Chapter 1
Computational Social Networks: Security and Privacy

Mostafa Salama, Mrutyunjaya Panda, Yomna Elbarawy, Aboul Ella Hassanien, and Ajith Abraham

Abstract The continuous self-growing nature of social networks makes it hard to define a line of safety around these networks. Users in social networks are not interacting with the Web only but also with trusted groups that may also contain enemies. There are different kinds of attacks on these networks including causing damage to the computer systems and stealing information about users. These attacks are not only affecting individuals but also the organizations they are belonging to. Protection from these attacks should be performed by the users and security experts of the network. Advices should be provided to users of these social networks. Also security experts should be sure that the contents transmitted through the network do not contain malicious or harmful data. This chapter presents an overview of the social networks security and privacy issues and illustrates the various security risks and the tasks applied to minimize those risks. In addition, this chapter explains some of the common strategies that attackers often use and some possible counter measures against such issues.

M. Salama (✉)
British University in Egypt, Cairo, Egypt
e-mail: mostafa.salama@gmail.com

M. Panda
Department of ECE, Gandhi Institute of Engineering and Technology, Gunupur, 765022, India

Y. Elbarawy
Faculty of Computers and Information, BUE, Cairo, Egypt

A.E. Hassanien
Faculty of Computers and Information, Cairo University, Cairo, Egypt
e-mail: aboitcairo@gmail.com

A. Abraham
Machine Intelligence Research Labs (MIR Labs), Scientific Network for Innovation and Research Excellence, Auburn, WA, USA
e-mail: ajith.abraham@ieee.org

A. Abraham (ed.), *Computational Social Networks: Security and Privacy*,
DOI 10.1007/978-1-4471-4051-1_1,

Introduction

The Internet has 1,700 million users [26] and nearly 187 million web pages [8, 15, 42]. In this way, it has become the largest source of information worldwide. Web search engines (WSEs), for example, Google, Bing, etc., are an essential tool for finding specific data among this incalculable amount of information. WSEs are easy to use, and they retrieve search results quickly. Accordingly, it can be argued that these tools have played a crucial role in the success of the World Wide Web [15, 42, 56, 57]. The demand for solid expertise in social network analysis (SNA) has recently exploded [3, 9, 21, 24, 36] due to the popularity of social networking websites such as Facebook, Twitter, Netlog, etc., and automated data collection techniques. The main target in social network security is to enjoy the benefits of social networks while mitigating the security risks. This could be applied through determining the risks and security threats that may affect the organization using these networks. Several threats and security risks are facing the social network media, and the victims of these threats may be the users of these networks, or the community they are related to, or even the city they are living in.

Web 2.0 and social networking are easy targets for attacks as they allow users to upload different types of content. Also the continuing growth of Web 2.0 and social networking adds some new threats every day. The threats could be divided into two forms, an input form through input to the users' information that are not correct like rumors. The second form is an output form, through gathering information from different users and networks to finally get a complete picture. In the first form, social networking sites can be a source of personal and organizational information leaks. Social networks contain a wealth of personal information. People share their date of birth, email address, home address, family ties, and pictures. Some of that information would not be valuable by itself, but having a clear picture of everything about a person can give attackers ideas and information required to perform other attacks such as credit card fraud or identity theft. Any real-life targeted attack can be made much more effective through access to additional information about the intended victim. Or more simple when we post something like looking forward to the family vacation next week at Sharm El Sheikh. Obviously for anyone that our house will be empty for a whole week and as we know most of any social network users are not familiar with all people in their contact list and some of them we even do not know well, and hence, how can we trust that our new 52″ flat-screen TV, which we just purchased, will not be stolen. If an employee in a company posts a message "Our boss just laid off 40 employees, I heard that there may be more next Sunday," this message might indicate that the company is doing poorly and continuing with losses, and shareholders start to sell off their stocks and reduce the company value. So users need to be careful about what information is posted or shared and try to make contact with people only whom we know for sure so that should make us less vulnerable to malicious attacks [3, 24, 36, 40, 55]. Also it is important to provide advices and solutions required to minimize those risks through different procedures like demonstrating the information security policies that may be applied in the organization.

The second form is the vulnerability to malware and harmful attacks through contents transmitted through the network. Users may be tricked into pasting and executing malicious javascript in their browser, which also lead them to unknowingly sharing the content. For example, Facebook Inc. maintained that it is investigating a rash of unsolicited graphic images that hit some users' accounts recently. "We experienced a coordinated spam attack that exploited a browser vulnerability. Facebook engineers have been working to reduce this browser vulnerability," Facebook spokesman Andrew Noyes said in a statement emailed to Reuters [58]. So it is important to manage and track the contents uploaded by different users, and social network security experts should also work on the browser vulnerability.

This chapter has the following organization. Section "Social Networks: Privacy Analysis" briefly describing the social network privacy analysis. Section "Social Network Security Risks" discusses the different risks and attacks that face the social networks. Section "Preventive Measures on Security" introduces some preventive measures on security. Sections "Case Study 1: Social Network Analysis in Terrorist Network Dataset" and "Case Study 2: Social Networks Concepts to Visualize Terrorist Networks" introduce an implemented case study on social network security on terrorist network dataset. Finally, opportunities, challenges, and conclusions are discussed in section "Conclusions."

Social Networks: Privacy Analysis

Privacy concerns with social networking services have become controversial and a much publicized topic since the creation and increasing popularity of social networking sites such as Bebo, Myspace, and Facebook. Issues relating to stalking, identity theft, sexual predators, and employment consistently arise, as well as the ethics regarding data storage and the management and sharing of such data than someone who barely uses the site [23, 39]. A security issue occurs when a hacker gains unauthorized access to a site's protected coding or written language. Privacy issues do not necessarily have to involve security breaches. The potential harm to an individual user really boils down to how much a user engages in a social networking site, as well as the amount of the information they are willing to share. A user with more viewers or a part several groups is a lot more likely to be harmed by a breach than someone who barely uses the site [23].

Online social networks are immensely popular, with some claiming over 200 million users [27]. Users share private content, such as personal information or photographs, using online social networks applications. Users must trust the online social networks service to protect personal information even as the online social networks provide benefits from examining and sharing that information. Several works that address the privacy issue can be found in the literature. For example, authors in [4] presented Persona, an online social network where users dictate who may access their information. Persona hides user data with attribute-

based encryption, allowing users to apply fine-grained policies over who may view their data. Persona provides an effective means of creating applications in which users, not the online social networks, defining policy over access to private data. They described group-based access policies and the mechanisms needed to provide decryption and authentication by both groups and individuals. Authors demonstrated the versatility of operations in the proposed Persona, which provides privacy to users and the facility for creating applications like those that exist in current.

Privacy could be used for protection of social networking platforms and protection for social networking APIs [17]. Many researchers tackled this problem. For example, authors in [12] proposed a version of the probabilistic neural network that is privacy-preserving by evaluating a test point by the algorithm without any party knowing the data owned by the other parties. An analysis of the proposed algorithm from the standpoint of security and computational performance is presented. Salonas [54] proposed an NP-hard-based algorithm on data aggregation to solve privacy problem. They suggested the use of a genetic algorithm for solving the microaggregation problem. A comparative analysis of six social network site (SNS) report including Facebook [60], Hi5 [25], LinkedIn [34], LiveJournal [35], MySpace [41], and Skyrock [51] has been reviewed and discussed in [6]. The privacy-specific characteristics of each social network were examined under the following headings: registration information, real identities vs. pseudonyms, privacy controls, photo tagging, accessibility of member information to others, advertising, data retention, account deletion, third-party applications, and collection of nonuser personal information. This report also attempts to identify where sites have made particularly strong or weak choices with regard to privacy and to identify opportunities for improved privacy protection on SNS [6].

Social Network Security Risks

Risks associated with social networks can be classified into two main realms:

1. Risk associated with the organizations uses those social networks for official or personal reasons as if they are vulnerable to anyone of the major attacks, the organization system could fail.
2. Risks to the people (vertices) use those networks associated with identity theft or even more their personal belongings (e.g., home). In 2009, for instance [45], an employee of a Hawaii hospital illegally accessed a patient's electronic medical records, then posted the patient's name and confidential medical details on her MySpace page. This violation of Health Insurance Portability and Accountability Act policy did not deter the employee, who was later sentenced to 1 year in prison.

To minimize risks in social networks, we should (1) only publish information that we are perfectly comfortable with, depending on what we want to accomplish; (2) add only people we trust to our contact list; (3) avoid clicking unexpected links coming from people we do not know; and (4) never fully trust anyone we do not know that well.

Social Networks: Major Malicious Attacks

Social networks contain a wealth of information including birth dates, email addresses, family ties, home addresses, photos, and affiliations, which all the attackers need [47].

- Email addresses are entered into databases that are later used for spam campaigns. Email addresses that are derived from social networks can be further categorized to improve the impact of the campaign–race, age, country, and other factors can be used as filters in such a database so that its market price is higher than just any normal email address database [47].
- Date-of-birth data is used by different companies to confirm people's identities over the telephone. Criminals do not have databases, but they do have tools to automate "date-of-birth" searches in social networking sites [47].

Attackers may use social networking services to spread malicious code, compromise users' computers, or access personal information about a user's identity, location, contact information, and personal or professional relationships. You may also unintentionally reveal information to unauthorized individuals by performing certain actions.

Common Threats to Social Networking Services

The following are some of the common threats to social networking services [38]:

Viruses

The popularity of social networking services makes them ideal targets for attackers who want to have the most impact with the least effort. By creating a virus and embedding it in a website or a third-party application, an attacker can potentially infect millions of computers just by relying on users to share the malicious links with their contacts [38].

Tools

Attackers may use tools that allow them to take control of a user's account. The attacker could then access the user's private data and the data for any contacts that share their information with that user. An attacker with access to an account could also pose as that user and post malicious content [38].

Social Engineering Attacks

Social engineering relies on exploiting the human element of trust [22]. The first step in any social engineering attack is to collect information about the attacker's target. Social networking websites can reveal a large amount of personal information, including resumes, home addresses, phone numbers, employment information, work locations, family members, education, photos, and private information. Social media websites may share more personal information than users expect or need to keep in touch. A study by the University of Virginia cites that out of the top 150 Facebook applications, all of which are externally hosted, 90.7% of applications needed nothing more than publicly available information from members. However, all of these applications were given full access to personal information not necessary for operation but supplied by the user granting the applications' total access to their account [16]. Attackers may send an email or post a comment that appears to originate from a trusted social networking service or user. The message may contain a malicious URL or a request for personal information. By following the instructions, the user may disclose sensitive information or compromise the security of the system. An example of this kind of attack is called phishing, which is a fraudulent attempt to steal personal information such as usernames, passwords, and credit card details. Phishing is usually made through emails and appears to come from a well-known organization and is targeted to steal users' personal information. Often times phishing attempts appear to come from sites, services, and companies with which the users do not even have an account.

The best way to protect from phishing is to learn how to recognize a phish [44]:

- Generic greeting. Phishing emails are usually sent in large batches. To save time, Internet criminals use generic names like "first bank name customer," so they do not have to type all recipients' names out and send emails one-by-one.
- Forged link. Even if a link has a name you recognize somewhere in it, it does not mean it links to the real organization. Roll your mouse over the link and see if it matches what appears in the email. If there is a discrepancy, do not click on the link. Also, websites where it is safe to enter personal information begin with "https" – the "s" stands for secure. If you do not see "https," then do not proceed [16, 22, 44].
- Requests personal information. The point of sending phishing email is to trick you into providing your personal information. If you receive an email requesting your personal information, it is probably a phishing attempt.

- Sense of urgency. Internet criminals want you to provide your personal information now. They do this by making you think something has happened that requires you to act fast. The faster they get your information, the faster they can move on to another victim.

Identity Theft or Fake Identity

Attackers may be able to gather enough personal information from social networking services to assume our identity or the identity of one of our contacts. Even a few personal details may provide attackers with enough information to guess answers to security or password reminder questions for email, credit card, or bank accounts. In addition to this, underground forums sell personal information. The data can be mined and stored somewhere in the dark corners of the Internet waiting for a criminal to pay the right price for it. Criminals can use this information to obtain birth certificates/passports/other documentation and fake real-life identities. Some countries have looser controls than others, but in general, identity theft is something that already happens regularly. An example of this kind of attack is the Sybil attacks. In a Sybil attack, a malicious user takes on multiple identities and pretends to be multiple, distinct nodes (called Sybil nodes or Sybil identities) in the system. With Sybil nodes comprising a large fraction (e.g., more than one third) of the nodes in the system, the malicious user is able to "out vote" the honest users, effectively breaking previous defenses against malicious behaviors. For example, virtually all protocols for tolerating Byzantine failures assume that at least 2/3 of the nodes are honest. This makes these protocols vulnerable to Sybil attacks [14].

To handle these attacks, we may use a central authority that verifies credentials unique to an actual human being can control Sybil attacks easily. For example, if the system requires users to register with government-issued social security numbers or driver's license numbers, then the barrier for launching a Sybil attack becomes much higher. The central authority may also instead require a payment for each identity. Unfortunately, there are many scenarios where such designs are not desirable. For example, it may be difficult to select/establish a single entity that every user worldwide is willing to trust. Furthermore, the central authority can easily be a single point of failure. Finally, requiring sensitive information or payment in order to use a system may scare away many potential users.

A defense against Sybil attacks in social networks is the Sybil guard. Sybil guard leverages the existing human established trust relationships among users to bind both the number and size of Sybil groups. All honest nodes and Sybil nodes in the system form a social network. An undirected edge exists between two nodes if the two corresponding users have strong social connections (e.g., colleagues or relatives) and trust each other not to launch a Sybil attack. If two nodes are connected by an edge, we say the two users are friends. Notice that here, the edge indicates strong trust, and the notion of friends is quite different from friends in other systems such as online chat rooms. An edge may exist between a Sybil node and an honest node if a malicious user (Khaled) successfully fools an honest user (Lyla)

into trusting her. Such an edge is called an attack edge, and we use g to denote the total number of attack edges. The authentication mechanism in Sybil guard ensures that regardless of the number of Sybil nodes Khaled creates, Lyla will share an edge with at most one of them (as in the real social network). Thus, the number of attack edges is limited by the number of trust relation pairs that the adversary can establish between honest users and malicious users. While the adversary has only limited influence over the social network, we do assume it may have full knowledge of the social network. The degree of the nodes in the social network tends to be much smaller than n (number of honest nodes), so the system would be of little practical use if nodes only accepted their friends. Instead, Sybil Guard bootstraps from the given social network a protocol that enables honest nodes to accept a large fraction of the other honest nodes. Each pair of friends shares a unique symmetric secret key (e.g., a shared password) called the edge key [63]. The edge key is used to authenticate messages between the two friends (e.g., with a message authentication code) because only the two friends need to know the edge key, and key distribution is easily done out-of-band (e.g., via phone calls). A node can also revoke an edge key unilaterally simply by discontinuing use of the key and discarding it.

Third-Party Applications

Some social networking services may allow you to add third-party applications, including games and quizzes, which provide additional functionality. Social media websites are advanced web applications, as their use requires a high level of interaction and capabilities. Be careful using these applications, even if an application does not contain malicious code, it might access information in your profile without your knowledge. This information could then be used in a variety of ways, such as tailoring advertisements, performing market research, sending spam email, or accessing your contacts. For example, emerging techniques include using custom Facebook applications to target users. Facebook applications are written by third-party developers and often have minimal security controls [48–50, 53].

Public Comments

Public comments may contain links to false locations designed to make failure of systems of certain organizations which are the target, and as we know, most staffs are using social networks.

Preventive Measures on Security

The attack graph represents collections of possible attack scenarios (sequences of actions) that an intruder might make to lead to a security breach in the network.

Measuring Network Security Using Attack Graphs

A topographical analysis of known critical points in the network can yield measurable data on overall system security. Analysis can produce an attack graph showing most vulnerable paths to/within the network, and hence, the network resistance to attacks can be quantified and measured.

An Ant Colony Optimization Algorithm for Network Vulnerability Analysis

AntNAG (ant network attack graph), an ant colony optimization algorithm for minimization analysis of large-scale network attack graphs. Each ant incrementally constructs a critical set of exploits. Each exploit is associated with a pheromone trail that indicates the desirability of including that exploit into an ant's solution. The first step is to set parameters and initialize pheromone trails. Then repeated iterations of the algorithm are run until some termination condition is met (e.g., a maximum number of iterations is reached). Within each iteration, each ant starts with an empty set and constructs a critical set of exploits by incrementally adding exploits until all attack scenarios are hit. The critical sets of exploits constructed by ants may contain redundant exploits, which are eliminated. After that, the iteration's best solution is improved by a local search heuristic. Finally, the pheromone trails are updated using a global updating rule.

Attack Tree

Attack trees are used to analyze attributes of the security of the network. The root node of the tree is the global target of the attacker, nodes represent the attacks, and the children nodes are refinements of this goal. The example in [37], the tree shows the goal of the attacker is to obtain a free lunch. The tree lists three possible ways to reach this goal. Lower levels in the tree explain how these subgoals are refined as well.

Social Networking Security and Privacy Study (2011)

The study reported in [5] is based on survey results from hundreds of users representing over 20 countries. The research was conducted over a 2-week span between September and October 2011. Users are asked about their experiences and feelings on social networking usage, security, and privacy. The results highlight some deficiencies that must be addressed by social network providers and the security community in order to provide a safe, fertile ground for continued growth and advancement on social platforms [1, 5] (Figs. 1.1–1.3).

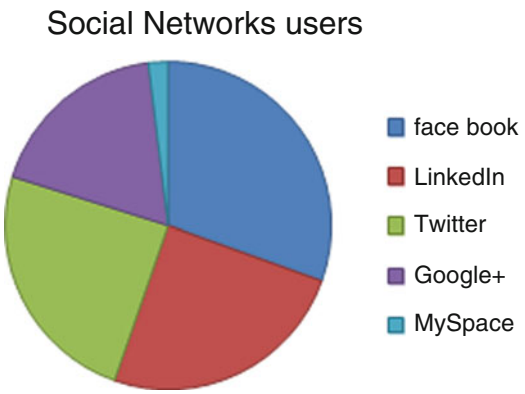

Fig. 1.1 Social network users [1]

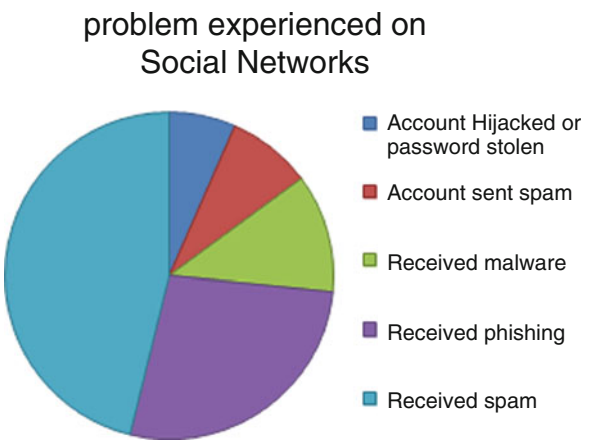

Fig. 1.2 Problem experienced on social networks [5]

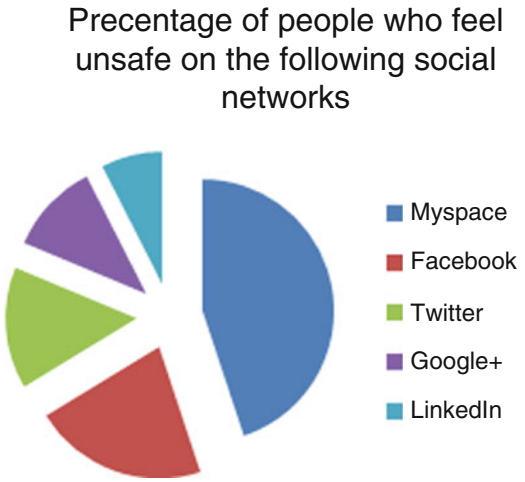

Fig. 1.3 Percentage of people who feel unsafe on the following social networks [5]

Case Study 1: Social Network Analysis in Terrorist Network Dataset

Following are the step-by-step procedures that are to be adopted while analyzing a social network.

Algorithm 1 Adopted while analyzing a social network

Step-1: Identification of a suitable target by the investigator.
Step-2: The research on the subject matter should be conducted thoroughly. For example, the investigator should explore who knows whom and how well do they know each other in order to discover the channel of information flow in the network.
Step-3: A database is to be created based on the information gathered from Step-2 in a binary matrix format in a node-by-node manner, as shown in Table 1.1 below.
Step-4: The investigator should investigate the basics of software that are to be used for analyzing the compiled data in order to provide everything from basic knowledge to expert advice.
Step-5: Finally, actual analysis is to be done which further can be used to identify the possible tactics to disrupt or improve the networks under investigation.

The relationship matrix in Table 1.1 is identified based on the number of nodes available in a network, where the data are entered by placing 0's and 1's into a spread sheet. The 0's indicate no connection where 1 represents a link. Sometimes, a signed matrix with $+1$ (positive relationship), 0 (no relationship), and -1(negative relationship) may also be considered to understand the relationships among the nodes. Further, if there exists a strong relationship, then in place of mentioning $+1$ in the spreadsheet, we may use 5 or 10, etc., based on their strength in relationships. Once the relationship matrix is obtained, the social network analysis software is then able to interpret them.

Example Scenario

Step-1: Based on the list of Foreign Terrorist Organizations, SNA is used to perform the social network analysis.

Step-2: Open sources are used to collect basic informations about each group, and then their affiliations with other groups are obtained from the list provided.

Step-3: Excel spreadsheet is used for the data compilation by putting 1's and 0's in order to signify the relations and obtain the binary matrix.

Table 1.1 Relationship matrix

A	B
1	0
0	1

Table 1.2 Betweenness centrality

	Betweenness	nbetweenness
1	213.00	15.123
2	123.00	6.349
3	47.97	2.872
4	42.11	2.981

Table 1.3 Closeness centrality

	inFarness	inCloseness
1	9	100
2	10	78
3	11	65
4	15	90

Step-4: We then perform the social network analysis using UCINET tool [24] to run the experiments on the data in matrix format and found performance measures like betweenness and closeness centrality [59] in order to interpret the results, as shown below in Tables 1.2 and 1.3, respectively:

From the betweenness property [59], we know that it finds the number of times that a node lies along the shortest path between two others. Hence, the result says that the node-1 poses higher betweenness between all others.

From the result shown, it is quite evident that node-1 with incloseness score of 100 has the lowest total of geodesic distances from other nodes. At the same time, the node-4 with its inFarness score of 15 produces largest geodesic distances from other nodes.

Step-5: Finally, network visualization is made, as shown below for completing our social network analysis.

From Fig. 1.4, it can be seen that Al-Qaeda is the center node, whereas Jaish-e-ahmed and Hamas are playing the most significant roles in the network. Further, Hezbollah has the highest betweenness because of its link with Al-Qaeda, Hamas, and all others. At the same time, Al-Aqsa Martyre brigade has the highest farness because of its highest geodesic distance from Al-Queda.

Case Study 2: Social Networks' Concepts to Visualize Terrorist Networks

Visualizing social networks are of immense help to the social network researchers in understanding new ways to present and manage data and effectively convert that data into meaningful information [55]. A number of visualization tools have been proposed for effective visualizing social networks including Pajek [18], NetVis, Krackplot, IKnow, InFlow, Visone, JUNG, and Prefuse, to name a few. Another source of online collaboration has also been visualized to better understand interactions that are provided in a discussion form [13]. Visualizing tasks for better

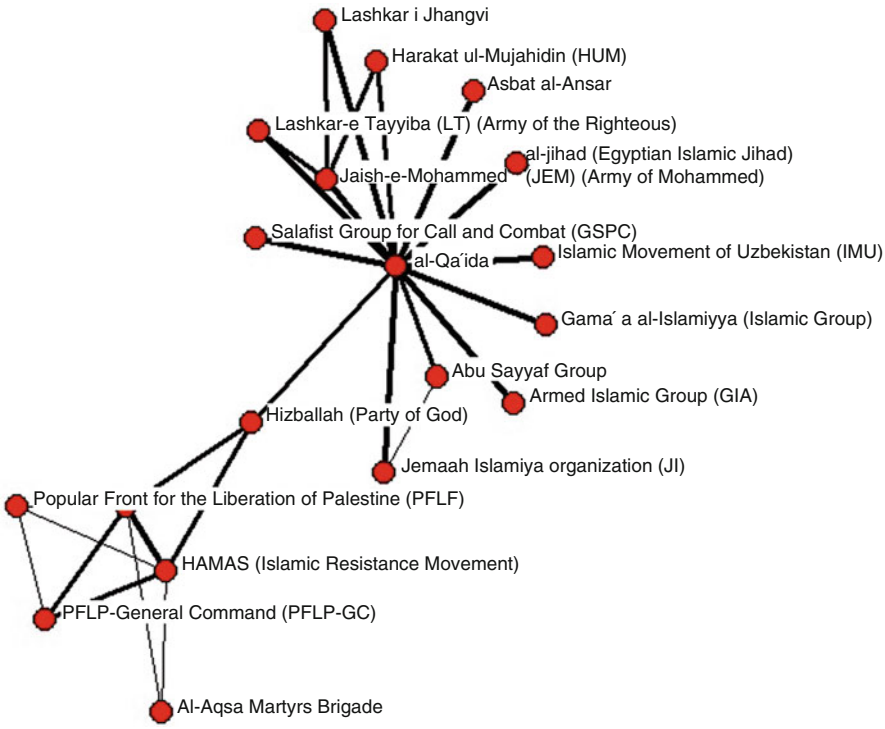

Fig. 1.4 Network visualization of foreign terrorist network data

collaboration during software development has been proposed [13] to address issues of coordination and geographical distribution of developer teams. Visualizing social networks using query interfaces for wikis and blogs [36] is used to provide the end users with more user-friendly alternatives.

Terrorism deals with violent acts aiming to simulate fear, coercion, or intimidation [11, 28, 46]. It is an established fact that terrorism poses both direct and indirect threats to normal life. Even though terrorist strikes destroy only a small fraction of the direct economy of a country, their large effect on economic outcomes is well known [20]. It is sad to note that technical development is not only pulled by the demand for high-tech products but is also highly influenced by some external environments, for example, terrorism. As shown by the aftermath of the 9/11 attacks, Bali, Madrid, and London bombings, some changes have occurred in the day-to-day living of citizens of those countries and around the world [2, 29, 43, 62].

After the 9/11 attacks, lots of efforts have been done to develop effective methods for antiterrorism strategies. Visualization is very important part for analyzing such a network since it can quickly provide good insight into the network structure, major members, and their properties [19]. Analyzing huge networks is not an easy task, and there is a need to reduce the complexity of these networks, which is

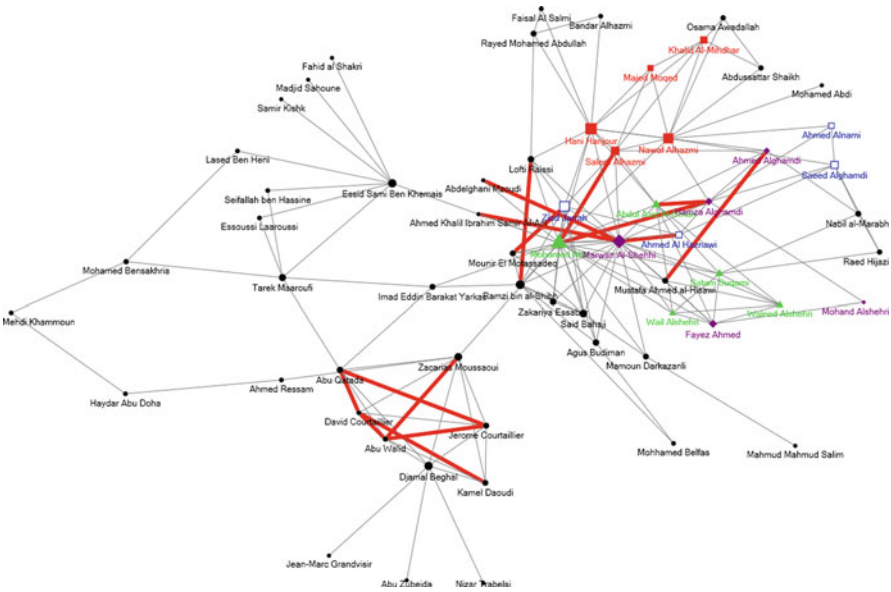

Fig. 1.5 Terrorists network with highlighted link suggestions using SDD reduction (rank 10)

usually depicted in the form of huge matrices. Matrix factorization method is a well-established approach, and Semidiscrete decomposition (SDD) is highly suitable for dealing with huge networks. Empirical results using the 9/11 network data illustrate the efficiency of the proposed approach [52]. The analysis of general complex networks is well described in [7] and [10]. This work is closely related to the link prediction, which is well elaborated by Liben-Nowell and Kleinberg [33]. Koren et al. [30] discussed the usage of matrix factorization methods for recommendation systems.

The obtained experiment is based on the dataset involving 9/11 attacks from [31]. Change from zero to one in the reduced matrix can be in wider sense considered as a link suggestion. In different fields, the suggestion can have different meanings. In the terrorist network, we can consider them as a suggestion to investigate, whether the link truly exists in reality; for more details, a reader can refer to [52]. The results for parameter setting with rank equal to 10 are illustrated in Fig. 1.5. Same coloring is used as in the original paper [31] by Krebs. Green triangles for flight AA #11, which crashed into the WTC North, full red squares for flight AA #77 which crashed into Pentagon, empty blue squares for flight UA #93 which crashed into Pennsylvania, and full purple diamonds for flight UA #175 which crashed into WTC South.

Edges drawn in bold red are suggestions obtained by the mentioned reduction. As evident, the suggested links are in the group of Zacarias Moussaoui, Abu Qatada, David Courtaillier, Jerome Courtaillier, Abu Walid, Kamel Daoudi, and Djamal Beghal. This group is also connected using several subgroups in the original

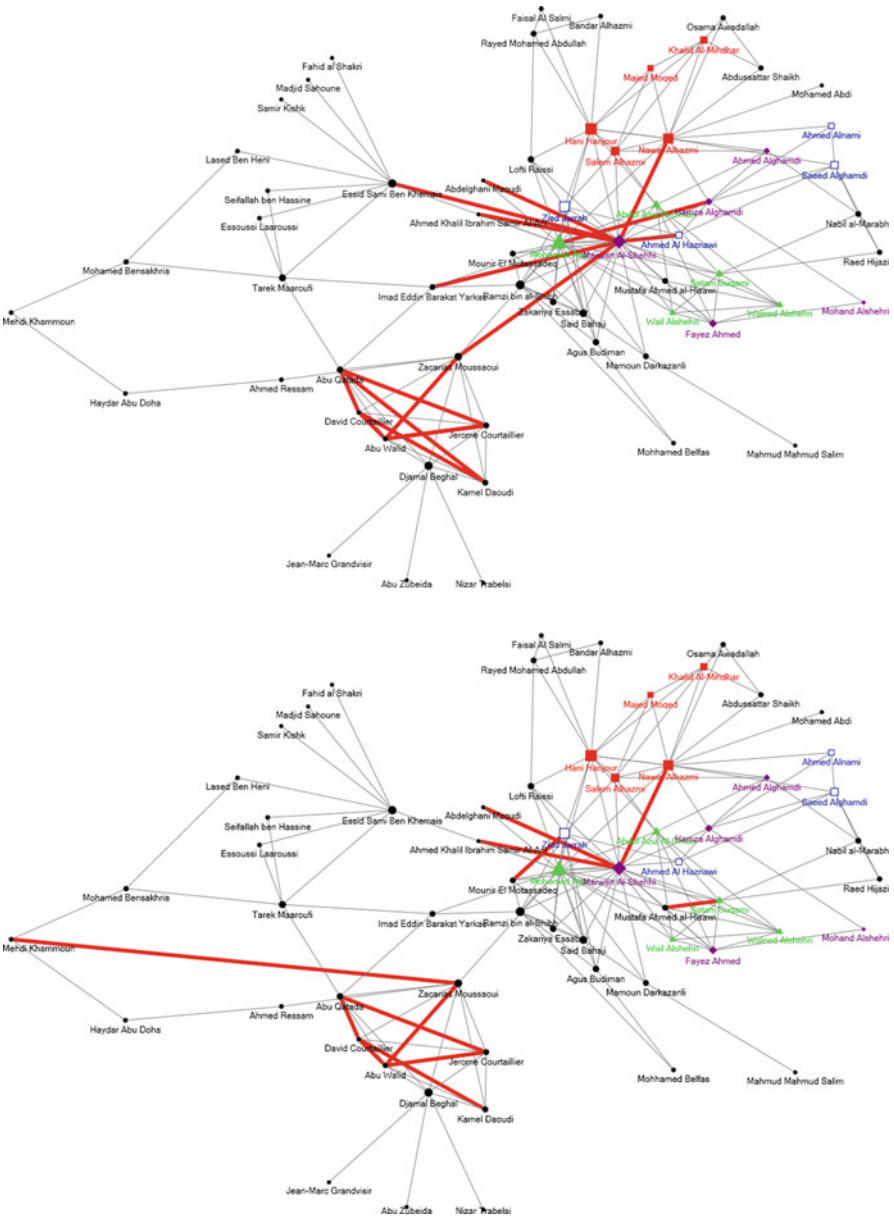

Fig. 1.6 Terrorists network with highlighted link suggestions using SDD reduction (rank 5 and 20)

data; therefore, the proposed method suggests their stronger interconnection. The same holds for the suggested link between Ramzi bin al-Shibh and Lofti Raissi as it connects two different groups of individuals. Remaining suggestions can be explored in a similar way.

Results obtained using rank parameter setting equal to 20 (that means lower ratio of reduction) are shown in the right part of Fig. 1.6. Less reduction in this case means less suggestions, but the suggestion obtained for rank 20 is not subset of suggestions for rank 10. As SDD always tries to minimize the error function, the reduction process is not straightforward – for example, the links between Mehdi Khammoun and Zacarias Moussaoui, Mustafa Ahmed al-Hisawi and Satam Suqami, as well as the link between Marwan Al-Shehhi and Nawaf Alhazmi, are present at rank 20 but disapper at rank 10. The remaining links are still present at rank 10. Similar situation is with the setting $k = 5$ (left part of Fig. 1.6), which gives us 16 suggestions – using stronger reduction, we have obtained more suggestions, but not all suggestions from rank 10 are present.

Conclusions

As social networking gains users, it will increasingly be targeted by attackers, just as instant messaging and other media have been. Security risks can put the individual or a company in a compromising position or at serious risk. Aside from not using these sites at all, end-user education, alongside documented policies and procedures, is the most fundamental protection that exists. A well-informed user will not only help to maintain security but will also educate others on these issues and establish best practices, which can be standardized and updated as applications mature or as new applications come along. Institutions would be advised to consider carefully the implications before promoting significant use of such services.

Clear understanding of structural properties of a criminal network may help analysts target critical network members for removal or surveillance and locate network vulnerabilities where disruptive actions can be effective such as non negative matrix [32]. Appropriate network analysis techniques, therefore, are needed to mine criminal networks and gain insight into these problems. This chapter bridges this gap by combing social network analysis method and security risks and required prevention techniques to help users to protect themselves from other members in a social network.

References

1. Abadi, M., Jalili, S.: An ant colony optimization algorithm for network vulnerability analysis. Iran. J. Electr. Electron. Eng. **2**(3), 106–120 (2006)
2. Abadie, A., Gardeazabal, J.: Terrorism and the world economy. Eur. Econ. Rev. **52**(1), 1–27 (2008)
3. Antheunis, M.L., Valkenburg, P.M., Peter, J.: Getting acquainted through social network sites: testing a model of online uncertainty reduction and social attraction. Comput. Hum. Behav. **26**, 100–109 (2010)

4. Baden, R., Bender, A., Spring, N., Bhattacharjee, B., Starin, D.: Persona: an online social network with user-defined privacy. ACM SIGCOMM Comput. Commun. Rev. **39**(4), 50–55 (2009)
5. Barracuda Networks Inc.: Social Networking Security and Privacy Study. Barracuda Labs, Belgium (2011)
6. Barrigar, J.: Social network site privacy: a comparative analysis of six sites. The Office of the Privacy Commissioner of Canada, Feb 2009. http://www.priv.gc.ca/information/pub/sub_comp_200901_e.pdf. Accessed on Feb 2012
7. Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., Hwang, D.U.: Complex networks: structure and dynamics. Phys. Rep.**424**, 175–308 (2006)
8. Boyd, D., Ellison, N.: Social network sites: definition, history and scholarship. J. Comput. Mediat. Commun. **13**(1), 210–230 (2007)
9. Carley, K.M.: Dynamic network analysis. In: Breiger, R., Carley, K., Pattison, P. (eds.) Dynamic Social Network Modeling and Analysis: Workshop Summary and Papers, pp. 133–145. Committee on Human Factors, National Research Council, Washington, DC (2003)
10. Costa, L.F., Rodrigues, F.A., Travieso, G., Boas, P.R.V.: Characterization of complex networks: a survey of measurements. Adv. Phys. **56**, 167–242 (2007)
11. Czinkota, M.R., Knight, G.A., Liesch, P.W., Steen, J.: Positioning terrorism in management and marketing: research propositions. J. Int. Manage. **11**(4), 581–604 (2005)
12. Das, K., Bhaduri, K., Kargupta, H.: A local asynchronous distributed privacy preserving feature selection algorithm for large peer-to-peer networks. Knowl. Inf. Syst. J. **24**(3), 341–367 (2009)
13. De Nooy, W., AMrvar, A., Batagelig, V.: Exploratory Social Network Analysis with Pajek. Cambridge university press, New York (2004)
14. Douceur. J.: The Sybil attack. In: First International Workshop on Peer-to-Peer Systems, Cambridge, MA, USA, pp. 251–260 (2002)
15. Erola, A., Castell-Roca, J., Viejo, A., Mateo-Sanz, J.M.: Exploiting social networks to provide privacy in personalized web search. J. Syst. Softw. **84**(10), 1734–1745 (2011)
16. Felt, A., Evans, D.: Privacy protection for social networking APIs, In Proceedings of Web 2.0 Security and Privacy (W2SP 2009), Oakland, California (2009)
17. Felt, A., Evans, D.: Privacy Protection for Social Networking APIs. University of Virginia Charlottesville, Virginia (2008)
18. Freeman, L.: Visualizing social network. J. Soc. Struct. **1**(1), 151–161 (2000)
19. Freeman, L.C.: Social network visualization. In: Methods of Encyclopedia of Complexity and Systems Science, pp. 8345–8363 (2009)
20. Frey, B.S.: How can business cope with terrorism? J. Policy Model. **31**(5), 779–787 (2009)
21. Grace, J., Gruhl, D., et al.: Artist remains: through analysis of on-line community comments. In proc. of J. Grace edns, (2007)
22. Granger, S.: Social engineering fundamentals, part I: hacker tactics. (cited 5/12/11). Available on: http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics, (2001)
23. Gross, R., Acquisti, A.: Information revelation and privacy in online social networking sites (the facebook case). Available at: http://www.fastcompany.com/articles/2008/10/social-networking-security.html. Accessed 8 Jan 2012
24. Halgin, D.: An introduction to UCINET and NetDraw. In: Proceedings of the NIPS UCINET and NetDraw Workshop 2008, Harvard University, pp. 1–47 (2008)
25. Hi5: http://hi5.com. Accessed on 2011
26. Internet world stats: http://www.internetworldstats.com/stats.htm (2008)
27. Kadushin, C.: Who benefits from network analysis: ethics of social network research. Soc. Netw. **27**, 139–145 (2005)
28. Koh, W.T.H.: Terrorism and its impact on economic growth and technological innovation. Technol. Forecast. Soc. Change **74**(2), 129–138 (2007)
29. Kollias, C., Messis, P., Mylonidis, N., Paleologou, S.: Terrorism and the effectiveness of security spending in Greece: policy implications of some empirical indings. J. Policy Model. **31**(5), 788–802 (2009)

30. Koren, Y., Bell, R., Volinsky, C.: Matrix factorization techniques for recommender systems. IEEE Comput. **42**, 30–37 (2009)
31. Krebs, V.E.: Uncloaking terrorist networks. First Monday **7**, (2002)
32. Lee, D., Seung, H.: Learning the parts of objects by non-negative matrix factorization. Nature **401**, 788–791 (1999)
33. Liben-Nowell, D., Kleinberg, J.: The link-prediction problem for social networks. J. Am. Soc. Inf. Sci. Technol. **58**, 1019–1031 (2007)
34. LinkedIn: http://www.linkedin.com. Accessed on 2012
35. LiveJournal: http://www.livejournal.com. Accessed on 2012
36. Matsuo, Y., et al.: Polyphonet: an advanced social network extraction system from the web. In: Proceedings of the International Conference on World Wide Web (www 06), New York, pp. 397–406 (2006)
37. Mauw, S., Oostdijk, M.: Foundations of attack trees. In: Proceedings of the 8th International Conference of Information Security and Cryptology (ICISC 2005), Seoul Korea, pp.186–198 (2005)
38. McDowell, M., Morda, D.: Socializing securely: using social networking services. United States Computer Emergency Readiness Team (US-CERT), Washington, DC (2011)
39. Moor, J.H.: Towards a theory of privacy for the information age. SIGCAS Comput. Soc. **40**(2), 31–34 (2010)
40. Moustafa, W., Deshpande, A., Namata, G., Getoor, L.: Declarative analysis of noisy information networks. In: Proceedings of the IEEE 27th International Conference on Department of Computer Science, Data Engineering Workshops (ICDEW), Hannover, pp. 106–111, (2011)
41. MySpace: http://www.myspace.com
42. Netcraft: http://news.netcraft.com (2009)
43. Paraskevas, A., Arendell, B.: A strategic framework for terrorism prevention and mitigation in tourism destinations. Tour. Manage. **28**(6), 1560–1573 (2007)
44. PhishingTank: What is phishing? (cited 6/12/11). Available from: http://www.phishtank.com/what-is-phishing.php
45. PricewaterhouseCoopers: Security for social networking. Available on: http://www.pwc.com/en_US/us/it-risk-security/assets/security-social-networking.pdf, (2010)
46. Reid, E.F., Chen, H.: Mapping the contemporary terrorism research domain. Int. J. Hum. Comput. Stud. **65**(1), 42–56 (2007)
47. Sancho, D.: Security guide to social networks, A Trend Micro White Paper, Aug, (2009).
48. schrock, A.: Examining social media usage: technology clusters and social network relationships. First Monday **14**(1), (2009)
49. Shani, G., Chickering, M., Meek, C.: Mining recommendations from the web. In: Proceedings of the 2008 ACM Conference on Recommender System, Lausanne, pp. 35–42 (2008)
50. Sheldon, P.: The relationship between unwillingness to communicate and students Facebook use. J Media Psychol. Theor. Method Appl. **20**(2), 67–75 (2008)
51. Skyrock: http://www.Skyrock.com. Accessed on 2012
52. Snasel, V., Horak, Z., Abraham, A.: Link suggestions in terrorists networks using semi discrete decomposition. In: Sixth International Conference on Information Assurance and Security (IAS), USA, IEEE, ISBN 978-1-4244-7408-0, pp. 337–339 (2010)
53. Soghoian, C.: Hackers target facebook apps. CNet News, (cited 5/12/11). Available from: http://news.cnet.com/8301-13739-3-9904331-46.html (2008)
54. Solanas, A.: Privacy protection with genetic algorithms. Stud. Computat. Intel. **92**, 215–237 (2008)
55. Tantipathananandh, C., Breger-wolf, T., Kempe, D.: A framework for community identification in dynamic Social network. In: Proceedings of the KDD 2007, San Jose, CA, USA, pp. 717–726 (2007)
56. Thellwal, M.: Social networks, gender and friending, analysis of myspace profiles. J. Am. Soc. Inf. Sci. Technol. **591**(8), 1321–1330 (2008)
57. Tufekci, Z.: Grroming, gossip facebook and myspace: what can we learn about these sites from those who wont assimilate? Inf. Commun. Soc. **11**(4), 544–564 (2008)

58. http://www.facebook.com/note.php?note_id=324110600939875. Accessed on 2012
59. http://en.wikipedia.org/wiki/Betweenness. Accessed on 2012
60. http://www.facebook.com. Accessed on 2012
61. Walther, J., Vander Heide, B., Kim, S., Westerman, D., Tang, S.T.: The role of friends appearance and behaviour on evaluations of individuals on facebook: are we known by the company we keep? Hum. commun. Res. **34**, 28–49 (2008)
62. Wolf, Y., Frankel, O.: Terrorism: toward an overarched account and prevention with a special reference to pendulum interplay between both parties. Aggress. Viol. Behav. **12**(3), 259–279 (2007)
63. Yu, H., Kaminsky, M., Gibbons, P.B., Flaxman, A.: SybilGuard: defending against sybil attacks via social networks. SIGCOMM'06 **16**(3), 576–589 (2006)