Generic Taxonomy of Social Engineering Attack

A. Cik Feresa Mohd Foozy[1,*] ,B. Rabiah Ahmad[1] ,C. Mohd Faizal Abdollah[1] ,D. Robiah Yusof[2] and E. Mohd Zaki Mas'ud[3]
[1] Faculty of Computer Science and Multimedia Technology, UTHM
[1, 2, 3] Faculty of Information Technology and Communication, UTEM

*Corresponding email: feresa@uthm.edu.my
rabiah@utem.edu.my
faizalabdollah@utem.edu.my

Abstract

Social engineering is a type of attack that allows unauthorized access to a system to achieve specific objective. Commonly, the purpose is to obtain information for social engineers. Some successful social engineering attacks get victims' information via human based retrieval approach, example technique terms as dumpster diving or shoulder surfing attack to get access to password. Alternatively, victims' information also can be stolen using technical-based method such as from pop-up windows, email or web sites to get the password or other sensitive information. This research performed a preliminary analysis on social engineering attack taxonomy that emphasized on types of technical-based social engineering attack. Results from the analysis become a guideline in proposing a new generic taxonomy of Social Engineering Attack (SEA).

Keywords: Computer Security, Human-based social engineering, Social Engineering, Technical-based social engineering

1. INTRODUCTION

Detecting social engineering attack is not an easy process[1]. Although many detection tools have been introduced to reduce risk from social engineering attack, these attack is still increasing every year [2].

Losing data in a system can bring impact to users especially when it associated with financial and important data of a company. If this incident happens, its show that system is not secure enough to protect data.

In general, an attacker attempts to attack system or network by analyzing activities on user's network and then hack the system. The rational of this process is to steal the important information to let them get access to the system as example the online banking password.

This article is structured in four sections as follows: In section 2, a review of previous studies in social engineering attack according to its categories. In section 3, a discussion about methodology involved in identifying the categories of social engineering attacks. Section 4 is analysis on the previous study that contribute the outcome of propose taxonomy and finally, in section 5 is result and further work for the next research.

2. LITERATURE REVIEW

Previous studies in social engineering attack are very focus. Many studies in this area discussed several types of social engineering attack from management point of view. However, technical part also should be considered to be discussed. The significant to understand social engineering attack categories are to mitigate this problem from growing since most attacks are using the advance technologies and tools. Thus, this section will review related works of social engineering attack.

2.1. SOCIAL ENGINEERING ATTACK

Information security threat can be divided into two types such as technical hacking and social engineering attack. Both of the attacks give the high impact on the security and privacy of the user since the data can be stolen and manipulated for their own purpose.

The purpose of social engineering attack is to get direct access by using physical or digital access to an organization's information or information system [3].

According to Peltier [4], the goal of social engineers are to trick people into giving them what they want. Moreover, Orgill, Romney, Bailey, & Orgill [5] defined the social engineering is a technique used by hackers or other attackers to gain access to information technology systems by getting the needed information such as username and password from a person rather than breaking into the system through electronic or algorithmic hacking methods. Twitchell [6] also defined that social engineering as obtaining unauthorized access to information.

However, Nyamsuren & Ho-Jin [7] has been defined that social engineering is not only the manipulation of people, but it also can include unauthorized access to physical items or exploitation of any available information.

The chronology of definition in social engineering attack before year 2006 addressed human based attack employ physiological skill to gain the information.

However, in 2006 until recently, Peltier [4], Nyamsuren and Ho-Jin [7], Huber et al. [8], Sandouka [9], Abraham and Chengalur-Smith [2],Bezuidenhout et al. [10] and Janczewski and Lingyan[11] has discovered social engineering attack can be categorized into two group of technology-based and human-based social engineering attack. Thus, this shows that social engineering attack can be done using human psychological and technical-based such as pop-up windows, mail attachments, online scam and vishing [9] and [11].

2.1.1. HUMAN- BASED SOCIAL ENGINEERING ATTACK

Human-based social engineering attack will use person to person method such as impersonate the important user, use third party authorization, utilize in person, dumpster diving and shoulder surfing, creating a sense of urgency and simple persuasion. Granger [12], Orgill et al. [5], Thornburgh [3], Tiantian [1], Mills [13]and Kvedar et al.[14] discussed the term and defense approach of physical and human based social engineering attack in their studies.

2.1.2. TECHNICAL- BASED SOCIAL ENGINEERING ATTACK

Two experiments have been done by R¨oßling et.al [15] to get the security data using social engineering. The first experiment is to get the login information for randomly chosen members of the firm and the second experiment tried to get access to the firm's mail server from one administrator by using vishing and phishing social engineering attack.

Maggi et al.[16] have written a short paper to show the status result of the data collection system that has been developed to examine the various types of phishing campaigns. The study is focusing on the voice channel and also to analyzes instant messages and suspicious emails and extracts telephone numbers, URLs and popular words from the content.

Moreover, Peltier [4], Huber et al.[8], Sandouka et al. [9], R¨oßling et al.[15], Abraham and Chengalur-Smith [2] and Bezuidenhout et al.[10] also studied about technical-based social engineering attack. However, the study that has been done is specific for some

technical-based social engineering attacks and not covered all social engineering attacks. In this paper, the outcome taxonomy will give the general view about social engineering attacks to understand these attacks types.

2.1.3. HUMAN-BASED AND TECHNICAL- BASED SOCIAL ENGINEERING ATTACK

In addition, the researches in human and technical based social engineering also has been studied by Nyamsuren and Ho-Jin [7] that doing an analysis about the impact of social engineering in ubiquitous environment and how to preventing it. For Janczewski and Lingyan [11], a conceptual model of social engineering attack has been developed and examine how to mitigate it. Moreover, Kotenko et al.[17] also developed an approach which is based on trees based approach for security analysis of information systems that consider the social engineering attack and software-technical attack.

3. METHODOLOGY

The aim of this paper is to classify the social engineering attack according to its category. The information in this study is retrieved from the various databases such as from ACM Digital Library, SpringerLink, IEEE Xplore, ScienceDirect, Google, Google Scholar and Yahoo. According to these databases, a statistic analysis on every selected article on social engineering attack has been done to propose Social Engineering Attack Taxonomy.

There are three phases contribute in this analysis such as Planning, Analysis and Development. In the planning phase, there are two steps for analysis phase preparation. Step 1 is information searching about social engineering by using a few databases. After that step 2 is identification and collection data of Social Engineering category and Social Engineering Attack.

For Analysis phase, information that has been identified and collected will go through two steps as below:

Step 1: Analysis of Social Engineering category
Step 2: Analysis of Social Engineering Attack classification

The purpose of the first step is to identify attacks are belong with human-based social engineering attack or technical-based social engineering attack. Attack classification step is required in this analysis because there are many social engineering attacks have been identified so far and it will be discussed in the next sub topic. These attacks are hard to countermeasures since the technologies growing fasters and it is important to classify the attacks. Therefore, this paper will does a preliminary analysis on social engineering attack by comparing the attacks type. As a result, an analysis has been conducted by reviewing the social engineering research in order to propose social engineering attack taxonomy. **Figure 3**, show the overview of the analysis process.

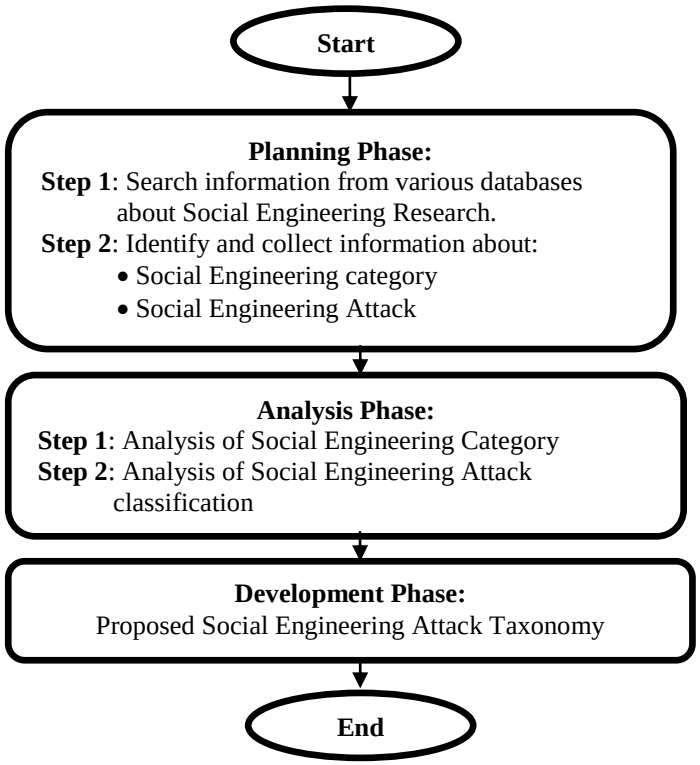

Figure 3: Overview of the Analysis Process

3.1. CLASSIFICATION SOCIAL ENGINEERING ATTACK

Some researchers of social engineering attack have classified the attacks according to the human-based social engineering and technical-based social engineering.

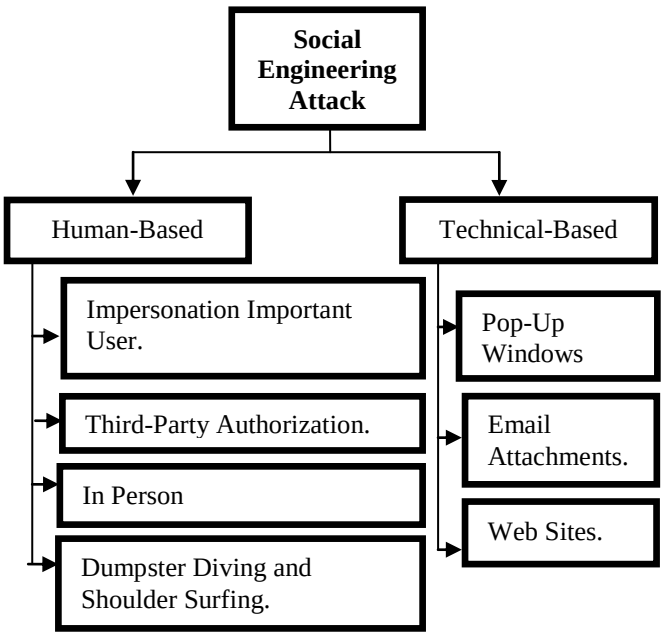

Figure 3.1: Social Engineering Attack [4].

Thornburgh [3] divided social engineering attack into two type of attack such as Shoulder surfing and Dumpster Diving. Peltier [4] also has split the social engineering attack into two categories such as human-based social engineering attack and technical-based social engineering attack as shown in **Figure 3.1**. According to Twitchell [6], Social Engineering Attack can be divided into four types as depicted in **Figure 3.2**.

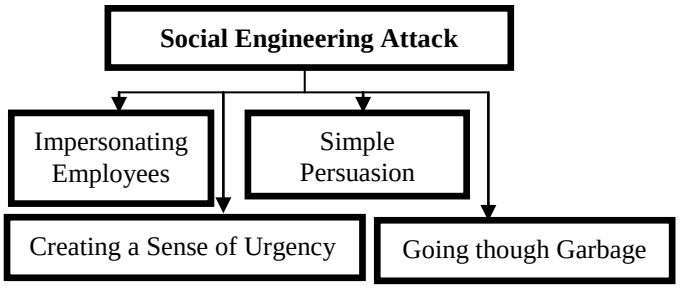

Figure 3.2: Social Engineering Attack [6].

In addition, Nyamsuren and Ho-Jin[7], have done a research about the possible impacts of social engineering in ubiquitous environment and the ways of preventing it. **Figure 3.3** shows list of social engineering attack for ubiquitous environment by Nyamsuren and Ho-Jin[7].

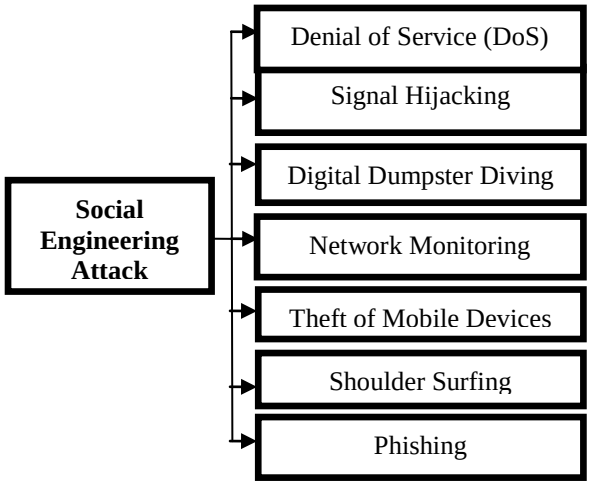

Figure 3.3: Social Engineering Attack [7].

Moreover, **Figure 3.4** has been proposed by Sandouka et al. [9]. Sandouka et al. [9] also divided social engineering attack into two categories such as physiological and technical but Sandouka et al. [9] did not listed the attacked according to these categories.

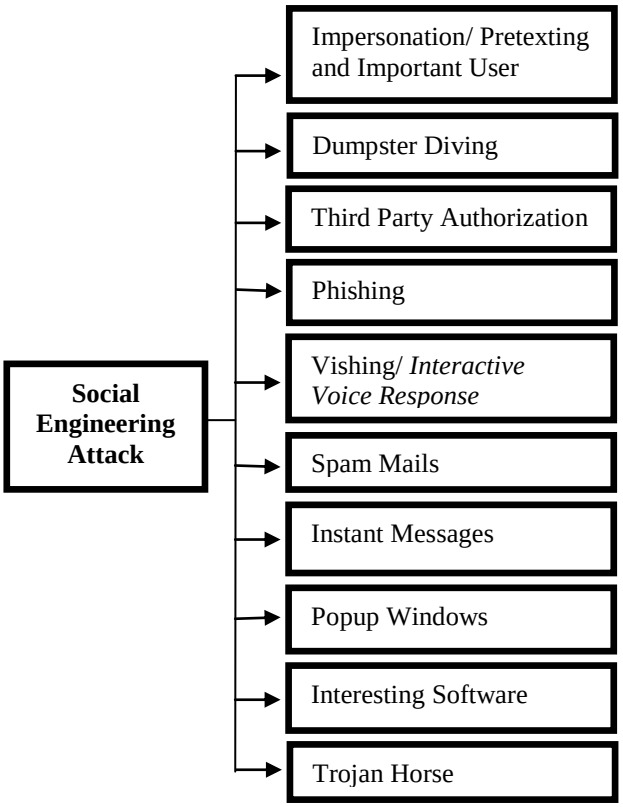

Figure 3.4: Social Engineering Attack [9].

Bezuidenhout et al. [10] also split the social engineering attack into two perspective. Even though, the term is different but actually they are discussing the same category of psychological perspective and computer science perspective.

Janczewski and Lingyan [11] has listed both categories of attacks and for human based attack as illustrated in **Figure 3.5**:

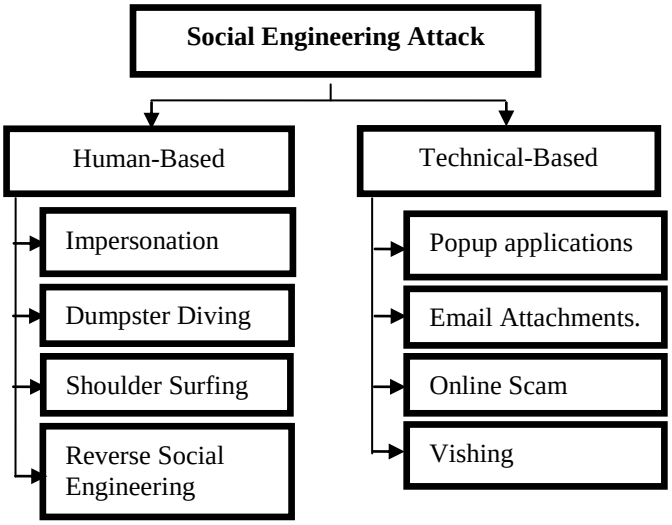

Figure 3.5: Social Engineering Attack [11].

According to **Figure 3.1** until **Figure 3.5**, it shows some differences and similarity between the studies of social engineering attack. The multiplicity of attack under social engineering makes it beneficial to propose social engineering attack taxonomy in order to understand overview of this area.

4. ANALYSIS AND FINDING

In order to proposed social engineering attack taxonomy, two analyses about human-based social engineering and technical-based social engineering attack have been done. The symbol of "√" is to show it has been discussed in that study.

4.1. ANALYSIS ON HUMAN-BASED SOCIAL ENGINEERING ATTACK

There are several types of human-based social engineering attack that has been listed by researchers. Hence, **Table 4.1,** shows human-based social engineering attacks studied by **[4]**, **[6]**, **[7]**, **[9]**, **[11].**

Table 4.1: Analysis on Human-Based Social Engineering Attack (Item found= √)

Author / Attack	[4]	[6]	[7]	[9]	[11]
Impersonation and Important User.	√	√		√	√
Third-Party Authorization	√			√	
In Person	√				
Dumpster Diving and Shoulder	√	√	√	√	√
Creating a Sense of Urgency		√			
Simple Persuasion		√			
Reverse Social Engineering					√

According to the above table, it shows that the listed human-based social engineering attack on the table above has been discussed in the previous study. Impersonation and Important User, Third-Party Authorization, Dumpster Diving and Shoulder have more than one similarity with others research paper. However, four attacks have not been discussed in other publications.

4.2. ANALYSIS ON TECHNICAL-BASED SOCIAL ENGINEERING ATTACK

There are 14 types of technical-based social engineering attack has been discussed in the previous study. Hence, the table below shows the analysis of technical-based social engineering attacks.

Table 4.2: Analysis on Technical-Based Social Engineering Attack (Item found= √)

Author / Attack	[4]	[9]	[7]	[11]
Trojan Horse		√		
Pop-Up Windows	√	√		√
Email	√			√
Software		√		
Web Sites	√			
Signal Hijacking			√	
Network Monitoring			√	
Phishing		√	√	
Spam/Scam		√		√
Instant Messages		√		
Denial of Service (DoS)			√	
Digital Dumpster Diving			√	
Vishing		√		
Theft on Mobile Devices			√	√

Based on **Table 4.2**, there are 14 types technical-based social engineering attack has been covered in the 5 publications. Pop-ups windows, email, phishing, spam or scam, theft on Mobile devices has been discussed more than one publication. However, others is only been discussed by one publication.

5. RESULT

As a result from the analysis section, it shows that the listed attacks are relevant to be proposed in social engineering attack taxonomy. Even though, there is only a publication mention about the attack, it still relevant to be listed as part of social engineering attack since it has been discussed in the previous studies.

5.1. SOCIAL ENGINEERING ATTACK TAXONOMY

With reference to **Figure 5.1**, the taxonomy of information security threat based on study has been developed to get the clear view about social engineering attack. In **Figure 5.1**, there are few types of human-based technology social engineering attack such as impersonation and important user, third-party authorization, in person, dumpster diving and shoulder surfing, creating a sense of urgency and simple persuasion. In technical-based social engineering attack, there are trojan horse, pop-up windows, email attachments, software, network monitoring, phishing, spam mails, web sites, instant messages, denial of service (DoS), digital dumpster diving and signal hijacking.

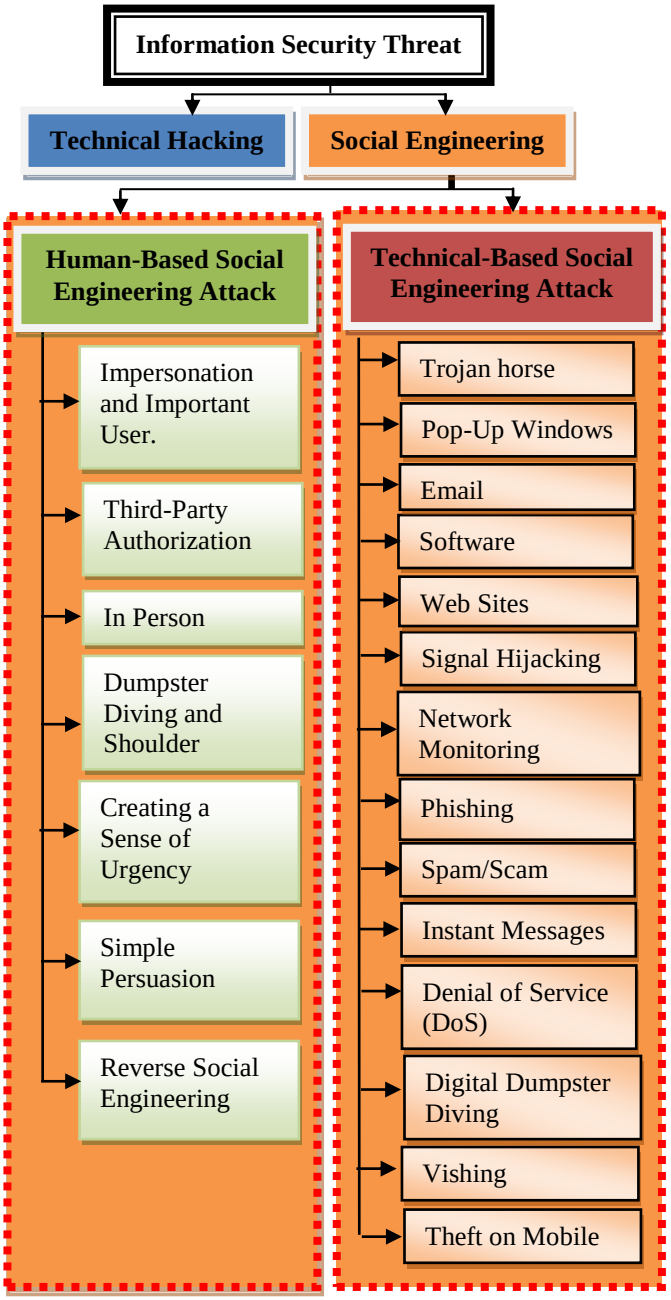

Figure 5.1: Proposed Taxonomy of Social Engineering Attack (SEA)

6. CONCLUSION AND FUTURE WORK

In this study, the researchers have reviewed and analyze the social engineering attack in specific view. Moreover, the discussion about the attack is more on the management perspective. This paper has done preliminary analysis in both views to generate a generic taxonomy that grouping attacks under the suitable categories. From the analysis, social engineering attack taxonomy has been proposed which consist of human-based social engineering attack and technical-based social engineering attack. Under these categories, few attacks have been listed based on the attack comparison. This paper is a preliminary worked for social engineering defense mechanism by using intrusion detection system. This will contributes ideas in how to identify type of social engineering attack since its still lack and rough about type of attack in social engineering. Furthermore, these attacks are still growing and there should be an alternative to mitigated it effectively.

REFERENCES

[1] Tiantian, Q. *An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering*. in *Intelligence and Security Informatics, 2007 IEEE*. 2007.

[2] Abraham, S. and I. Chengalur-Smith, *An overview of social engineering malware: Trends, tactics, and implications.* Technology in Society, 2010. **32**(3): p. 183-196.

[3] Thornburgh, T., *Social engineering: the "Dark Art"*, in *Proceedings of the 1st annual conference on Information security curriculum development*. 2004, ACM: Kennesaw, Georgia. p. 133-135.

[4] Peltier, T.R., *Social engineering: Concepts and solutions*. Information Security and Risk Management, 2006: p. 9.

[5] Orgill, G.L., et al., *The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems*, in *Proceedings of the 5th conference on Information technology education*. 2004, ACM: Salt Lake City, UT, USA. p. 177-181.

[6] Twitchell, D.P., *Social engineering in information assurance curricula*, in *Proceedings of the 3rd annual conference on Information security curriculum development*. 2006, ACM: Kennesaw, Georgia. p. 191-193.

[7] Nyamsuren, E. and C. Ho-Jin. *Preventing Social Engineering in Ubiquitous Environment*. in *Future Generation Communication and Networking (FGCN 2007)*. 2007.

[8] Huber, M., et al. *Towards Automating Social Engineering Using Social Networking Sites*. in *Computational Science and Engineering, 2009. CSE '09. International Conference on*. 2009.

[9] Sandouka, H., A.J. Cullen, and I. Mann. *Social Engineering Detection Using Neural Networks*. in *CyberWorlds, 2009. CW '09. International Conference on*. 2009.

[10] Bezuidenhout, M., F. Mouton, and H.S. Venter. *Social engineering attack detection model: SEADM*. in *Information Security for South Africa (ISSA), 2010*. 2010.

[11] 11.Janczewski, L.J. and F. Lingyan. *Social engineering-based attacks: Model and new zealand perspective*. in *Computer Science and Information Technology (IMCSIT), Proceedings of the 2010 International Multiconference on*. 2010.

[12] Granger, S. *Social Engineering Fundamentals, Part I: Hacker Tactic*. 2001 [cited 2011 7th March 2011]; Available from: http://www.knowyourenemy.eu/attachments/File/NsP-docs/CompleteSocialEngineeringDoc.pdf.

[13] Mills, D., *Analysis of a social engineering threat to information security exacerbated by vulnerabilities exposed through the inherent nature of social networking websites*, in *2009 Information Security Curriculum Development Conference*. 2009, ACM: Kennesaw, Georgia. p. 139-141.

[14] Kvedar, D., M. Nettis, and S.P. Fulton, *The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition.* J. Comput. Small Coll., 2010. **26**(2): p. 80-87.

[15] R¨oßling, G., et al., *Social engineering: a serious underestimated problem*, in *Proceedings of the 14th annual ACM SIGCSE conference on Innovation and technology in computer science education*. 2009, ACM: Paris, France. p. 384-384.

[16] Maggi, F., A. Sisto, and S. Zanero, *A social-engineering-centric data collection initiative to study phishing*, in *Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security*. 2011, ACM: Salzburg, Austria. p. 107-108.

[17] Kotenko, I., M. Stepashkin, and E. Doynikova. *Security Analysis of Information Systems Taking into Account Social Engineering Attacks*. in *Parallel, Distributed and Network-Based Processing (PDP), 2011 19th Euromicro International Conference on*. 2011.