Social Engineering in Social Networking Sites: Phase-Based and Source-Based Models

Abdullah Algarni and Yue Xu

***Abstract*—Social networking sites (SNSs), with their large numbers of users and large information base, seem to be perfect breeding grounds for exploiting the vulnerabilities of people, the weakest link in security. Deceiving, persuading, or influencing people to provide information or to perform an action that will benefit the attacker is known as "social engineering". While technology-based security has been addressed by research and may be well understood, social engineering is more challenging to understand and manage, especially in new environments such as SNSs, owing to some factors of SNSs that reduce the ability of users to detect the attack and increase the ability of attackers to launch it. This work will contribute to the knowledge of social engineering by presenting the first two conceptual models of social engineering attacks in SNSs. Phase-based and source-based models are presented, along with an intensive and comprehensive overview of different aspects of social engineering threats in SNSs.**

***Index Terms*—Social engineering, social networking sites, information security, deception, privacy .**

I. Introduction

Threats in information security generally come through the vulnerabilities of technologies or the vulnerabilities of people. However, while technology-based threats are well discussed, and addressed in many studies, human-based threats seem to be less attractive to researchers in the information technology field, perhaps because of the complexity of understanding and predicting the human behaviors that lead to human vulnerabilities. Social engineering is the type of security attack that exploits those vulnerabilities to meet the desires of the attacker [1]. It has been found that social engineering attacks pose the most significant security risks; they are more challenging to control [2], [3]. Currently, cyber attacks have more to do with manipulating humans than ever [4].

Since the first recognizable appearance of social networking sites (SNSs) in 1997, with the social network site SixDegrees.com [5], people have been attracted to those sites to construct their profiles and communicate with each other in different ways depending on the nature of the site. SNSs also have been implementing a wide variety of technical features that enable people, companies, organizations, or governmental institutions to do a variety of services [5]. As the numbers of users of SNSs have been increasing dramatically, the amount of sensitive and private information of people, companies, organizations, or governmental institutions and their activities is also increasing dramatically. This not only makes SNSs attractive to faithful users but also makes them perfect breeding grounds for malicious users and attackers. Information is always under threat, and it can be intercepted, modified, or exposed. The facilities that are setup to monitor such attacks are also constantly under attack [6]. Such attacks shape the challenges of providing usability and sociability, which are the main purposes of SNSs, as well as ensuring integrity, confidentiality, and availability, which are standard principles of security.

The aim of this paper is to present phase-base and source-base models of social engineering threats in SNSs. This aim can be achieved through answering three main questions concerning social engineering threats in SNSs:

1) How does the social engineer plan and perform the attack?
2) How do SNSs help social engineers to plan and launch the attack?
3) How do victims fall for attacks on SNSs?

The rest of this paper is organized as follows. In Section II, we explain the motivation to study social engineering in SNSs. Section III describes the method and related works. In Section IV, we present two conceptual models of social engineering in SNSs, one is phase-based, and the other is source-based. We conclude in Section V.

II. Motivation to Study Social Engineering in SNSs

The Institute of Management and Administration (IOMA) reported social engineering as the top security threat for 2005. They indicate that social engineering threats, which are human-based, are on the rise owing to continued improvements in protections against technology-based threats [7]. According to a survey done by Dimension Research (2011) on 850 IT and security professionals located in the United States, Canada, the United Kingdom, Germany, Australia, and New Zealand, 48% of participants had been victims of social engineering and had experienced 25 or more attacks in 2010 and 2011. Social engineering attacks cost victims an average of $25,000 to $100,000 per security incident, the report states. Of the participants, 39% believe that the SNSs are the most common source of social engineering threats, and only 26% of the participants in that survey actively train employees on social engineering threats. Although many organizations recognize the importance of controlling security threats, many fail to recognize the dangers of social engineering attacks [8].

A study that included more than 4,000 users of Facebook

Manuscript received May 5, 2013; revised July 23, 2013.

Abdullah Algarni and Yue Xu are with Queensland University of Technology, Science and Engineering Faculty, Brisbane, Australia (e-mail: abdullahayedm.algarni@student.qut.edu.au, yue.xu@qut.edu.au).

found that most participants are willing to provide large amounts of personal information in SNSs, thus exposing themselves to various physical and cyber risks [9]. Now, the use of SNSs as the main tool of social interaction results in a loss of privacy [10]. This therefore opens users and their originations or networks to becoming targets of major security threats [11].

Through providing an introduction to security issues in the area of SNSs, and highlighting some threats in SNSs, the European Network and Information Security Agency (ENISA) indicates that SNSs can be dangerous weapons in the hands of spammers, unscrupulous marketers, and social engineers who may take criminal advantage of users [12]. Nagy and Pecho (2009) have analyzed and validated the possibilities of misusing SNSs due to irresponsible behavior of users [13]. In addition, the baseline success rate for using information obtained from SNSs in phishing attacks has been established [14]. Because of the lack of users' awareness, social engineering is considered a low-cost and effective form of attack [15]. Moreover, some researchers have started investigating in automating social engineering, hijacking, and phishing in social networking sites [16], [17].

The risk of social engineering in SNSs is expected to increase in the future because of the fact that the information that users provide about themselves are the most valuable elements to the social networking site providers. Therefore, SNSs' providers will keep encouraging users to reveal and share more personal information. Researchers have given examples of some of the tactics that are used by the providers of SNSs to persuade users to share their personal information [18], [19]. Providers of SNSs use such information in marketing and advertisements in which they select specific groups of users, based on their specifications, to receive specific product advertisements; therefore, we expect there to be an increase in social engineering exploits in the future, unless effective countermeasures are deployed. SNSs are also expected to continue being the perfect place for social engineers to launch their attacks owing to other characteristics, such as easy and free joining and the variety of content that social engineers can make and use, such as news, stories, hyperlinks, photos, videos, and applications, which can be employed in many different attacks [20].

III. Method and Related Works

A holistic model for social engineering attacks has been proposed by Nohlberg and Kowalski (2008) [21]. However, their proposed model was based in the real life situation. Although social engineering in SNSs shares some characteristics of real life social engineering; however, social networking sites have other specific and unique characteristics. West, Mayhorn, Hardee, and Mendel (2009) have divided the factors that lead users to make poor security decisions into three categories: 1) user factors, such as problem solving limitation and decision making heuristic and experience; 2) technology factors, such as the credible appearance and personal relevance of an e-mail or a website that tricks the users; and 3) environmental factors, such as time pressure and inattention blindness, where users may not perceive details of the threat [22]. By looking at SNSs, we can see that they have specific and unique user, technological, and environmental factors that require a specific conceptualization.

In this paper, we present phase-based and source-based models of social engineering in SNSs using literature study.

The literature we have studied included some actual experimental research who have investigated the viability of using SNSs in social engineering attacks, e.g. [9], [14], [23], [24], interviewing information security specialists with years of extensive experience in social engineering, e.g. [25], and many other studies that review the state of the art in social engineering and SNSs' security. This has given us a comprehensive understanding of the concept, and allowed us to model it based on different perspectives.

IV. Models Describing Social Engineering in SNSs

A. Phase-Base Model

In order to model social engineering in SNSs, first we need to explain and conceptualize how the social engineer influences, persuades, and deceives victims to get them to offer up wanted information, or to perform actions that the social engineer wants them to do. Figure 1 explains the eight phases that social engineers in SNSs need to go through in order to trick the victims. The success of a social engineering attack is based on how well the attacker performs the following eight phases:

Phase 1: Using suitable gates of SNSs to gather information. Phase 1 involves information gathering about the victims in order to understand their vulnerabilities. This is an important phase in order to choose a perfect tactic and develop a good plan [26]. The information that will be gathered can be any available personal or organizational information, such as name, age, work, position, interests, hobbies, address, banks the victims deals with, friends the victim trusts, or even the car a victim dreams to have. Some of the information available might not be useful by its own; however, it can be used by a social engineer to gain more information that is valuable [27]. In section 3.2, we will explain the different gates of SNSs that social engineers can use to reach and gather such information.

Phase 2: Determining the tactic and developing a plan. Depending on the information gathered in the previous phase, and the goal the social engineers want to achieve, the social engineer will determine which tactic would be more suitable and successful to trick the victim. This phase also involves developing a good plan to reach the goal. The plan can include "pretexting," in which a social engineer creates a setting designed to persuade the victim to fall for the trick [28]. There are many commonly used techniques in social engineering. Those techniques include but are not limited to the following:

1) "Phishing," which is enticing a victim to download an attachment or to click on an embedded hyperlink [29]. This technique can be used to gather privacy information; manipulate users to type or provide critical information, such as their usernames and passwords [30]; or installing malicious backdoor programs that allow the attacker full access to the system [31]. Phishing attacks accounted for more than a quarter of all reported computer crimes in 2007 [32]. SNSs can be used to gather information such

as e-mail addresses, or any information that helps to trick the user to fall victim to phishing. Moreover, SNSs can be used easily and effectively to attract victims to respond to phishing.

2) "Persuasion and bribery," which is attempting to persuade an employee to do an action even if this action bypasses company rules. There are multiple means of persuasion, and one of them is giving a bribe to an employee [32].
3) "Shoulder surfing," This technique involves looking over an unsuspecting user's shoulder while the user is entering his/her user name and password or while he/she is doing his/her work. This is a kind of spying to gain valuable information [32]. This can be done in SNSs easily by spying over the activities, posts, tags, or comments that are made by the users.
4) "Spam," which involves sending messages to various people to ask for certain personal information, to get them to buy or sell products and services, or to ask them to participate or donate for charitable works [30].
5) "Dumpster diving," which is looking for valuable information in a company dumpster to find a phone directory, for example [32]. This can be done in SNSs, through diving into users' profiles, groups, events, and pages to look for any valuable information that can help directly or indirectly.
6) "Reverse attack," in which the attacker does not establish contact with the victim. Rather, the social engineer tricks victims into contacting him/her. In this case, the victim will be extremely trusting of the attacker, and the attacker will take the chance to ask the victim to give up any information or to do any action [33].

Phase 3: Relying on one or more socio-psychological factors. People, in general, think that they are good at detecting deception and lies. However, research indicates that people have weakness and therefore perform poorly in detecting social engineering attacks [34], [35]. On the organizational level, the findings of a study done by [36] suggest that social engineers could succeed even among those organizations that identify themselves as being aware of social engineering techniques. Marett, Biros, and Knode (2004) have explained that the reason why people are weak and perform poorly in detecting deception is because of the "lie detector bias," which is the assumption that most people are telling the truth [37]. Most of the books and studies that have been published regarding social engineering indicate that the main causes of human weaknesses that lead people to fall victim to social engineers are human socio-psychological characteristics [3], [30], [38], [39]. Human socio-psychological factors that influence users to certain behavior (e.g., liking, reciprocity, scarcity, social proof, fear, and strong affect) have been studied in marketing, in order to persuade customers to buy certain products [40].

Phase 4: Using suitable gates of SNSs to reach the victim. SNSs are not only useful for information gathering; they are also offer cheap and effective means of reaching victims and applying effective tricks [41]. Suitable gates will be discussed in more detail in the following section, the source-base model.

Phase 5: Wearing a suitable hat and playing a suitable character. The social engineer in this phase, based on the information gathered, the developed tactics and plan, and the socio-psychological factors, will choose a specific character to play. This character can be a very poor person, a sexy girl, a wonderful friend, or any other suitable character. Social engineers can also impersonate a real, well-known person to the victim, such as a real friend, boss, relative, or even a real famous person [42]. This task is much easier in social networking sites where users can make multiple fake profiles and choose their names, photos, location, and other details easily. At the same time, it is more difficult for the victim to uncover the deception through a social networking site than in a face-to-face, real-life situation. The social engineer, who may wear any hat that helps him/her to attract any victim, depending on the victim's vulnerabilities, can use the distance, anonymity, and absence of authentication mechanisms to abuse a victim [43]. The suitable hat shapes the character that the social engineer plays to make the victim feel trusting and safe and, therefore, to encourage the victim to accept the trick.

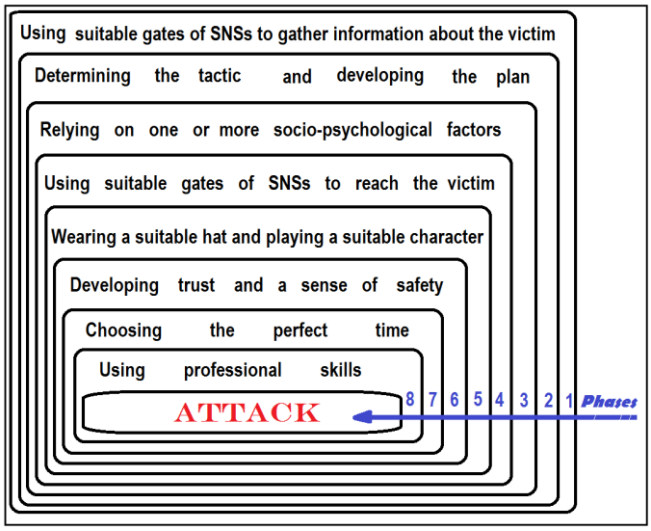

Fig. 1. Phase-based model of social engineering in SNSs.

Phase 6: Developing trust and a sense of safety. The success of social engineering is strongly tied to two main concepts: trust and safety. Those two concepts are related to human psychology and the experience of the victim. If the victim feels that he/she trusts the social engineer, or feels a sense of safety toward the trick made by the social engineer, then the probability of the success of the trick will be high. This requires that the social engineer go through additional tricks or wait for a certain amount of time before launching the attack. Trust and a sense of safety can affect social engineering in the following ways:

1) Trust: It plays a vital role in social engineering; however, *trust* is a complicated word with multiple dimensions that lead to multiple meanings. It is used as a word or concept with no real definition [44]. Nevertheless, some researchers (e.g., [45], [46] indicate that some people have a greater tendency to trust generally than do others. The trusting nature among human beings is not similar, and people believe what others say, depending on the

trust they build. According to Mitnick and Simon (2001), a person who is under-trusting stands to lose a given benefit or opportunity, is paranoid, and always tense. Whereas, those who are overly trusting will monitor their actions less often and will be less efficient and possibly incompetent; therefore, social engineers will target them, which could result in the loss of money or useful information. Being overly trusting limits the cognitive functions of people in relation to their surroundings, such that they become so comfortable that their thoughts, actions, and attention is limited, thus making them subjects of manipulation [47].

2) Safety. According to Pyszczynski, Greenberg, and Solomon, (1997), when people are threatened, they will alter their behavior depending on the number of risks they can accommodate. This modification is a psychological reaction that is determined by the seriousness of an attack and the amount of loss that they think will be incurred because of the occurrence of a hazard [48]. For attackers, the ability to determine the maximum amount of threat that a person is willing to accommodate determines when to launch an attack [1]. Pyszczynski, Greenberg, and Solomon, (1997), has introduced a relationship between behavior and threat through the health belief model (HBM) [48]. This theory indicates that the probability of performing a risky action is determined by the perceived threat of taking that action and the perceived benefit of taking that action. The HBM indicates also that the perceived threat of taking an action is determined by the susceptibility to the threat and the seriousness of the threat [48]. Aldoory and Van Dyke (2006) went further, stating that the problems of performing a risky action have been associated with the HBM and the situational theory of publics [49]. The latter suggests that a population can be classed depending on how they behave, that is whether they are active or passive [50]. The psychological issues concerned with this theory include 1) the extent of activity in the behavior, 2) familiarization with problems, and 3) the knowledge of constraints [51].

Phase 7: Choosing the perfect time. This phase involves seizing the best moment to launch the attack. Time pressure, for example, can affect the decisions that people make [52]. Time pressure affects the logical functioning of human judgment, and, therefore, under it, the victim is more willing to accept arguments that should be challenged [53]. In SNSs, a social engineer can watch the victims' activities, posts, comments, and mode statuses to find the perfect moment to launch the attack or apply the planned trick.

Phase 8: Using professional skills. The last task of the social engineer will determine the success of all of the previous phases. It involves performing a good scenario and dialogue with the victim, and avoiding any mistake that can help the victim to discover the deception [1]. The scenario and dialogue in SNSs can involve interaction with the victim through chatting, for example, or it can be through the content of the pages, profiles, and the walls, such as posts, tags, and comments. The professional skills include, for example, tact, persuasion, flattering, lobbying, or any social skills, depending on the situation of the victim and the type of trick.

B. Source-Base Model

In the previous model (Fig. 1), we have described the different phases of the social engineering attack. In phase 1 and phase 4, we have mentioned that there are different gates or sources of threats that the social engineer can enter through or use to gather information in order to understand the victim, to reach the victim, or to launch the attack trick. In this section we will explain those gates in more detail and discuss how different social engineering tactics or attacks work. The source-based model of social engineering in SNSs is shown in Fig. 2. The three sources or gates of threats in SNSs are the following:

1) Insecure privacy setting

Most SNSs classify users in relation to others, as a "friend," "friend of friend," or "unfriend" (public users). Some of them also allow users to divide their friends into different groups; each group has different privacy setting. However, by recognizing SNSs, we can see that a large percentage of users' profiles are set to be shown publicly to any users in the social networking site, or even to any user from outside that site who uses any web search engine, such as Google or Yahoo!. Research indicates that the profile details of more than 100 million Facebook users were publicly accessible through search engines [9]. Other profiles are set to be shown to friend-of-friend users, or to all friends. The risk associated with making those profiles accessible or shown to others is high, and it is more dangerous for those who make their profiles shown publicly, than those who are open to friend-of-friend users or to all friends.

Users who own public profiles either set their profiles to be accessible publicly intentionally for different reasons, or because they did not change the default privacy setting of their profiles [9]. The steps that the social engineers go through in order to gain any information from any user of SNSs is illustrated in Fig. 3. The more "Yes" the social engineer faces through the activity diagram, the more easily and quickly he/she reach the goal; the more "No" he/she faces, the more difficult it is to reach the goal.

The users of SNSs are highly willing to reveal private or personal information on their profiles [9]. This information includes their names, birthdays, work, locations, telephone numbers, addresses, e-mail addresses, real photos, and many others critical information. Users, with the information they reveal online, expose themselves to social engineers who can use this information to launch various physical and cyber attacks. Their home addresses and e-mail addresses, for example, can be used in phishing [14]. Photos, names, birthdays, and addresses can be valuable information for pretexting, identity theft, impersonation, and other kinds of threats [23].

Profile publicity, availability, or accessibility to or by strangers, even if they are a friend of friend, is not a threat for the user alone, and it can lead to three types of threats. The first is individual vulnerability, where an individual is open to identity theft, physical attack, phishing, and so on [23]. The second is friends' vulnerability, for example, the attacker impersonates a user to gain the trust of one of his/her friends

[33]. The third is organization vulnerability, where, for example, an attacker crosses an organization's security defenses through impersonating one of its employees [29], or manipulates one of its employees to perform an action that leads to an attack on the organization, such as downloading malicious software that aims to attack the organization's system.

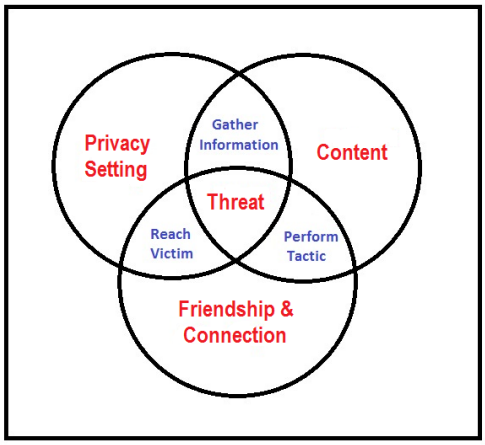

Fig. 2. Source-based model of social engineering in SNSs.

2) Friendship and connection with strangers

People have some psychological motives, such as entertainment or meeting new people, that can encourage them to talk with strangers over the Internet [54], [55]. Social engineers can use the psychological trick of starting a "friendship" with the victims in order to build trust between the attacker and the victims, and then abuse this trust to launch an attack. This type of attack could be to gain critical information from the victim or to get the victim to perform an action that benefits the attacker and hurts the victim or his/her organization [25]. Finding new friends is one of the most common features of SNSs. This allows social engineers to find any user easily by using the search engine of that site or using any other web search engine, in some cases, and then sending a friendship request.

Most SNSs allow any user to choose the name, photo, age, school, and other personal information freely. This makes it easy for the social engineer to impersonate any identity in order to gain trust from the victim. When the victim accepts the friendship invitation, the social engineer can establish a direct connection, engage in small talk, or act as if he/she has the same interests, problems, or experiences of the victim [10]. Moreover, being in a "friend list" of a victim, allows the social engineer to spy on posts or activities that the victim makes. Moreover, some social network sites automatically recommend new friends for the users depending on some common elements, such as friends, schools, or groups in common. This feature can lead to another important other technique of social engineering called reverse attack. In this attack, the social engineer connects to the victim's friends first, so that the victim gets tricked into contacting the social engineer him/herself [33].

Social engineers can also use specialized spamming software such as FriendBot, to automate sending friendship invitations [12]. Another example of such software is "Facebook blaster," which can be used to collect a huge number of users' IDs and send huge amounts of friend requests and messages to users [24]. This is a very dangerous tool because it can select specific groups of users based on specific criteria to launch a specific attack. That is, it possible for the attacker to target specific organization's employees with specific attacks, such as phishing, viruses, or malware, and the success probability of such attacks is high.

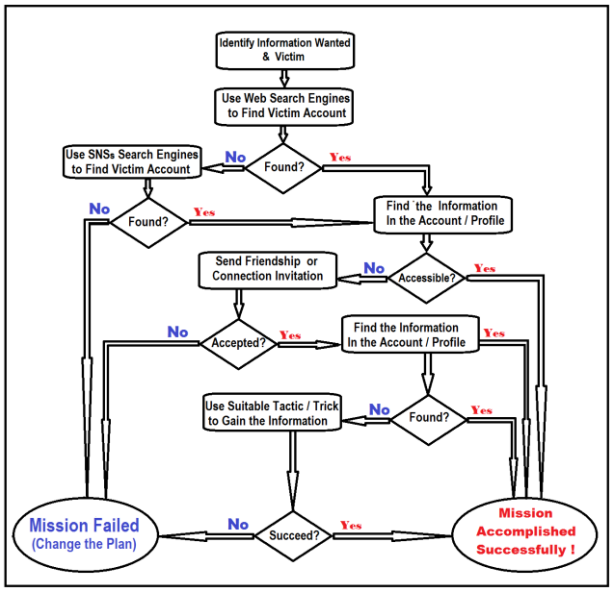

Fig. 3. Activity diagram for information gaining in SNSs.

3) Insecure dealing with content

Content is all available information in users' profiles and different pages or groups, such as news stories, blog, tags, posts, notes, videos, photos, hyperlinks, and so on. Users of Facebook, for example, share more than 30 billion pieces of content each month [20]. Insecure dealing with the content available on the SNSs leads people to fall victim to many social engineering threats. The content may have malicious software such as viruses and worms. This can be embedded in the posts or messages through a hyperlink that leads to an executable file, for example, or to a hyperlink of a page that includes another hyperlink to an executable file with some instructions that trick the victim to download that file [12].

Phishing is also a potential threat of dealing insecurely with content. Phishing can be posted in SNSs as a story, offer, or alert message that attract victims to download an attachment or click on an embedded hyperlink. The aim of phishing is to manipulate users to provide critical information, such as username and password [30], or to install malicious backdoor programs that allow the attacker full access to the system [31].

Spam is another example of such threats, and it is a critical issue, since research suggests that SNSs may replace e-mail as a means of communication [12]. Moreover, for those SNSs that allow users to post HTML in their profiles, users are vulnerable to cross-site scripting attacks (XSS), which enable attackers to install client-side script into a profile that is viewed by other users [12]. In addition, there is "defamation" and "ballot stuffing," which are forms of attack that aim to destroy the reputation of a person or system [56].

Finally, the social engineer can use the content to trick the victim to reveal some information when they comment under

that content or when they share it. Commenting and sharing provide an alternative means of interaction with victims when the victim rejects the friendship invitation that the social engineer has sent. Groups, pages, and events accounts that allow users to post, comment, tag, and read are perfect ground for social engineers who want to reach large numbers of victims.

V. Conclusion

SNSs are among the most common means of social engineering attacks. In this paper, we have explained the risks associated with SNSs in terms of social engineering. We have presented two conceptual models; each is based on different aspects. Phase-based, and source-based models have been presented along with an intensive and comprehensive overview of social engineering attacks in social networks sites. We have explained that successful attackers of SNSs go through eight different phases, and come from three common sources. By using these two models, researchers can get a fuller picture of social engineering threats in SNSs, and take one of many possible directions of further research.

References

[1] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*, Wiley, 2001.

[2] C. Hadnagy, *Social engineering: The art of human hacking*, Wiley, 2010.

[3] D. P. Twitchell, "Social engineering in information assurance curricula," in *Proc. The 3rd annual conference on Information security curriculum development*, 2006, pp. 191-193.

[4] B. Blunden, "Manufactured Consent and Cyberwar," in *Proc. LockDown Conferenc*, 2010.

[5] N. B. Ellison, "Social network sites: Definition, history, and scholarship," *Journal of Computer‐Mediated Communication*, vol. 13, pp. 210-230, 2007.

[6] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: challenges and opportunities," April 2010.

[7] S. T. Thompson, "Helping the hacker? Library information, security, and social engineering," *Information Technology and Libraries*, vol. 25, pp. 222-225, 2013.

[8] R. G. Brody, "Flying under the radar: social engineering," *International Journal of Accounting and Information Management*, vol. 20, pp. 335-347, 2012.

[9] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in *Proc. the 2005 ACM workshop on Privacy in the electronic society*, 2005, pp. 71-80.

[10] D. Rosenblum, "What anyone can know: The privacy risks of social networking sites," *Security & Privacy, IEEE*, vol. 5, pp. 40-49, 2007.

[11] R. Gibson, "Who's really in your top 8: network security in the age of social networking," in *Proc. The 35th annual ACM SIGUCCS fall conference*, 2007, pp. 131-134.

[12] G. Hogben, "Security issues and recommendations for online social networks," *ENISA position paper*, vol. 1, 2007.

[13] J. Nagy and P. Pecho, *Social Networks Security*, pp. 321-325, 2009.

[14] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Communications of the ACM*, vol. 50, pp. 94-100, 2007.

[15] T. Mataracioglu and S. Ozkan, "User Awareness Measurement Through Social Engineering," *arXiv preprint arXiv:1108.2149*, 2011.

[16] M. Huber, S. Kowalski, M. Nohlberg, and S. Tjoa, "Towards automating social engineering using social networking sites," in *Computational Science and Engineering, 2009. CSE'09. International Conference on*, 2009, pp. 117-124.

[17] M. Huber, "Automated social engineering, proof of concept," *Royal Institute of Technology Stockholm*, 2009.

[18] G. M. Weiksner, B. Fogg, and X. Liu, "Six patterns for persuasion in online social networks," *Persuasive Technology*, 2008, pp. 151-163.

[19] B. Fogg and D. Iizawa, "Online persuasion in Facebook and Mixi: a cross-cultural comparison," *Persuasive Technology*, 2008, pp. 35-46.

[20] S. Abu-Nimeh, T. Chen, and O. Alzubi, "Malicious and spam posts in online social networks," *Computer*, vol. 44, pp. 23-28, 2011.

[21] M. Nohlberg and S. Kowalski, "The cycle of deception: a model of social engineering attacks, defenses and victims," in *Proc. The Second International Symposium on Human Aspects of Information Security and Assurance (HAISA 2008)*, 2008, pp. 1-11.

[22] R. West, C. Mayhorn, J. Hardee, and J. Mendel, "The Weakest Link: A Psychological Perspective on Why," *Social and Human Elements of Information Security: Emerging Trends*, 2009.

[23] S. Alim, D. Neagu, and M. Ridley, "Axioms for vulnerability measurement of online social network profiles," *Information Society (i-Society), 2011 International Conference on*, 2011, pp. 241-247.

[24] D. Michalopoulos and I. Mavridis, *Surveying Privacy Leaks Through Online Social Network*, 2010.

[25] Y. Scheelen, D. Wagenaar, M. Smeets, and M. Kuczynski, *The devil is in the details: Social Engineering by means of Social Media*, 2012.

[26] T. Thornburgh, "Social engineering: the dark art," in *Proc. The 1st annual conference on Information security curriculum development*, 2004, pp. 133-135.

[27] G. L. Orgill, G. W. Romney, M. G. Bailey, and P. M. Orgill, "The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems," in *Proc. The 5th conference on Information technology education*, 2004, pp. 177-181.

[28] M. Workman, "Wisecrackers: A theory‐grounded investigation of phishing and pretext social engineering threats to information security," *Journal of the American Society for Information Science and Technology*, vol. 59, pp. 662-674, 2008.

[29] K. Coronges, R. Dodge, C. Mukina, Z. Radwick, J. Shevchik, and E. Rovira, *The Influences of Social Networks on Phishing Vulnerability*, pp. 2366-2373, 2012.

[30] J. Mohebzada, A. El Zarka, and A. Bhojani, "COE444 Spring 2010: Research Project Report," 2010.

[31] S. D. Applegate, "Social Engineering: Hacking the Wetware," *Information Security Journal: A Global Perspective*, vol. 18, pp. 40-46, 2009.

[32] R. L. Richardson, "CSI survey 2007: The 12th annual computer crime and security survey," Computer Security Institute, 2007.

[33] D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, and C. Pu, "Reverse social engineering attacks in online social networks," *Detection of Intrusions and Malware, and Vulnerability Assessment*, 2011, pp. 55-74.

[34] T. Qi, "An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering," *Intelligence and Security Informatics, 2007 IEEE*, 2007, pp. 152-159.

[35] S. Grazioli, "Where did they go wrong? An analysis of the failure of knowledgeable Internet consumers to detect deception over the Internet," *Group Decision and Negotiation*, vol. 13, pp. 149-172, 2004.

[36] D. Kvedar, M. Nettis, and S. P. Fulton, "The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition," *Journal of Computing Sciences in Colleges*, vol. 26, pp. 80-87, 2010.

[37] K. Marett, D. P. Biros, and M. L. Knode, "Self-efficacy, training effectiveness, and deception detection: A longitudinal study of lie detection training," in *Intelligence and Security Informatics*, ed: Springer, 2004, pp. 187-200.

[38] M. Bezuidenhout, F. Mouton, and H. Venter, "Social engineering attack detection model: SEADM," *Information Security for South Africa (ISSA), 2010*, 2010, pp. 1-8.

[39] M. Pattinson, C. Jerram, K. Parsons, A. McCormac, and M. Butavicius, "Why do some people manage phishing e-mails better than others?" *Information Management & Computer Security*, vol. 20, pp. 18-28, 2012.

[40] R. B. Cialdini, *Influence: Science and practice*, Boston: Allyn & Bacon, 2001.

[41] W. Luo, J. Liu, J. Liu, and C. Fan, *An Analysis of Security in Social Networks*, pp. 648-651, 2009.

[42] T. R. Peltier, "Social Engineering: Concepts and Solutions," *Edpacs*, vol. 33, pp. 1-13, 2006.

[43] A. Orita and H. Hada, "Is that really you?: an approach to assure identity without revealing real-name online," in *Proc. the 5th ACM workshop on Digital identity management*, 2009, pp. 17-20.

[44] T. Bhuiyan, A. Josang, and Y. Xu, "Trust and reputation management in web-based social network," *Web Intelligence and Intelligent Agents*, pp. 207-232, 2010.

[45] Y.-H. Chen and S. Barnes, "Initial trust and online buyer behaviour," *Industrial Management & Data Systems*, vol. 107, pp. 21-36, 2007.

[46] A. Charbaji and S. E. L. Jannoun, "Individuality, willingness to take risk, and use of a personal e-card: A Lebanese study," *Journal of Managerial Psychology*, vol. 20, pp. 51-58, 2005.
[47] M. Workman, "A test of interventions for security threats from social engineering," *Information Management & Computer Security*, vol. 16, pp. 463-483, 2008.
[48] I. M. Rosenstock, "Historical origins of the health belief model," *Health Education & Behavior*, vol. 2, pp. 328-335, 1974.
[49] J. E. Grunig, D. Moss, and T. MaCmanus, "A situational theory of publics: Conceptual history, recent challenges and new research," *Public relations research: An international perspective*, vol. 3, pp. 48, 1997.
[50] L. Aldoory and M. A. Van Dyke, "The roles of perceived "shared" involvement and information overload in understanding how audiences make meaning of news about bioterrorism," *Journalism & Mass Communication Quarterly*, vol. 83, pp. 346-361, 2006.
[51] O. Brafman and R. Brafman, *Click: The Forces Behind How We Fully Engage With People, Work, and Everything We Do: Crown Pub*, 2011.
[52] K. R. Hammond, *Judgments under stress*, Demand: Oxford University Press, 2000.
[53] R. E. Petty, P. Briñol, and Z. L. Tormala, "Thought confidence as a determinant of persuasion: The self-validation hypothesis," *Journal of Personality and Social Psychology*, vol. 82, pp. 722-741, 2002.
[54] J. Peter, P. M. Valkenburg, and A. P. Schouten, "Characteristics and motives of adolescents talking with strangers on the Internet," *CyberPsychology & Behavior*, vol. 9, pp. 526-530, 2006.
[55] S. Vandoninck, L. d'Haenens, R. De Cock, and V. Donoso, "Social networking sites and contact risks among Flemish youth," *Childhood*, vol. 19, pp. 69-85, 2011.
[56] L. A. Cutillo, R. Molva, and T. Strufe, "Safebook: A privacy-preserving online social network leveraging on real-life trust," *Communications Magazine, IEEE*, vol. 47, pp. 94-101, 2009.

Abdullah Algarni is a faculty member at Institute of Public Administration, Saudi Arabia. His previous works included training, teaching, consultation and research. He is currently a doctoral candidate at Queensland University of Technology (QUT), Brisbane, Australia. He has completed his Master degree in Computer Science from Western Michigan University, Kalamazoo, United States, in 2009, and Bachelor degree in Computer Science from King Abdulaziz University, Jeddah, Saudi Arabia, in 2005. His current research interests are mainly in the area of social engineering, human behaviour, and information security.

Yue Xu obtained a PhD in Computer Science from University of New England, Armidale, NSW, Australia, in 2000. Currently, she is an associate professor in the School of Electrical Engineering and Computer Science, Queensland University of Technology (QUT), Brisbane, Australia. Previously, she was a Senior lecturer and Lecturer at QUT. Before joining QUT, she was a Lecturer in University of Tasmania, a visiting research scholar in Chinese University of Hong Kong, Research Associate Professor in Institute of Software, Chinese Academy of Sciences.

Associate Professor Xu's current research interests include data mining and web intelligence, especially association rule mining and Web based recommender and reputation systems. She has published over 140 refereed papers. She has been a program committee member for many conferences and the workshop chair of the International Workshop on Web Personalization and Recommender Systems from 2007 to 2013. She is also the guest editor of a special issue on Journal of Emerging Technologies in Web Intelligence and a special issue on Journal of Web Intelligence and Agent Systems.