The Catman's Lair

Hacker Resource Files

http://www.pryde-lands.com/catman/

WARNING - Contents of this file are for educational purposes only. It is strongly suggested that you do not use this knowledge for illegal purposes!

Presented at the 13th National Computer Security Conference,
Washington, D.C., Oct. 1-4, 1990.

Concerning Hackers Who Break into Computer Systems

Dorothy E. Denning
Digital Equipment Corp., Systems Research Center
130 Lytton Ave., Palo Alto, CA 94301
415-853-2252, denning@src.dec.com

Abstract

A diffuse group of people often called ``hackers'' has been characterized as unethical, irresponsible, and a serious danger to society for actions related to breaking into computer systems. This paper attempts to construct a picture of hackers, their concerns, and the discourse in which hacking takes place. My initial findings suggest that hackers are learners and explorers who want to help rather than cause damage, and who often have very high standards of behavior. My findings also suggest that the discourse surrounding hacking belongs at the very least to the gray areas between larger conflicts that we are experiencing at every level of society and business in an information age where many are not computer literate. These conflicts are between the idea that information cannot be owned and the idea that it can, and between law enforcement and the First and Fourth Amendments. Hackers have raised serious issues about values and practices in an information society. Based on my findings, I recommend that we work closely with hackers, and suggest several actions that might be taken.

1. Introduction

The world is crisscrossed with many different networks that are used to deliver essential services and basic necessities -- electric power, water, fuel, food, goods, to name a few. These networks are all publicly accessible and hence vulnerable to attacks, and yet virtually no attacks or disruptions actually occur.

The world of computer networking seems to be an anomaly in the firmament of networks. Stories about attacks, breakins, disruptions, theft of information, modification of files, and the like appear frequently in the newspapers. A diffuse group called ``hackers'' is often the target of scorn and blame for these actions. Why are computer networks any different from other vulnerable public networks? Is the difference the result of growing pains in a young field? Or is it the reflection of deeper tensions in our emerging information society?

There are no easy or immediate answers to these questions. Yet it is important to our future in a networked, information-dependent world that we come to grips with them. I am deeply interested in them. This paper is my report of what I have discovered in the early stages of what promises to be a longer investigation. I have

concentrated my attention in these early stages on the hackers themselves. Who are they? What do they say? What motivates them? What are their values? What do that have to say about public policies regarding information and computers? What do they have to say about computer security?

From such a profile I expect to be able to construct a picture of the discourses in which hacking takes place. By a discourse I mean the invisible background of assumptions that transcends individuals and governs our ways of thinking, speaking, and acting. My initial findings lead me to conclude that this discourse belongs at the very least to the gray areas between larger conflicts that we are experiencing at every level of society and business, the conflict between the idea that information cannot be owned and the idea that it can, and the conflict between law enforcement and the First and Fourth Amendments.

But, enough of the philosophy. On with the story!

2. Opening Moves

In late fall of 1989, Frank Drake (not his real name), Editor of the now defunct cyberpunk magazine W.O.R.M., invited me to be interviewed for the magazine. In accepting the invitation, I hoped that something I might say would discourage hackers from breaking into systems. I was also curious about the hacker culture. This seemed like a good opportunity to learn about it.

The interview was conducted electronically. I quickly discovered that I had much more to learn from Drake's questions than to teach. For example, he asked: ``Is providing computer security for large databases that collect information on us a real service? How do you balance the individual's privacy vs. the corporations?'' This question surprised me. Nothing that I had read about hackers ever suggested that they might care about privacy. He also asked: ``What has [the DES] taught us about what the government's (especially NSA's) role in cryptography should be?'' Again, I was surprised to discover a concern for the role of the government in computer security. I did not know at the time that I would later discover considerable overlap in the issues discussed by hackers and those of other computer professionals.

I met with Drake to discuss his questions and views. After our meeting, we continued our dialog electronically with me interviewing him. This gave me the opportunity to explore his views in greater depth. Both interviews appear in ``Computers Under Attack,'' edited by Peter Denning [DenningP90].

My dialog with Drake increased my curiosity about hackers. I read articles and books by or about hackers. In addition, I had discussions with nine hackers whom I will not mention by name. Their ages ranged from 17 to 28.

The word ``hacker'' has taken on many different meanings ranging from 1) ``a person who enjoys learning the details of computer systems and how to stretch their capabilities'' to 2) ``a malicious or

inquisitive meddler who tries to discover information by poking around .. possibly by deceptive or illegal means ...'' [Steele83] The hackers described in this paper satisfy both of these definitions, although all of the hackers I spoke with said they did not engage in or approve of malicious acts that damage systems or files. Thus, this paper is not about malicious hackers. Indeed, my research so far suggests that there are very few malicious hackers. Neither is this paper about career criminals who, for example, defraud businesses, or about people who use stolen credit cards to purchase goods. The characteristics of many of the hackers I am writing about are summed up in the words of one of the hackers: ``A hacker is someone that experiments with systems... [Hacking] is playing with systems and making them do what they were never intended to do. Breaking in and making free calls is just a small part of that. Hacking is also about freedom of speech and free access to information -- being able to find out anything. There is also the David and Goliath side of it, the underdog vs. the system, and the ethic of being a folk hero, albeit a minor one.''

Richard Stallman, founder of the Free Software Foundation who calls himself a hacker according to the first sense of the word above, recommends calling security-breaking hackers ``crackers'' [Stallman84]. While this description may be more accurate, I shall use the term ``hacker'' since the people I am writing about call themselves hackers and all are interested in learning about computer and communication systems. However, there are many people like Stallman who call themselves hackers and do not engage in illegal or deceptive practices; this paper is also not about those hackers.

In what follows I will report on what I have learned about hackers from hackers. I will organize the discussion around the principal domains of concerns I observed. I recommend Meyer's thesis [Meyer89] for a more detailed treatment of the hackers' social culture and networks, and Meyer and Thomas [MeyerThomas90] for an interesting interpretation of the computer underground as a postmodernist rejection of conventional culture that substitutes ``rational technological control of the present for an anarchic and playful future.''

I do not pretend to know all the concerns that hackers have, nor do I claim to have conducted a scientific study. Rather, I hope that my own informal study motivates others to explore the area further. It is essential that we as computer security professionals take into account hackers' concerns in the design of our policies, procedures, laws regulating computer and information access, and educational programs. Although I speak about security-breaking hackers as a group, their competencies, actions, and views are not all the same. Thus, it is equally important that our policies and programs take into account individual differences.

In focusing on what hackers say and do, I do not mean for a moment to set aside the concerns of the owners and users of systems that hackers break into, the concerns of law enforcement personnel, or our own concerns as computer security professionals. But I do recommend that we work closely with hackers as well as these other groups to design new approaches and programs for addressing the concerns of all. Like ham radio operators, hackers exist, and it is in our best interest that we learn to communicate and work with

them rather than against them.

I will suggest some actions that we might consider taking, and I invite others to reflect on these and suggest their own. Many of these suggestions are from the hackers themselves; others came from the recommendations of the ACM Panel on Hacking [Lee86] and from colleagues.

I grouped the hackers' concerns into five categories: access to computers and information for learning; thrill, excitement and challenge; ethics and avoiding damage; public image and treatment; and privacy and first amendment rights. These are discussed in the next five subsections. I have made an effort to present my findings as uncritical observations. The reader should not infer that I either approve or disapprove of actions hackers take.

3. Access to Computers and Information for Learning

Although Levy's book ``Hackers'' [Levy84] is not about today's security-breaking hackers, it articulates and interprets a ``hacker ethic'' that is shared by many of these hackers. The ethic includes two key principles that were formulated in the early days of the AI Lab at MIT: ``Access to computers -- and anything which might teach you something about the way the world works -- should be unlimited and total,'' and ``All information should be free.'' In the context in which these principles were formulated, the computers of interest were research machines and the information was software and systems information.

Since Stallman is a leading advocate of open systems and freedom of information, especially software, I asked him what he means by this. He said: ``I believe that all generally useful information should be free. By `free' I am not referring to price, but rather to the freedom to copy the information and to adapt it to one's own uses.'' By ``generally useful'' he does not include confidential information about individuals or credit card information, for example. He further writes: ``When information is generally useful, redistributing it makes humanity wealthier no matter who is distributing and no matter who is receiving.'' Stallman has argued strongly against user interface copyright, claiming that it does not serve the users or promote the evolutionary process [Stallman90].

I asked hackers whether all systems should be accessible and all information should be free. They said that it is OK if some systems are closed and some information, mainly confidential information about individuals, is not accessible. They make a distinction between information about security technology, e.g., the DES, and confidential information protected by that technology, arguing that it is the former that should be accessible. They said that information hoarding is inefficient and slows down evolution of technology. They also said that more systems should be open so that idle resources are not wasted. One hacker said that the high costs of communication hurts the growth of the information economy.

These views of information sharing seem to go back at least as far as the 17th and 18th Centuries. Samuelson [Samuelson89] notes that

``The drafters of the Constitution, educated in the Enlightenment tradition, shared that era's legacy of faith in the enabling powers of knowledge for society as well as the individual.'' She writes that our current copyright laws, which protect the expression of information, but not the information itself, are based on the belief that unfettered and widespread dissemination of information promotes technological progress. (Similarly for patent laws which protect devices and processes, not the information about them.) She cites two recent court cases where courts reversed the historical trend and treated information as ownable property. She raises questions about whether in entering the Information Age where information is the source of greatest wealth, we have outgrown the Enlightenment tradition and are coming to treat information as property.

In a society where knowledge is said to be power, Drake expressed particular concern about what he sees as a growing information gap between the rich and poor. He would like to see information that is not about individuals be made public, although it could still be owned. He likes to think that companies would actually find it to their advantage to share information. He noted how IBM's disclosure of the PC allowed developers to make more products for the computers, and how Adobe's disclosure of their fonts helped them compete against the Apple-Microsoft deal. He recognizes that in our current political framework, it is difficult to make all information public, because complicated structures have been built on top of an assumption that certain information will be kept secret. He cites our defense policy, which is founded on secrecy for military information, as an example.

Hackers say they want access to information and computing and network resources in order to learn. Both Levy [Levy84] and Landreth [Landreth89] note that hackers have an intense, compelling interest in computers and learning, and many go into computers as a profession. Some hackers break into systems in order to learn more about how the systems work. Landreth says these hackers want to remain undiscovered so that they can stay on the system as long as possible. Some of them devote most of their time to learning how to break the locks and other security mechanisms on systems; their background in systems and programming varies considerably. One hacker wrote ``A hacker sees a security hole and takes advantage of it because it is there, not to destroy information or steal. I think our activities would be analogous to someone discovering methods of acquiring information in a library and becoming excited and perhaps engrossed.''

We should not underestimate the effectiveness of the networks in which hackers learn their craft. They do research, learn about systems, work in groups, write, and teach others. One hacker said that he belongs to a study group with the mission of churning out files of information and learning as much as possible. Within the group, people specialize, collaborate on research project, share information and news, write articles, and teach other about their areas of specialization. Hackers have set up a private system of education that engages them, teaches them to think, and allows them to apply their knowledge in purposeful, if not always legal, activity. Ironically, many of our nation's classrooms have been criticized for providing a poor learning environment that seems to emphasize memorization rather than thinking and reasoning. One hacker

reported that through volunteer work with a local high school, he was trying to get students turned on to learning.

Many hackers say that the legitimate computer access they have through their home and school computers do not meet their needs. One student told me that his high school did not offer anything beyond elementary courses in BASIC and PASCAL, and that he was bored by these. Hans Huebner, a hacker in Germany who goes by the name Pengo, wrote in a note to the RISKS Forum [Huebner89] : ``I was just interested in computers, not in the data which has been kept on their disks. As I was going to school at that time, I didn't even have the money to buy [my] own computer. Since CP/M (which was the most sophisticated OS I could use on machines which I had legal access to) didn't turn me on anymore, I enjoyed the lax security of the systems I had access to by using X.25 networks. You might point out that I should have been patient and wait[ed] until I could go to the university and use their machines. Some of you might understand that waiting was just not the thing I was keen on in those days.''

Brian Harvey, in his position paper [Harvey86] for the ACM Panel on Hacking, claims that the computer medium available to students, e.g., BASIC and floppy disks, is inadequate for challenging intellectual work. His recommendation is that students be given access to real computing power, and that they be taught how to use that power responsibly. He describes a program he created at a public high school in Massachusetts during the period 1979-1982. They installed a PDP-11/70 and let students and teachers carry out the administration of the system. Harvey assessed that putting the burden of dealing with the problems of malicious users on the students themselves was a powerful educational force. He also noted that the students who had the skill and interest to be password hackers were discouraged from this activity because they also wanted to keep the trust of their colleagues in order that they could acquire ``superuser'' status on the system.

Harvey also makes an interesting analogy between teaching computing and teaching karate. In karate instruction, students are introduced to the real, adult community. They are given access to a powerful, deadly weapon, and at the same time are taught discipline and to not abuse the art. Harvey speculates that the reason that students do not misuse their power is that they know they are being trusted with something important, and they want to live up to that trust. Harvey applied this principle when he set up the school system.

The ACM panel endorsed Harvey's recommendation, proposing a three-tiered computing environment with local, district-wide, and nation-wide networks. They recommended that computer professionals participate in this effort as mentors and role models. They also recommended that outside of schools, government and industry be encouraged to establish regional computing centers using donated or re-cycled equipment; that students be apprenticed to local companies either part-time on a continuing basis or on a periodic basis; and, following a suggestion from Felsenstein [Felsenstein86] for a ``Hacker's League,'' that a league analogous to the Amateur Radio Relay League be established to make contributed resources available for educational purposes.

Drake said he liked these recommendations. He said that if hackers were given access to powerful systems through a public account system, they would supervise themselves. He also suggested that Computer Resource Centers be established in low-income areas in order to help the poor get access to information. Perhaps hackers could help run the centers and teach the members of the community how to use the facilities. One of my colleagues suggested cynically that the hackers would only use this to teach the poor how to hack rich people's systems. A hacker responded by saying this was ridiculous; hackers would not teach people how to break into systems, but rather how to use computers effectively and not be afraid of them.
In addition, the hackers I spoke with who had given up illegal activities said they stopped doing so when they got engaged in other work.

Geoff Goodfellow and Richard Stallman have reported that they have given hackers accounts on systems that they manage, and that the hackers have not misused the trust granted to them. Perhaps universities could consider providing accounts to pre-college students on the basis of recommendations from their teachers or parents.
The students might be challenged to work on the same homework problems assigned in courses or to explore their own interests. Students who strongly dislike the inflexibility of classroom learning might excel in an environment that allows them to learn on their own, in much the way that hackers have done.

4. Thrill, Excitement, and Challenge

One hacker wrote that ``Hackers understand something basic about computers, and that is that they can be enjoyed. I know none who hack for money, or hack to frighten the company, or hack for anything but fun.''

In the words of another hacker, ``Hacking was the ultimate cerebral buzz for me. I would come home from another dull day at school, turn my computer on, and become a member of the hacker elite. It was a whole different world where there were no condescending adults and you were judged only by your talent. I would first check in to the private Bulletin Boards where other people who were like me would hang out, see what the news was in the community, and trade some info with people across the country. Then I would start actually hacking. My brain would be going a million miles an hour and I'd basically completely forget about my body as I would jump from one computer to another trying to find a path into my target. It was the rush of working on a puzzle coupled with the high of discovery many magnitudes intensified. To go along with the adrenaline rush was the illicit thrill of doing something illegal. Every step I made could be the one that would bring the authorities crashing down on me. I was on the edge of technology and exploring past it, spelunking into electronic caves where I wasn't supposed to be.''

The other hackers I spoke with made similar statements about the fun and challenge of hacking. In SPIN magazine [Dibbel90], reporter Julian Dibbell speculated that much of the thrill comes from the dangers associated with the activity, writing that ``the technology just lends itself to cloak-and-dagger drama,'' and that ``hackers

were already living in a world in which covert action was nothing more than a game children played.''

Eric Corley [Corley89] characterizes hacking as an evolved form of mountain climbing. In describing an effort to construct a list of active mailboxes on a Voice Messaging System, he writes ``I suppose the main reason I'm wasting my time pushing all these buttons is simply so that I can make a list of something that I'm not supposed to have and be the first person to accomplish this.'' He said that he was not interested in obtaining an account of his own on the system. Gordon Meyer says he found this to be a recurring theme: ``We aren't supposed to be able to do this, but we can'' -- so they do.

One hacker said he was now working on anti-viral programming. He said it was almost as much fun as breaking into systems, and that it was an intellectual battle against the virus author.

5. Ethics and Avoiding Damage

All of the hackers I spoke with said that malicious hacking was morally wrong. They said that most hackers are not intentionally malicious, and that they themselves are concerned about causing accidental damage. When I asked Drake about the responsibility of a person with a PC and modem, his reply included not erasing or modifying anyone else's data, and not causing a legitimate user on a system any problems. Hackers say they are outraged when other hackers cause damage or use resources that would be missed, even if the results are unintentional and due to incompetence. One hacker wrote ``I have ALWAYS strived to do NO damage, and inconvenience as few people as possible. I NEVER, EVER, EVER DELETE A FILE. One of the first commands I do on a new system is disable the delete file command.'' Some hackers say that it is unethical to give passwords and similar security-related information to persons who might do damage. In the recent incident where a hacker broke into Bell South and downloaded a text file on the emergency 911 service, hackers say that there was no intention to use this knowledge to break into or sabotage the 911 system. According to Emmanuel Goldstein [Goldstein90], the file did not even contain information about how to break into the 911 system.

The hackers also said that some break-ins were unethical, e.g., breaking into hospital systems, and that it is wrong to read confidential information about individuals or steal classified information. All said it was wrong to commit fraud for personal profit.

Although we as computer security professionals often disagree with hackers about what constitutes damage, the ethical standards listed sound much like our own. Where the hackers' ethics differs from the standards adopted by most in the computer security community is that hackers say it is not unethical to break into many systems, use idle computer and communications resources, and download system files in order to learn. Goldstein says that hacking is not wrong: it is not the same as stealing, and uncovers design flaws and security deficiencies [Goldstein89].

Brian Reid speculates that a hacker's ethics may come from not being raised properly as a civilized member of society, and not appreciating the rules of living in society. One hacker responded to this with ``What does `being brought up properly' mean? Some would say that it is `good' to keep to yourself, mind your own business. Others might argue that it is healthy to explore, take risks, be curious and discover.'' Brian Harvey [Harvey86] notes that many hackers are adolescents, and that adolescents are at a less developed stage of moral development than adults, where they might not see how the effects of their actions hurt others. Larry Martin [Martin89] claims that parents, teachers, the press, and others in society are not aware of their responsibility to contribute to instilling ethical values associated with computer use. This could be the consequence of the youth of the computing field; many people are still computer illiterate and cultural norms may be lagging behind advances in technology and the growing dependency on that technology by businesses and society. Hollinger and Lanza-Kaduce speculate that the cultural normative messages about the use and abuse of computer technology have been driven by the adaption of criminal laws [HollingerLanza-Kaduce88], which have been mainly in the last decade. They also speculate that hacking may be encouraged during the process of becoming computer literate. Some of my colleagues say that hackers are irresponsible. One hacker responded ``I think it's a strong indication of the amount of responsibility shown that so FEW actually DAMAGING incidents are known.''

But we must not overlook that the differences in ethics also reflect a difference in philosophy about information and information handling resources; whereas hackers advocate sharing, we seem to be advocating ownership as property. The differences also represent an opportunity to examine our own ethical behavior and our practices for information sharing and protection. For example, one hacker wrote ``I will accept that it is morally wrong to copy some proprietary software, however, I think that it is morally wrong to charge $6000 for a program that is only around 25K long.'' Hence, I shall go into a few of the ethical points raised by hackers more closely. It is not a simple case of good or mature (us) against bad or immature (hackers), or of teaching hackers a list of rules.

Many computer professionals argue the moral questions by analogy, e.g., see Martin [Martin89]. The analogies are then used to justify their judgement of a hacker's actions as unethical. Breaking into a system is compared with breaking into a house, and downloading information and using computer and telecommunications services is compared with stealing tangible goods. But, say hackers, the situations are not the same. When someone breaks into a house, the objective is to steal goods, which are often irreplaceable, and property is often damaged in the process. By contrast, when a hacker breaks into a system, the objective is to learn and avoid causing damage. Downloaded information is copied, not stolen, and still exists on the original system. Moreover, as noted earlier, information has not been traditionally regarded as property. Dibbel [Dibbel90] says that when the software industries and phone companies claim losses of billions of dollars to piracy, they are not talking about goods that disappear from the shelves and could have been sold.

We often say that breaking into a system implies a lack of caring

for the system's owner and authorized users. But, one hacker says that the ease of breaking into a system reveals a lack of caring on the part of the system manager to protect user and company assets, or failure on the part of vendors to warn managers about the vulnerabilities of their systems. He estimated his success rate of getting in at 10-15%, and that is without spending more than an hour on any one target system. Another hacker says that he sees messages from vendors notifying the managers, but that the managers fail to take action.

Richard Pethia of CERT (Computer Emergency Response Team) reports that they seldom see cases of malicious damage caused by hackers, but that the break-ins are nevertheless disruptive because system users and administrators want to be sure that nothing was damaged. (CERT suggests that sites reload system software from secure backups and change all user passwords in order to protect against possible back doors and Trojan Horses that might have been planted by the hacker. Pethia also noted that prosecutors are generally called for government sites, and are being called for non-government sites with increasing frequency.) Pethia says that break-ins also generate a loss of trust in the computing environment, and may lead to adoption of new policies that are formulated in a panic or management edicts that severely restrict connectivity to outside systems. Brian Harvey says that hackers cause damage by increasing the amount of paranoia, which in turn leads to tighter security controls that diminish the quality of life for the users. Hackers respond to these points by saying they are the scapegoats for systems that are not adequately protected. They say that the paranoia is generated by ill-founded fears and media distortions (I will return to this point later), and that security need not be oppressive to keep hackers out; it is mainly making sure that passwords and system defaults are well-chosen.

Pethia says that some intruders seem to be disruptive to prove a point, such as that the systems are vulnerable, the security personnel are incompetent, or ``it's not nice to say bad things about hackers.'' In the N.Y. Times, John Markoff [Markoff90] wrote that the hacker who claimed to have broken into Cliff Stoll's system said he was upset by Stoll's portrayal of hackers in ``The Cuckoo's Egg'' [Stoll90]. Markoff reported that the caller said: ``He [Stoll] was going on about how he hates all hackers, and he gave pretty much of a one-sided view of who hackers are.''

``The Cuckoo's Egg'' captures much of the popular stereotypes of hackers. Criminologist Jim Thomas criticizes it for presenting a simplified view of the world, one where everything springs from the forces of light (us) or of darkness (hackers) [Thomas90]. He claims that Stoll fails to see the similarities between his own activities (e.g., monitoring communications, ``borrowing'' monitors without authorization, shutting off network access without warning, and lying to get information he wants) and those of hackers. He points out Stoll's use of pejorative words such as ``varmint'' to describe hackers, and Stoll's quote of a colleague: ``They're technically skilled but ethically bankrupt programmers without any respect for others' work -- or privacy. They're not destroying one or two programs. They're trying to wreck the cooperation that builds our networks.'' [Stoll90, p. 159] Thomas writes ``at an intellectual

level, [Stoll] provides a persuasive, but simplistic, moral imagery of the nature of right and wrong, and provides what -- to a lay reader -- would seem a compelling justification for more statutes and severe penalties against the computer underground. This is troublesome for two reasons. First, it leads to a mentality of social control by law enforcement during a social phase when some would argue we are already over-controlled. Second, it invokes a punishment model that assumes we can stamp out behaviors to which we object if only we apprehend and convict a sufficient number of violators. ... There is little evidence that punishment will in the long run reduce any given offense, and the research of Gordon Meyer and I suggests that criminalization may, in fact, contribute to the growth of the computer underground.''

6. Public Image and Treatment

Hackers express concern about their negative public image and identity. As noted earlier, hackers are often portrayed as being irresponsible and immoral. One hacker said that ``government propaganda is spreading an image of our being at best, sub-human, depraved, criminally inclined, morally corrupt, low life. We need to prove that the activities that we are accused of (crashing systems, interfering with life support equipment, robbing banks, and jamming 911 lines) are as morally abhorent to us as they are to the general public.''

The public identity of an individual or group is generated in part by the actions of the group interacting with the standards of the community observing those actions. What then accounts for the difference between the hacker's public image and what they say about themselves? One explanation may be the different standards. Outside the hacking community, the simple act of breaking into systems is regarded as unethical by many. The use of pejorative words like ``vandal'' and ``varmint'' reflect this discrepency in ethics. Even the word ``criminal'' carries with it connotations of someone evil; hackers say they are not criminal in this sense. Katie Hafner notes that Robert Morris, who was convicted of launching the Internet worm, was likened to a terrorist even though the worm did not destroy data [Hafner90].

Distortions of events and references to potential threats also create an image of persons who are dangerous. Regarding the 911 incident where a hacker downloaded a file from Bell South, Goldstein reported ``Quickly, headlines screamed that hackers had broken into the 911 system and were interfering with emergency telephone calls to the police. One newspaper report said there were no indications that anyone had died or been injured as a result of the intrusions. What a relief. Too bad it wasn't true.'' [Goldstein90] In fact, the hackers involved with the 911 text file had not broken into the 911 system. The dollar losses attributed to hacking incidents also are often highly inflated.

Thomas and Meyer [ThomasMeyer90] say that the rhetoric depicting hackers as a dangerous evil contributes to a ``witch hunt'' mentality, wherein a group is first labeled as dangerous, and then enforcement agents are mobilized to exorcise the alleged social evil. They see

the current sweeps against hackers as part of a reaction to a broader fear of change, rather than to the actual crimes committed.

Hackers say they are particularly concerned that computer security professionals and system managers do not appear to understand hackers or be interested in their concerns. Hackers say that system managers treat them like enemies and criminals, rather than as potential helpers in their task of making their systems secure. This may reflect managers' fears about hackers, as well as their responsibilities to protect the information on their systems. Stallman says that the strangers he encounters using his account are more likely to have a chip on their shoulder than in the past; he attributes this to a harsh enforcer mentality adopted by the establishment. He says that network system managers start out with too little trust and a hostile attitude toward strangers that few of the strangers deserve. One hacker said that system managers show a lack of openness to those who want to learn.

Stallman also says that the laws make the hacker scared to communicate with anyone even slightly ``official,'' because that person might try to track the hacker down and have him or her arrested. Drake raised the issue of whether the laws could differentiate between malicious and nonmalicious hacking, in support of a ``kinder, gentler'' relationship between hackers and computer security people. In fact, many states such as California initially passed computer crime laws that excluded malicious hacking; it was only later that these laws were amended to include nonmalicious actions [HollingerLanza-Kaduce88]. Hollinger and Lanza-Kaduce speculate that these amendments and other new laws were catalyzed mainly by media events, especially the reports on the ``414 hackers'' and the movie ``War Games,'' which created a perception of hacking as extremely dangerous, even if that perception was not based on facts.

Hackers say they want to help system managers make their systems more secure. They would like managers to recognize and use their knowledge about design flaws and the outsider threat problem. Landreth [Landreth89] suggests ways in which system managers can approach hackers in order to turn them into colleagues, and Goodfellow also suggests befriending hackers [Goodfellow83]. John Draper (Cap'n Crunch) says it would help if system managers and the operators of phone companies and switches could coopererate in tracing a hacker without bringing in law enforcement authorities.

Drake suggests giving hackers free access in exchange for helping with security, a suggestion that I also heard from several hackers. Drake says that the current attitude of treating hackers as enemies is not very conducive to a solution, and by belittling them, we only cause ourselves problems.

I asked some of the hackers whether they'd be interested in breaking into systems if the rules of the ``game'' were changed so that instead of being threatened by prosecution, they were invited to leave a ``calling card'' giving their name, phone number, and method of breaking in. In exchange, they would get recognition and points for each vulnerability they discovered. Most were interested in playing; one hacker said he would prefer monetary reward since he was supporting himself. Any system manager interested in trying

this out could post a welcome message inviting hackers to leave their cards. This approach could have the advantage of not only letting the hackers contribute to the security of the system, but of allowing the managers to quickly recognize the potentially malicious hackers, since they are unlikely to leave their cards. Perhaps if hackers are given the opportunity to make contributions outside the underground, this will dampen their desire to pursue illegal activities.

Several hackers said that they would like to be able to pursue their activities legally and for income. They like breaking into systems, doing research on computer security, and figuring out how to protect against vulnerabilities. They say they would like to be in a position where they have permission to hack systems. Goodfellow suggests hiring hackers to work on tiger teams that are commissioned to locate vulnerabilities in systems through penetration testing. Baird Info-Systems Safeguards, Inc., a security consulting firm, reports that they have employed hackers on several assignments [Baird87]. They say the hackers did not violate their trust or the trust of their clients, and performed in an outstanding manner. Baird believes that system vulnerabilities can be better identified by employing people who have exploited systems.

One hacker suggested setting up a clearinghouse that would match hackers with companies that could use their expertise, while maintaining anonymity of the hackers and ensuring confidentiality of all records. Another hacker, in describing an incident where he discovered a privileged account without a password, said ``What I (and others) wish for is a way that hackers can give information like this to a responsible source, AND HAVE HACKERS GIVEN CREDIT FOR HELPING! As it is, if someone told them that `I'm a hacker, and I REALLY think you should know...' they would freak out, and run screaming to the SS [Secret Service] or the FBI. Eventually, the person who found it would be caught, and hauled away on some crazy charge. If they could only just ACCEPT that the hacker was trying to help!'' The clearinghouse could also provide this type of service.

Hackers are also interested in security policy issues. Drake expressed concern over how we handle information about computer security vulnerabilities. He argues that it is better to make this information public than cover it up and pretend that it does not exist, and cites the CERT to illustrate how this approach can be workable. Other hackers, however, argue for restricting initial dissemination of flaws to customers and users. Drake also expressed concern about the role of the government, particularly the military, in cryptography. He argues that NSA's opinion on a cryptographic standard should be taken with a large grain of salt because of their code breaking role.

Some security specialists are opposed to hiring hackers for security work, and Eugene Spafford has urged people not to do business with any company that hires a convicted hacker to work in the security area [ACM90]. He says that ``This is like having a known arsonist install a fire alarm.'' But, the laws are such that a person can be convicted for having done nothing other than break into a system; no serious damage (i.e., no ``computer arson'') is necessary. Many of our colleagues admit to having broken into systems in the past, e.g., Geoff Goodfellow [Goodfellow83] and Brian Reid [Frenkel87];

Reid is quoted as saying that because of the knowledge he gained breaking into systems as a kid, he was frequently called in to help catch people who break in. Spafford says that times have changed, and that this method of entering the field is no longer socially acceptable, and fails to provide adequate training in computer science and computer engineering [Spafford89]. However, from what I have observed, many hackers do have considerable knowledge about telecommunications, data security, operating systems, programming languages, networks, and cryptography. But, I am not challenging a policy to hire competent people of sound character. Rather, I am challenging a strict policy that uses economic pressure to close a field of activity to all persons convicted of breaking into systems. It is enough that a company is responsible for the behavior of its employees. Each hacker can be considered for employment based on his or her own competency and character.

Some people have called for stricter penalties for hackers, including prison terms, in order to send a strong deterrent message to hackers. John Draper, who was incarcerated for his activities in the 1970's, argues that in practice this will only make the problem worse. He told me that he was forced under threat to teach other inmates his knowledge of communications systems. He believes that prison sentences will serve only to spread hacker's knowledge to career criminals. He said he was never approached by criminals outside the prison, but that inside the prison they had control over him.

One hacker said that by clamping down on the hobbyist underground, we will only be left with the criminal underground. He said that without hackers to uncover system vulnerabilities, the holes will be left undiscovered, to be utilized by those likely to cause real damage.

Goldstein argues that the existing penalties are already way out of proportion to the acts committed, and that the reason is because of computers [Goldstein89]. He says that if Kevin Mitnick had committed crimes similar to those he committed but without a computer, he would have been classified as a mischief maker and maybe fined $100 for trespassing; instead, he was put in jail without bail [Goldstein89]. Craig Neidorf, a publisher and editor of the electronic newsletter ``Phrack,'' faces up to 31 years and a fine of $122,000 for receiving, editing, and transmitting the downloaded text file on the 911 system [Goldstein90].

7. Privacy and the First and Fourth Amendments

The hackers I spoke with advocated privacy protection for sensitive information about individuals. They said they are not interested in invading people's privacy, and that they limited their hacking activities to acquiring information about computer systems or how to break into them. There are, of course, hackers who break into systems such as the TRW credit database. Emanuel Goldstein argues that such invasions of privacy took place before the hacker arrived [Harpers90]. Referring to credit reports, government files, motor vehicle records, and the ``megabytes of data piling up about each of us,'' he says that thousands of people legally can see and use this data, much of it erroneous. He claims that the public has been

misinformed about the databases, and that hackers have become scapegoats for the holes in the systems. One hacker questioned the practice of storing sensitive personal information on open systems with dial-up access, the accrual of the information, the methods used to acquire it, and the purposes to which it is put. Another hacker questioned the inclusion of religion and race in credit records.

Drake told me that he was concerned about the increasing amount of information about individuals that is stored in large data banks, and the inability of the individual to have much control over the use of that information. He suggests that the individual might be co-owner of information collected about him or her, with control over the use of that information. He also says that an individual should be free to withhold personal information, of course paying the consequences of doing so (e.g., not getting a drivers license or credit card). (In fact, all Federal Government forms are required to contain a Privacy Act Statement that states how the information being collected will be used and, in some cases, giving the option of withholding the information.)

Goldstein has also challenged the practices of law enforcement agencies in their attempt to crack down on hackers [Goldstein90]. He said that all incoming and outgoing electronic mail used by ``Phrack'' was monitored before the newsletter was shutdown by authorities. ``Had a printed magazine been shut down in this fashion after having all of their mail opened and read, even the most thick-headed sensationalist media types would have caught on: hey, isn't that a violation of the First Amendment?'' He also cites the shutdown of several bulletin boards as part of Operation Sun Devil, and quotes the administrator of the bulletin board Zygot as saying ``Should I start reading my users' mail to make sure they aren't saying anything naughty? Should I snoop through all the files to make sure everyone is being good? This whole affair is rather chilling.'' The administrator for the public system The Point wrote ``Today, there is no law or precedent which affords me ... the same legal rights that other common carriers have against prosecution should some other party (you) use my property (The Point) for illegal activities. That worries me ...''

About 40 personal computer systems and 23,000 data disks were seized under Operation Sun Devil, a two-year investigation involving the FBI, Secret Service, and other federal and local law enforcement officials. In addition, the Secret Service acknowledges that its agents, acting as legitimate users, had secretly monitored computer bulletin boards [Markoff90a]. Markoff reports that California Representative Don Edwards, industry leader Mitchell Kapor, and civil liberties advocates are alarmed by these government actions, saying that they challenge freedom of speech under the First Amendment and protection against searches and seizures under the Fourth Amendment. Markoff asks: ``Will fear of hackers bring oppression?''

John Barlow writes ``The Secret Service may actually have done a service for those of us who love liberty. They have provided us with a devil. And devils, among their other galvanizing virtues, are just great for clarifying the issues and putting iron in your spine.'' [Barlow90] Some of the questions that Barlow says need to be addressed include ``What are data and what is free speech?

How does one treat property which has no physical form and can be infinitely reproduced? Is a computer the same as a printing press?'' Barlow urges those of us who understand the technology to address these questions, lest the answers be given to us by law makers and law enforcers who do not. Barlow and Kapor are constituting the Computer Liberty Foundation to ``raise and disburse funds for education, lobbying, and litigation in the areas relating to digital speech and the extension of the Constitution into Cyberspace.''

8. Conclusions

Hackers say that it is our social responsibility to share information, and that it is information hoarding and disinformation that are the crimes. This ethic of resource and information sharing contrasts sharply with computer security policies that are based on authorization and ``need to know.'' This discrepancy raises an interesting question: Does the hacker ethic reflects a growing force in society that stands for greater sharing of resources and information -- a reaffirmation of basic values in our constitution and laws? It is important that we examine the differences between the standards of hackers, systems managers, users, and the public. These differences may represent breakdowns in current practices, and may present new opportunities to design better policies and mechanisms for making computer resources and information more widely available.

The sentiment for greater information sharing is not restricted to hackers. In the best seller ``Thriving on Chaos,'' Tom Peters [Peters87] writes about sharing within organizations: ``Information hoarding, especially by politically motivated, power-seeking staffs, has been commonplace throughout American industry, service and manufacturing alike. It will be an impossible millstone around the neck of tomorrow's organizations. Sharing is a must.'' Peters argues that information flow and sharing is fundamental to innovation and competetiveness. On a broader scale, Peter Drucker [Drucker89] says that the ``control of information by government is no longer possible. Indeed, information is now transnational. Like money, it has no `fatherland.' ''

Nor is the sentiment restricted to people outside the computer security field. Harry DeMaio [DeMaio89] says that our natural urge is to share information, and that we are suspicious of organizations and individuals who are secretive. He says that information is exchanged out of ``want to know'' and mutual accommodation rather than ``need to know.'' If this is so, then some of our security policies are out of step with the way people work. Peter Denning [DenningP89] says that information sharing will be widespread in the emerging worldwide networks of computers and that we need to focus on ``immune systems'' that protect against mistakes in our designs and recover from damage.

I began my investigation of hackers with the question: who are they and what is their culture and discourse? My investigation uncovered some of their concerns, which provided the organizational structure to this paper, and several suggestions for new actions that might be taken. My investigation also opened up a broader question: What are the clashing discourses that the hackers stand at the battle lines of? Is it owning or restricting information vs. sharing

information -- a tension between an age-old tradition of controlling information as property and the Englightenment tradition of sharing and disseminating information? Is it controlling access based on ``need to know,'' as determined by the information provider, vs. ``want to know,'' as determined by the person desiring access? Is it law enforcement vs. freedoms granted under the First and Fourth Amendments? The answers to these questions, as well as those raised by Barlow on the nature of information and free speech, are important because they tell us whether our policies and practices serve us as well as they might. The issue is not simply hackers vs. system managers or law enforcers; it is a much larger question about values and practices in an information society.

Acknowledgments

I am deeply grateful to Peter Denning, Frank Drake, Nathan Estey, Katie Hafner, Brian Harvey, Steve Lipner, Teresa Lunt, Larry Martin, Gordon Meyer, Donn Parker, Morgan Schweers, Richard Stallman, and Alex for their comments on earlier versions of this paper and helpful discussions; to Richard Stallman for putting me in contact with hackers; John Draper, Geoff Goodfellow, Brian Reid, Eugene Spafford, and the hackers for helpful discussions; and Richard Pethia for a summary of some of his experiences at CERT. The opinions expressed here, however, are my own and do not necessarily represent those of the people mentioned above or of Digital Equipment Corporation.

References

ACM90
``Just say no,'' Comm. ACM, Vol. 33, No. 5, May 1990, p. 477.

Baird87
Bruce J. Baird, Lindsay L. Baird, Jr., and Ronald P. Ranauro, ``The Moral Cracker?,'' Computers and Security, Vol. 6, No. 6, Dec. 1987, p. 471-478.

Barlow90
John Barlow, ``Crime and Puzzlement,'' June 1990, to appear in Whole Earth Review.

Corley89
Eric Corley, ``The Hacking Fever,'' in Pamela Kane, V.I.R.U.S. Protection, Bantam Books, New York, 1989, p. 67-72.

DeMaio89
Harry B. DeMaio, ``Information Ethics, a Practical Approach,'' Proc. of the 12th National Computer Security Conference, 1989, p. 630-633.

DenningP89
Peter J. Denning, ``Worldnet,'' American Scientist, Vol. 77, No. 5, Sept.-Oct., 1989.

DenningP90
Peter J. Denning, Computers Under Attack, ACM Press, 1990.

Dibbel90
  Julian Dibbel, ``Cyber Thrash,'' SPIN, Vol. 5, No. 12, March 1990.

Drucker89
  Peter F. Drucker, The New Realities, Harper and Row, New York, 1989.

Felsenstein86
  Lee Felsenstein, ``Real Hackers Don't Rob Banks,'' in full report on
  ACM Panel on Hacking [Lee86].

Frenkel87
  Karen A. Frenkel, ``Brian Reid, A Graphics Tale of a Hacker
  Tracker,'' Comm. ACM, Vol. 30, No. 10, Oct. 1987, p. 820-823.

Goldstein89
  Emmanuel Goldstein, ``Hackers in Jail,'' 2600 Magazine, Vol. 6, No. 1,
  Spring 1989.

Goldstein90
  Emmanuel Goldstein, ``For Your Protection,'' 2600 Magazine, Vol. 7,
  No. 1, Spring 1990.

Goodfellow83
  Geoffrey S. Goodfellow, ``Testimony Before the Subcommittee on
  Transportation, Aviation, and Materials on the Subject of
  Telecommunications Security and Privacy,'' Sept. 26, 1983.

Hafner90
  Katie Hafner, ``Morris Code,'' The New Republic, Feb. 16, 1990,
  p. 15-16.

Harpers90
  ``Is Computer Hacking a Crime?" Harper's, March 1990, p. 45-57.

Harvey86
  Brian Harvey, ``Computer Hacking and Ethics,'' in full report on
  ACM Panel on Hacking [Lee86].

HollingerLanza-Kaduce88
  Richard C. Hollinger and Lonn Lanza-Kaduce, ``The Process of
  Criminalization: The Case of Computer Crime Laws,'' Criminology,
  Vol. 26, No. 1, 1988, p. 101-126.

Huebner89
  Hans Huebner, ``Re: News from the KGB/Wiley Hackers,'' RISKS Digest,
  Vol. 8, Issue 37, 1989.

Landreth89
  Bill Landreth, Out of the Inner Circle, Tempus, Redmond, WA, 1989.

Lee86
  John A. N. Lee, Gerald Segal, and Rosalie Stier, ``Positive
  Alternatives: A Report on an ACM Panel on Hacking,'' Comm. ACM,
  Vol. 29, No. 4, April 1986, p. 297-299; full report available from
  ACM Headquarters, New York.

Levy84
Steven Levy, Hackers, Dell, New York, 1984.

Markoff90
John Markoff, ``Self-Proclaimed `Hacker' Sends Message to Critics,''
The New York Times, March 19, 1990.

Markoff90a
John Markoff, ``Drive to Counter Computer Crime Aims at Invaders,''
The New York Times, June 3, 1990.

Martin89
Larry Martin, ``Unethical `Computer' Behavior: Who is Responsible?,''
Proc. of the 12th National Computer Security Conference, 1989.

Meyer89
Gordon R. Meyer, The Social Organization of the Computer Underground,
Master's thesis, Dept. of Sociology, Northern Illinois Univ., Aug.
1989.

MeyerThomas90
Gordon Meyer and Jim Thomas, ``The Baudy World of the Byte Bandit:
A Postmodernist Interpretation of the Computer Underground,'' Dept.
of Sociology, Northern Illinois Univ., DeKalb, IL, March 1990.

Peters87
Tom Peters, Thriving on Chaos, Harper & Row, New York, Chapter VI, S-3,
p. 610, 1987.

Samuelson89
Pamela Samuelson, ``Information as Property: Do Ruckelshaus and
Carpenter Signal a Changing Direction in Intellectual Property Law?"
Catholic University Law Review, Vol. 38, No. 2, Winter 1989, p.
365-400.

Spafford89
Eugene H. Spafford, ``The Internet Worm, Crisis and Aftermath,''
Comm. ACM, Vol. 32, No. 6, June 1989, p. 678-687.

Stallman84
Richard M. Stallman, Letter to ACM Forum, Comm. ACM, Vol. 27,
No. 1, Jan. 1984, p. 8-9.

Stallman90
Richard M. Stallman, ``Against User Interface Copyright'' to appear
in Comm. ACM.

Steele83
Guy L. Steele, Jr., Donald R. Woods, Raphael A. Finkel, Mark R.
Crispin, Richard M. Stallman, and Geoffrey S. Goodfellow, The
Hacker's Dictionary, Harper & Row, New York, 1983.

Stoll90
Clifford Stoll, The Cuckoo's Egg, Doubleday, 1990.

Thomas90
Jim Thomas, ``Review of The Cuckoo's Egg,'' Computer Underground

Digest, Issue #1.06, April 27, 1990.

ThomasMeyer90
Jim Thomas and Gordon Meyer, ``Joe McCarthy in a Leisure Suit: (Witch)Hunting for the Computer Underground,'' Unpublished manuscript, Department of Sociology, Northern Illinois University, DeKalb, IL, 1990; see also the Computer Underground Digest, Vol. 1, Issue 11, June 16, 1990.