Taylor & Francis
Taylor & Francis Group

Journal of Computer Information Systems

ISSN: 0887-4417 (Print) 2380-2057 (Online) Journal homepage: https://www.tandfonline.com/loi/ucis20

Social Network Analysis of a Criminal Hacker Community

Yong Lu, Xin Luo, Michael Polgar & Yuanyuan Cao

To cite this article: Yong Lu, Xin Luo, Michael Polgar & Yuanyuan Cao (2010) Social Network Analysis of a Criminal Hacker Community, Journal of Computer Information Systems, 51:2, 31-41, DOI: 10.1080/08874417.2010.11645466

To link to this article: https://doi.org/10.1080/08874417.2010.11645466

Published online: 11 Dec 2015.

Submit your article to this journal

Article views: 499

View related articles

Citing articles: 2 View citing articles

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=ucis20

SOCIAL NETWORK ANALYSIS OF A CRIMINAL HACKER COMMUNITY

YONG LU
Pennyslvania State University
Hazleton, PA 18202

MICHAEL POLGAR
Pennsylvania State University
Hazleton, PA 18202

XIN LUO*
The University of New Mexico
Albuquerque, NM 87131

YUANYUAN CAO
Xi’an Jiaotong University
Shanxi Province 710061, China

ABSTRACT

Computer crime hackers have been identified as a primary threat to computer systems, users, and organizations. Much extant research on hackers is conducted from a technical perspective and at an individual level of analysis. This research empirically examines the social organization of a hacker community by analyzing one network called Shadowcrew. The social network structure of this infamous hacker group is established using social networking methods for text mining and network analysis. Analysis of relationships among hackers shows a decentralized network structure. Leaders are identified using four actor centrality measures (degree, betweenness, closeness, and eigenvector) and found to be more involved in thirteen smaller sub-groups. Based on our social network analysis, Shadowcrew exhibits the characteristics of deviant team organization structure.

Keywords: hacker; hacker groups; Shadowcrew; social organization; network analysis

1. INTRODUCTION

As organizations are increasingly dependent on information technologies for sustainability and profitability, defending digital information assets against misuse or hacking has assumed vital importance. This serious phenomenon, coupled with burgeoning occurrences of information security breaches, is amplified in a plethora of business scenarios. In essence, identity theft and financial fraud conducted by hackers have evolved into serious and pervasive threats to consumers and the financial services industry. Computer hackers, both individually and as a group, have been identified as a primary threat to computer systems and users [18]. The CSI 2008 Computer Crime & Security Survey, the world’s most widely quoted survey on computer crime, found that financial fraud and identity theft conducted by hackers had a high cost to organizations, with an average loss close to $500,000 for each respondent’s organization [39]. Financial institutions lose billions of dollars each year to identity theft and consumers face additional hardships. The Federal Trade Commission (FTC) estimated that 8.3 million American consumers, or 3.7 percent of the adult population, became victims of identity theft in 2005.

To combat the computer and information security problems, a new industry has emerged to provide numerous products and solutions, including firewalls, encryption systems, operations security, virtual private networks (VPN), physical security, access controls, and biometrics. However, these technologies are not used as often as they could be, due in part to lack of user awareness or dearth of expertise [12, 14].

Much of the extant research on information security has been at the technical level and conducted primarily by computer scientists, mathematicians, and computer engineers [44]. Information security publications tend to employ one logical methodology: describe the security issue, offer options for a solution, and then describe technological procedural alternatives for each potential solution [47]. Furthermore, information security is not merely a matter of technological advancements and cannot be addressed satisfactorily with hardware and software alone. Rather, information security is also a matter of understanding and managing people who interact with technologies and practice security countermeasures [28, 37]. This comprehensive perspective is grounded in the fact that success of computer security depends on the effective behavior of users [42]. As such, the salient key to derailing potential security threats is an amalgamation of technical and behavioral as well as procedural countermeasures. In the arena of information systems (IS) security research, Siponen [41] and Straub *et al*. [44] 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.

Prior studies [43] incorporated the theory of general deterrence into a management decision to invest in IS security and found that security countermeasures resulted in significantly lower computer abuse. In addition, Parker [35] articulated that computer security is not primarily a technological subject but rather a subject of psychological and sociological behavior of people. He argued that computers do neither commit errors, omissions, or crimes nor write viruses. His contention is congruent with different studies by Stanton *et al*. [42], Thomson and Solms [49], Straub and Welke [45] in that most of computer security problems are rooted in human behaviors because people’s misbehaviors may subsequently be manifested in computers. In response, it has been proposed that solutions to these security-related problems, which may be somewhat practically alleviated by technological countermeasures, must also stem from an analysis of people in terms of their actions, their awareness/perceptions, and their attitudes [23, 34, 37, 42, 49]. Notwithstanding these scholarly

** Dr. in Luo is the corresponding author. He can be reached at Luo mgt.unm.edu.*

Received: February 15, 2010 Revised: April 23, 2010 Accepted: June 23, 2010

efforts devoted to gauging and fathoming user behaviors, there is a corresponding lack of knowledge about computer hacking from a psychological or sociological behavior perspective. In essence, empirical evidence for studying how hackers behave in terms of leading and/or responding to communications for malicious activities in online social organizations is still lacking. This paucity of cross-disciplinary and multi-level examination of information security, particularly in the area of hacker studies, motivated us to shed light on this domain.

Academic research from a variety of disciplines has contributed to our understanding of hacker attack methods [18], subculture [48], and motivations [46]. Studies by Meyer [33] and Holt [21] 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 groups or networks to understand social relationships and organizational patterns within hacker communities, as Schultz [40] called for further studies on the relationships with hacker communities. To bridge this gap, this research draws on theories from sociology and examines the social organization of a hacker community from a network perspective and discloses its fundamental social structure that hackers used to organize themselves to pursue hacking activities.

2. RESEARCH PURPOSE

Considering the advancement and rapid development of computer technology and the information security industry over the past decade, we presuppose that it is possible that the nature and structure of hacker communities have changed. For instance, some hackers have become involved in online terrorism [52] or other forms of organized crime [25]. Parsky's legislative hearing in Congress [36] found that a pattern emerged: groups of hackers become profit-driven. 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 wherein hackers and other criminals buy and sell credit card numbers and bank account information. Hackers have organized and shifted toward a "professionalization" of computer crimes [38].

In response to these new trends in hacking groups and activities, this study applies social network analyses and technologies to empirically examine the fundamental social network structure of a hacker group. Recent studies suggest that hackers have grown more sophisticated and are sometimes involved with organized crimes [18, 52]. This implies that more complex hacker social organizations provide greater capacities for their members.

Shadowcrew was a complex and highly-structured malicious hacker group that committed to identity theft and credit card fraud. We use the Shadowcrew network as a case study that may help researchers examine other hacking groups. The use of social network methods can also help future research to study organizational networks and criminal structures.

The remainder of this article is organized as follows. We first revisit hacker history, providing the context for our study. Then we review previous studies on hacker's social organization. This is followed by presenting our research questions that are addressed using social network analysis measures. We then proceed to describe our research methodology. Finally, we present our network data analysis and discuss results. The conclusions are then presented, followed by research limitations and implications.

3. COMPUTER HACKERS

There are several terms attached to hackers and different types of classification systems [18]. This study adopts Holt's definition [21] which refers to a hacker as *any individual with a profound interest in computers and technology that has used this knowledge to access computer systems with or without authorization from the system owners*. Hackers have existed since computing was in its infancy, and have changed computing subcultures and organizations with social movements and improvements in computer technology. In the late 1950s, the term 'hacker' was coined to refer to an unorthodox problem solver and master programmer who developed elegant and innovative solutions to overcome the limitations of early computers [27].

When computer technology moved from universities to military applications in the 1960s, the conception of hacker shifted as a consequence of the turbulent social climate. Hackers of this period believed information should be free to help people understand how things work. This notion became the centerpiece of the ideas of "Hacker Ethic" which formed the roots of the hacker culture [27, 48]. During the 1980s, a new breed of computer users challenged the existing hacker culture. IBM's PC brought computer technology to the new generation and into more businesses and homes than ever. Modems also increased the number of individuals online and changed the shape of the computer underground [18]. Computer Bulletin Board System allowed hackers to form groups for sharing information and bragging about their exploits.

Hacker culture became further divided during the 1980s with the posting of "The Hacker Manifesto" written by a member of a hacker group called "Legion of Doom." The author, named "The Mentor," railed against adults, schools, and law enforcement. He encouraged hackers to explore and seek knowledge even if they break into computer and network systems. This document demonstrated the increasing criminal nature of hacker activities. The growing security incidents and criminal cases on cyberspace also reinforced the notion of hackers as digital cowboys or outlaws on the electronic frontier [18, 20].

With the boom of the World Wide Web and the ubiquity of the PC in the 21st century, actions, groups, and representations of hackers became further differentiated by motivation, affiliation, and activity. More advanced technologies have become available for hackers and new web communication tools now can connect the hacker group members with more cohesion. The wide-spread hacking resources and skills attract more and more newcomers. Spurred by big profits, professional criminal hackers have replaced amateur thrilling-seeking hackers and represented as the biggest threat on the Internet [38, 48]. Hacker groups are becoming involved in more complex socio-technical systems, which require us to take new approaches to study hacker communities and their activities.

4. SOCIAL ORGANIZATIONS OF HACKERS

Best and Luckenbill [4] defined social organization as *the patterns of relationships among people and more specifically as a network of social relations*. Traditionally, many social researchers have examined patterns or networks at either a social psychological or social structural level of analysis. Social psychological analysis makes the individual the center of attention, explaining individual behaviors (such as goals or means to these goals) in relation to social norms and conditions [32]. At a wider level of analysis, structural research examines larger and more formal behaviors, linkages, and organizations, identifying social structures and comparing groups of people in firms, social networks, or even entire social institutions [4].

Studies of social organization reflect an intermediate level between the social psychological and social structural levels. In organizational studies, the focus is a group or a pattern of social interaction rather than the individual or the society [4]. Therefore, the social organization of deviants refers to the patterns of relationships among deviant actors involved in the pursuit of deviance. Studies of the social organization of deviants move beyond analyses of deviant individuals and behaviors to inform our understanding of both the social forces leading to deviance and the social structures of deviant groups [13]. In other words, why do deviant groups evolve and how are they organized?

Best and Luckenbill [3-4] offered a theoretical framework to understand the social organization of deviants and deviant groups. They classified deviants into five levels of organizational sophistication based on four characteristic dimensions (see Table 1). Formal organizations are extended, with elaborate division of labor, mutual participation and association. Teams lack extended organization, while peers also lack elaborate division of labor. Colleagues are characterized only by mutual association.

Using this framework, a study by Meyer [33] found that hackers were colleagues because they formed a subculture and shared information but they did not participate in hacking with others. Holt [21] also applied this framework to study the subculture and social organization of hackers. He found that hackers tended to perform hacks alone but had loose social networks to share information and introduce sub-cultural norms to new hackers. The organizational form of deviant groups may be related to the scope of harm caused by deviants. Best and Luckenbill [3] described five propositions about this relationship between social organization and harm. They suggested that more complex deviant social organization is associated with greater capacity for deviance, more extensive socialization and membership services, more security, and greater involvement in deviance among members.

Although previous studies have provided great insight into the values and beliefs that hackers hold, they have some limitations that should be addressed. First, much extant research on hackers has been conducted at the individual level. These prior studies only examined the elements from an individual hacker's perspective, treating elements such as technology, knowledge, and resource as the characteristics or attributes of a hacker. Meyer [33] and Holt [21] applied qualitative methods to classify hackers as colleagues, but they did not locate organizational forms along with a dimension of social organization or examine the consequences of organizational variation among hackers.

Moreover, several researchers suggest that hackers have grown more sophisticated and sometimes constitute teams. In fact, several hacker groups appear to meet the criteria of a team, including the Chaos Computer Club, the Cult of the Dead Cow, and the l0pht [18]. There is also growing evidence that hackers are sometimes involved in organized crimes [52] or terrorist groups [25]. This trend implies that increasingly complex deviant social organization is linked to greater capacity for deviance by the members. Given these limitations of previous research and new trends among hacker groups as well as the potential association between organizational complexity and harm caused by deviance, it is important to undertake new analyses on hacker groups. It is also useful to examine the social organization of computer hackers with new approaches and to build our understanding of the current nature of hackers' organizational relations and patterns.

5. RESEARCH QUESTIONS FOR SOCIAL NETWORK ANALYSIS

Social network analysis (SNA) techniques are designed to discover patterns of interaction between social actors in social networks. They are especially useful for studying criminal networks including those associated with computer hackers [31]. In essence, SNA is capable of empirically uncovering network organization, identifying central individuals, discovering patterns of interaction, and detecting subgroups [11, 53]. SNA helps discover the roles and importance of members in a hacker community, potentially providing leverage against harmful activities by a hacker group.

All social networks consist of two sorts of elements: actors and relations between actors. In graph theory, these elements are called nodes and links. In many studies of social networks, actors are people, with characteristics or attributes such as age, sex, education, criminal record, physical strength, and temperament. In our analyses, actors are computer hackers or agents involved in a criminal network. A relationship or linkage *may* or may not exist between two people. The existence of a relationship indicates that both persons are directly linked to each other; the nature and strength of relationships may also vary.

In addition to relational or structural forms among people, there are three other important aspects of social networks: the characteristics of the network structure as a whole (e.g. network centralization), the characteristics of a position that a person occupies in a network structure (e.g. actor centrality), and subgroups with a network. In this paper, we study and describe a hacker network using specific social network measures. We use measures of social network centralization to describe the structure of the network. We use several centrality measures to describe

TABLE 1: Characteristics of Social Organization of Deviants

	Characteristic			
Form of Organization	Mutual association	Mutual participation	Elaborate division of labor	Extended organization
Loners	No	No	No	No
Colleagues	Yes	No	No	No
Peers	Yes	Yes	No	No
Teams	Yes	Yes	Yes	No
Formal organizations	Yes	Yes	Yes	Yes

network leadership. We apply betweenness centrality to examine the influence of leaders. Finally, we employ analysis of cliques to identify and describe subgroups in the network.

Building on existing research and social network research methods, this article addresses four specific research questions:

1. What is the *network centralization* of a computer hacker network?
2. Are there members of a hacker network who stand out as critical *leaders*?
3. How strongly do leaders *influence* a hacker network?
4. What *subgroups* exist and interact in a hacker network?

We will call these questions of *network centralization, leadership, leadership influence,* and *subgroups*. Our research develops and uses empirical methods to identify a hacker community and to analyze their social and structural relationships. A clear understanding of these structural properties in a hacker network may help analysts more efficiently and effectively target critical network members for surveillance or removal and secure network vulnerabilities from disruptive actions.

5.1. Network Centralization

Network centralization is a quality of a group. It indicates the extent to which a network is organized around one or more central points, such as a node or a centroid [17, 51]. More centralized networks exhibit a wheel-like structure (see Figure 1) where a smaller number of nodes in the center are surrounded by larger numbers of other nodes. In more decentralized networks, nodes in the network are more equally interconnected. Therefore, centralization also reflects variability in measures of actor centrality. Centralization is one measure of the integration or cohesion of a network. In the most centralized network, one actor has a high centrality score while others have low centrality scores. In a more decentralized network, actors have similar centrality scores, while no single actor 'stands out.'

Three commonly used measures for network centralization include degree centralization, betweenness centralization, and closeness centralization [17]. Degree centralization is higher when centralized actors have a high number of direct relationships or ties with a large number of other network members, while peripheral actors have fewer relationships (as in a wheel structure). It is the lowest when actors have equal numbers of relationships (as in a circle graph). Betweenness centralization reflects the extent to which actors occupy positions between two or more network members. Group closeness centralization is related to centralized actors who are able to traverse a small number of relations to reach all other members. It is the highest in a star graph (e.g. Figure 1).

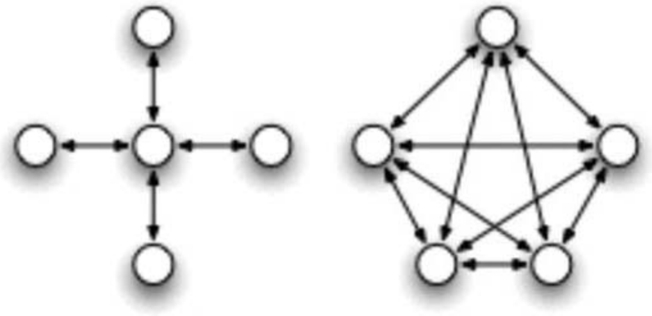


Figure 1: A Centralized Network and A Decentralized Network

5.2. Actor Centrality and Leadership

One of the primary uses of SNA is the identification of the most central or most well-connected actors in a network. Actor centrality is based on the concept that "actors, who are the most important or the most prominent, are usually located in strategic locations within the network" [51]. Centrality measures such as degree, betweenness, closeness, and eigenvector centrality indicate the importance of an actor in a network (see Table 2).

Degree centrality measures who are the most involved in a network of relationships. It is defined as the number of possible direct links. Actors with high degree scores are often leaders, experts, or hubs in a network. It has been shown that these popular nodes can be a network's "Achilles' Heel" whose failure or removal will cause the network to quickly fall apart [2, 22].

Betweenness centrality measures the extent to which a particular actor lies between other nodes in a network. The betweenness of a node is defined as the number of geodesics (shortest paths between two nodes) passing through it. Betweenness measures information flows through an individual. It can show whether an individual plays the role of a broker or gatekeeper. A broker exchanges between two other actors, and a gatekeeper withholds information from passing between actors. Removing an actor with high betweenness can disrupt the flow of information through the network and cause fragmentation.

Closeness centrality reflects how close an actor is to the other actors in a network. It is the average distance of an actor to the other actors in a network (e.g. the highest in a star network, Figure 1). This measures how easy it is for one actor to be able to communicate with others in the network.

Eigenvector Centrality reflects one's connections to other well-connected people. An individual has a high eigenvector centrality if the person is connected to many agents that are themselves well-connected. An individual connected to many isolated people in an organization will have a much lower score. Isolation of the individual who has a high eigenvector centrality is likely to have little effect on the network [5].

5.3. Cliques and Subgroups

A network can often be partitioned into subgroups consisting of individuals who closely interact with each other. A clique in a network is a maximal complete sub-graph of three or more nodes, all of which are adjacent to each other while there are no other nodes that are also adjacent to all the members of the clique [51]. There are certain sub-groups of a network in which the actors have more relevant ties and are more closely and intensely tied to one another than they are to other actors in the network. Clique measures can help answer these questions:

1. Are there particular actors that appear to play network roles? For example, do some act as leaders, nodes that connect a graph, or who are isolated from groups?
2. How separate are the cliques or sub-graphs? Do they overlap and share members, or do they divide a network into factions?

6. DATA COLLECTION AND DATA PROCESSING

6.1. The Research Setting

The research examined the social organization of an international hacker network called Shadowcrew, which engaged

TABLE 2: Measures of Centrality in a Network

Type of Centrality	Meaning	Interpretation
Degree	A node has high degree centrality in a network if it is directly connected to a larger number of other nodes.	Individual more likely to diffuse new information and more likely to know information. Isolation of this person may impair a network or system.
Betweenness	A node has high betweenness if more often falls along (geodesic) paths between other nodes in a network.	Individual plays role of a broker or gatekeeper. Removing an actor with high betweenness can disrupt the flow of information through the network and cause fragmentation.
Closeness	A node is close to others in a network if it has a low average distance (a shorter path) to the other actors.	Individual can more easily 'reach' others in a network, minimizing degrees of separation. For example, it can show how easy it is for one actor to communicate with others in a network.
Eigenvector	A node has a high eigenvector centrality if it is connected to many others that are themselves well-connected.	Individual who is most connected to most other critical people. Isolation of this person is likely to have little effect.

in identity theft and credit card fraud. In 2004, the U.S. Secret Service concluded Operation Firewall, an 18-month investigation into members of the Shadowcrew Website where blocks of purloined card numbers were bought and sold. This investigation led to the arrests of more than twenty individuals in the United States and several individuals in foreign countries [50]. The U.S. Department of Justice described the Web site, http://www.shadowcrew.com, as one of the largest illegal online centers for illegitimate identification and credit information.

Before Shadowcrew was shut down, it had members from around the globe engaged in malicious computer hacking and dissemination of stolen credit cards, debit cards, bank account numbers, and falsified identity documents. The Department of Justice alleged that Shadowcrew members bought and sold about 1.7 million stolen credit card numbers which caused losses to merchants, banks, and others in excess of $4 million. Former U.S. Attorney Scott Christie claimed that the business Shadowcrew conducted proved these gangs were "highly structured and very well organized" [30]. Shadowcrew was organized into different levels of power as Administrators, Moderators, Reviewers, Vendors, and General Members. Shadowcrew is such a significant and complex network organization that it becomes an appropriate case for us to study hacker social organizations.

6.2. Data Collection

One hundred and eighty two texts were collected and formed the original data set for this study of Shadowcrew. Of these texts, 157 were collected through LexisNexis Academia via an exact matching Boolean Keyword search for "Shadowcrew." The media searched with LexisNexis included major newspapers, magazines, journals, and law reviews such as *The New York Times*, *The Washington Post, USA Today, Business Week, U.S. Fed News*, and *Department of Justice Documents*. The time frame for the data set was all available dates. According to the LexisNexis sorting function, the most relevant articles were selected. Sources for the 25 other texts identified using Google were open source web sites, trial transcripts, and a key court proceedings.

After collecting the 182 original texts, researchers carefully reviewed each text to make sure it was relevant to the research subject. Duplicate copies were deleted, leaving 115 texts for further data analysis, which is referred to as Shadowcrew data set. Table 3 lists the sources of these 115 texts. This Shadowcrew data set contained 14,222 unique concepts and 185,102 total concepts. A concept is a single idea represented by a single word or a phrase, which is displayed as a node in a network map [15]. The number of unique concepts considered each concept only once, whereas the much larger number of total concepts also considers repetitions of concepts per text.

Texts are a widely used source of information to study criminal and covert groups [9]. In general, the credibility of the coding samples can be increased by using a large corpus that integrates various text types from a variety of sources [10]. This Shadowcrew data set is suitable to study Shadowcrew's network because this data set is from many different sources, such as newspapers,

TABLE 3: List of text sources

Publication name	Number of texts
U.S. Fed News	12
International Herald Tribune	10
The New York Times	10
Government Publications & Documents	9
Baseline Magazine.com	8
Department of Justice Documents	8
eWeek.com	7
The Business	7
Business Week	6
Newsweek	5
USA Today	5
The Washington Post	5
Berkeley Technology Law Journal	4
CQ Federal Department and Agency Documents	4
U.S. Newswire	4
Wall Street Journal Abstracts	3
U.S. District Court Cases, Combined	3
CNNMoney.com	2
Kiplinger Publications	1
The New Zealand Herald	1
New England Journal on Criminal and Civil Confinement	1
Total	115

journals, magazines, web pages, and court proceedings. Since the Shadowcrew Website (http://www.shadowcrew.com) was shut down by the law enforcement agencies, text searching is the only possible approach for collecting information about this hacker group from public sources.

6.3. Data Processing: From Texts to Meta-Matrix Data

AutoMap, an emerging text mining tool [15], was employed to extract the social organizational network from the Shadowcrew data set. The quality of the network (or map) extracted from the text can be enhanced by pre-processing the data prior to running the analysis. Text pre-processing condenses the data to the concepts that capture the features of the texts that are relevant in a certain context or corpus. In AutoMap, pre-processing is a semi-automated process that involves four major techniques: named-entity recognition, deletion, stemming, and thesaurus creation and application [16].

Named-entity recognition retrieves proper names (i.e., people, places, and organizations), numerals, and abbreviations from texts [29]. Deletion removes non-content bearing concepts such as conjunctions and articles from text, thus reducing the number of concepts needed to be considered when creating thesauri [8]. Stemming detects inflections and derivations of concepts in order to convert each concept to its respective morpheme [24]. KSTEM stemmer was implemented in the pre-processing [26]. Thesaurus creation and application associates specific concepts with more abstract concepts (generalization thesaurus) or meta-matrix entities (meta-matrix thesaurus). A generalization thesaurus translates text-level concepts into higher-level concepts. The researchers created a generalization thesaurus that associates the instances of relevant named entities, aliases, and misspellings. A meta-matrix thesaurus associates text terms with meta-matrix entities, thus enabling the extraction of the structure of social and organizational networks from textual data. In texts, the links between words (concepts) are implicit. Therefore, extracting a network from a text requires an inference process. The links between concepts must be extracted based on the semantic, syntactic, and contextual information given in a text [16]. In the next step, the researchers applied the thesaurus to the Shadowcrew data set and conducted multiple sub-matrix text analysis in AutoMap. One network for Shadowcrew Data Set was extracted for network analysis.

7. NETWORK DATA ANALYSIS AND RESULTS

Organizational Risk Analyzer [7] and UCINET [6] were used to visualize the network and generate reports. Several features of the visualized network stand out (see Figure 2). There are a total of twenty three nodes (agents) and three of these nodes are isolates (agents who are not directly linked to other agents). They are Albert Gonzalez, Chad Hatten, and Karin Andersson, who are shown on the top-right of Figure 2. There are two agents, Alexsi Kolarov and Kaspar Kivi, who are connected with each other but separate from other agents.

Network centralization looks at the centrality measures at a network wide level. It demonstrates how centralized or decentralized the network is as a whole. The values for network degree, network betweenness, and network closeness are 26.9%, 4.1%, and 9%, respectively. All these three measures are relatively low. This implies that, in general, Shadowcrew is a decentralized network. To identify leadership, we then generate and compare measures of actor centrality. Table 4 shows the top five individuals in the network according to four centrality measures that determine an individual's prominence or importance in the network. The table is annotated with the meaning and a potential interpretation for each measure.

Degree centrality measures how many other people are connected to a particular agent. An individual has high degree of centrality when connected to a larger number of others. In Table 4, Brandon Monchamp and Andrew Mantovani have the highest values of degree centrality, and thus are most likely to know or

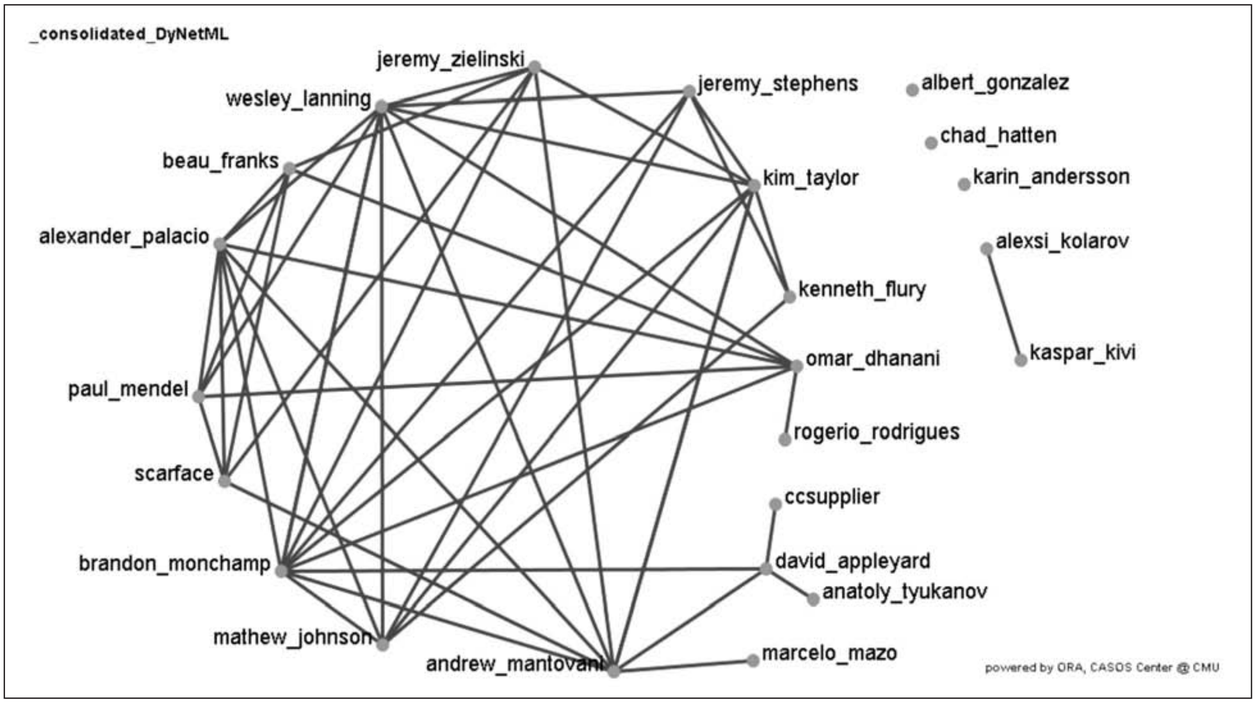


Figure 2: Agent Network for Shadowcrew

diffuse new information. Isolation of either person could cripple the network for a short time [10, 51].

Betweenness shows that information can most easily flow through an agent. In Table 4, Scarface has the highest value of betweenness, serving a broker or gatekeeper, while Mantovani scores almost as high. Removing a person who is centrally located between others can disrupt the flow of information and cause fragmentation of a network. Closeness measures how close an agent is to the other agents. In Table 4, Kenneth Flury has the highest value of closeness, which means it is easy for him to communicate with others in the network. Mantovani is nearly as close as to other agents, reinforcing that he plays a central leadership role. Eigenvector centrality reflects one's connections to other well-connected people. An individual has a high eigenvector centrality if the person is connected to many agents that are themselves well-connected. Isolation of the individual who has a high eigenvector centrality is likely to have little effect to the network [5]. In Table 4, Andrew Mantovani has the highest eigenvector centrality value, indicating that he is connected to most other critical individuals.

TABLE 4: Key Actors

Measure	Rank	Value	Name of agent
Degree centrality	1	0.977	Brandon Monchamp
	2	0.909	Andrew Mantovani
	3	0.568	David Appleyard
	4	0.500	Wesley Lanning
	5	0.432	Kim Taylor
Betweenness	1	0.178	Scarface*
		0.175	Andrew Mantovani
		0.116	Paul Mendel
		0.083	Wesley Lanning
		0.068	Alexander Palacio
Closeness	1	0.138	Kenneth Flury
		0.133	Andrew Mantovani
		0.130	Kim Taylor
		0.128	Scarface*
		0.120	Beau Franks
Eigenvector centrality	1	0.241	Andrew Mantovani
	2	0.223	David Appleyard
	3	0.143	Brandon Monchamp
	4	0.066	Kim Taylor
	5	0.060	Wesley Lanning

* This is the nickname or member ID for the person.

Table 4 clearly indicates that Andrew Mantovani stands out in almost every category. He is ranked first in eigenvector centrality and second in degree centrality, betweenness, and closeness. These results make sense because Andrew Mantovani is one of the co-founders and administrators of Shadowcrew network. Because Andrew Mantovani stands out as a key agent, we should know how this individual could be influenced and whom he may influence. To unveil this, we look at the sphere of influence around him. The sphere of influence for an individual identifies the set of actors that influence and are influenced by that actor [10]. Among all twenty three people in the network, there are eight agents who connect directly to Mantovani, including many of the other central figures such as Monchamp and Scarface (see Figure 3). This graph shows that leaders are related to other central figures, and thus can have a high degree of actual and potential influence.

A clique is a sub-set of a network in which the agents are closely tied to one another. As shown in Table 5, there are 13 cliques in this network. Two cliques (#1 and #2) are composed of 5 of the 23 agents. Seven cliques (#3, #4, #5, #7, #11, #12, and #13) are composed of 4 of the 23 agents. Four cliques (#6, #8, #9, and #10) are composed of 3 of the 23 agents. Figure 4 shows that there are seven agents who do not belong to any clique.

Furthermore, Figure 5 presents how "adjacent" each agent (row) is to each clique (column). Rogerio Rodrigues, for example, is adjacent to one fourth of the members of clique #5. Four agents, Brandon Monchamp, Adrew Mantovani, Wesley Lanning, and Alexander Palacio, are adjacent to one or more members of all the 13 cliques. This implies that those four agents can disseminate information to each or all of the 13 sub-groups.

We are also interested in the extent to which these sub-groups overlap. As such, we examine these questions by looking at share

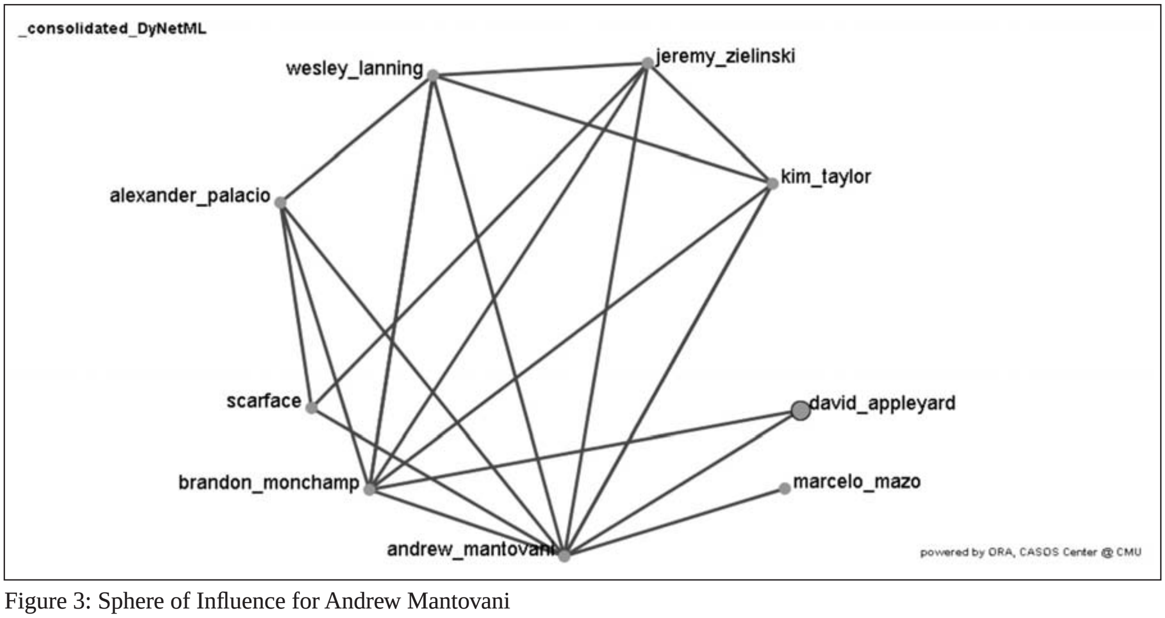


Figure 3: Sphere of Influence for Andrew Mantovani

membership in a clique. As shown in Figure 6, the two agents Wesley Lanning and Brandon Monchamp are "closest" in the sense that they share membership in five of the thirteen cliques.

8. SUMMARY AND DISCUSSION

Much extant research on hackers has been conducted from a technical perspective and at an individual level of analysis. To further extend this line of research, we suppose that social network analysis can be used as an instrumental tool for locating important individuals within current hacking groups by examining news reports, court proceedings, and other communication documents. We believe this network approach can provide important and valuable information to IS researchers and information security practitioners. In essence, this research employed social network analysis to describe the social network structure of a criminal computer hacker group. Quantitatively summarizing relationships among hackers culled from a set of 115 textual documents containing over 14,000 unique concepts, we were able to synthesize empirical data about Shadowcrew's membership and social organization.

To answer the research questions relating to the structure of a modern hacker network, the possible leadership cues and influences in such a network, and the existence of subgroups and their relationships with other social networking members, we found that Shadowcrew is a decentralized network including several influential leaders. We identified leaders that have high scores on multiple indicators of network centrality. We then showed that one leader could influence many others in the network, illustrating this influence with a network graph. We quantified the relationships among twenty-three individuals and empirically identified several group leaders. Finally we quantified each person's connections to any of thirteen sub-groups or cliques within the hacker network. Analyses of cliques show that some

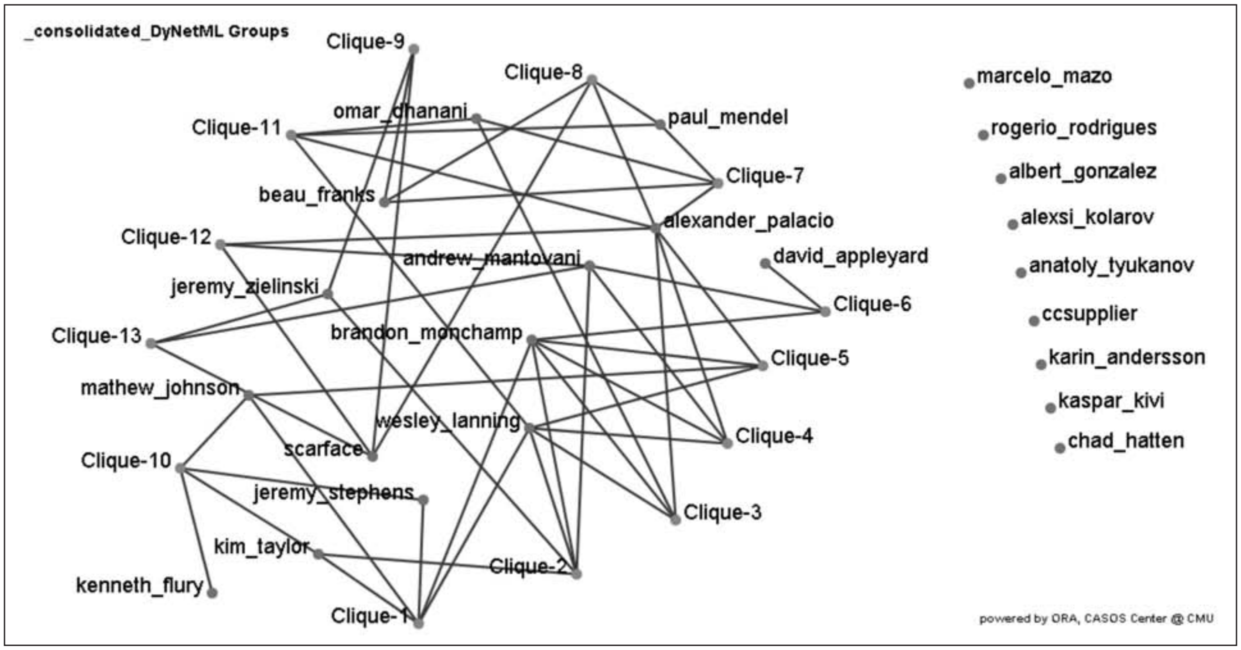


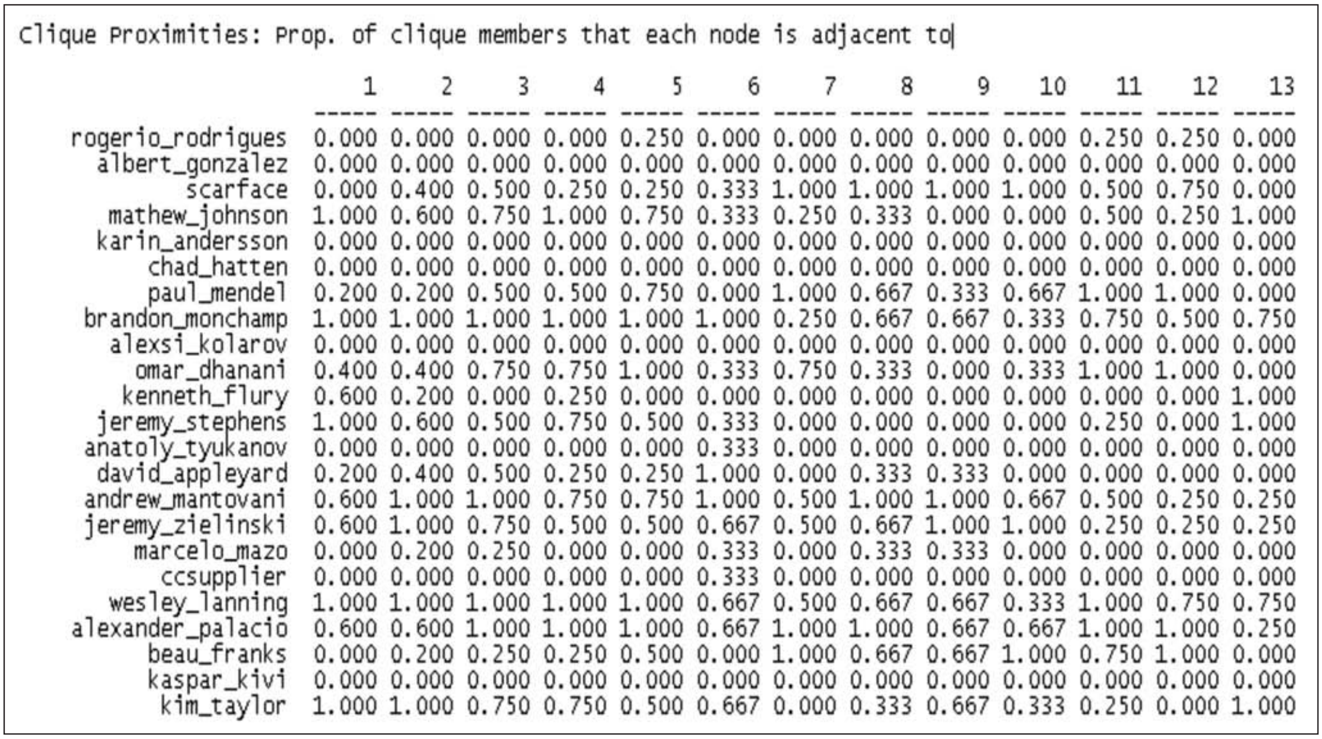
Figure 4. Cliques

TABLE 5: Cliques

Clique#	Agents				
1	Mathew Johnson	Brandon Monchamp	Jeremy Stephens	Wesley Lanning	Kim Taylor
2	Brandon Monchamp	Andrew Mantovani	Jeremy Stephens	Wesley Lanning	Kim Taylor
3	Brandon Monchamp	Andrew Mantovani	Wesley Lanning	Alexander Palacio	
4	Mathew Johnson	Brandon Monchamp	Wesley Lanning	Alexander Palacio	
5	Brandon Monchamp	Omar Dhanani	Wesley Lanning	Alexander Palacio	
6	Brandon Monchamp	David Appleyard	Andrew Mantovani		
7	Scarface	Paul Mendel	Alexander Palacio	Beau Franks	
8	Scarface	Andrew Mantovani	Alexander Palacio		
9	Scarface	Andrew Mantovani	Jeremy Zielinski		
10	Scarface	Jeremy Zielinski	Wesley Lanning	Alexander Palacio	
11	Paul Mendel	Omar Dhanani	Alexander Palacio	Beau Franks	
12	Paul Mendel	Omar Dhanani	Alexander Palacio	Beau Franks	
13	Mathew Johnson	Kenneth Flury	Jeremy Stephens	Kim Taylor	

members of the hacker network were more directly involved in sub-groups than others.

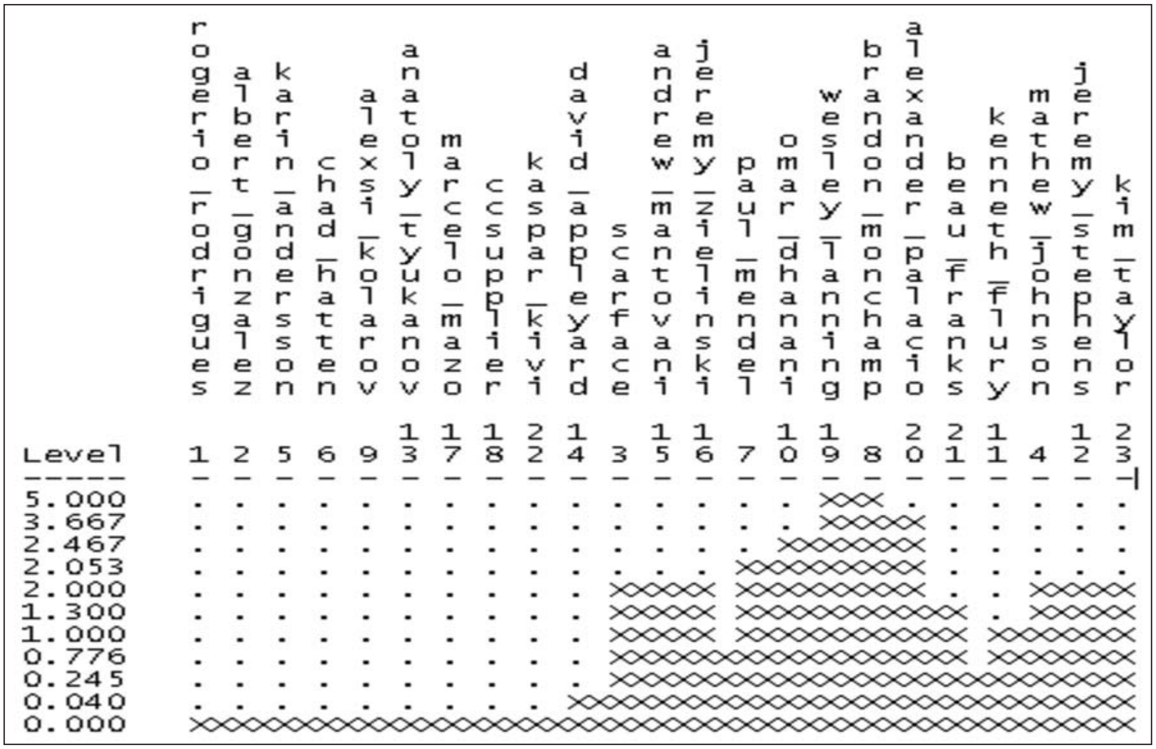
Previous studies have indicated that computer hackers were often loosely affiliated as colleagues and sometimes more organized as peers or teams [4]. Although we showed that the Shadowcrew hackers were part of a decentralized network, not everyone in this group had the same type of role or position. It was organized into different power as administrators, moderators, reviewers, vendors, and general members, which suggests that Shadowcrew had elaborate division of labor. In sum, Shadowcrew had the three characteristics of a team as Best & Luckenbill (1994) proposed: elaborate division of labor, mutual participation, and association. Therefore, we concluded that Shadowcrew had developed a team organization structure.



```
Clique Proximities: Prop. of clique members that each node is adjacent to|

                        1     2     3     4     5     6     7     8     9    10    11    12    13
                    ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- -----
 rogerio_rodrigues  0.000 0.000 0.000 0.000 0.250 0.000 0.000 0.000 0.000 0.000 0.250 0.250 0.000
   albert_gonzalez  0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000
          scarface  0.000 0.400 0.500 0.250 0.250 0.333 1.000 1.000 1.000 1.000 0.500 0.750 0.000
     mathew_johnson 1.000 0.600 0.750 1.000 0.750 0.333 0.250 0.333 0.000 0.000 0.500 0.250 1.000
    karin_andersson 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000
        chad_hatten 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000
        paul_mendel 0.200 0.200 0.500 0.500 0.750 0.000 1.000 0.667 0.333 0.667 1.000 1.000 0.000
   brandon_monchamp 1.000 1.000 1.000 1.000 1.000 1.000 0.250 0.667 0.667 0.333 0.750 0.500 0.750
     alexsi_kolarov 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000
       omar_dhanani 0.400 0.400 0.750 0.750 1.000 0.333 0.750 0.333 0.000 0.333 1.000 1.000 0.000
      kenneth_flury 0.600 0.200 0.000 0.250 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 1.000
    jeremy_stephens 1.000 0.600 0.500 0.750 0.500 0.333 0.000 0.000 0.000 0.000 0.250 0.000 1.000
   anatoly_tyukanov 0.000 0.000 0.000 0.000 0.000 0.333 0.000 0.000 0.000 0.000 0.000 0.000 0.000
    david_appleyard 0.200 0.400 0.500 0.250 0.250 1.000 0.000 0.333 0.333 0.000 0.000 0.000 0.000
   andrew_mantovani 0.600 1.000 1.000 0.750 0.750 1.000 0.500 1.000 1.000 0.667 0.500 0.250 0.250
   jeremy_zielinski 0.600 1.000 0.750 0.500 0.500 0.667 0.500 0.667 1.000 1.000 0.250 0.250 0.250
       marcelo_mazo 0.000 0.200 0.250 0.000 0.000 0.333 0.000 0.333 0.333 0.000 0.000 0.000 0.000
         ccsupplier 0.000 0.000 0.000 0.000 0.000 0.333 0.000 0.000 0.000 0.000 0.000 0.000 0.000
     wesley_lanning 1.000 1.000 1.000 1.000 1.000 0.667 0.500 0.667 0.667 0.333 1.000 0.750 0.750
  alexander_palacio 0.600 0.600 1.000 1.000 1.000 0.667 1.000 1.000 0.667 0.667 1.000 1.000 0.250
        beau_franks 0.000 0.200 0.250 0.250 0.500 0.000 1.000 0.667 0.667 1.000 0.750 1.000 0.000
        kaspar_kivi 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000
         kim_taylor 1.000 1.000 0.750 0.750 0.500 0.667 0.000 0.333 0.667 0.333 0.250 0.000 1.000
```

Figure 5: Clique Proximities



```
          r                                  a
          o         a           a j       b l
          g a k     n       d   n e       r e       j
          e l a   a a       a   d r     w a x     m e
          r b r   l t       v   r e     e n a   k a r
          i e i   e o m     i   e m   o s d n   e t e
          o r n c x l a   k d   w y p m l o d b n h m
          _ t _ h s y r c a _   _ _ a a e n e e n e y k
          r _ a a i _ c c s a   m z u r y _ r a e w _ i
          o g n d _ t e s p p s a i l _ _ m _ u t _ s m
          d o d _ k y l u a p c n e _ d l o p _ h j t _
          r n e h o u o p r l a t l m h a n a f _ o e t
          i z r a l k _ p _ e r o i e a n c l r f h p a
          g a s t a a m l k y f v n n n n h a a l n h y
          u l s t r n a i i a a a s d a i a c n u s e l
          e e o e o o z e v r c n k e n n m i k r o n o
          s z n n v v o r i d e i i l i g p o s y n s r

                    1 1 1 2 1   1 1   1 1   2 2 1   1 2
Level     1 2 5 6 9 3 7 8 2 4 3 5 6 7 0 9 8 0 1 1 4 2 3
-----     - - - - - - - - - - - - - - - - - - - - - - -|
5.000     . . . . . . . . . . . . . . . XXX . . . . . .
3.667     . . . . . . . . . . . . . . . XXXXX . . . . .
2.467     . . . . . . . . . . . . . . XXXXXXX . . . . .
2.053     . . . . . . . . . . . . . XXXXXXXXX . . . . .
2.000     . . . . . . . . . . XXXXX XXXXXXXXX . . XXXXX
1.300     . . . . . . . . . . XXXXX XXXXXXXXXXX . XXXXX
1.000     . . . . . . . . . . XXXXX XXXXXXXXXXX XXXXXXX
0.776     . . . . . . . . . . XXXXXXXXXXXXXXXXX XXXXXXX
0.245     . . . . . . . . . . XXXXXXXXXXXXXXXXXXXXXXXXX
0.040     . . . . . . . . . XXXXXXXXXXXXXXXXXXXXXXXXXXX
0.000     XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

FIGURE 6: Hierarchical Clustering of Overlap Matrix

9. RESEARCH LIMITATIONS

We are aware that research on IS can be carried out in a wide range of settings and by a variety of strategies, and acknowledge that there is no perfect research because different strategies carry comparative strengths and weaknesses. In the future, prospective studies can extend our knowledge in two major directions, addressing some limitations of this study.

First, single group studies have limited generalizability. This study is no exception. Future studies should examine other settings to see if the research methods and findings can be applied to other hacker communities. The current study only investigated one malicious hacker group. Although Shadowcrew is a significant and complex case, further studies for other types of hacker groups (e.g., centralized communities) would extend our understanding of hacker social organization.

Second, this study collected data from text searching and extracted the social network from text documents (i.e., newspaper articles, trial transcripts, and court proceedings) because the Shadowcrew Website was shut down by the law enforcement agencies. Future studies are expected to collect data from existing hacker Web sites, blogs, and forums. One of the most important elements of hackers is their relationship to technology. As it is increasingly evident that hackers utilize new Web tools for communication and social networking [36], it would be interesting to reveal the social network structure from their Web activities.

10. IMPLICATIONS FOR RESEARCH

Although computer hackers are often organized criminals, extant research on hackers has been conducted at the individual level of analysis. Behavioral, analytical, and empirical research approaches in this particular arena are limited. Our research drew on theories from sociology and examined the social organization of a hacker community from a network perspective. Based on the empirical evidence, we were able to disclose the social organization's fundamental social structures, such as decentralized network, leadership, spheres of influence, and cliques, which hackers used to organize themselves.

This network approach to studying hacker groups provides more comprehensive insights to their criminal activities and organization patterns. This study can pave the way for future studies on criminal organization networks. For instance, we conjecture that a potential research area is *membership fluidity among networks*. It is not uncommon that many hackers also join other hacker groups and may partake and continue their hacking activities. Albert Gonzalez, the informant for the Secret Service in the Shadowcrew case, continued his hacking activities and online illegal trading in another hacking group. He was accused of stealing 130 million credit/debit cards, the biggest data breach in U.S. history from Heartland Payment Systems [19]. Therefore, it would be significant to examine the membership fluidity among hacker's networks to effectively fathom their activities and destabilize their organizations.

11. IMPLICATIONS FOR PRACTICE

This research is timely and important to the information security industry. It helps us more profoundly analyze and fight against computer hacker groups. The study not only deepens our understanding relating to the social organization structure of hacker groups, but also provides a viable approach for law enforcement agencies to analyze and monitor the activities and movements of hacker communities.

Intelligence analysts often face huge volume of information with the pressing need to rapidly evaluate complex social-technical systems. This predicament sometimes may delay practitioners' response to possibly catastrophic incidents. For example, even though the U.S. intelligence had received several warning messages about Umar Abdulmutallab's intention to bomb the airplane during Christmas of 2009, they failed to connect the dots and disrupt this case [1]. One of their explanations is that they received hundreds and thousands of this type of messages every day. They were overwhelmed by huge amount of information and could not quickly follow the right trail.

Network analysis tools can provide intelligence analysts and security community with great power in data collection, analysis, visualization, and reporting issues. A clear understanding of the structural properties in a hacker network or criminal network can help law enforcement agencies more efficiently and effectively target critical leaders, implement necessary development for elimination or surveillance, and locate network vulnerabilities to destabilize the criminal network.

REFERENCES

[1] Abdulmutallab, U. F. (Febrary 12, 2010). Umar Farouk Abdulmutallab. Available: http://topics.nytimes.comtop/reference/timestopics/people/a/umar_farouk_abdulmutallab/index.html

[2] Albert, R., Jcong, H., and Baraba´si, A.-L., "Error and Attack Tolerance of Complex Networks," *Nature,* vol. 406, pp. 378-382, 2000.

[3] Best, J. and Luckenbill, D. F., "The Social Organization of Deviants," *Social Problems,* vol. 28, pp. 14-31, 1980.

[4] Best, J. and Luckenbill, D. F., *Oragnizing Deviance*, 2nd ed. New Jersey: Prentice Hall, 1994.

[5] Bonacich, P., "Factoring and Weighting Approaches to Status Scores and Clique Identification," *Journal of Mathematical Sociology,* vol. 2, pp. 113-120, 1972.

[6] Borgatti, S., Everett, M. G., and Freeman, L. C., "Ucinet 6 for Windows: Software for Social Network Analysis," ed. Harvard, MA: Analytic Technologies, 2002.

[7] Carley, K., *et al.*, "ORA User's Guide 2007," Carnegie Mellon University, School of Computer Science, Institute for Software Research, Technical Report Pittsburgh, PA 2007.

[8] Carley, K. M., "Coding Choices for Textual Analysis: A Comparison of Content Analysis and Map Analysis," in *Sociological Methodology 23,* P. Marsden, Ed., ed Oxford: Blackwell, 1993, pp. 75-126.

[9] Carley, K. M., "Dynamic Network Analysis," in *Dynamic Social Network Modeling and Analysis: Workshop Summary and Papers*, R. Breiger, K. M. Carley, and P. Pattison, Eds., ed: Committee on Human Factors, National Research Council, 2003, pp. 133-145.

[10] Carley, K. M., *et al.*, "Toward an Interoperable Dynamic Network Analysis Toolkit," *Decision Support Systems,* vol. 43, pp. 1324-1347, 2007.

[11] Chau, M. and Xu, J., "Mining Communities and Their Relationships in Blogs: A Study of Online Hate Groups," *International Journal of Human-Computer Studies,* vol. 65, pp. 57-70, 2007.

[12] Choobineh, J., *et al.*, "Management of Information Security:

Challenges and Research Directions," *Journal of the Association for Information Systems*, vol. 20, pp. 958-971, 2007.

[13] Cloward, R. A. and Ohlin, L. E., *Delinquency and Opportunity*. New York: Free Press, 1960.

[14] Dhillon, G. and Backhouse, J., "Current Directions in Information Security Research: Toward Socio-Organizational Perspectives," *Information Systems Journal,* vol. 11, pp. 127-153, 2001.

[15] Diesner, J. and Carley, K. M., "AutoMap 1.2- Extract, Analyze, Represent, and Compare Mental Models from Texts," Carnegie Mellon University, School of Computer Science, Institute for Software Research International, Technical Report CMU-ISRI-04-100, 2004.

[16] Diesner, J. and Carley, K. M., "Revealing Social Structure from Texts: Metamatrix Text Analysis as a Novel Method for Network Text Analysis," in *Causal Mapping for Information Systems and Technology Research: Approaches, Advances, and Illustrations*, V. K. Narayanan and D. J. Armstrong, Eds., ed Harrisburg, PA: IDEA Group Publishing, 2005, pp. 81-108.

[17] Freeman, L., "Centrality in Social Networks: Conceptual Clarification," *Social Networks,* vol. 1, pp. 215-239, 1979.

[18] Furnell, S., *Cybercrime: Vandalizing the Information Society*. Boston, MA: Addison-Wesley 2002.

[19] Gaudin, S. (Febrary 12, 2010). Government Informant is Called Kingpin of Largest U.S. Data Breaches. Available: http://www.computerworld.com/s/article/9136787/Government_informant_is_called_kingpin_of_largest_U.S._data_breaches

[20] Gibson, W., *Neuromancer*. New York: Ace Books, 1983.

[21] Holt, T. J., "Hacks, Cracks, and Crime: An Examination of the Subculture and Social," Ph.D., Criminology and Criminal Justice, University of Missouri, St. Louis, Missouri, 2005.

[22] Homle, P., *et al.*, "Attack Vulnerability of Complex Networks," *Physical Review E,* vol. 65, 2002.

[23] Johnston, A. C. and Warkentin, M., "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly,* vol. 34, 2010.

[24] Jurafsky, D. and Marton, J. H., *Speech and Language Processing*. Upper Saddle River, New Jersey: Prentice Hall, 2000.

[25] Kleen, L. J., "Malicious Hackers: A Framework for Analysis and Case Study," MA, Air Force Institute of Technology, 2001.

[26] Krovetz, R., "Word Sense Disambiguation for Large Text Databases," PhD, University of Massachusetts., 1995.

[27] Levy, S., *Hackers: Heros of the Computer Revolution*. New York: Dell, 1984.

[28] Loch, K. D., Carr, H. H., and Warkentin, M. E., "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly,* vol. 16, pp. 173-186, 1991.

[29] Magnini, B., *et al.*, "A WordNet-based Approach to Named Entities Recognition," presented at the SemaNet'02: Building and Using Sematic Networks, Taipei, Taiwan, 2002.

[30] McCormick, J. and Gage, D. (September 26, 2008). Shadowcrew: Web Mobs. Available: http://www.baselinemag.com/c/a/Security/Shadowcrew-Web-Mobs/

[31] Memon, N., Hicks, D., and Harkiolakis, N. I., "A Data Mining Approach to Intelligence Operations," in *Data Mining, Intrusion Detection, Information Assurance and Data Networks Security 2008,* Washington, USA, 2008.

[32] Merton, R. K., *Social Theory and Social Structure*. New York: Free Press, 1968.

[33] Meyer, G. R., "The Social Organization of the Computer Underground " Master, Northern Illinois University, 1989.

[34] Ng, B.-Y., Kankanhalli, A., and Xu, Y., "Studying users' computer security behavior: A health belief perspective," *Decision Support Systems,* vol. 46, pp. 815-825, 2009.

[35] Parker, D. B., *Computer Security Management*: Prentice Hall, 1981.

[36] Parsky, L., "Legislative Hearing on H.R. 5318, the "Cyber-Security Enhancement and Consumer Data Protection Act of 2006"," in *Committee on the Judiciary Subcommittee on Crime, Terrorism and Homeland Security*, ed, 2006.

[37] Rhodes, K., "Operations security awareness: the mind has no firewall," *Computer Security Journal,* vol. 18, 2001.

[38] Richardson, R., "CSI Survey 2007: The 12th Annual Computer Crime and Security Survey," Computer Security Institute 2007.

[39] Richardson, R., "CSI Survey 2008: The 13th Annual Computer Crime and Security Survey," Computer Security Institute 2008.

[40] Schultz, E., "Taking a stand on hackers," *Computers & Security,* vol. 21, pp. 382-384, 2002.

[41] Siponen, M. T., "An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice," *European Journal of Information Systems,* vol. 14, pp. 303-315, 2005.

[42] Stanton, J. M., *et al.*, "Behavioral information security: two end user survey studies of motivation and security practices," in *the Tenth America s Conference on Information Systems*, New York City, New York, 2004.

[43] Straub, D. W., "Effective IS Security: An Empirical Study," *Information Systems Research,* vol. 1, pp. 255-276, 1990.

[44] Straub, D. W., Goodman, S., and Baskerville, R., "Framing of Information Security Policies and Practice," in *Information Security Policies, Processes, and Practices*, D. W. Straub, S. Goodman, and R. Baskerville, Eds., ed Armonk, NY: M. E. Sharpe, 2008.

[45] Straub, D. W. and Welke, R. J., "Coping with systems risk: security planning models for management decision making," *MIS Quarterly,* vol. 22, pp. 441-469, 1998.

[46] Taylor, P. A., *Hackers: Crime in the Digital Sublime*. New York: Routledge, 1999.

[47] Taylor, R. W., *et al.*, *Digital Crime and Digital Terrorism*. Upper Saddle River, NJ: Pearson Education Inc. , 2006.

[48] Thomas, D., *Hacker Culture*. Minneapolis, MN: University of Minnesote Press, 2002.

[49] Thomson, M. E. and Solms, R. V., "Information security awareness: educating your users effectively," *Information Management and Computer Security,* vol. 6, 1998.

[50] United States Secret Service. (September 26, 2008). U.S. Secret Service Operation Firewall Nets 28 Arrests International Undercover Investigation Prevents Milllions in Financial Loss. Available: http://www.ustreas.gov/usss//press/pub2304.pdf.

[51] Wasserman, S. and Faust, K., *Social Network Analysis: Methods and Applications*. Cambridge: Cambridge University Press, 1994.

[52] Williams, P., "Transnational Criminal Networks," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, J. Aquilla and D. Ronfeldt, Eds., ed, 2001.

[53] Xu, J. and Chen, H., "Criminal Network Analysis and Visualization," *Commun. ACM,* vol. 48, pp. 100-107, 2005.