MIS Quarterly

SPECIAL ISSUE

MOVING TOWARD BLACK HAT RESEARCH IN INFORMATION SYSTEMS SECURITY: AN EDITORIAL INTRODUCTION TO THE SPECIAL ISSUE

By: **M. Adam Mahmood**
University of Texas at El Paso
mmahmood@utep.edu

Mikko Siponen
University of Oulu, Finland
mikko.siponen@oulu.fi

Detmar Straub
Georgia State University
dstraub@gsu.edu

H. Raghav Rao
State University of New York at Buffalo
mgmtrao@buffalo.edu

T. S. Raghu
Arizona State University
raghu.santanam@asu.edu

Introduction

The *MIS Quarterly* Special Issue on Information Systems Security in the Digital Economy received a total of 80 manuscripts from which we accepted nine for publication in the Special Issue. To introduce the readers to the special issue papers, we have chosen to digress from the tradition of summarizing the papers in-depth and, instead, would like to take this opportunity to encourage researchers to conduct more black hat information security research as opposed to the present emphasis on conducting mostly white hat research.

Black Hats Versus White Hats Versus Grey Hats

What exactly is this white hat versus the black hat dichotomy? When making movies about the Old American West, filmmakers made a symbolic distinction at times between the good guys, wearing white hats, and the bad guys, wearing black hats. If, for the sake of our basic theme, we can adopt this distinction momentarily, we would like to go on to asseverate that the information systems field is heavily overemphasizing research on white hats to the detriment of studies on black hats. It is easy to see how this would, quite naturally, occur. Scholars have better access to white hats, although even here, white hat managers do not typically want to share detailed information about their losses and have responded in this manner for some time (Hoffer and Straub 1989). Thus it is a readier access to data that has led information security researchers to gravitate toward white hat issues.

Whereas we could offer more extensive evidence of the prevalence of white hat IS research studies, a quick review of the papers in this special issue indicates that only the paper by Abbasi, Zhang, Zimbra, Chen, and Nunamaker attempts to empirically represent the activities of black hats, but even with this representation, we are at arm's length from black hat motivations and future dark plans.

We need to state unequivocally that our argument for more emphasis on the black hat type of research in no way diminishes the contributions of the white hat papers in this special issue. These white hat studies, along with the black hat (or quasi-black hat) study just mentioned, increase our knowledge of information security immensely. Four papers (Smith, Winchester, Bunker, and Jamiesen; Siponen[2] and Vance; Spears and Barki; and Bulgurcu, Cavusoglu, and Benbasat) help us understand user resistance to regulatory compliance, factors that contribute to this resistance, and possible avenues for overcoming it. The Johnston and Warkentin study shows that fear appeals influence end user intentions to adopt recommended individual computer security actions with respect to spyware. The paper by Gordon, Loeb, and Sohail uncovers the positive impact of voluntary disclosure of information security breaches on market value whereas the Galbreth and Shor paper implies that the software industry, being in a competitive market with or without disclosure of security breaches by firms, is less likely to invest in security. The Anderson and Agarwal paper makes clear to us that the intention to comply with security requirements in the home computer environment is affected by critical cognitive, social, and psychological factors.

Returning to our previous argument, and without gainsaying any prior research in the area, we would again like to stress that information security research has long been dominated by studies that focus on white hats. From the beginning, these studies have primarily attempted to capture the thinking and activities of black hats through surrogates, including such mechanisms as asking white hats to report on why black hats act the way they do and what damages they have caused (Straub 1990). There are, however, compelling reasons for IS researchers to shift from low hanging fruit like white hat studies to the harder-to-reach fruit of black hat studies. First, without a better and truer understanding of the antisocial behavior that prompts individuals to attack computer systems, we cannot readily design the most effective countermeasures.

Second, black hat data is now becoming more accessible. The Internet provides us direct entry into black hat initiatives and actions. Whereas in the past we had to rely on anecdotes such as those related by Cliff Stoll in his famous book *The Cuckoo's Egg*, today hackers congregate in online hacker communities. Here they share their ideas about breaking computer security and, in some case, they share their exploits. The so-called grey hats, those who are dedicated to testing security, but not necessarily causing harm, could also be interesting avenues for gathering new forms of data. Grey hats may be the closest surrogates we have to black hats.

Third, we need to move pointedly away from studies that ask students to think like malefactors. The most determined criminal mind cannot even be remotely simulated by ordinary citizens who may have parking or speeding tickets on their record, but little else; students may sometimes be used legitimately as surrogates in social and criminological experiments, but certainly not always (Garberg and Libkuman 2009; Gordon et al. 1986). Moreover, gaining direct access to black hat data will increase our knowledge exponentially. Asking students to think and act in an antisocial way is not only unlikely to yield much generalizable knowledge, but it also either is or borders on being unethical. In the research ethics domain, this is known as "inflicted insight." In this case, subjects learn something about themselves that is painful, not redemptive, and might even lead them astray at some point in their lives, none of which might have taken place if they had not participated in the research.

Fourth, IS scholars working directly with black hat data would be a breath of fresh air and inspire more good work in the domain. It could lead to more researchers, especially those with technical skills, lurking in hacker communities. In short, there could be a virtuous cycle of research initiatives set in motion.

Fifth, on a broader level, our ability to understand black hat behavior in various contexts will help us slow the spread of and limit the impact from such security breaches and in the process enhance the societal value of information security research. Not only will we understand black hats better, but the countermeasures so designed should lead to lessening the damage caused by criminals.

New (and Some Old) Sources of Data on Black Hat Activities

We provide now with some examples of possible data sources for conducting black hat research. Two rich sources of data are the U.S. Securities and Exchange Commission (SEC) and the Computer Emergency Response Team (CERT) at Carnegie Mellon University where firms report their information security incidents. With regard to *modus operandi* for collecting actual data, we recommend the use of IT employees as surrogates for hackers who willfully violate and test security protocols; naturally this would need to be done with permission from their supervisors. Such actions are only possible when there is no retribution for such violations and grey hats, ultimately being helpful to the organization, are thus held

[2] Please take note that because Mikko Siponen was an editor for the Special Issue, a wholly independent and unbiased process was used to evaluate his submission to the Special Issue. A noted security scholar not associated with the Special Issue in any way (and also not on *MIS Quarterly*'s editorial board) served as Senior Editor on this paper.

harmless.[3] Another possible way for collecting black hat data is to focus on those employees who do not have privileges on certain resources and yet make consistent attempts to access those resources. The behavior of such insider threat employees would be revealed through, for example, log data of enterprise single sign-on systems that typically monitor all authentication and authorization activities. Yet another possible way for collecting black hat information is to use a decoy system such as the "honeypot" (Stallings and Brown 2008; Ryu et al. 2010). Honeypots are filled with fabricated information that looks real and valuable. They are designed to lure black and grey hats into the system to collect information about antisocial behavior, which will work if legitimate users do not enter and use the system. Finally, a rich source of data could be the search engine logs. These logs can provide search patterns for nefarious keywords both at the session level and at the query level; these can be identified and used as proxy data for research into black hat behavior.

Conclusion

We are confident that, over time, information security research has become more sophisticated, more relevant, and more rigorous and that this Special Issue clearly demonstrates this trend. We can also proffer that the increasing number of scholars in the IS community who are turning their attention to security research can improve the richness and depth of their research by seeking out new, even unique sources of data that reveal the underlying mechanisms of computer crime and the effectiveness of organizational responses to this behavior. It would be encouraging to be able to say with equal confidence that the community will indeed take up this challenge and push our scientific knowledge of IS security into new realms.

References

Garberg, N. M., and Libkuman, T. M. 2009. "Community Sentiment and the Juvenile Offender: Should Juveniles Charged with Felony Murder Be Waived into the Adult Criminal Justice System?," *Behavioral Sciences & the Law* (27:4), pp. 553-575.

Gordon, M. E., Slade, L. A., and Schmitt, N. 1986. "The 'Science of the Sophomore' Revisited: From Conjecture to Empiricism," *Academy of Management Review* (11:1), pp. 191-207.

Hoffer, J. A., and Straub, D. W. 1989. "The 9 to 5 Underground: Are You Policing Computer Crimes?," *Sloan Management Review* (30:4), pp. 35-43.

Ryu, C., Sharman, R., Rao, H. R., and Upadhyaya, S. 2010. "Security Protection Design for Deception and Real System Regimes: A Model and Analysis," *European Journal of Operational Research* (201:2), pp. 545-556.

Stallings, W., and Brown, L. 2008. *Computer Security: Principles and Practice*, Upper Saddle River, NJ: Prentice Hall.

Straub, D .W. 1990. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.

[3] So-called "tiger teams" are sometimes employed by organizations to perform this very role.