A New Hacker Taxonomy

(Marc Rogers, Graduate Studies, Dept. of Psychology,
University of Manitoba)

The lack of an agreed upon definition of what the term hacker means has been and will be a hurdle for researchers attempting to study individuals involved in hacking activities (Chantler, 1996; Parker, 1998; Rogers 1999). As a result of the broad, misused, and often over use of the term hacker, the term has become generic and refers to a rather diverse community (i.e., crackers, coders, script kiddies, programmers, criminals, etc.) (Chantler, 1996; Parker, 1998; Post, 1996; Rogers, 1999). The term hacker describes the activity involved in, but does not accurately reflect any of the differences in those individuals engaged in the activity (Post, 1996). Hackers are not a homogeneous group (Chantler, 1996; Denning, 1998; Post, 1996; Sterling 1992).

The psychological and criminological studies to date have been hampered by other factors as well. Many studies relied on the subject’s own classification as a hacker with no corroborating evidence (i.e., arrest record). Other studies were conducted via the Internet, which can cause negatively impact on the validity of the study. These studies had no way of measuring or controlling for a person answering the surveys several times (Rogers, 1999). Most studies used subjects from only a subset of the larger hacker community. Often subjects have been college students engaged in software piracy (Sacco & Zureik, 1990). These subjects are hardly representative of the entire hacker community and the findings cannot be generalized to the larger heterogeneous hacker community (Rogers, 1999; Skinner & Fream, 1997).

Hacker Categories

In order to arrive at some type of understanding about the motivation of individuals engaged in hacking the generic hacker term needs to be broken down into more useful and empirically valid categories (Chantler, 1996).

Fortunately there have been some studies that have attempted to granulize or operationally define the term hacker into more useful subcategories (Chantler, 1996; Landreth, 1985; Parker, 1998; Post, 1996;). Many of the studies used data from the popular media, self report surveys, or personal observations.

One of the first attempts to more clearly define the hacker community was Landreth (1985). Landreth proposed a classification system based on the activities the hacker was involved in. He developed six categories; novice, student, tourist, crasher, thief.

The novice was considered the least experienced, and their activities were viewed as petty mischief making (Landreth, 1985). The student was just that, a student. Rather than work on homework they occupied their time exploring others’ systems. They were bright and usually found school boring and unchallenging (Landreth). The tourist hacked out of sense of adventure. The reward of hacking was the thrill of having been there (Landreth). The tourists appeared to have a need to test themselves. The crasher was a destructive hacker who intentionally damaged information and systems (Landreth). Landreth indicated that they were the most unpleasant of his classification system. The thief was believed to be the rarest of hackers (Landreth). Thieves profited from their activities, and were the most professional of all the categories.

Another criminologist, Hollinger (1988) studied computer criminal activity within a university population. The study concluded that hackers followed a guttman-like progression from less skilled activities to more technically elite crimes. Hollinger indicated that the individuals fit into three categories: pirates, browsers, and crackers. The pirates were the least technically proficient and confined their activities to copyright violations (pirating software). The browsers had moderate technical ability and gained unauthorized access to other people’s files. They did not usually damage or copy the files (Hollinger). The crackers had the most technical ability and were the most serious abusers (Hollinger). Their activities ranged from copying files to damaging programs and systems.

Chantler (1996) attempted a larger scale ethnographic study of the hacker underground. Chantler indicated that there were several attributes that could be used to categorize hackers. The attributes were the hacker’s activities, their prowess at hacking, their knowledge, motivation, and how long they had been hacking. Chantler used these attributes to arrive at three categories; elite group, neophytes, and losers and lamers.

The elite group displayed a high level of knowledge and were motivated by a desire to achieve, self-discovery, and for the excitement and challenge (Chantler, 1996). The neophytes displayed a sound level of knowledge, but most were still learning. They were followers and usually went where the elite group had been (Chantler). The losers and lamers, displayed little evidence of intellectual ability. They were motivated by a desire for profit, vengeance, theft, espionage etc. (Chantler).

Chantler (1996) concluded that only 30% of the hackers community fell into the elite group, 60% where neophytes, and 10% were losers and lamers.

More recent studies such as Power (1998) subdivided hackers into, sport intruders, competitive intelligence, and foreign intelligence. Sport intruders were the stereotypical Internet hackers. These people break into systems, deface web pages, and commit other acts of computer vandalism (Power). Competitive intelligence professionals maintain an ethical approach, avoid illegal activities, and fall into the realm of competitive espionage (Power). The last group, foreign intelligence, maintains the goal of advancing a nation's security or economic interests often at the expense of another country (Power).

Parker (1998) indicated that there were seven significant profiles of cybercriminals; pranksters, hacksters, malicious hackers, personal problem solvers, career criminals, extreme advocates, and malcontents, addicts, and irrational and incompetent people.

Pranksters were defined as individuals that perpetrate tricks on others. Their intent was not to inflict any long lasting harm (Parker, 1998). Hacksters were defined in terms similar to Levy’s (1985) first generation hackers. They usually explored others’ computer systems for education, curiosity, competition, or out of some form of social justice (Parker).

Malicious hackers were defined in terms similar to “crackers”. These individuals intended to cause harm and or loss (Parker, 1998). An example of a malicious hacker would be the creators of computer viruses (Parker). Personal problem solvers turned to crime after more traditional problem solving methods failed. They saw crime as a quick and easy way to solve their problems (Parker). Parker indicated that in his surveys, personal problem solvers were the most common type.

Career criminals earned part or all of their income from criminal activities. Some had other jobs, and others had ties to organized crime (Parker, 1998). Extreme advocates were equated with terrorists. These individuals were thought to have strong social, political and religious views (Parker). These individuals attempted to change conditions by engaging in crime.

Parker’s last category, malcontents, addicts, and irrational and incompetent people were the most difficult category to describe and protect against (Parker, 1998).

They included the mentally ill, the chemically dependent, and the criminally negligent.

Research indicates that the hacker community itself maintains a loose hierarchy. The hierarchy is made up of the elite, ordinary, and darksiders (Adamski, 1999). The elite hackers write their own software and attack tools (e.g., automated programs designed to discover or take advantage of a vulnerability in a system or network). The ordinary hacker group consists of those individuals that use these tools (e.g., script kiddies) (Adamski). The ordinary group is also made up of individuals who focus on breaking into systems (crackers) and those who attack phone systems (i.e., attacking telephone company computer switches) (phreakers). The darksiders are involved in malicious or predatory behavior (i.e., information brokers, or using hacking for financial gain) (Adamski).

Other research has focused on internal as opposed to external attackers. These individuals commit illegal activity against their own organizations (Post, 1996; Post et al., 1998; Shaw et al., 1998;). Post (1996) labeled these individuals as “dangerous insiders”. The findings on these individuals indicated that they were predominately introverts, experiencing social and personal frustration, and often they could be classified as suffering from a computer dependency (Post et al.; Shaw et al.). These individuals also displayed loose ethical boundaries and a disregard for notions of private or proprietary property (Post et al.; Shaw et al.).

One of the mitigating factors within the dangerous insider group was a sense of entitlement combined with a narcissistic personality (Post et al., 1998). These individuals believed they were owed special recognition by their organizations and would seek revenge if they did not receive it (Post et al.).

Post et al., (1998) also found a lack of empathy by the dangerous insiders toward their victims, and attributions of blame ascribed to victims as well. The study concluded that a lack of empathy was indicative of individuals with narcissistic and anti-social personalities.

New Taxonomy

Combining the previous research on classifying hackers, and the apparent hierarchy found in the hacking community itself, seven distinct (although not necessarily mutually exclusive) categories become apparent; newbie/tool kit (NT), cyber-punks (CP)[1], internals (IT), coders (CD),

[1] Cyber-punk does not refer to the science fiction genre centering around the author William Gibson’s work.

old guard hackers (OG), professional criminals (PC), and cyber-terrorists (CT). These categories are seen as comprising a continuum from lowest technical ability (NT), to highest (OG-CT) [2].

The NT category includes those persons who have limited computer and programming skills. These persons are new to hacking and rely on already written pieces of software, referred to as tool kits, to conduct their attacks. The tool kits are readily available on the Internet.

The CP category is compromised of persons who usually have better computer skills and some programming capabilities. They are capable of writing some of their own software albeit limited and have a better understanding of the systems they are attacking. They also intentionally engage in malicious acts, such as defacing web pages, and sending junk mail (known as spamming). Many are engaged in credit card number theft and telecommunications fraud.

The IT can be made up of disgruntled employees or ex-employees who are usually quite computer literate and may be involved in technology related jobs. They are able to carry out their attacks due to the privileges they have

[2] A possible eighth category is the political activist. The true motivation for their activity and speculation regarding their activities precludes discussion at this time.

been or had been assigned as part of their job function. This group accounts for nearly 70% of all computer related criminal activity (Power, 1997).

The OG, appear to have no criminal intent although there is an alarming disrespect for personal property (Parker, 1998; Chantler, 1996). The OG embraces the ideology of the first generation hackers and appears to be interested in the intellectual endeavor.

The PC and CT groups are probably the most dangerous. They are professional criminals and ex-intelligence operatives who are guns for hire (Post, 1996). They specialize in corporate espionage, are usually extremely well trained, and have access to state of the art equipment. It has been theorized that the professional category has expanded since the dissolution of several of the eastern block intelligence agencies (Denning, 1998; Post et al., 1998; Parker, 1998; Post, 1996).

The majority of research and media attention has been focused on cyber-punks. There has been little or no research on the other categories (Rogers, 1999).

Psychological Profiles

Despite the attention being focused on criminal hackers today, we still know very little about them (Rogers, 1999). There has been few if any real empirical studies conducted on hackers or criminal hackers (Rogers, 1999). The few studies available have focused on those individuals falling into the CP category (Rogers, 1999). The findings from these studies cannot be generalized to any of the other categories.

The available data indicates that individuals classified as CP are primarily; Caucasian, 12-30 years, from middle class families. They are loners, who have limited social skills and perform poorly in school (Chandler, 1996; Littman 1995; Hafner & Markoff, 1995; Sperling, 1992). They are usually not career oriented, but show an aptitude with computers and other electronic equipment (Chantler, 1996; Littman).

Contrary to media portrayal these individuals are rarely a sociopath or psychopath bent on world domination (the fact that none have been identified yet could be due to the limited group that has been studied).

The computer becomes a method for these individuals to gain control over a certain portion of their lives (Karnow et al., 1994; Sperling, 1992). Hacking is a solitary activity, in which the individual is master over their machine. The computer and Internet also provide a cloak of anonymity for these individuals. There is no real face to face interaction. These individuals can be whomever they wish to portray. It is an opportunity to be someone with power and prestige. This is reflected in the use of nicknames often taken from science fiction or science fantasy. These individuals are not happy with who they actually are and use the computer as a means of escapism (Hafner & Markoff, 1995).

Interestingly, these individuals on the one hand indicate they are loners yet they display a strong need to belong to a larger social group (Hafner & Markoff, 1995; Sperling, 1992). The larger hacker community contains several groups or clubs that these individuals belong to. The hacker community holds yearly conventions to discuss attacks and law enforcement efforts to control their activity. There are also hacker specific newsgroups, chat channels, and periodicals (i.e., 2600 Magazine).

Cyber-punks (CP) have a tendency to brag about their exploits. This may be due in part to their desire to be admired by their hacking peers (Post, 1996; Sperling, 1992). The bragging often results in them coming to the attention of law enforcement (Rogers, 1999). The bragging and willingness to talk about their exploits continues even while in custody and during interviews with law enforcement (Hafner & Markoff, 1995; Littman, 1995).

Despite the common hacker rhetoric, most attacks are malicious in nature which may indicate that these individuals have unresolved anger and feel a need to strike out at something or someone (Post, 1996; Sperling, 1992). These individuals may not feel comfortable with people so they strike out at computers and networks, rationalizing that corporations are immoral and need to be taught a lesson (Post).

A survey of hackers by Post (1996) indicated that they had self-perceptions of being loners, under achievers, and socially inept. The hackers in the survey claimed that they were motivated by the challenge, the excitement to succeed, and to learn for the pure intellectual satisfaction (Post). These seem more the motivations of the first generation hackers, and are clearly not corroborated in the documented attacks (Howard, 1997). However, some of the respondents did include vengeance, sabotage and fraud as motivating factors (Post).

The research findings on the cyber-punk group indicate that these individuals have characteristics that are consistent with the stereotypes derived from the media (Parker, 1998). The motivation of these individuals seems not to be as altruistic as their cultural myth would claim. The driving forces appear to be greed, revenge, maliciousness, and power (Hafner & Markoff, 1995; Littman, 1995; Sperling, 1992; Stoll, 1985). Despite some of the claims of a psychological addiction to hacking, there appears to be no empirical support.

Conclusion

It goes without saying that the fact that some individuals within the hacker community choose to engage in criminal activities is problematic. Psychological theories of crime postulate that because a hacker sub-culture or sub-class exists, and the activity is being reinforced (i.e., media attention, high paying jobs, movies), criminal hacking will not disappear on its own but will continue to flourish if left unchecked (Gattiker & Kelly, 1997).

The security industry, law enforcement, and governments need to be extremely cautious not to generalize findings from the limited research to the entire hacker community. There is no generic profile of a hacker (Denning, 1998, Parker, 1998; Post, 1996). A great deal more research is required to determine if psychological profiles can be derived for any of the sub-categories, which seem to exist within the larger hacker community.

If criminal hackers are indeed the “dreaded enemy” of the Internet and general network security, then it is paramount that they be better understood and not just conveniently applied a meaningless label. As Sun Tzu stated in his book The Art of War, "..If you know yourself but not the enemy, for every victory gained you will also suffer a defeat".

References

Adamski, A. (1999). Crimes related to the computer network. Threats and opportunities: A criminological perspective. Available: www.infowar.com/new.

Chantler, N. (1996). Profile of a computer hacker. Florida: Infowar.

Chandler, A. (1996). The changing definition and image of hackers in popular discourse. International Journal of the Sociology of Law, 24, 229-251.

Denning, D. (1998). Information Warfare and Security. Reading: Addison-Wesley.

Gattiker, U., & Kelley, H. (1997). Techno-crime and terror against tomorrow’s organization: What about cyberpunks? Available HTTP: Hostname: ncsa.com Directory: library.

Hafner, K. & Markoff, J. (1995). Cyberpunks: Outlaws and hackers on the computer frontier. Toronto: Simon and Schuster.

Hollinger, R. (1988). Computer hackers follow a guttman-like progression. Social Sciences Review, 72, 199-200.

Howard, J. (1997). Analysis of security incidents on the internet. Unpublished doctoral dissertation, Carnegie Mellon University, Pennsylvania.

Karnow, C., Landels, R. & Landels, D. (1994). Recombinant culture: crime in the digital network. Available HTTP: Hostname: cpsr.org Directory: privacy.

Landreth, B. (1985). Out of the inner circle. Redmomd: Microsoft Books.

Levy, S. (1985). Hackers. New York: Dell

Littman, J. (1997). The Watchman: The twisted life and crimes of serial hacker kevin poulsen. Toronto: Little Brown & Company.

Littman, J. (1995). The fugitive game: online with kevin mitnick. Toronto: Little Brown & Company.

Parker, D. (1998). Fighting computer crime: A new framework for protecting information. New York: John Wiley & Sons, Inc.

Post, J. (1996). The dangerous information system insider: Psychological perspectives. Available HTTP: Hostname: infowar.com

Post, J., Shaw, E., Ruby, K. (1998). Information terrorism and the dangerous insider. Paper presented at the meeting of InfowarCon'98, Washington, DC.

Power, R. (1998). Current and future danger. Computer Security Institute.

Rogers, M. (1999). Psychology of hackers: Steps toward a new taxonomy. Available HTTP: www.infowar.com

Sacco, V., & Zureik, E. (1990). Correlates of computer misuse: Data from a self-reporting sample. Behaviour and Information Technology, 9, 353-369

Shaw, E., Ruby, K., & Post, J. (1998). The Insider threat to information systems: The psychology of the dangerous insider. Security Awareness Bulletin, 2, 1-10.

Skinner, W., & Fream, A. (1997). A social learning theory analysis of computer crime among college students. Journal of Research in Crime and Delinquency, 34, 495-518.

Sterling, B. (1992). The Hacker crackdown: Law and disorder on the electronic frontier. Toronto: Bantam Books.

Stoll, C. (1985). The cuckoos egg: Tracking a spy through the maze of computer espionage. New York: Mass Market Paperback.

Tzu, S. (1985). The Art of War. New York: Delacorte Press.