Social Engineering:
The Neglected Human Factor for Information Security Management

Xin (Robert) Luo, The University of New Mexico, USA

Richard Brody, The University of New Mexico, USA

Alessandro Seazzu, The University of New Mexico, USA

Stephen Burd, The University of New Mexico, USA

ABSTRACT

Effective information systems security management combines technological measures and managerial efforts. Although various technical means have been employed to cope with security threats, human factors have been comparatively neglected. This article examines human factors that can lead to social engineering intrusions. Social engineering is a technique used by malicious attackers to gain access to desired information by exploiting the flaws in human logic known as cognitive biases. Social engineering is a potential threat to information security and should be considered equally important to its technological counterparts. This article unveils various social engineering attacks and their leading human factors, and discusses several ways to defend against social engineering: education, training, procedure, and policy. The authors further introduce possible countermeasures for social engineering attacks. Future analysis is also presented.

Keywords: *Human Factors, Information Security, Personality Traits, Security Management, Social Engineering*

INTRODUCTION

Information systems (IS) security management depends not only on technological measures but also on managerial endeavors. A plethora of technological methods have been developed to address various security issues but human factors that contribute to significant security breaches have been comparatively neglected. The salient key to derailing potential aggressors is a combination of technical, behavioral, and procedural countermeasures. Imagine receiving a phone call in which someone claiming to work for an official agency suggests that you reveal certain information to help repair an urgent system problem. You willingly help the caller who is, in reality, a fraudster seeking access to private information. The success of this social engineering attack relies on the natural helpfulness of human users, their psychological weaknesses, and their tendencies to be unaware of the value of the information they possess and to be sloppy about shielding their information.

DOI: 10.4018/irmj.2011070101

Within the context of computer and information security, social engineering (SE) is a combination of techniques used to manipulate victims into divulging confidential information or performing actions that compromise security (Mitnick & Simon, 2002). SE attackers, in general, tend to exploit human cognitive biases. SE attacks are non-technical intrusions that rely on human interactions, potentially bypassing technological security mechanisms. Workman (2007) explained that the emotional aspect of the interaction distracts human users and serves to interfere with the potential victim's ability to carefully analyze the content of the message delivered by social engineers (p. 316). He further indicated that, due to human factors, *knowing better but not doing better* is one of the key scholarly and practical issues that has not been fully addressed, particularly in the IS security management paradigm (Workman, 2008). SE is undoubtedly one of the weakest links in the domain of IS security management, because it is beyond technological control and subject to human nature.

Prior studies on SE generally tended to focus on technological cues triggering the attacks. Behavioral factors for the SE attacks are not usually described and systematically analyzed. As such, this paper contributes to the literature of IS security by holistically analyzing the human behavioral factors that are associated with SE attacks. In addition to extending previous research on SE, we specifically study behaviors and personality traits that are rooted in social psychology and criminology. We believe that this study can theoretically advance behavioral IS security research in the domain of SE management and control, and could also pragmatically inform organizational decision-makers of how individual employees can deal with the ever increasingly sophisticated SE attacks. It is hoped that this study can offer instrumental insights to the often neglected human aspects of information systems security management.

The remainder of this paper is organized as follows. We first revisit the theoretical bases in social psychology in order to analyze three key aspects related to SE. Then we further draw on criminology and social psychology to discuss the personality traits versus SE attack vulnerabilities. The technical and non-technical means that SE attackers can employ are presented next, followed by a proposed multi-dimensional approach including policies, procedures, standards, employee training and awareness programs, and incident response for more effective and efficient IS security management. The paper concludes with a discussion of future SE analysis and suggestions for future research.

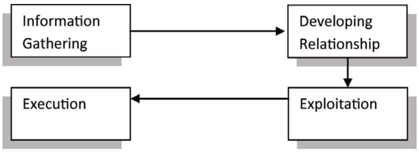
PSYCHOLOGICAL ASPECTS

Recent research has discovered that there are certain terms and techniques that are associated with SE and go perhaps far beyond technology and more so into human error and social psychology (Peltier, 2006). Three key aspects of social psychology, *alternative routes to persuasion* (i.e., central route and peripheral route), *attitudes and beliefs that affect human interactions*, and *techniques for persuasion and influence*, could help explain the emotional cues for manipulated SE attacks (Peltier, 2006).

In a central route to persuasion, SE attackers persuade victims to provide desired information without fabricating unreal scenarios. Thus, this comparatively direct route, which depends on the responder's logical thinking toward the marshaled information from the attacker, does not normally succeed. The other route, *peripheral route to persuasion*, can be leveraged by SE attackers to bypass logical argument and counterargument and seek to trigger intrusion. In the peripheral route to persuasion, the attacker tends to make the intended victim more susceptible to persuasion by triggering strong emotions such as fear or excitement in order to interfere with the victim's ability to respond.

Attitudes and beliefs refer to the differences between the victim's attitude and beliefs about the SE attacker and SE attacker's attitudes and beliefs about his anticipated or definite victims. Rooted in social psychology, *persuasion and influence techniques* rely on peripheral routes

Figure 1. Four-step social engineering attack (adapted from Allen, 2006)



to persuasion that are effective to influence others. Six factors can constitute effectual persuasions: authority, scarcity, liking and similarity, reciprocation, commitment and consistency, and social proof (Rusch, 1999).

Furthermore, SE attacks are categorized into human-based and technology-based intrusions. Human-based attacks are interactions between the attacker and the victim who possesses valuable information. In contrast, technology-based attacks access confidential information by employing computer software programs such as pop-up windows, e-mail attachments, and websites, etc. While maliciously generated e-mail attachments and websites seek the victim's natural tendency to trust others to divulge information or perform actions, a vicious script-embedded pop-up window manipulates the victim's psychological fear of getting into trouble by repeatedly prompting the victim to re-enter his/her user username and password because the network connection was interrupted and the window will surreptitiously deliver the information entered to the attackers.

According to Allen (2006), and as shown in Figure 1, a typical SE attack is composed of four steps: information gathering, relationship development, exploitation, and execution. An SE attacker initially gathers information about the target(s) such as names, phone numbers, birth dates from publicly-accessible information such as directories and organizational charts. Applying this information, he then can try to build rapport with the intended victim to gain his/her trust. Exploiting the established trust, the SE attacker can then persuade the victim to perform desired actions (i.e., revealing confidential information) which would not normally occur otherwise. In the last stage, the attacker uses the information collected from the victim to carry out attacks.

PERSONALITY TRAITS

This section discusses how SE attackers can exploit different psychological phenomena to specifically recognize the psychological and/or behavioral vulnerabilities of the potential victim in a bid to obtain desired information. These leading psychology-driven personality traits for possible SE attacks include *diffusion of responsibility*, *chance for ingratiation*, *trust relationship*, and *guilt* (Peltier, 2006).

Originating from social psychology and criminology, diffusion of responsibility explains that an individual (i.e., criminal) acting alone, compared with an individual group member, would be held more responsible for behavior leading to a negative consequence. Relating this psychological trigger to SE, researchers have found that targeted victims are made to believe that they are not solely responsible for their actions and this trait works well with *moral duty* when the individual victim conceives that what he/she responds to is of vital importance to the company or its employees (Gragg, 2003; Peltier, 2006). As such, the victim surmises that his/her actions could make the difference between success and failure of the company or the so-called *employee* (the actual SE attacker). Thus, the victim tends to comply with the request to avoid the feeling of guilt.

According to Peltier (2006), chance for ingratiation is when victims are led to believe that compliance with a request will enhance their chances of receiving some benefit. This process includes such psychological motives as gaining advantage over a competitor and getting in good with management. *Authority* plays a vital role since people are conditioned to respond to authority figures without painstakingly verifying their legitimacy (Gragg, 2003). Peltier (2006) also found that gender issue, normally opposite sex, can trigger effective and positive persuasions resulting in successful SE intrusions. This perspective is in line with such research as Guadagno and Cialdini (2002) in that a charming or sweet voice of the opposite sex can generally lead to more effective and successful persuasions or interpersonal influences.

SE attackers also tend to establish trust relationships with their intended victims through seemingly innocent conversations or email communications. Human nature is to trust others until they prove they are not trustworthy (Peltier, 2006). Many people, especially customer service agents, help desk receptionists, and business assistants or secretaries who are trained to assist people and not to question the validity of each request, tend to trust others and are naturally helpful. Trust can be built through a number of small interactions which SE attackers try to maintain with the victims. A sign of positive trust is when the victims can recognize the attacker's voice and are willing to converse with and assist the attacker. Some seemingly *mundane* information, such as knowing someone is on vacation and names of children, spouse and pets, can be effortlessly revealed by these victims through a series of slow and casual yet deceitful correspondence and are of vital value to SE attackers, who then can implement a fraudulent plan.

Successful SE attacks can also be triggered by feelings such as guilt and sympathy. Human users have a tendency to believe other's expressed attitudes (e.g., sad voice), behaviors (e.g., facial signs), and statements (e.g., poor performance) are true, and these individuals may attempt to avoid guilt. SE attackers may exploit this weakness by confiding with the intended victims that they have failed to accomplish things and their survival solely depends on the victims' assistance, otherwise significant consequence (normally sad or negative) may occur.

SOCIAL ENGINEERING TECHNIQUES

There are various technical and non-technical means that SE attackers can employ, such as pretexting, phishing, online social engineering, shoulder surfing, and dumpster diving, in order to collect data which can be processed for the attackers to access privileged information. Since users are not aware of the value of the information they possess and are thus careless about protecting it, they tend to reveal weaknesses which may result in unnoticeable (for users themselves) mistakes that potential SE attackers can manipulate.

As the most commonly used SE technique, pretexting is the act of creating and using a contrived scenario to persuade a potential victim to voluntarily reveal information or perform actions. In the business domain, pretexting can be used to manipulate such victims as junior company service representatives into disclosing sensitive information such as customer information, account details, and telephone records through a telephone conversation. Alternatively, the SE attacker might pretend to be a senior member of an organization, pressuring junior members into disclosing useful information which he can leverage to set up remote access to the organization's resources. This simple yet effective attack focuses on the vulnerable psychological aspect of a human user who tends to be helpful to satisfy *customers or important users* of the organization.

Phishing, by contrast, is a two-time scam technique of fraudulently obtaining private information. Typically the attacker sends a masqueraded e-mail that appears to originate from a legitimate business, such as a bank or credit card company, requesting "verification" of information and warning of some significant consequences if it is not in accordance with the request. A variant is use of a counterfeit interactive voice response system to harvest personal information such as pin numbers, social security numbers, and account numbers. Phishing attackers may pretend to be a customer service or help desk agent who might be able to deceive victims, who are seeking assistance, to divulge private information.

Two additional human-behavioral SE approaches are shoulder surfing and dumpster diving, which might be the oldest forms of SE attack. Shoulder surfing is when someone peeks over victim's shoulder to obtain his/her private information such as access codes and passwords which the victim types on a keypad (i.e., to enter the office or corporate building). The process of engaging in shoulder surfing assumes that the attacker can memorize the victim's confidential information entered and reproduce it for malicious use subsequently. To obtain potentially useful information, attackers may also resort to seemingly useless garbage. Dumpster diving is the practice of sifting through commercial or residential trash to find items that have been discarded for being unusable by their owners. Some SE attackers presuppose that sensitive information, such as manuals, phone books, checks, credit card and bank statements or other corporate commercial records, might be carelessly thrown away. They can use discarded information to obtain private information and to launch SE attacks subsequently.

EFFECTIVE DEFENSES AGAINST SOCIAL ENGINEERING

Because of the sophisticated personality traits that different individuals posses, it is almost impossible to fully protect organizations against SE attacks. As the weakest link of the security management frontline, SE intrusions that are triggered by human factors cannot be simply deferred or mitigated through a technical route which is relatively straightforward against software or hardware malfunctions. As such, technology (i.e., firewall, biometric authentication, and data encryption) alone cannot be the panacea. Instead, a multi-dimensional approach including technology, policies, procedures, standards, employee training and awareness programs, and incident response should be employed to more effectively and efficiently cope with the ever-present threat to the IS security management.

A policy conveys instructions from an organization's senior-most management to those who make decisions, take actions, and perform other duties (Whitman & Mattord, 2009). According to Peltier (2006), organizations should 1) develop clear, concise security policies that are enforced consistently throughout the organization; 2) develop simple rules defining what information is sensitive and develop a data classification policy (i.e., use internal website to answer questions and give advice); and 3) require the requestors identity when restricted actions are required. Despite the inherent personality traits that employees posses across departments, an information security policy can ensure a clear direction on what is expected of employees within the organization (Gragg, 2003). Pragmatically, with strong support from senior management, employees who comply with and have paid attention to such policy may more effectively respond to questionable requests and resist the intruder's pleas. The policy can also guide employees to think seriously about the information's value and further strengthen their confident resistance to persuasion. From a theoretical perspective, Petty et al. (2002) employed persuasion theory and found that increasing employee confidence by laying out clear policies decreases the chance that the persuader will have undue influence on an employee.

A procedure is series of actions that are always carried out by the same method and in the same order to achieve the same result. Policy dictates the circumstances that trigger the procedure and the same procedure might be triggered by multiple policies. This relationship between policy and procedure must be ongoing and consistently reinforced to employees. Based on the recommendations offered by Mitnick and Simon (2002) and Thornburgh (2004), organizations should facilitate prompt recognition of and appropriate reaction to SE attacks by training employees to recognize and properly respond to requestors who: 1) refuse to give a callback number; 2) make out-of-the ordinary requests; 3) claim senior authority; 4) stress urgency; 5) threaten negative consequences of noncompliance; 6) show discomfort when questioned by employees; and 7) use the name dropping technique. Along with these practical procedures, it is essential that proper procedures be emphasized, reinforced, and implemented throughout organizations, as suggested by (Peltier, 2006). For instance, employees who work in the business service areas (i.e., front desk) must require proper identification confirmation from anyone to perform a service.

A standard should also fortify the process of identification validation (e.g., business badge and phone number or caller-ID cross-examination with the relevant department) as well as the management of password (e.g., no Post-it notes entailing passwords left in the office). In addition, password procedure and standard such as the frequency of password change and sophistication of password setup must be bolstered and maintained by both IT department and management so as to avoid password change/reset request over the phone or email. To thwart dumpster divers, organizations should also more securely manage disposed commercial materials by utilizing business shredders on a regular (preferably daily) basis.

Mitigation measures should also shed light on human behavioral aspects through employee security education, training, and awareness (SETA) programs in organizations. To tackle acts of human error or failure, SETA can benefit organizations in terms of improving employee behavior, informing members of the organization about where to report violations of policy, and enabling the organization to hold employees accountable for their actions (Whitman & Mattord, 2008). A consistent SETA implementation enables employees to understand the value of the organization's information and to understand their role in overall SE protection strategy (i.e., better resistance to persuasion). To more effectively facilitate the implementation of SETA endeavors, it has been suggested by Peltier (2006), Gragg (2003), and Whitman and Mattord (2008) that such concrete intra-organizational initiatives as distributing newsletters, bulletins, posters, or internet WebPages to disseminate up-to-date security news, recognizing employees for their proper reactions and responses to security threats, circulating regular and creative reminders for the potential dangers, and developing "information security awareness days", etc., shall have a positive impact on the behavioral responses and reactions of employees with regard to potential SE attack recognition and discrimination.

FUTURE RESEARCH

SE attacks are unpredictable because they can surface from external and internal sources. However, we believe that the likelihood of such attacks can be mitigated if employees, at all levels of the organization, perceive their importance to the overall SE protection strategy and thereby exert concerted efforts to lessen the impact of SE attacks. Nonetheless, we must recognize the dilemma that, due to the inevitable exposure to SE attacks, organizations and their employees are at a manifest disadvantage facing infrequent SE intrusions and yet need to be on constant vigilance whereas the SE aggressors can practice SE attacks willingly.

With the mushrooming emergence of social network websites including Classroom.com, MySpace.com, Facebook.com and YouTube.com where inexperienced college students look to keep in touch with their friends and expand social connections, SE aggressors might easily exploit the illogical social reactions of these potential victims to aggravate our campaign against SE attacks. It is hoped that proper security tactics and defends, along with education efforts, shall also be rendered to expanded population segments in a bid to minimize the danger toward SE in our everyday's life. Future research is therefore encouraged to gauge and analyze how SE can be conducted through these social networks and further into organization's networks.

CONCLUSION

Albeit a low-tech level attack, SE can manipulate victims to divulge confidential information due to our illogical understanding or misconception triggered by inherent personality traits. Therefore, in addition to advanced technologies counterattacking various security intrusions, human factors must be equally accounted for effective IS security management. Exploiting the cognitive biases of humans and corporate policies to obtain access to desired resources, SE aggressors can circumvent organization's network infrastructure which however is vulnerable to this seemingly old-fashioned manipulation. To be able to defend themselves from being victimized, employees must withhold commitments from potential SE threats through the consistent implementation of SETA which organizations must continuously instigate with vigilance.

REFERENCES

Allen, M. (2006). *Social Engineering: A Means to Violate a Computer System*. Bethesda, MD: SANS Institute.

Gragg, D. (2003). *A Multi-Level Defense Against Social Engineering*. Bethesda, MD: SANS Institute.

Guadagno, R. E., & Cialdini, R. B. (2002). Online Persuasion: An Examination of Gender Differences in Computer-Mediated Interpersonal Influence. *Group Dynamics*, *6*(1), 38–51. doi:10.1037/1089-2699.6.1.38

Mitnick, K., & Simon, W. (2002). *The Art of Deception: Controlling the Human Element of Security*. New York, NY: John Wiley & Sons.

Peltier, T. (2006). Social Engineering: Concepts and Solutions. *Information System Security*, *15*(5), 13–21. doi:10.1201/1086.1065898X/46353.15.4.20060901/95427.3

Petty, R. E., Brinol, P., & Tormala, Z. L. (2002). Thought Confidence as a Determinant of Persuasion: The Self-Validation Hypothesis. *Journal of Personality and Social Psychology*, *82*(5), 722–741. doi:10.1037/0022-3514.82.5.722

Rusch, J. (1999). *The Social Engineering of Internet Fraud.* Paper presented at the INET'99 Conference, San Jose, CA.

Thornburgh, T. (2004). *Social Engineering: the "dark art"*. Paper presented at the 1st Annual Conference on Information Security Curriculum Development, Kennesaw, GA.

Whitman, M. E., & Mattord, H. J. (2008). *Management of Information Security* (2nd ed.). Florence, KY: Course Technology.

Whitman, M. E., & Mattord, H. J. (2009). *Principles of Information Security* (3rd ed.). Florence, KY: Course Technology.

Workman, M. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information System Security*, *16*(6), 315–331. doi:10.1080/10658980701788165

Workman, M. (2008). 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*, *59*(4), 662–674. doi:10.1002/asi.20779

Xin (Robert) Luo is an Assistant Professor of Management Information Systems and Information Assurance in the Anderson School of Management at the University of New Mexico, USA. He earned his Ph.D. in Information Systems from Mississippi State University. His teaching and research interests include information assurance, e-commerce/m-commerce, and cross-cultural management. His research has been published in journals including Journal of the Association for Information Systems, European Journal of Information Systems, Communications of the ACM , Decision Support Systems, Communication of the Association for Information Systems, Journal of Organizational and End User Computing, Information Management and Computer Security, Cross-Cultural Management, Journal of Information Privacy and Security, International Journal of Information Security & Privacy, Information Systems Security, and Journal of Internet Banking and Commerce*, etc.*

Richard Brody is the Douglas Minge Brown Professor of Accounting in the Anderson School of Management at the University of New Mexico. He earned his Ph.D. from Arizona State University, his M.S. from Colorado State University and his B.S. from the University of Delaware. He is a Certified Public Accountant, a Certified Fraud Examiner and a Forensic Certified Public Accountant. Professor Brody's research addresses issues related to forensic accounting, auditing and corporate governance. Recent research has focused on issues such as corporate fraud, identity theft, mandatory auditor rotation, the outsourcing of income tax returns to India and the impact of corporate governance structure on auditor judgment.

Alessandro Seazzu is the director of UNM's Center for Information Assurance Research and Education (CIARE). Through CIARE, UNM has been designated by the NSA and DHS as a Center of Academic Excellence in Information Assurance and was recently selected as the host site for one of the FBI's Regional Computer Forensics Laboratory. He has been a faculty member with the Anderson School since 1995. His areas of research and study have been in virtual environments in security and human behavior in security.

Stephen Burd is an Associate Professor of Management in the Anderson School of Management at the University of New Mexico. He earned his Ph.D. from Purdue University in 1983. His teaching and research interests include computer and software architecture, system and network administration, healthcare technology and cost-effectiveness, and database management. He is Associate Director for UNM's Center for Information Assurance Research and Education and is Secretary and Treasurer of the New Mexico Telehealth Alliance. He is a Certified Public Accountant licensed in Maryland.