CERIAS Tech Report 2005-43

THE DEVELOPMENT OF A MEANINGFUL HACKER TAXONOMY: A TWO DIMENSIONAL APPROACH

by mkr@cerias.purdue.edu

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

The Development of a Meaningful Hacker Taxonomy: A Two Dimensional Approach

Marcus K. Rogers, Computer and Information Technology, Purdue University,
(mkr@cerias.purdue.edu)

Abstract

The current paper extends and matures the earlier taxonomy framework of the author (Rogers, 1999), and provides a preliminary two dimensional classification model. While there is no one generic profile of a hacker, studies indicate that there are at least eight primary classification variables: Novices (NV), Cyber-Punks (CP), Internals (IN), Petty Thieves (PT), Virus Writers (VW), Old Guard hackers (OG), Professional Criminals (PC), and Information Warriors (IW), and 2 principal components, skill and motivation. Due to the complex nature and interactions of these variables and principal components, the traditional one-dimensional continuum is inadequate for model testing. A modified circular order circumplex is presented as a better method for developing a preliminary hacker taxonomy. The paper discusses the importance of developing a meaningful understanding of the hacker community and the various sub-groups. Directions for future research are also discussed.

Keywords: Hackers, cyber crime, computer criminals, psychology, circumplex, taxonomy,

The entire field of information assurance and security has grown at a staggering rate. The private sector, governments, military, and academia have realized the importance of securing network infrastructures. Various studies and surveys indicate that even though businesses have increased expenditures on information technology safeguards, the annual losses due to network security breaches are increasing yearly (Berinato, 2004; Melek, 2004). As an example, identity theft now rates as the fastest growing non-violent criminal activity (Federal Trade Commission, 2003).

It is apparent that we need to do more than just spend more money on technology in the hope that these technical controls will solve our problems. We also need to start understanding the individuals behind the attacks (Rogers & Ogloff, 2004; Skinner & Fream, 1997; Taylor & Loper, 2003). Knowing your enemy is not a new concept; it has been part of military and business strategy for centuries (Tzu, 6th cent. B.C./ 1983). In order to assist in our understanding of whom the "enemy" is in this new battle, we first need to identify those individuals intent on destroying, disrupting, and using/abusing our networks, systems, and data. Collectively these individuals have been referred to as "hackers."

The term hacker, to most people, conjures up a mental image of a young male 14 - 18years of age, sitting behind a computer into the wee hours of the night using his technical prowess to attack the faceless immoral corporations (Parker, 1998; Taylor & Loper, 2003). Misinformation and ignorance on the part of the media and, unfortunately, information security vendors, has resulted in the stereotype being embedded into the public's psyche. This is problematic, as this stereotype hinders our efforts to effectively understand the characteristics and motivations of computer criminals and the computer underground (Adamski, 2002; Furnell, 2002; Rogers & Ogloff, 2004).

Apart from conjuring up an inaccurate picture of whom is responsible for a large portion of the risk our IT infrastructures are facing, the use of one generic category is analogous to attempting to understand criminal activity by lumping the entire spectrum of traditional criminals (i.e., shoplifters to homicidal psychopaths) into one generic group[1]. The idea seems ludicrous, yet this is what we are currently doing with the criminal domain of computer crimes. As several authors have commented, a clear picture of the motives of hackers is necessary and long over due (Fotinger & Zeigler, n.d.; Loper, 2000; Woo, 2003).

This paper moves beyond the stereotypes, as well as the fear and uncertainty and doubt (FUD), and presents a framework for truly understanding the various subgroups that are speculated as making up the hacker subculture. The paper presents a model for grouping the various classes of individuals that fall under the hacker umbrella into categories that are more meaningful and provide suggestions for future study.

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 (Furnell, 2002; Rogers, 1999; Rogers & Ogloff, 2004, Woo, 2003). There have been only limited studies, mostly dated, that have attempted to granulize or operationally define the term hacker into more useful subcategories (Chantler, 1996; Fotinger & Zeigel, n.d.; Furnell, 2002, Landreth, 1985; Loper, 2000; Parker, 1998; Post, 1996). Unfortunately, many of the studies used data from the popular media, pseudo self-report surveys, and personal observations, which were culturally biased. Even with the current increase in computer crime rates, there has been a lack of empirical studies based on a solid scientific method in this area.

In 1999 the author developed a preliminary taxonomy based on the limited historical research on classifying hackers, and the self-reported hierarchy found in the hacking community (Rogers, 1999). This model has been used by various other researchers, but has never been sufficiently validated and is now is quite dated (Fotinger & Zeigel, n.d.; Woo, 2003). Furnell (2002) in the UK, has also defined categories of hackers, that expanded upon the author's original model. The current model uses the author's original work, the work of Furnell (2002), as well as the work of Gordon (2001), to construct a more updated preliminary taxonomy. The taxonomy uses eight primary categories[2]:

1. Novice (NV)
2. Cyber-punks (CP)[3]
3. Internals (IN)
4. Petty Thieves (PT)
5. Virus Writers (VW)

[1] The intent here was not to indicate that the term hacker and criminal were synonymous, but to illustrate flawed reasoning.

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

[3] Cyber-punk does not refer to the science fiction genre centering on the author William Gibson's work.

6. Old guard hackers (OG)
7. Professional criminals (PC)
8. Information Warriors (IW)

These categories are seen as comprising a range of technical abilities and motivations, with the lowest technical skill level being the Novice group, and the highest, the Information Warfare group. These eight categories are hypothesized as representing a foundation for the development of a mature hacker taxonomy based on the principal components of skill level and motivation. The model's constructs (i.e., identifying first order characteristics) is consistent with other classification models developed for whitecollar criminals, fraudsters, and Internet pedophiles (Ferraro & Casey, 2005; Hayes & Prenzler, 2003).

The Novice (NV) category includes those persons who have limited computer and programming skills (Chantler, 1996; Rogers, 1999). These persons are new to hacking and rely on pre-written pieces of software, referred to as tool kits, to conduct their attacks. The tool kits are readily available on the Internet. This category includes the younger individuals who are attracted to deviant computer behavior. The primary motivation for this group is based on thrill seeking and ego stroking (Furnell, 2002; Rogers, 1999). These individuals want to be accepted into the hacker sub-culture and in order to prove their worth, they attempt to "rack up" trophies. This behavior is similar to that found in youth gangs, where those wanting to be full members must commit some crime in order to prove themselves. The factors of low technical skills and knowledge, and eagerness to prove their worth, make for a dangerous combination (Rogers, 1999). The wide spread distributed denial of service attacks perpetrated by Mafia Boy in Canada is a good example of what this category is capable of.

The Cyber Punk (CP) category is compromised of persons who usually have better computer skills and some programming capabilities (Rogers, 1999). They are capable of writing some of their own software albeit in limited fashion (e.g., simple scripts) 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. This group's motivation is hypothesized as being the desire for media attention and in some cases, monetary gain (Furnell, 2002; Rogers, 1999). This category is the group that we are the most familiar with. They come to the attention of authorities because of their choice of targets, usually high profile victims that will attract media attention. Once caught, they often become media darlings and some go onto fame and fortune within the consulting profession (e.g., Kevin Mitnick). They often support themselves by using stolen credit information or through identity theft (Furnell, 2002). Not all CP are involved in blatant criminal acts such as credit card theft or ID theft.

Internals (IN) represent the greatest risk; yet, they tend to be the least publicized category (Bishop, 2004; Catan, 2004; Krebsbach, 2004). Historically insiders have been the most costly attackers from both an impact and cost perspective (Randazzo, 2004). The Internals group is primarily made up of disgruntled employees/ex-employees who violate the level of trust they have been given, and using elevated system/access privileges inherent to their job functions, attack their own organization's systems (Randazzo, 2004). The skill level for this group is

somewhat elevated due to the fact that individuals in this category are often IT professionals and sometimes administrators. The motivation most often reported is revenge centered (Shaw et al., 1998; Quigley, 2002). Internals feel they have been slighted, wrongfully terminated or overlooked by management and rationalize that their actions are justified (Shaw et al., 1998). Shaw et al., (1998) identified risk factors of Internals that, when combined with the proper environmental factors (e.g., stress), trigger attacks. These risk factors (e.g., lack of empathy, sense of entitlement, poor interpersonal skills etc.) are common amongst IT professionals in general (Shaw et al., 1998).

The Petty Thieves (PT) become involved with hacking activities as a method to further their criminal activities (Parker, 1998; Rogers, 1999). These individuals are not really interested in notoriety; in fact, this is hazard to their continued success. This group has been attracted to technology and the Internet due to the fact that their traditional targets have moved into this realm (e.g., banks, credit cards, naive people etc.). The successful use of technology is crucial in order for them to fulfill their need for money. They learn the prerequisite skills necessary to perpetrate the crime or the con, and often display a maturation of skills (Parker, 1998). This group is motivated by financial gain, greed, and in some cases revenge.

The Old Guard (OG), appear to have no criminal intent although there is an alarming disrespect for personal property (Gordon 2001; Parker, 1998). The OG embraces the ideology of the first generation hackers and appears to be interested in the intellectual endeavor. This group has deep technical skills and often writes the code and scripts that are used by the less skilled individuals. Although these individuals rarely use the scripts themselves, they readily post them and indirectly encourage their use by the other members of the hacker society (Taylor, 1999). The primary motivations for this group are curiosity and the need for intellectual challenge.

The Virus Writers (VW) is a bit of an anomaly. It is difficult to determine exactly were they fit into the taxonomy. This category is a prime example of how each of the groups may in fact contain sub-groups of their own. Gordon (2001) has indicated that there is a continuum of behaviors and maturity within this category, and that individuals eventually age out of this deviant behavior once they hit their middle to late twenties. The VW group is included in the continuum as a placeholder only as far more research is required for this category.[4]

The Professional Criminals (PC) and Information Warrior (IW) 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 speculated 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).

Despite the potential risk from these groups, we know very little about their make up. The Professional Criminals (PC), unlike the Petty Thief group, are true professionals who put their technical skills and ability to use in furtherance of their criminal enterprise. Similar to the professional criminals in the traditional criminal domain, they are motivated by money and financial gain. They are not interested in fame or bragging rights and, while they may take a

[4] Readers interested in the virus writers are directed to the studies conducted by Sarah Gordon; see reference section.

warped kind of professional pride in a job well done, they tend never to be caught or even come to the attention of the authorities. This group has a high degree of technical acumen, and are more mature both chronologically and psychologically/developmentally. They are often "employed" by organized criminal groups who have recognized the criminal potential of using technology and the Internet (Keegan, 2002; Rogers & Ogloff, 2003).

The Information warfare (IW) category is comprised of those individuals whose job it is to conduct or defend against attacks designed to destabilize, disrupt, or affect the integrity of data or information systems that command and control decisions are based upon (Rogers, 1999; Sewell, 2004). This group includes traditional and non-traditional state sponsored technology based warfare. These individuals are highly trained, highly skilled, and motivated by patriotism.

Circumplex

Now that hypothetical categories have been developed, it is necessary to test these categories or at least represent them in some visual form that allows for future testing. The traditional method would be to construct two separate continuums; one with motivation as the primary axis and the other with skill level and plot each category on these axes (Rogers, 1999). However, this method does not allow for the study of interactions between the two principal components of skill and motivation (Dean 2004; Rogers, 1999; Seigfried, 2004). A continuum is more suited for simple structures and relationships (Acton & Revelle, 2004). An alternate method for representing relationships that are complex, and whose variables are interrelated, is the circumplex.

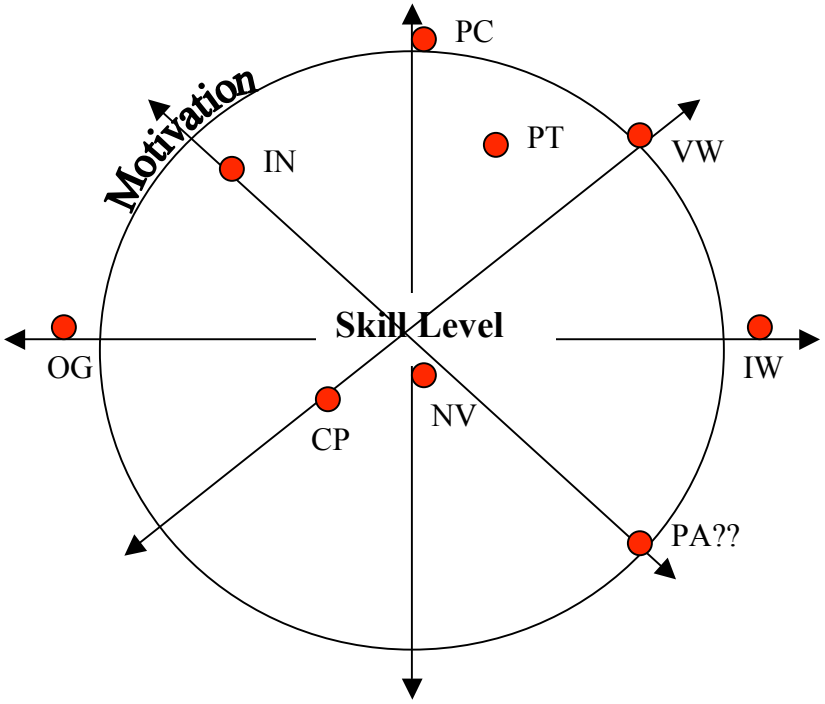
Circumplex models have been used to represent and study various behavioral concepts such as cognitive abilities, interpersonal traits, and psychopathologies (Acton & Revelle, 2004; Wiggins, 1979). The circumplex can be used to represent different concepts (e.g., simple graphical representation, circular order, exact circumplex relations between variables). For our purposes, it is more parsimonious to use the circumplex to guide and bound the development of the hacker taxonomy by way of a modified circular order circumplex (Acton & Revelle, 2004).

With circular order, the position of the variable on the circumference and the radius are significant; related variables are located nearer to each other, negatively correlated variables are located opposite each other, and unrelated variables are orthogonal. In order to represent the primary classification criterion of skill level and motivation, a modification of the traditional circular order approach was used. In the modified model, the position of variables to each other represents the motivation component using the standard circular ordering criteria (e.g., opposite and orthogonal). The modification arises as the position of the variable relative to the origin is used to represent the skill level (i.e., variables farther out from the center on the radius have a higher skill level).

As this is a first attempt at identifying and mapping these variables, the model is not meant to represent the exact relationships but merely a foundation for future testing and development. When examining the circumplex, it seems that the eight primary categories capture the essence of the relationships between the groups on both dimensions of skill and motivation. What is unclear, however, is whether eight categories are sufficient to study all relationships

between groups (e.g., Guttman-like progressions, mentoring, aging out etc.). It is speculated that each of the eight primary classification variables will need to be sub-divided based on empirical analysis before more subtle relationships will become apparent. The model also suggests that the inclusion of a political activist group (PA) may increase the overall usefulness of a classification model (see Figure 1).

Figure 1: Hacker Circumplex



Note: Novice (NV), Cyber-punks (CP), Petty Thieves (PT), Virus writers (VW), Old Guard hackers (OG), Professional Criminals (PC), Information Warriors (IW), Political Activists (PA??). PA is included as a discussion point only.

Conclusion

The current paper presents a framework for the development of a hypothetical hacker taxonomy based on a circumplex approach. Such a taxonomy is required in order to effectively study the phenomenon of deviant computer behavior. Taxonomies have been used with other criminal domains such fraud and pedophiles/Internet child pornography (Ferraro & Casey, 2005; Hayes & Prenzler, 2003). Since hacking actually encompasses a range of skills and motivations, a model that is able to represent complex relationships is necessary (Dean, 2004; Rogers & Ogloff, 2004; Seigfried, 2004).

The updated, preliminary framework developed is based on eight classification variables and uses a modified circular order circumplex model to map the categories on two principal domains, skill and motivation. It is apparent that the categories chosen do not form a perfect circumplex (see Figure 1). However, the circumplex does act as a basis for further discussion and the development of a more mature model based on empirical testing.

Using the circumplex model, relationships between variables can be "eye balled" and future research questions can be easily identified (e.g., does hacking truly follow a Guttmann-like progression?). The validity of the model can also be more easily tested and the model matured to a point where it can be useful to not only researchers, but to the law enforcement community as well.

Obviously, more empirical research is required in order to mature the hacker circumplex. Future studies should examine the exact relationship between classification variables using empirically derived zero order correlation coefficients. It is anticipated that the model will go through several iterations before a definitive framework is derived.

The security industry, law enforcement, and governments need to be extremely cautious not to generalize from anecdotal evidence and limited research to the entire hacker community. While there is no generic profile of a hacker, there are discriminating characteristics between the sub groups that fall under the larger umbrella of the term hacker (Furnell, 2002; Rogers, 1999; Rogers & Ogloff, 2004).

A great deal more research is required to determine if meaningful psychological profiles can be developed for the hacker community. If criminal hackers are indeed the "dreaded enemy" of the Internet and the new globally connected society, 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 the enemy and you know yourself, you need not fear the result of a hundred battles (pp. 18)."

References

Acton, S. & Revelle, W. (2004). Evaluation of ten psychometric criteria for circumplex structure. *Methods of Psychological Research Online 2004, 9*.

Adamski, A. (1999). *Crimes related to the computer network. Threats and opportunities: A criminological perspective*. Retrieved October 15, 2001, from http://www.infowar.com/new.

Bishop, T. (2004). *Association of certified fraud examiners 2004 report to the Nation on occupational fraud and abuse*.

Canton, D. (2004). *Inside breaches pose a threat, too*. Retrieved September 2, 2004, from http://web.lexis-nexis.com

Catan, T. (2004). *Employee scrutiny: Insiders pose the greatest threat*. Retrieved July 11, 2004, from http://web.lexis-nexis.com

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

Chantler, N. (1996). *Profile of a computer hacker*. Retrieved October 15, 2001, from http://www.Infowar.com.

Berinato, S. (2003). *The state of information security 2003*. Retrieved July 23, 2004 from http://www.csoonline.com/read/100103/survey.html.

Dean, N. (2004). *Computer criminal typology determination*. Unpublished Masters Directed Project, Purdue University, West Lafayette, Indiana, USA.

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

Federal Trade Commission. (2004). *ID theft: When bad things happen to your good name*. Retrieved August 14, 2004 from http://www.consumer.gov/idtheft/

Ferraro, M. & Casey, E. (2005). *Investigating child exploitation and pornography.* Burlington, MA: Elsevier Academic Press.

Fotinger, C. & Zeigler, W. (nd). *Understanding a hacker's mind: A psychological insight into the hijacking of identities.* Retrieved July 5, 2005 from, http://www.donau-uni.ac.at/de/studium/fachabteilungen/tim/zentren/zpi/studienangebot/security/DanubeUniversityHackersStudy.pdf.

Furnell, S. (2002). *Cybercrime: Vandalizing the information society*. Boston: Addison-Wesley.

Gordon, S. (2001). *Virus writes: The end of innocence*. Retrieved January 15, 2004, from http://www.research.ibm.com/SciPapers.

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

Hayes, H. & Prenzler, T. (2003). *Profiling fraudsters.* Final Report to Crime Prevention Queensland, February 2003, Brisbane Australia.

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

Keegan, C. (2002). Cyber terrorism risk. *Financial Executive, 18*(8), 35-37.

Krebsbach, K. (2004). *The Enemy Within*. Retrieved September 2, 2004, from http://web.lexis.com

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

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

Loper, K. (2000). *Profiling hackers: Beyond psychology.* Presented at the Annual Meeting of the

American Academy of Sociology, November 15, 2000, San Francisco.
Melek, A. (2004). *Deloitte 2004 global security survey*. Retrieved August 9, 2004 from http://www.deloitte.ca
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.* Retrieved October 15, 2004 from http://www.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.
Quigley, A. (2002). *Inside job: Ex-employees and trusted partners may pose the greatest threats to network security*. Retrieved September 2, 2004, from http://web.lexis-nexis.com
Randazzo, M., Keeney, M., Cappell, D., & Moore, A. (2004). *Insider threat study: Illicit cyber activity in the banking and finance sector*: Carnegie Mellon.
Rogers, M. (1999). *Psychology of hackers: Steps toward a new taxonomy.* Retrieved October 15, 2001 from http://www.infowar.com.
Rogers, M. & Ogloff, J. (2004). A comparative analysis of Canadian computer and general criminals. *Canadian Journal of Police & Security Services, Spring 2004*, 366-376.
Sacco, V., & Zureik, E. (1990). Correlates of computer misuse: Data from a self-reporting sample. *Behaviour and Information Technology, 9,* 353-369
Seigfried, K. (2004). *A critical analysis of the FBI's computer crime adversarial matrix.* Unpublished paper, Purdue University, West Lafayette, Indiana, USA.
Sewell, W. (2004). Protecting against cyber terrorism. *Public Works, 135(3), 39-43.*
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.
Taylor, P. (1999). *Hackers*. London, England: Routledge.
Taylor, R. & Loper, D. (2003). Computer crime. In C.R. Swanson, N.C. Chamelin, & L. Territo (Eds.), *Criminal Investigation* (pp. 584-625). St. Louis, MO: McGraw Hill.
Tzu, S. (1985). *The Art of War.* (J. Clavell, Ed.) New York: Delacorte Press. (Original work published 6th cent. B.C.).
Wiggins, J. S. (1979). A psychological taxonomy of trait-descriptive terms: I. The interpersonal domain. *Journal of Personality and Social Psychology*, 37, 395-412.
Woo, H. J. (2003). *The hacker mentality: Exploring the relationship between psychological variables and hacking activities.* Unpublished Dissertation, University of Georgia, Athens, GA.