THE HACKER ETHIC

Sarah Granger
University of Michigan ACM Chair
3411 EECS Bldg
1301 Beal
Ann Arbor, MI 48109
(313)741-5240
sgranger@engin.umich.edu

BACKGROUND

The 'hacker ethic' can be a peculiar concept to those unfamiliar with hacking and what really is. In fact, the entire definition of 'hacking' is somewhat obscure. Hacking originated as a challenge between programmers. Programmers at MIT are known for coining the term. Individuals would 'hack at code' meaning that they would work at programming problems until they could manipulate their computers into doing exactly what they wanted. The MIT hackers began with simple programs and moved on to fiddling with UNIX machines, especially those on the Arpanet. Hackers started freely distributing their code to their friends and eventually to their friends across the network. This gave rise to a notion that software should be free. Eventually this was taken to the extreme information and network access should also be free.

Several definitions for 'hacker' exist. *The New Hacker's Dictionary* states the following definitions:

'1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities,...2. One who programs enthusiastically,...4. An expert at a particular program...as in 'a UNIX hacker'...7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations. 8...A malicious meddler who tries to discover sensitive information by poking around. Hence *password hacker, network hacker.*" (218) The hacker most often referred to in general is the hacker in definition no. 8, whereas most programmers refer to hackers by definition no. 1. Many of those who consider themselves hackers or are considered by others to be hackers fit into more than one of the definitions above. The 'hacker ethic' stems from these ideas.

The 'hacker ethic' is a belief that essentially all information should be open and available to anyone. Information to a hacker includes program code and programs themselves. Information also includes files of any sort that are available anywhere on computer networks. Sometimes hackers go as far as believing that other users' computer accounts, passwords, and e-mail should be open to their inquiries. This is when hacking becomes 'system cracking.' The plain fact of the matter is that hacking is a very difficult ethical issue and causes several problems regarding creation and enforcement of policies and laws.

Ethics in the Computer Age, Gatlinburg, TN, USA

SYSTEM SECURITY

It is the responsibility of the keeper of a computer system or network to insure system security. The person(s) usually in charge of such a task is the System Administrator (SysAdmin) or the System Operator (SysOp). SysAdmins on most systems keep them free of software bugs, security holes, backdoors, worms, viruses, Trojan horses, and all other kinds of dangerous entities that end up on public systems and sites. System security has several levels. Security exists on the user level such as password protection and file permissions. On the administrator level are several tools such as logs which record every move a user makes, even including keystrokes on occasion. These tricks allow the SysAdmin or SysOp to monitor all activity on the system thereby detecting any unusual occurrences.

The argument which a hacker who breaks into a system often uses is as follows: "If I can do it, and you have not taken the precautions to keep me out, then I cannot be held accountable for, nor punished for acts that have occurred because of your, or administrative/ government omission or lack of safeguard." (Rezmierski, 2) Certainly a blatant lack of security is not only stupid but also infringement upon the expectations of the users of the system. Users expect a certain amount of security on their system and if they don't have it, they cannot trust the system and therefore will cease to use that system. If a system is at all commercial, which most are today, that can cause financial problems as well as security problems.

The argument the hacker or intruder makes is a viable argument. If a hacker finds a hole and exploits that hole on systems. A certain level of trust must be maintained. This is where the hacker ethic becomes fuzzy. Hackers should be held legally accountable for their infringements upon system security. In some cases

where crackers are specifically sent in to find holes as in Tiger Teams, the act of finding the hole is necessary in order to figure out how to patch it. This action is known and condoned by the SysAdmin. However, when an individual or group goes against policy to invade a system where it is known that such break-ins are not only unethical and unwise but illegal, that individual should be punishable by law.

POLICY

Policy regarding system security is slim and has historically been lenient. In 1986 the *Computer Fraud and Abuse Act* was passed to help alleviate this problem. This applies to hackers because they almost always use pseudonyms to hide their identities while searching through foreign systems. To catch those who made infractions under this act, the Chicago Computer Fraud and Abuse Task Force began in 1987. This task force, along with the Secret Service and the 1990 Project Sundevil, brought hacking into the news as a serious offense. Several hackers were apprehended and a few have and/or are serving prison terms.

On the Internet the law is somewhat confusing. It is difficult to determine where a break-in occurs,, what damage is done, the cost of the damage, and precisely who did the damage. In *The Cuckoo's Egg*, by Cliff Stoll, Stoll tells a story of a group of hackers who intrudes upon his system. He ends up going through every security agency in the country and a few outside the country in order to finally catch the hackers in the act and discover their origin. The task of apprehending hackers is a very difficult and time-consuming one. Usually it requires permits, warrants, and wiretaps. The government does not easily agree to do these things and even when it does, it is no assuring factor that the intruder(s) will be unveiled.

Once the hacker is found, usually he or she is prosecuted by the system that was intruded upon. In many cases this is several systems. Most cases are specifically focused on certain areas of networks at government research centers and universities. At the University of Michigan, policy clearly states that any account used incorrectly or anyone who uses someone else's computer account will be prosecuted accordingly. The UofM policy states the following: "Any member of the University community who, without authorization, accesses, uses, destroys, alters, dismantles or disfigures the University information technologies, properties or facilities...has engaged in unethical and unacceptable conduct."(UofM, 1) Later it states that the University will take disciplinary action up to and including non-reappointment, discharge, dismissal, and/or legal action" (UofM, 2) for violation of the policy. This is a newer, more strict policy that has worked so far in that those who are found intruding upon any of the university computer systems have been expelled and/or legally prosecuted in court.

CONCERNS AND CONCLUSION

The hacker community used to only consist of a small, elite group. This has been changing as computers are becoming more accessible to all areas of society. These people defend each other in their belief that systems are free to any outside access. However, they hide under pseudonyms knowing full well the legal implications of their actions. Originally the hacker was known as the white middle-class teenage boy whose parents neglected him and either knew nothing of computers themselves or worked in the field and had initially sparked the boy's interest. For example, Robert Tappan Morris, a college student at Cornell University who unleashed the famous internet worm, is the son of Robert Morris, an NSA programmer. RTM admitted that his father's influence had affected his decision to become directed toward the same types of endeavors.

Although hackers do not consider their actions unethical, the general user population on a system does, as do the System Administrators and owners of the system. This causes problems when the two sides try to communicate in a legal setting. The accused believes he did no wrongdoing whereas the law states otherwise. Bruce Sterling in The Hacker Crackdown suggests, "any teenager enthralled by computers, fascinated by the ins and outs of computer security and attracted by the lure of specialized forms of knowledge and power, would do well to forget all about hacking and set his (or her) sights on becoming a fed."(Sterling, 217) This may be good advice for a potential hacker to take as policy thickens and punishment becomes more stringent.

References:

Rezmierski, Virginia, "Information Regarding Assignments" handout, The University of Michigan, 1994.

Russell, Deborah and Gangemi Sr., G.T. Computer Security Basics, Sebastopol, CA: O'Reilly and Associates, Inc., 1991.

Sterling, Bruce, The Hacker Crackdown, New York: Bantam Books, 1992.

Stoll, Cliff, The Cuckoo's Egg, New York: Pocket Books, 1989.

The New Hacker's Dictionary, Second Ed., compiled by Eric S. Raymond, Cambridge, Massachussetts: The MIT Press, 1993.

The University of Michigan, "Policy: Proper Use of

Information Resources, Information Technology, and
Networks at The University of Michigan," May 1990.