Symantec Security Response

WHITE PAPER

Convergence of Virus Writers and Hackers: Fact or Fantasy?

by Sarah Gordon
Symantec Security Response
Symantec Corporation

Qingxiong Ma
Southern Illinois University

INSIDE

Contents

Abstract

The Theory of Planned Behavior (TPB) is one of the most influential and popular conceptual frameworks used to predict human behavior. In this paper, the authors utilize TPB to define a methodology for examining the ethical belief systems of hackers and for deriving predictors of their behaviors. While related research has been carried out on the psychology of virus writers, research on hackers has not been as well-covered. Thus, these findings, when compared and contrasted with empirical research on virus writers, offer the reader the first scientifically modeled insight on the psychological convergence (or lack thereof) in the communities. The analysis of these results will eventually allow comparison between the two subject groups, focusing on cognitive factors such as personal obligation, social pressure, and self-control. Findings will consider the expected effectiveness of varied deterrent and educational techniques, as well as offer insight for public policy, legislation, and educational efforts.

Introduction

Many existing studies on hacking and hackers have focused on topics such as technology investigations and digital forensics (Shinder, 2002), vulnerability assessment, networking security awareness and good practices (Cole 2002; O'Donnell, Pollino & Schiffman 2001), hackers' ethics (Himanen, Torvalds & Castells, 2001), hacker communication and information sharing models (Gordon, 1999; Gordon, 1999), and application and system programming (Matthew & Stones, 1998; Rubini & Corbett, 2001). Additionally, most previous studies on hackers have been conducted by practitioners such as consultants, IT professionals, or security agencies; very often, these studies relied heavily on a single interview or proxy populations rather than real hackers (Denning, 1998; Rogers, 2001).

The situation with research related to viruses and virus writers is somewhat more advanced. There are many good technical studies related to viruses including but not limited to (Perriot, Ferrie & Szor, 2002; Ferrie & Szor, 2001; Szor & Ferrie, 2001). Additionally, scientific studies of virus writers have been conducted using multiple personal interviews with real virus writers, using email, IRC, face-to-face interaction, and survey techniques. The research presents empirical evidence of motivations that virus writers give for creating and making available viruses, as well as offering insight into methods for lessening the phenomenon. Among the most cited motivations are a perceived technical challenge, a desire for peer recognition, and a desire to educate people about security issues (Gordon, 1994; Gordon, 1996; Gordon, 1999; Gordon, 2000).

In order to compare the motivations of virus writers and hackers, this study will attempt to overcome some of the shortcomings of the previous research related to hackers and provide a psychological perspective for helping to increase practitioners' understanding about individuals who engage in computer hacking.

Goals and Objectives

This study is designed to identify hacking motivations and factors that determine hacking behaviors and to propose some effective interventions for reducing deviant behaviors and cybercrimes. Specifically, this study attempts to fulfill the following objectives:

1. Identify stated motivations for hacking behavior
2. Identify foundational beliefs of computer hackers regarding computer-mediated transactions
3. Identify predictors of computer-hacking behavior
4. Provide practical suggestions for public policy-making, legislation, and education based upon these motivations, beliefs, and predictors

Research Model and Hypothesis

This study is accomplished through development and application of a theory-based intention prediction. Such a prediction will be based on well-established rational choice theory, ethical theory, and theories of reasoned action and planned behavior.

RATIONAL CHOICE THEORY

One of the best-known theories used to explain criminal dispositions is rational choice theory, which views deviant behavior as occurring when an offender decides to risk violating the law after considering his or her own personal situation (need for money, personal values, learning experiences) and situational factors (how well a target is protected, how affluent the neighborhood is, how efficient the local police happen to be) (Clarke & Felson, 1993). This theory is helpful in thinking about different ways to reduce opportunities for crime.

THE THEORY OF REASONED ACTION AND THE THEORY OF PLANNED BEHAVIOR

The theory of reasoned action can be summarized (Keel, 1997) in eight points:

1. The human being is a rational actor
2. Rationality involves an end/means calculation
3. People (freely) choose behavior, both conforming and deviant, based on their rational calculations
4. The central element of calculation involves a cost benefit analysis: pleasure versus pain
5. Choice, with all other conditions equal, will be directed toward the maximization of individual pleasure
6. Choice can be controlled through the perception and understanding of the potential pain or punishment that will follow an act judged to be in violation of the social good, the social contract
7. The state is responsible for maintaining order and preserving the common good through a system of laws (this system is the embodiment of the social contract)
8. The Swiftness, Severity, and Certainty of punishment are the key elements in understanding a law's ability to control human behavior

The TPB evolved from the Theory of Reasoned Action (TRA); it has emerged as one of the most influential and popular conceptual frameworks for the study of human action (Ajzen, 2002). In general, TPB suggests that a person's intent to perform a certain behavior is based on three determinants: (1) their attitude toward performing the behavior, (2) any perceived social pressure toward performing it (subjective norms), and (3) the perception that they have the ability and resources needed to perform the behavior (perceived behavioral control). Citing Ajzen:

'In their respective aggregates, behavioral beliefs produce a favorable or unfavorable attitude toward the behavior; normative beliefs result in perceived social pressure or subjective norm; and control beliefs give rise to perceived behavioral control. In combination, attitude toward the behavior, subjective norm, and perception of behavioral control lead to the formation of a behavioral intention.' (Ajzen, 2002. pp.1)

Empirical studies indicate that TPB is very useful in predicting a wide range of behavior (Sheppard et al., 1988; Madden et al., 1992); it has been used by many researchers trying to predict and understand human behavior in various contexts such as recycling (Boldero, 1998), ethical behavior (Kurland, 1995), college course selection (Randall, 1994), leisure activity selection (Ajzen & Driver 1992), and seat belt use (Trafimow & Fishbein, 1994 [in Lynch & Gomaa, 2003]). (Swanson, 1982; Christie, 1981) suggest that such theories provide a potential foundation for research on computer-user behavior.

Ethical Theory and Philosophy

Ethics have long been studied in psychology, sociology, business, and IT/IS (Trevino, 1986, 1990; Mason, 1986; Pearson, 1996). Ethical systems may be public and formalized[1]; or they may be "underground" and informal[2]. For example, an understanding between gang members that no one will provide the police with any information regarding crime perpetrated by any fellow gang member.

For hackers, the concept of ethics is seen as important in guiding behavior (Chandler, 1996; Denning, 1998; Spafford, 1997). Almost every established hacker group has its own beliefs and ethical code; there are even Web sites and books dedicated to hacker ethics (Himanen, 2001). The issue of ethics among virus writers is still relatively immature and focuses mainly on discussions related to virus writing versus viral code distribution (Gordon, 2000).

The ethical systems in virus and hacking culture tend to be informal, although some rules are occasionally formalized by publication, *2600* and *Hactivismo*. Generally within these ethical systems, the end is seen as justifying the means. The main problem with this form of reasoning ignores inherent difficulties of knowing all possible "ends" in massively distributed systems such as the Internet[3].

[1] For example, published codes of ethics by groups such as ACM, IEEE.
[2] For example, an understanding between gang members that no one will provide the police with any information regarding crime perpetrated by any fellow gang member.
[3] This idea was first advanced by Dr. Eugene Spafford, Purdue University.

There is growing empirical support for the addition of a moral obligation construct to add to the power of TPB to predict and explain ethical behavior. As early as 1983, (Gorsuch & Ortberg, 1983) proposed adding personal norms as a predictor to TPB. In 1991, (Randall and Gibson, 1991) extended TPB with moral obligation and tested it in a healthcare context. They found that adding a measure of moral obligation increased the predictive ability of the model. In their study, the theory of reasoned action was applied to the theory of planned behavior for use in predicting the intent to pirate computer software. Chang (1998) found that the theory of planned behavior was the better predictor of intentions and perceived behavioral control explained more of the variance than did attitudes. (Park, 2000) suggested that the relationship between subjective norms and attitudes could be explained by conceptualizing two types of attitudes – personal attitude toward the behavior and social attitudes toward the possible consequences of behaviors to others. In the study of volunteer decision making, (Warburton & Terry, 2000) cited that moral beliefs, or convictions about the rightness or wrongness of an action, might be reflected in the intention to engage or not engage in a particular act.

Although these well-established theories are in different areas, the underlying principles are similar and their major constructs overlap. For example, rational choice theory considers "attitude," and "situational factors," which are similar in meaning to "attitude," "normative pressure" and "perceived controls" in TPB. Due to the high predictive power of TPB (Sutton, 1998), the framework of the proposed study is adapted from TPB, but incorporates the elements of ethical philosophy.

Theoretically, either direct or belief-based measures of attitude, subjective norm, and perceived behavioral control can predict behavioral intention. Either measure can therefore be used to predict intentions. However, most of the studies performed to date have used the direct approach (TPB, 2003). In our research model (Figure 1), we will use the direct approach; all the relationships in the model will be tested. The following are the statements of the hypotheses:

H1 Personal moral obligation has a negative impact on hacking intention

H2 Personal moral obligation has a negative impact on attitude toward hacking

H3 Social norms[4] positively impact hacking intention

H4 Social norms positively impact attitude toward hacking

H5 Attitude toward hacking positively impacts hacking intention

H6 Perceived Control[5] positively impacts hacking intention

H7 Hacking self-efficacy[6] positively impacts hacking intention

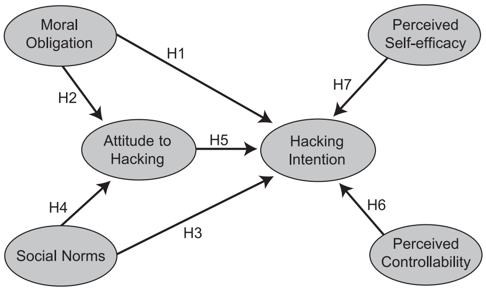

Figure 1. Research model.

[4] Appendix B.
[5] The belief concerning how easy or difficult an activity will be.
[6] The belief that one will be able to successfully perform an activity.

Research Methodology

To accomplish the objectives of this study, four major steps were taken.

1. Elicitation of beliefs

Beliefs of hackers related to hacking behaviors were collected and analyzed. These beliefs were found to consist of positive and negative outcomes of hacking, social influences, and facilitating/inhibiting factors. The data was obtained in part by using surveys, interviews, email, and electronic chat; additional beliefs were compiled from face-to-face conversations. Using a content analysis approach, the beliefs were classified into behavioral beliefs, normative beliefs, and control beliefs.

2. Design of survey instrument

The survey was designed, based on data obtained in (1). As this research is still in progress, the actual survey is online at http://mypage.siu.edu/cgqm/friend.html). See Appendix A for an overview of the survey questions.

3. The survey was made available

A request for participants was issued via various sources[7], in order to elicit responses from an appropriate number of subjects to satisfy requirement for statistical significance.

4. The survey responses were analyzed

The responses were analyzed using a structure equation modeling tool (SPSS) to perform the regression analysis[8].

5. The research model was assessed and hypotheses tested

Subjects

The target population is people who have compromised the security of a remote computer using the Internet or a dial-up modem regardless of gender, age, nationality, and profession. According to Hair et al. (1995), the minimum sample size in terms of the ratio of subjects to free model parameters is 10:1. In this study, there will be six basic constructs composed of 20 predictive variables. Therefore, the valid sample used in this study should be at least 200.

Results

Using intention as the dependent variable and moral obligation, self-efficacy, perceived-control, and social norms as predictors, a regression analysis was conducted. From this table, one can see that “moral obligation” and “self-efficacy” are significant predictors of intention to hack, and “social norms” and “perceived-control” are not.

The first two factors together can explain 45% of the variance of intention to hack. Between these two factors, moral obligation has the strongest, but negative effect on intention. The next strongest factor is self-efficacy. Perceived control has a slight influence on intention to hack, but the effect is insignificant.

[7] The perception of community standards and values.

[8] The final data will be analyzed using LISREL or a comparable analysis package.

Model	Unstandardized Coefficients	Standardized Coefficients	T	Significance Level
Moral Obligation	-.658	-.442	-2.868	.008
Perceived Control	.257	.231	1.434	.163
Self-Efficacy	.701	.439	2.767	.010
Social Norms	.111	.091	.558	.581

Table 1. Regression results with intention to hack as dependent variable.

In order to have an overview of each relationship in the research model, the results of research hypotheses are summarized in Table 2. In summary, the data collected supports three out of the seven hypotheses in this study.

Hypothesis	Relationships	Supported?
H1	Moral → Intention	Yes
H2	Moral → Attitude	Yes
H3	SN → Intention	No
H4	SN → Attitude	No
H5	Attitude → Intention	No
H6	Control → Intention	No
H7	SE → Intention	Yes

Table 2. Results of research hypotheses.

Implications

The strength of the path co-efficients from the analysis help to determine which factor is most important in influencing intention and behavior. This in turn helps to determine what might be the most effective interventions for preventing or reducing the hacking intention.

For example, if social norms were found to be the strongest factor in determining intention, the initial intervention effort should be focused on that factor. In a practical sense, the results of the study are interesting to management, policy-makers, and educators for several reasons.

First, in the TPB model, social norm is generally a strong indicator of behavioral intention. However, in the computer-hacking setting, our data so far showed the standardized co-efficient of the relationships between social norms and intent to hack was only .091, indicating that this is not true. This result suggests that most computer hackers tend to be self-motivated or self-centered individuals; they are not likely to be easily influenced by friends or family members.

This finding is in stark contrast to research on virus writers that shows peer recognition and approval to be one of the core motivators for virus writing. Indeed, among virus writers, relationships with parents and peers tend to be within social norms. Thus, in order to have a better understanding about these behaviors and to derive a widely applied theoretical model, TPB needs further testing with different group of subjects in various settings.

Second, the preliminary results of this study suggest that moral obligation is the strongest factor impacting hacking intention. The correlation of moral obligation with intent to hack is -.442; thus, moral obligation has a negative impact on intention to hack; that is, the more important moral obligation is, the less strong the intent to hack. The data suggests that the most effective approach to prevent computer hacking is to enhance the moral obligations of potential hackers. Thus, computer system administrators and educators should consider expending more effort and allocating more resources for moral education. This is consistent with previous findings related to virus writers (Gordon, 2000).

However, as discussed earlier, there are forms of "ethics" in these countercultures. The challenge is to create realistic educational opportunities that allow for exploring the real issues, without incorporating dogma, or falling prey to premature consensus thinking about what the ethical model should look like. This is a topic for future research.

Third, the positive effect of self-efficacy on computer use is traditionally supported in the study of information technology diffusion and adoption (Compeau and Higgins 1995; Lopez and Manson 1997; Agarwal et al., 2000). The result of this study confirmed this relationship. However, while with regard to computer using and learning, self-efficacy is important and should be augmented; in terms of computer hacking, self-efficacy should not be enhanced.

As experience is one of the most important factors influencing self-efficacy, computer system security practitioners should make efforts to reduce the experience or chances of successful computer hacking; for example, do not allow for hacking demonstrations or exhibitions to be held on the Internet or at conferences. While in practice this appears similar to the reasoning that virus-writing contests are "bad" because the activity is "bad" in and of itself, the underlying justification here relates more to self-efficacy and its effect rather than value judgment.

Finally, as some hacking behaviors are highly contextual in nature, eliminating hacking efficacy while enhancing overall systems knowledge is certainly a topic for future research.

Fourth, the results of this study also tell us that the perceived behavioral control is not an important factor influencing intention to hack. This finding implies that techniques such as firewalls, intrusion detection, and antivirus software may not deter computer hackers from hacking. That is, increasing the difficulty to hack may not be an effective way to prevent hacking.

Additionally, exploring and addressing other psychological factors would seem wise.

For example, in the virus-writing community, displacement and diffusion of responsibility is common., which is consistent with Bandura's displacement model (see Figure 2).

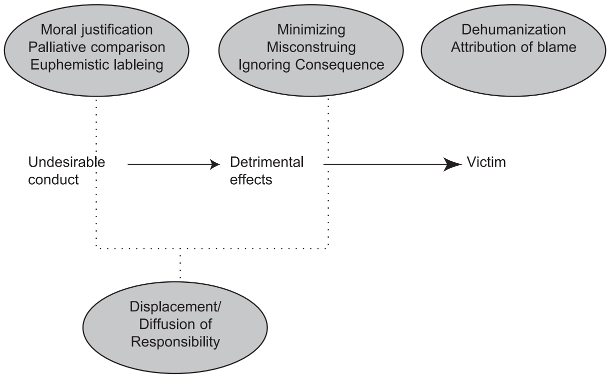

Figure 2: Bandura's Displacement Model[9].

[9] Note. Diagram based on (Bandura, Barbaranelli, Caprara, & Pastorelli, 1996).

While in the early days of virus writing, dehumanization and blame of the victim were commonplace, this has decreased. Today, the displacement commonly involves minimizing, ignoring or misconstruing consequences, palliative comparison, and euphemistic labeling. For example, studying viruses in an uncontrolled environment may be referred to as "research."

Thus, effective interventions for decreasing displacement might focus on expanding educational efforts to include examining ethics related to computer viruses, as well as maximizing the consequences of irresponsible virus writing and/or distribution. While (Gordon, 2000) showed that legal intervention was not likely to have a significant impact on virus writing, as legal consequence continues to occur closer to the actual event, this could change. This is a topic for future research.

In the hacking community, dehumanization and attribution of blame is somewhat more common; misconstruing or ignoring the consequences of the act is somewhat prevalent; and moral justification is extremely commonplace[10], based on the public communication of hackers on public mailing lists. Thus, it is not surprising that personal moral obligation factors highly in attitudes toward an intention to hack. Therefore, interventions designed to humanize other computer users, sensitize young people to the human aspect of computing, and maximize the consequence of both negative and positive acts. And, an increased emphasis on understanding ethics could help lessen the ability of young people to minimize or misconstrue consequences.

In terms of the convergence between the virus-writing and hacking communities, this preliminary research tends to indicate that convergence, at least in terms of collaboration, is not likely in the short term. According to (London, 1995), collaboration is unlikely to work well when there are power inequalities among the parties, or where groups are too large. In addition to this, for a true collaborative process to evolve, motivations and goals need to be similar. The disparities of motivation and worldview are not the only factors likely to act against convergence; (Macey & Skvoretz, 1998) also point out the crucial role of trust on the collaborative process. The issue of trust in these underground communities is an interesting topic for future research applicable to understanding the collaboration and convergence of these two communities, as is research that applies the principles of self-organizing communities.

Thus, given the combination of the results provided by TPB, the different mindset and motivation of the two communities, and the decentralized nature of the groups, the opportunity for convergence would seem to be limited, at least in the short term.

[10] Based on public communication of hackers on public mailing lists.

Conclusion

The results of this preliminary work show that the application of TPB to hacker motivation and prevention is likely to yield a large amount of useful data. Most importantly, this approach represents an objective and scientific approach to determining the likely impact of various approaches designed to deter hacking.

Changes to any one or more determinants may facilitate a change in behavioral intention or control; the greater the weight of a given factor, the more likely it is that changing the factors will influence intention and behavior.

In terms of public policy, it appears that self-efficacy plays an important role in a person's intent to hack. Thus, by attempting to limit the efficacy of the hacker, some moderation of the hacking action, over and above the simple result provided by increasing the difficulty of hacking, may be achieved. Thus, policies that increase the organizational control and investigation of hacking activity may prove to be an effective deterrent in terms of reducing hacker activity.

In terms of educational impact, the results of an increased ethical understanding on the part of the hacker community is hard to estimate; however, based on the TPB model used here, a shift in the internal moral compass of would-be hackers is likely to be a highly-effective determinant in terms of end-stage behavior.

Finally, regularly using the instrument designed in this study may provide clinicians, corporations, and interested academics with an additional tool for use in benchmarking and diagnostics. Further research would be to apply TPB to numerous behaviors in the computing space, as well as to compare the results provided with in-depth psychological interviews and interventions with some of those involved. In this manner, the validity of the research model can be proven, by measuring the corresponding shifts in behavior and perception based on observation.

Simply put, what we believe influences what we do. Thus, identifying beliefs is the first step toward categorizing and analyzing the underlying cognitions. Once the beliefs have been identified, and the underlying cognitions categorized and analyzed, appropriate interventions can be designed and implemented. The interventions suggested herein are first steps. Theoretically, the application of TPB to hacking, virus writing, and other forms of antisocial computing behavior is likely to yield an objective criteria for comparing and contrasting differences in motivations, beliefs, and attitudes, providing a baseline for designing appropriate interventions and reducing the occurrence of these undesirable behaviors.

References

Ajzen, I. (2002), "Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior," *Journal of Applied Social Psychology*, 32, pp.665–683.

Ajzen, I. & Driver, B. (1992), "Prediction of leisure participation from behavioral, normative, and control beliefs - an application of the theory of planned behavior," *Leisure Sciences*, 13, pp.185–204.

Ajzen, I. & Driver, B. (1992), "Application of the theory of planned behavior to leisure choice," *Journal of Leisure Research*, 24, pp.207–224.

Bandura, A., Barbaranelli, C., Caprara, G., and Pastorelli, C. (1996), "Mechanisms of moral disengagement in the exercise of moral agency," *Journal of Personality and Social Psychology*, 71.

Boldero. J. (1998), "The prediction of household recycling of newspapers: The role of attitudes, intentions, and situational fact," *Journal of Applied Social Psychology*, 25, pp.440–462, 1825–1834.

Chang, M., (1998), "Predicting unethical behavior: a comparison of the theory of reasoned action and the theory of planned behavior," *Journal of Business Ethics*, 17, pp.1825–1834.

Christie, B. (1981), *Face to file communication: a psychological approach to information systems*, New York. Wiley.

Clarke, R. & Felson, M. (1993), "Routine activity and rational choice, (Vol. 5)," *Advances in Criminology Theory*, New Brunswick: Transaction Publishers, Inc.

Compeau, D., & Higgins, C. (1995), "Computer self-efficacy: development of a measure and initial test," *MIS Quarterly*, 19(2), pp.189–211.

Denning, D. (1998), "Concerning hackers who break into computer systems," *Proceedings of the 13th National Computer Security Conference*, pp.653–664, Washington, D.C.

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

Cole, E. (2002), *Hackers beware: the ultimate guide to network security*, Indiana. SAMS publishing.

Ferrie, P. & Szor, P. (2001), "Zmist opportunities," *Virus Bulletin*, March 2001, p.6.

Gordon, S. (1994a), "Technologically enabled crime: shifting paradigms for the year 2000," *Computers and Security Journal, Special Edition*, Oxford, United Kingdom. Elsevier Science Publications.

Gordon, S., (1994b), "The generic virus writer," *Proc. Int. Virus Bull. Conf.* 1994.

Gordon, S., (1995), "Inside the mind of dark avenger," *Retrieved from:* http://www.research.ibm.com/antivirus/SciPapers/Gordon/Avenger.html. May 2003.

Gordon, S. (1996), "The generic virus writer II," *Proc. Int. Virus Bull. Conf.*, 1996.

Gordon, S. and Ford, R. (1999), "When worlds collide: information sharing for the security and anti-virus communities," *Proc. Int. Virus Bull. Conf.*, 1999.

Gordon, S., (2000), "Virus writers: the end of the innocence?," *Proc. Int. Virus Bull. Conf.*, 2000.

References (continued)

Gorsuch, R. L., & Ortberg, J., (1983), "Moral obligation and attitudes: their relation to behavioral intentions," *Journal of Personality and Social Psychology*, 44, pp.1025–1028.

Hair, J., Anderson, R., Tatham, R., and Black, W. (1984), *Multivariate data analysis with readings* (5th edition 1998). Englewood Cliffs, NJ Prentice-Hall.

Himanen, P., Torvalds L., & Castells, M. (2001), "The hacker ethic," *The hacker ethic and the spirit of the information age.* Random House Publishing.

Kurland, N., (1995), "Ethical intentions and the theories of reasoned action and planned behavior," *Journal of Applied Social Psychology*, 25(4) pp.297–313.

Lopez, D. and Manson, D., (1997), "A study of individual computer self-efficacy and perceived usefulness of the empowered desktop information system," *Journal of Interdisciplinary Studies*, Vol 10.

Lynch, A. and Gomaa, M., (2002), "Understanding the impact of technology on the propensity to engage in fraudulent behavior," University of South Florida.

Madden, T., Ellen, P. & Ajzen, I., (1992), "A comparison of the theory of planned behavior and the theory of reasoned Action," *Personality and Social Psychology Bulletin*. 18, pp.3–9.

Keel, R. (1997), "Rational choice and deterrence theory," *From* http://www.umsl.edu/~rkeel/200/ratchoc.html, *May 20, 2003.*

Mason, R., (1986), "Four ethical issues of the information age," *MIS Quarterly*, 10(1), 4.

Matthew & Stones, M. (1998), "Beginning Linux programming," *Linux Programming Series*, 1st edition, Addison-Wesley.

Nori, F., (2001), "I Love You," *An exhibition at the Frankfurt Museum of Modern Art*, Frankfurt, Germany.

O'Donnell, A., Pollino, D. & Schiffman, M., (2001), "Hacker's challenge 2: test your network," *Security & forensic skills*, McGraw-Hill Publishing.

Pearson, J. (1996), "Modeling the relative importance of ethical behavior criteria: a simulation of information systems professionals' ethical decisions," *The Journal of Strategic Information Systems*, 5, pp.275–291.

Perriot, F., Ferrie, P. & Szor, P. (2002), "Striking similarities: W32/Simile and metamorphic virus code," *Virus Bulletin*, May 2002 p.4.

Randall, D. (1994), "Why students take elective business ethics courses – applying the theory of planned behavior," *Journal of Business Ethics*, 13(5), pp.369–378.

Randall, D. & Gibson, A., (1991), "Ethical decision-making in the medical profession – an application of the theory of planned behavior," *Journal of Business Ethics*, 10, pp.111–122.

Rogers, M. (2001), "A social learning theory and moral disengagement analysis of criminal computer behavior: an exploratory study," *Doctoral Thesis*. University of Manitoba. Winnipeg, Canada.

References (continued)

Rogers, M. (1999), "Modern-day robin hood or moral disengagement: understanding the justification for criminal computer activity," University of Manitoba. Winnipeg, Canada.

Rubini, A. & Corbet, J., (2001), *Linux device drivers.* 2nd edition, O'Reilly & Associates.

Sheppard, B., Hartwick, J., & Warshaw, P. (1988), "The theory of reasoned action: a meta-analysis of past research with recommendations for modifications and future research," *Journal of Consumer Research*, 15(3).

Shinder, D. (2002), *Scene of the cybercrime*, Syngress Publishing.

Sutton, S. (1998), "Predicting and explaining intentions and behavior: how well are we doing?" *Journal of Applied Social Psychology*, 28(15) pp.1317–1338.

Szor, P. & Ferrie. P., (2001), "Hunting for metamorphic," *Proc. Int. Virus Bull. Conf.* 2001.

Spafford, E. . 1997, "Are hacker break-ins ethical?" *Ermann, Williams, & Shauf, (Eds.) Computers, Ethics, and Society.* pp.77–88. New York: Oxford.

Swanson, E.B. (1982), "Measuring user attitude in MIS research: a review," *OMEGA*, 10, pp.157–165.

TPB (2003), "Theory of planned behavior FAQ," *Retrieved from* http://www-unix.oit.umass.edu/~aizen/faq.html, *June 11, 2003.*

Trafimow, D. and Fishbein, M. (1994), "The importance of risk in determining the extent to which attitudes affect intentions to wear seat belts," *Journal of Applied Social Psychology*, 24(1) pp.1–11.

Trevino, L. (1986), "Ethical decision making in organizations: a person-situation interactionist model," *Academy of Management Review*, 11, pp.601–617.

Trevino, L. & Youngblood, S. (1990), "Bad apples in bad barrels: a causal analysis of ethical decision-making behavior," *Journal of applied Psychology*, 75, pp.378–385.

Warburton, J. & Terry, D. (2000), "Volunteer decision making by older people: a test of a revised theory of planned behavior," *Basic and Applied Social Psychology*, 22, pp.243–255.

Appendix A: Survey Instrument

The survey was divided into Sections A, B, and C. Prior to responding, readers were presented with an Informed Consent notice and email contact information for the researchers.

SECTION A

Section A consisted of demographic information: Gender, age range, religion, education, category (that is, hacker, cracker, warez guy, script kid, virus writer). It also ascertained how often the respondents claim to have hacked in the past month, and whether they are part of a hacking group. Finally, respondents were asked whether they were afraid of going to jail, and whether they had thought about moral issues related to hacking.

SECTION B

Section B queried the respondents as to desire and intent to hack in the future, and feelings when hacking. These feelings were divided into three categories. In the first category, respondents feelings about his or her own behavior were assessed on a continuum from Harmful to Helpful , Positive to Negative, Wise to Foolish, Helpless to Powerful, and Enjoyable to Unenjoyable. The respondents' feelings about morals were assessed with three questions: "I would feel guilty if I hacked;" "Hacking goes against my principles;" "It would be morally wrong for me to hack." Questions related to ease and skill of hacking measured the relative importance the respondents placed on these factors; questions regarding feelings of people around them, such as friends and family, measured how the respondents perceived how others viewed hacking.

SECTION C

Section C queried the respondents' thoughts about the likelihood of various consequences/outcomes of hacking, such as expanding skill-sets, fostering awareness of security, feelings of power, satisfying curiosity, showing patriotism, gaining fame, providing peer recognition, helping society, stopping the spread of evil, profit, helping the employer, revenge, facilitating anonymity, and alleviating boredom. Then, the respondents' thoughts about the likelihood of the consequences were measured in light of the consequences as good/bad, important/unimportant, acceptable/ unacceptable, on a continuum.

Social norms were examined using questions about the opinions and impact of opinions of friends, family, and teachers. The respondents' thoughts about their own moral worldview and how they felt about hacking in light of that worldview were queried

Appendix B: Call for Participants

Requests for participation in the survey were issued electronically via email to known members of the hacking community, via Internet Relay Chat (IRC) to known and unknown hackers, via 5 public and private mailing lists to known and unknown hackers, and via both security- and hacking-related WWW sites.

About the Authors

Sarah Gordon is Senior Research Fellow at Symantec Security Response. Her current research areas include testing and standards for antivirus and security software, privacy issues, cyberterrorism and psychological aspects of human/computer interaction.

Sarah was responsible for security testing and recommendation for The United Nations, and participates in various initiatives for Homeland Security and Infrastructure Protection. She was chosen to represent the security industry in "Facts on File: Careers for Kids who Like Adventure", and is a reviewer for various technical security book publishers including Wiley publications. Her work in ethics, technology and profiling computer criminals is required coursework in various academic information security programs. She is committed to excellence in information security education, guest lecturing at Universities world-wide on topics ranging from virus writers and hackers to the truth about cyberterrorism.

Sarah graduated from Indiana University with special projects in both UNIX system security and ethical issues in technology. She is a member of the American Association for the Advancement of Science, The American Counseling Association, and the Association for Family Therapy and Systemic Practice in the UK. Prior to joining Symantec, she worked with the Massively Distributed Systems Group at IBM's Thomas J. Watson Research Laboratory in New York in the AntiVirus Research and Development Team. She may be reached at sgordon@symantec.com.

Qingxiong Ma is an Assistant Professor of Computer Information Systems at Central Missouri State University. He is a Ph.D. candidate in Management Information Systems at Southern Illinois University at Carbondale.

Ma received his MBA from Eastern Illinois University, Charleston, IL, in 1999. He has presented his works at the America's Conference on Information Systems and Decision Sciences Institute Annual Meetings. His research interests include information technology adoption/diffusion, electronic commerce, and information security management.

WORLD HEADQUARTERS

**20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408.517.8000
800.721.3934**

www.symantec.com

**For Product information
In the U.S. call toll-free
800.745.6054**

**Symantec has worldwide
operations in 36 countries.
For specific country
offices and contact numbers
please visit our Web site.**