we can see this as an improvement over "Our mistake was to get caught" or "What have those computer companies done for me," responses that would be typical of the earlier stages.

It's not scientifically valid to assign Patrick to a developmental stage on the basis of one quoted sentence. Also, not every researcher accepts Kohlberg's stages. But it doesn't really matter whether or not we use the specific details of Kohlberg's system. The important point is that Patrick is not some new kind of monster spawned by computer technology; he's a kid with all the strengths and weaknesses we expect from kids in other situations.

Compare a bunch of adolescents breaking into a computer system with another bunch of kids hot-wiring a car for a joyride. The latter would probably argue, with complete sincerity, that they were doing no harm, because the owner of the car recovered his property afterward. They didn't keep or sell it. It's a "naughty" prank to borrow someone's property in that way, but not really serious.

These hypothetical car thieves would be wrong, of course, in making that argument. They might lack the sensitivity needed to give weight to the victim's feelings of manipulation, of fear, of anger. They may not understand how the experience of such a random attack can leave a person feeling a profound loss of order and safety in the world--the feeling which leads half our population to hail Bernard Goetz as a hero to be emulated. Some adolescents don't have the empathy to see beyond the issue of loss of property. Some may show empathy in certain situations but not in others.

The point is that the computer raises no new issue, ethical or pragmatic. The password hacker who says "we aren't hurting anything by looking around" is exactly analogous to the joyrider saying "we aren't stealing the car permanently."

(The two cases need not seem analogous to an adolescent. There may be many computer abusers who would never break into a car for a joyride, but who don't understand that breaking into a computer account raises the same ethical issues. But the analogy still holds for us as adults.)

The professional car thief and the teenaged joyrider are both social problems, but they're different problems. To confuse the two--to treat the teenager like a career criminal--would be a disastrously self-fulfilling prophecy.

In the context of computer systems, there is a similar dichotomy. There are some career criminals who steal by electronic means. This small group poses a large problem for society, but it's not a new one. Thieves are thieves. Just as banks use special armored cars, they must also develop special armored computer systems. But the rest of us don't use armored cars for routine transportation, and we don't need armored computer systems for routine communication either.

Two Models for Moral Direction

What to do about it? Saying that the problems of computer ethics are like other ethical problems doesn't solve them. Many approaches are possible. We are starting to hear among computer experts the same debates we've heard for centuries among criminologists: prevention, deterrence, retribution, cure?

Among all the possible approaches, it may be instructive to consider two strongly opposed ones: first, control of the technology, and second, moral training. As examples of these approaches, compare the registration of automobiles with instruction in karate.

Automobile registration is certainly a good idea in helping the police control professional crime. As thieves have learned to steal cars for their parts, rather than to sell whole, the technology of registration has had to grow more sophisticated: we now see serial numbers on each major component, not just on the door frame. But registration doesn't help against joyriders.

Other technological security measures can help. Steering column locks have made joyriding harder, but not impossible. Many adolescents are expert locksmiths, not because they're dishonest but because locks and keys pose a technical challenge much like that of passwords in a computer system. Also, increased security has made the consequences of juvenile car theft more serious, because the easiest way to defeat a steering column lock is to destroy it by brute force.

The example of karate instruction shows a very different approach to the problem of adolescent moral limitations. Instead of using technology to limit the power of young people, this second approach deliberately empowers them. Skill in karate is a deadly weapon; to give that weapon to a young person is an affirmation of trust rather than suspicion.

Why do karate classes for kids work? Why don't they lead to an epidemic of juvenile murders? This could be an interesting question for psychological research. This paper can't present a definitive answer. But we can suggest some possibilities and use them to draw analogies for computer education.

One probable reason is that every person responds to his or her situation. If I know you're trusting me with something important, I'll try to live up to your trust. If I sense that you consider me untrustworthy, I may decide that I might as well live up to your low expectations.

Another vital reason, though, is that the technical instruction in karate techniques is part of a larger initiation into a certain culture and its rules. Karate schools don't begin by telling novices, "Here's how to kill someone." They begin with exercises to develop discipline and with a solemn oath not to abuse the art. But beginning students know that the exercises aren't just busywork; there is a true empowerment at the end of the road.

Empowerment in Computer Education

How can we teach young computer enthusiasts to be responsible members of the electronic community, without defining them as criminals? The analogy of karate instruction suggests that the answer is to combine ethical training with real empowerment. To turn this broad slogan into a practical program requires several changes in our approach to educational computing and to computing in general.

> Growth, like any ongoing function, requires adequate objects in the environment to meet the needs and capacities of the growing child, boy, youth, and young man, until he can better choose and make his own environment. It is not a "psychological" question of poor influences and bad attitudes, but an objective question of real opportunities for worthwhile experience.... Thwarted, or starved, in the important objects proper to young capacities, the boys and young men naturally find or invent deviant objects for themselves; this is the beautiful shaping power of our human nature. Their choices and inventions are rarely charming, usually stupid, and often disastrous; we cannot expect average kids to deviate with genius. [Goodman, pp. 12-13]

Paul Goodman was discussing traditional juvenile delinquents, not password hackers. But the problem is fundamentally the same. How can we provide a worthwhile culture for young computer enthusiasts to grow into?

1. Serious adult models. In karate instruction, discipline is not only for novices. The adult instructors follow the same discipline themselves. The ethical principles taught to beginners are taken seriously in the adult community. As a result, young students don't see the discipline of karate as an arbitrary imposition on them; they see it as part of what it means to be a full member of the community.

In the computer culture, adults rarely take seriously the idea of belonging to a community. The only ideal is the self-serving entrepreneur. Our heros are the ones who become millionaires by doing a slick marketing job on yet another spreadsheet program. The conversation over the dinner table is about tax loopholes and padding expense accounts. In this context, why should any young person listen to our moral lecturing?

Fundamentally what is needed is personal action by each individual computer professional. But an institution like the ACM can act to encourage this individual commitment. We can urge our colleagues to devote part of their time to pro bono publico activities, like other professionals. We can give special public recognition to computer professionals who choose a life of disinterested public service over the quest for personal gain. Some corporations allow their employees paid sabbatical leave for public service work; we should encourage this policy.

2. Access to real power. Another important part of the karate analogy is that there are not two kinds of karate, one for adults and one for kids. What beginners learn may be elementary, but it's a start down the same road traveled by experts. The community into which young karate students are welcomed is the real, adult community. That's not how things work with computers. How many adult computer scientists put up with CP/M, BASIC, and floppy disks? The technology available to most young people is not a simpler version of what experts use; it's a completely separate, more arcane, fundamentally less powerful medium. That medium--the programming languages, the file storage, the editing tools, and so on--is simply inadequate to challenging intellectual work.

The community of computer professionals has come to take for granted easy access to electronic communication with colleagues anywhere in the world. Those of us lucky enough to be on the Arpanet have instantaneous communication supported by taxpayers. Even the less fortunate who communicate over dialup networks like uucp, though, have the cost of their mail supported by computing facilities other than their own; the general agreement among even competing private businesses to forward one another's mail is a remarkable example of disinterested cooperation. Some of this mail traffic is serious business. But some of it is also "junk mail" like sf-lovers (for science fiction enthusiasts) and human-nets. Is it surprising that young computer enthusiasts want a slice of the pie too?

Adolescents are excluded not only from access to equipment but also from access to ideas. The password hackers' preoccupation with magic words and magic numbers is harmful to themselves as well as to the rest of us; it's an intellectual dead end that gives them no real insight into computer science. They learn a bag of isolated tricks rather than powerful ideas that extend to solving other kinds of problems. Instead of just telling them what's forbidden, we would do better to show them the path to our own understanding of algorithms, formal theory of computation, and so on. We all know you can't program well in BASIC; why do we allow manufacturers to inflict it on children?

To take positive steps toward this goal requires action on two fronts, access to technology and access to ideas. The latter requires training high school teachers who are themselves qualified computer scientists. In the long run, this means paying teachers salaries competitive with industry standards. That's a matter for government action. In the short run, the most fruitful approach may be for the ACM to promote active cooperation between university computer science departments and high schools. Perhaps college faculty and graduate students could contribute some of their time to the local high schools. (This is not a new idea; outside experts are donating time to secondary schools to help teach other areas of science. Such partnership brings its own problems, because both the goals and the techniques of college teaching are different from those of high school teaching. Still, this collaboration has sometimes been fruitful.)

The problem of access to equipment is economically more difficult, but it's getting easier. The availability of 32-bit microprocessors means that serious computational power should be affordable in the near future. The ACM should encourage equipment manufacturers to take the high school market seriously, as an investment in future technical workers. Another approach is for interested educators to establish regional computing centers for adolescents, not part of a particular school, where kids can come on their own time. Economies of scale may allow such centers to provide state-of-the-art equipment that a single high school couldn't justify economically.

3. Apprenticeship: challenging problems and access to expertise. The karate student is given not only access to a body of knowledge, but also the personal attention of a master in the field. The instructor is responsible for the moral development of his students as well as their technical skill. He steers them in the direction of challenges appropriate to each one's progress, and his own expertise is available to help the learner.

For many years, the MIT Artificial Intelligence Laboratory ran a computer system with no passwords and no file protection at all. (It was pressure from ARPA, not internal needs, that forced them to implement a password scheme.) Even now, the laboratory has a liberal "tourist" policy: anyone can have an account, provided that someone at the laboratory is willing to be his or her mentor. The philosophy behind this policy is that most "malicious" computer abuse is the result of ignorance and misunderstanding, rather than real maliciousness. With a particular person responsible for each new user, tourists learn to share the values of the community. They are taught that the vulnerability of MIT's system is a price researchers pay willingly for the open exchange of information that that vulnerability allows. Treated as legitimate members of the community, even young tourists quickly learn to act responsibly toward the group.

Not every computer facility can be expected to share the vision of MIT-AI. Certainly the computers that control the missiles and the banking transactions should not be so open to visitors. But a typical large company has several computers, not all equally sensitive. Many could allow access to young people in their communities in the evenings, especially if some of their professional staff members are interested in serving as volunteer mentors. It's the mentor/apprentice relationship that makes all the difference. Just giving a kid an account on your machine may be asking for trouble, but making a friend of the kid is a good investment.

In particular, universities often treat their undergraduate student users like irresponsible children. Undergraduates are generally second-class citizens, with limited access to the school's computing resources, including human resources (faculty). The ACM should encourage universities to allow undergraduates to function as true members of serious research teams, as graduate students do. This policy would provide both access to faculty mentors and challenging, useful tasks.

For secondary schools, the issue is partly one of curriculum. Too many teenagers are taught (not only in the schools but also in the magazines) that true computer expertise means knowing what number to POKE into what address in order to change the color of the screen on some brand of microcomputer. Such learning is not intellectually challenging. It does not lead to a feeling of fruitful apprenticeship.

4. A safe arena for moral experimentation. The beginning karate student might be afraid to try his or her skill with a fellow student, lest he or she injure or be injured. But it's safe to fight a match with a black belt instructor. "I won't hurt you," says the instructor, "and I won't let you hurt me."

Young people have a similar need for safety in moral experimentation. One of the reasons for the appeal of role-playing games like Dungeons and Dragons is that a player can say "I'm going to be a thief," or "I'm going to be evil," trying on these roles without actually harming anyone. Similarly, a good school should be a place where students feel safe, a kind of "ethics laboratory."

Neal Patrick's first exposure to an ethical dilemma should not have involved the FBI. He should have confronted the issue of information privacy while using a computer system in his school. He could have learned how his antisocial acts hurt and angered the legitimate users of the system, without risking really serious trouble for himself or for anyone else. For one thing, it's hard for a young person to understand the chain of reasoning from the abstract corporate owner of a computer system to the actual human beings whose lives are affected when that system breaks down. It's easier to understand the issues when the users are one's friends and classmates, and the social effects of malicious password hacking are immediately apparent.

(None of this is meant to excuse Patrick or the other 414s. Neither ignorance of the law nor misunderstanding the ethical issues is accepted in our culture as an excuse for lawbreaking. But the ACM is not a court of law meeting to settle Patrick's guilt or innocence. The question for us is how, as a society, we can act to make the next generation of teenagers less likely to paint themselves into this particular corner.)

As a practical matter, what's needed to build an ethics laboratory for computing students has already been recommended in another context: adequate computing power to support a user community, as opposed to a bunch of isolated, independent microcomputer users. Whether this means timesharing or a network of personal computers with a shared file server is a technical question beyond the scope of this paper. But sharing is essential. The ethical issues of a living community don't arise in the context of isolated individuals using microcomputers separately with no communication among them.

Appendix A: What is a Hacker?

In one sense it's silly to argue about the "true" meaning of a word. A word means whatever people use it to mean. We are not the Academie Francaise; we can't force Newsweek to use the word "hacker" according to our official definition.

Still, understanding the etymological history of the word "hacker" may help in understanding the current social situation.

The concept of hacking entered the culture at the Massachusetts Institute of Technology in the 1960s. Popular opinion at MIT posits that there are two kinds of students, tools and hackers. A "tool" is someone who attends class regularly, is always to be found in the library when no class is meeting, and gets straight As. A "hacker" is the opposite: someone who never goes to class, who in fact sleeps all day, and who spends the night pursuing recreational activities rather than studying. There is thought to be no middle ground.

What does this have to do with computers? Originally, nothing. But there are standards for success as a hacker, just as grades form a standard for success as a tool. The true hacker can't just sit around all night; he must pursue some hobby with dedication and flair. It can be telephones, or railroads (model, real, or both), or science fiction fandom, or ham radio, or broadcast radio. It can be more than one of these. Or it can be computers.

A "computer hacker," then, is someone who lives and breathes computers, who knows all about computers, who can get a computer to do anything. Equally important, though, is the hacker's attitude. Computer programming must be a hobby, something done for fun, not out of a sense of duty or for the money. (It's okay to make money, but that can't be the reason for hacking.)

A hacker is an aesthete.

There are specialties within computer hacking. An algorithm hacker knows all about the best algorithm for any problem. A system hacker knows about designing and maintaining operating systems. And a "password hacker" knows how to find out someone else's password. That's what Newsweek should be calling them.

Someone who sets out to crack the security of a system for financial gain is not a hacker at all. It's not that a hacker can't be a thief, but a hacker can't be a professional thief. A hacker must be fundamentally an amateur, even though hackers can get paid for their expertise. A password hacker whose primary interest is in learning how the system works isn't therefore required to refrain from stealing information or services, but someone whose primary interest is in stealing isn't a hacker. It's a matter of emphasis.

Ethics and Aesthetics

Throughout most of the history of the human race, right and wrong were very easy concepts. Each person was born into a particular social role, in a particular society, and what to do in any situation was part of the traditional meaning of the role. This social destiny was backed up by the authority of church or state.

This simple view of ethics was destroyed about 200 years ago, most notably by Immanuel Kant (1724-1804). Kant is in many ways the inventor of the 20th Century.

He rejected the ethical force of tradition, and created the modern idea of autonomy. Along with this radical idea, he introduced the centrality of rational thought as both the glory and the obligation of human beings. There is a paradox in Kant: Each person makes free, autonomous choices, unfettered by outside authority, and yet each person is compelled by the demands of rationality to accept Kant's ethical principle, the Categorical Imperative. This principle is based on the idea that what is ethical for an individual must be generalizable to everyone.

Modern cognitive psychology is based on Kant's ideas. Central to the functioning of the mind, most people now believe, is information processing and rational argument. Even emotions, for many psychologists, are a kind of theorem based on reasoning from data. Kohlberg's theory of moral development, cited at the beginning of this paper, interprets moral weakness as cognitive weakness, the inability to understand sophisticated moral reasoning, rather than as a failure of will. Disputed questions of ethics, like abortion, are debated as if they were questions of fact, subject to rational proof.

Since Kant, many philosophers have refined his work, and many others have disagreed with it. For our purpose, understanding what a hacker is, we must consider one of the latter, Soren Kierkegaard (1813-1855). A Christian who hated the established churches, Kierkegaard accepted Kant's radical idea of personal autonomy. But he rejected Kant's conclusion that a rational person is necessarily compelled to follow ethical principles. In the book Either-Or he presents a dialogue between two people. One of them accepts Kant's ethical point of view. The other takes an aesthetic point of view: what's important in life is immediate experience.

> The choice between the ethical and the aesthetic is not the choice between good and evil, it is the choice whether or not to choose in terms of good and evil. At the heart of the aesthetic way of life, as Kierkegaard characterises it, is the attempt to lose the self in the immediacy of present experience. The paradigm of aesthetic expression is the romantic lover who is immersed in his own passion. By contrast the paradigm of the ethical is marriage, a state of commitment and obligation through time, in which the present is bound by the past and to the future. Each of the two ways of life is informed by different concepts, incompatible attitudes, rival premises. [MacIntyre, p. 39]

Kierkegaard's point is that no rational argument can convince us to follow the ethical path. That decision is a radically free choice. He is not, himself, neutral about it; he wants us to choose the ethical. But he wants us to understand that we do have a real choice to make. The basis of his own choice, of course, was Christian faith. That's why he sees a need for religious conviction even in the post-Kantian world. But the ethical choice can also be based on a secular humanist faith.

A lesson on the history of philosophy may seem out of place in a position paper of computer scientists about a pragmatic problem. But Kierkegaard, who lived a century before the electronic computer, gave us the most profound understanding of what a hacker is. A hacker is an aesthete.

The life of a true hacker is episodic, rather than planned. Hackers create "hacks." A hack can be anything from a practical joke to a brilliant new computer program. (VisiCalc was a great hack. Its imitators were not hacks.) But whatever it is, a good hack must be aesthetically perfect. If it's a joke, it must be a complete one. If you decide to turn someone's dorm room upside-down, it's not enough to epoxy the furniture to the ceiling. You must also epoxy the pieces of paper to the desk.

Steven Levy, in the book Hackers, talks at length about what he calls the "hacker ethic." This phrase is very misleading. What he has discovered is the Hacker Aesthetic, the standards for art criticism of hacks. For example, when Richard Stallman says that information should be given out freely, his opinion is not based on a notion of property as theft, which (right or wrong) would be an ethical position. His argument is that keeping information secret is inefficient; it leads to unaesthetic duplication of effort.

The original hackers at MIT-AI were mostly undergraduates, in their late teens or early twenties. The aesthetic viewpoint is quite appropriate to people of that age. An epic tale of passionate love between 20-year-olds can be very moving. A tale of passionate love between 40-year-olds is more likely to be comic. To embrace the aesthetic life is not to embrace evil; hackers are not enemies of society. They are young and immature, and should be protected for their own sake as well as ours.

In practical terms, the problem of providing moral education to hackers is the same as the problem of moral education in general. Real people are not wholly ethical or wholly aesthetic; they shift from one viewpoint to another. (When they are not trained in philosophy, they may not recognize the shifts. That's why Levy says "ethic" when talking about an aesthetic.) The job of moral education is to raise the self-awareness of the young, to encourage their developing ethical viewpoint, and to point out gently and lovingly the situations in which their aesthetic impulses work against their ethical standards.

Appendix B: A Case Study

The purpose of this appendix is to show that the ideas presented here are not just abstract daydreaming; they've been put into practice at least once.

Since I'm writing this as a proposed ACM position paper, not as a personal statement, I've avoided the first person until this point. But in this appendix I'm describing my own work, and it would be both unnatural and dishonest for me to do that from a third-person stance.

The Lincoln-Sudbury Regional High School is a four-year public high school in Sudbury, Massachusetts. I was Computer Director there from 1979 to 1982. Before 1979 there was a computer (a PDP-8) in the school, run by the math department. The two math teachers who were most involved had proposed the creation of a separate computer department, partly to attract kids who didn't think of themselves as mathematically inclined, and partly because they couldn't both give the computer facility the attention it needed and also do the rest of their jobs.

My own learning about computers took place mainly at the Artificial Intelligence laboratories of MIT and Stanford. I decided to create an environment at the high school that would be as similar as possible to those labs. To me this meant a powerful computer system, with lots of software tools, an informal community spirit, and not much formal curriculum.

I installed a PDP-11/70 running version 7 Unix. The cost of the machine was paid 75% by a contribution from Digital Equipment Corporation and 25% by a special bond issue approved by the school committee. Lincoln-Sudbury is a Unix source licensee; we were an alpha test site for 2.9BSD, the PDP-11 version of Berkeley Unix. The installation, testing, and debugging of this new system was carried out entirely by students.

The administration of the facility is carried out by the Computer Center Users Society, a group of about 50 students and teachers. Members have keys to the computer center, and may use the facility evenings and weekends without adult supervision. Students also use the computer from home via modems.

In the early days of the new computer, many students took an individualistic approach to it. Some students sought power and status by writing game-playing programs, and including in the program a list of their enemies, who weren't allowed to play the game. Later, as the computer users became more of a community, students came to realize that a more profound kind of status comes from being a helpful expert, encouraging younger students to learn rather than standing in their way. This change was entirely the result of discussions among students; I did no lecturing on the subject.

The results of allowing unsupervised students in the room have been better than most people would predict, although not perfect. No equipment has been stolen or damaged in the evenings, but there has been damage to furniture through rough use. A couch was destroyed because its pillows were used too often as swords. Litter is a recurring problem; the room gets so messy that the students themselves complain, but sometimes they don't exert themselves to do anything about it.

What about password hacking? Well, there is some. The first time a student asked me how to turn off echoing to a terminal, I suspected that what he wanted was to write a login simulator, but I encouraged the project as one that provided a strong motivation to learn. I thought that the reaction of other students, when the project became public knowledge, would be enough to control password hackers. I was a little too optimistic; it took a good deal of struggle to make the point. The problem is a recurring one, partly because every year brings a new batch of unsocialized freshmen. But a strong deterrent is the fact that students aspire to "superuser" status, that is, a privileged account given to system administrators. Superuser candidates must be accepted both by the existing superusers, to ensure their technical competence, and by the entire CCUS membership, to ensure that they are trusted by the community. The students who have the skill and interest to be potential password hackers are also the ones who want to keep the trust of their colleagues.

Software maintenance and development is a challenge bearing much more intellectual fruit than password hacking, anyway. Many Lincoln-Sudbury students have written software that is distributed through Usenix and widely used outside the school. The most outstanding example is JOVE, an EMACS-like text editor written by Jonathan Payne while he was a student there.

Although I'm no longer at Lincoln-Sudbury, the facility still exists. It has all the same problems of malicious users that any computer does, but the problems lead to profound moral education when the villains and the victims are all fellow-students, friends, and professional colleagues. Putting the burden of dealing with these problems on the students themselves is a powerful educational force.

References

Goodman, Paul. Growing Up Absurd, New York: Random House, 1960.

Kohlberg, Lawrence. Essays on Moral Development, volume 1: The Philosophy of Moral Development, New York: Harper & Row, 1981.

MacIntyre, Alasdair. After Virtue, Notre Dame, Indiana: University of Notre Dame Press, 1981.

REAL HACKERS DON'T ROB BANKS
by Lee Felsenstein

Hackers! They're everywhere!

Breaking into bank and military computers! Spreading phony credit card numbers! Making free phone calls! And who knows what else?!

In the case of Tom Tcimpidis, the Los Angeles bulletin board operator who was arrested on charges that were later dropped, the magistrate who signed the arrest warrant commented that he had seen the movie "War Games" and therefore knew enough about this sort of thing. What's going on here?

There seems to be a "Hacker scare" in the making, in which sensational journalism can have a heyday, legislators and candidates have something to talk about in public, and which abates with some irrelevant laws passed, causing headaches for completely innocent people.

American history abounds with such scares, going all the way back to the Salem witch trials.

If we have learned anything about this phenomenon (scares, not hackers, that is), it should be that everyone who is potentially affected by a scare must speak up at once, or they will find themselves spoken for by representatives they never wanted.

THE TERMINOLOGY

As George Orwell pointed out in "1984", language is the first target of tyranny.

Those of us who use the term "hacker" properly, and who hope to wear that particular badge of honor, find now that the definition is being warped in such a way as to impart a tinge of criminality to our work.

To be a real hacker means to dedicate a substantial part of your life to the advancement of some application of a technology. It means going behind the backs of stuffed-shirrt administrators who think that despite their inability to do the technical work, they have royal prerogatives to push the technologists this way and that to satisfy obscure, largely symbolic organizational needs.

To be a real hacker means to make a magnificent obsession of creating some effect previously unknown, especially when others say you cannot or may not do it. You will impoverish yourself, devote your whole being to the task, and will go far beyond the limits which reasonable people place on unremunerative effort.

Did I forget to say that the effect which you strive for is not one that pays in monetary terms, only in terms of personal satisfaction? That comes with the territory also.

And now we find that our name is connected in the public mind with malicious teen-age delinquents who serve no good end. We find ourselves forced to apologize for others and explain that we are different.

This is a shame. There is no public consciousness of the fact that the first computers were dreamed up and built by hackers, that hackers were responsible for many of the concepts and utilities currently in everyday use in computer systems, and that hackers were responsible for the microcomputer as it is known today.

Rather than look at this record of accomplishment, the media has looked for the nearest problem, stuck the name to it, and is now engaged in whooping about how it's found something to be scared of. This is the creeping onset of tyrrany . We must not let this assault go unheeded! We must stand up for hackers and hacking or we will face more serious problems later.

THERE ARE HACKERS...

Hackers are essentially the fine artists of technology. Indeed, fine artists working with technologies like paints, film or musical instruments would qualify as hackers:

> "The fascination is with the machine itself. Contact with the tool is its own reward. Most hackers are young men for whom at an early age mastery became highly charged, emotional, colored by a particular desire for perfection, and focused on triumph over things. Their pleasure is in manipulating and mastering their chosen object, in proving themselves with it."
>
> -Sherry Turkle, "The Second Self", Simon & Shuster, 1984

Would not the above description apply to most fine artists? Who would not admit that an artist as great and as eccentric and unappreciated in his time as Van Gogh would be accepted in the company of computer hackers of today?

...AND THERE ARE CRACKERS

There are indeed people who use computers for malicious purposes. Some of these people even operate under color of law. As I write this the San Francisco papers are full of a developing scandal in which the San Francisco Police Department may have gained access to the files of the Public Defender's office and the Citizen's Police Review Office. What is known is that a Police Department administrator ordered a program written to give him access to the contents of all files in a Wang computer system -- which was shared among the various departments! Any real hacker would have spotted that vulnerability right away.

There are so many different forms of computer perfidy that the complete list would be unmanageable. We shall not play a game of comparison here, but we should bear in mind that amateurs do not have a corner on doing bad things with computers.

It is becoming accepted in the hacker community to refer to those whom the press misnames hackers, who use computers to gain unauthorized access to information and resources with malicious or criminal intent, as "crackers". These are the people who will disrupt a computer system (even a BBS operated by and for hackers) for the simple infantile joy of causing upset to others, and by extension, to society.

Crackers are willing to do things which cause loss to others if they can gain in some way. They usually rationalize their acts as causing some loss to a company or other large, anonymous entity, and therefore as not hurting anyone in particular. They may believe that since the company or government is engaged in activity which they see as morally questionable then the rules which society lays down do not apply to them in taking action against the entity, and that any gain which they realize in the process is earned. They do not understand that each individual must be the upholder of moral and ethical standards and cannot seek refuge in the immoral or unethical conduct of others.

The cracker feels himself to be in the tradition of the

American outlaw, hated and feared by the malefactors of great wealth, but honored by the common person as someone who is doing what they had dared only to dream of doing. Strangely enough, this outlook survives the fact than most outlaws don't care whom they hurt. The desire to strike back at unjust authority is strong.

We have always had crackers, petty social parasites, as long as there have been large social parasites who gain their way with manipulation of the legal system. An increasing technological spohistication is to be expected in this area as in all areas of society, especially with regard to "convivial" technologies such as microcomputers.

The cracker is, therefore, simply a more technologically adept outlaw.

THE UNION OF SETS

There is an area of overlap where hackery meets crackery, and too often the temptations of crackery are not opposed by the perceptible advantages of hackery. This is at the point where the claims of the telephone system catch up with the young hacker. When the first phone bill arrives after the modem, then the hacker has a problem.

Unfortunately (for the phone carriers) the solution is readily at hand. The hacker has made contact with many interesting people, and has had the oppportunity to collect many useful suggestions as to how to solve the Problem of the Phone Bill. Fortunately the providers of the phone system have made the misuse of credit card numbers ridiculously easy, and the fascinating corridors of the Telephone Empire are an inviting real-world target for the exploratory impulse which drives hackers. Some would argue that the telephone system is so open as to constitue an "attractive nuisance" in the legal sense of the word.

Necessity therefore impels the budding hacker toward the outlaw culture of crackery, and what is there for an alternative? What other path offers the ease of communication and the camaraderie of outlaws, the thrill of besting a technological behemoth and the plaudits of an unseen community of conspirators?

A FUTURE THAT WORKS

When will we learn to raise our sights above a punishment-based ethic that says; I don't care what you do but I DO care if you do what is forbidden? When are we going to say to youth; we DO care about your doing the right thing, and doing it better than we know how?

And in regards to hacking and cracking, when are we going to realize that with the application of a few obsolete and surplus resources and a little imagination and care we can break the connection between hacking and cracking? It's been done before.

Radio amateurs used to be a real problem before the airwaves were regulated. True, they had been responsible for most of the progress in radio and had given new technologies an invaluable proving ground as well as supplying a steady stream of talent to the industry. But they were inconvenient, playing havoc with the orderly takeover of radio by industry.

When the Federal Communications Commission was created and government regulation of the airwaves "for the public good" was promulgated, certain small slices of the spectrum were reserved for radio amateurs, and rules and procedures were established by which people could qualify to make use of these slices. The bandwidth resource was not large, so the amateurs had to develop ways to make optimal use of it, through nets, protocols, and improved equipment standards.

Unlike hamming with the radio spectrum, hacking deals with two elements, computing resources and communications resources. Neither of these are as scarce as the radio spectrum. Obsolete computers litter the landscape, with service lifetimes at least twice their depreciation schedules. No one knows what unused time is daily wasted on comunications nets, but the carriers do have an idea as to the magnitude of the problem connected with unauthorized credit card calls made by crackers. Right now they devote substantial resources to countering cracking. What lesser portion of these resources would they be willing to allocate to a program which wuld substantially reduce the problem and divert future crackers to more professional pursuits?

I suggest that an organization similar to the Amateur Radio Relay League (A.R.R.L.) be created with a charter to organize these resources and make them available to hackers under a program of mutual education and improvement of skills. There could be grades of hackers ranging from absolute beginners who possess only the most rudimentary skills to wizards who perform the equivalent of defending a thesis in submitting a hack to a committee of peers for critical judgment.

Various levels might have different levels of access to communications resource and computing resource. Since there would never be enough resource, there would be a constant challenge to develop ways to increase the efficiency of useage on a local and a long-distance basis. Co-operation would be essential in this effort and such co-operation would bring its own rewards. Those who try to crack this system would be subject to the most merciless and skilled countermeasures, developed by people just like them who know all the tricks. Peer pressure would work against the crackers who attempt to spoil things within the hacker's net.

The connection between hackery and crackery would be broken. Outlaws we will always have, but the allure of outlawry among young hackers will pale in comparison with the company of fellow hackers engaged in the pursuit of their art individually and collectively. Also, the "real hackers" would be able to turn their talents against the crackers outside of the hacker's net where that is appropriate.

Whenever anyone is spinning out a fantastic new order of things, it is wise to ask; "who would be on top?" I do not suggest that the government be involved in this effort. There is room for pluralism, in which several different hacker's nets operate simultaneously. The Hacker's League (to coin a title) would be simply another nonprofit educational and scientific organization, supported by donations from those who see a common interest in its success. The Homebrew Computer Club has lasted for ten years under this voluntarist concept, while other highly organized clubs have sunk under the weight of their internal political squabbles.

The Homebrew Club had to come to terms with the temptation to have a political structure early in its existence, and decided upon the approach of "governing least" and living in dread of being ignored by its members. Where it provided a communication resource, it was appreciated and supported. It succeeded by not attempting to speak or act for its members. Its Board of Directors is a thoroughly ordinary collection of people who appreciate being left alone.

In the suggested structure of the Hacker's League, there would have to be a few full-time people to perform some of the administrative and technical functions. We hackers know who the most important people are around the big computers and systems which we love so well. We know that the person who holds all the keys, whose goodwill must be cultivated is the person who proudly bears the title which is Latin for "doorkeeper".

The persons who fulfill these function is the hacker's organization would deserve the same title; Janitor.

An organization with titles like that would attract people for whom the main payoff is the ability to exercise their creative faculties co-operatively with the aim of facilitating mutual assistance among people who do not admit to a distinction between working with technology and playing with it. That's the long way of saying ; an organization of hackers, by hackers, and for hackers.