Chapter 12

The Social Network Structure of a Computer Hacker Community

Xubin Cao
Southwestern University of Finance and Economics, China

Yong Lu
Pennsylvania State University, USA

ABSTRACT

Computer hackers, both individually and as a group, have been identified as a primary threat to computer systems, users, and organizations. Although hacker groups are complex socio-technical systems, much extant research on hackers is conducted from a technical perspective and at an individual level of analysis. This research proposes a research model composed of five dimensions and their relations in order to study hacker’s social organization in the whole socio-technical context. Based on this model, the researcher applies network analysis methods to disclose the structure and patterns of a significant and complex hacker group, Shadowcrew. Network analysis tools are applied for data processing and data analysis. Three network measures: degree centrality, cognitive demand, and eigenvector centrality, are utilized to determine the critical leaders. Out-degree centrality is employed to analyze the relations among the five dimensions in the research model.

INTRODUCTION

Identity theft and financial fraud conducted by hackers have evolved into serious and pervasive threats to consumers and the financial services industry (Furnell, 2002). Computer hackers, both individually and as a group, have been identified as a primary threat to computer systems and users. The CSI Computer Crime & Security Survey, the world’s most widely quoted survey on computer crime, found that financial fraud, password sniffing, and malware infection cost organizations the most, with an average loss close to $289,000 for each respondent’s organization (Richardson, 2009).

Academic research from a variety of disciplines has contributed to our understanding of the hacker’s attack methods (Furnell, 2002), sub-culture (Thomas, 2002), and motivations (Taylor, 1999). Previous studies by Meyer (1989) and Holt
The Social Network Structure of a Computer Hacker Community

(2005) found that hackers were colleagues who had relatively loose social networks that they could share information and introduce subcultural norms to new hackers. However, much extant research on hackers is conducted at the individual level of analysis. Few studies examine hackers operating in group or network contexts to reveal their social relationships and organizational patterns within hacker communities. Straub et al. (2008) have noted that few projects have taken from a behavioral and sociological point of view to effusively address the human aspects associated with effective decision-making for security.

Besides, considering the advancement and rapid development of computer technology and information security industry over the past decade, it is entirely possible that the nature and structure of hacker’s social organization have changed. For instance, hackers have become involved in online terrorism (Williams, 2001) and organized crime (Kleen, 2001). The rapid developments of e-commerce, data warehousing, and data aggregation services have made hacking activities profitable. Hackers who once might have broken into computer systems out of curiosity or for bragging have turned to exploiting financial gains. An underground economy has developed where hackers and criminals buy and sell credit card numbers and bank account information. Hackers have shifted toward a “professionalization” of computer crimes (Richardson, 2007).

Facing the new trends in hacker groups and their activities, it is timely and important to study hacker’s social network structure (Parsky, 2006). This study proposes a research model including five dimensions and their relations to study hacker’s social organization. This model allows us to have a novel perspective on the social organization of hacker groups and place hackers in the whole network context to examine relations such as hacker to hacker, hacker to technology, and hacker to resource. Understanding social organizational structure of hacker groups enables us to identify vulnerabilities of the network and we have a much better chance to thwart hacker criminal activities. This research examines a criminal hacker network, Shadowcrew, to disclose its fundamental social structure that hackers used to organize themselves to pursue hacking activities.

The remainder of this article is organized as follows. Section 2 reviews the previous research on hacker’s social organization. A research model and research questions are proposed in Section 3. Section 4 is the research methodology, including data collection and data processing. Section 5 is the data analysis and results. Lastly, the researcher concludes the study in Section 6 and suggests future research directions.

SOCIAL ORGANIZATION OF HACKERS

Best and Luckenbill (1980) define social organization as the patterns of relationships among people and social organization as a network of social relations. The focus of social organization study is “a group or a pattern of social interaction, rather than the individual or the society” (Best and Luckenbill, 1994, p. 4). Therefore, the social organization of deviants refers to “the patterns of relationships among deviant actors involved in the pursuit of deviance” (p. 11). Studies of the social organization of deviants inform our understanding of the social aspects of them. Most deviants have relationships with one another and form associations. Thus, the social organization perspective allows researchers to consider how these relationships form, persist, and operate (Best and Luckenbill, 1994).

Best and Luckenbill (1994) offer a comprehensive theoretical framework for understanding the social organizational features of deviants. They classify five basic forms of deviants according to the dimension of organizational sophistication: loners, colleagues, peers, teams, and formal organizations. These organizational forms are defined in terms of four variables: mutual association,