

Generic Taxonomy of Social Engineering Attack and Defence Mechanism for Handheld Computer Study

Cik Feresa Mohd Foozy¹, Rabiah Ahmad², Mohd Faizal Abdollah², Robiah Yusof³, Mohd Zaki Mas'ud³

Faculty of Information Technology and Communication, Technical University of Malaysia Malacca (UTEM), Malaysia

p031020001@student.utm.edu.my, rabiah@utm.edu.my, faizalabdollah@utm.edu.my,
robiah@utm.edu.my, zaki.masud@utm.edu.my

Abstract—Tremendous increase in social engineering attacks sparks many researches to find the ways to prevent and detect the social engineering attacks. There are very limited numbers of studies that have focused on securing handheld computers from being attacked by social engineer. However, the lack of emergence analysis in social engineering attacks has led to less effective countermeasure to secure from this threat. This paper discusses a holistic review of social engineering attacks reported in various articles. The reviews cover all types of devices and handheld computers. Results from the analysis were used as the guideline in proposing a new generic taxonomy of social engineering attacks and defence mechanism.

Keywords— Defence Mechanism, Handheld Computer, Network Security, Social Engineering Attacks

I. INTRODUCTION

A handheld computer is defined as a very small, lightweight device that provides functionality like a laptop computer [1]. Examples of handheld computers are Palm and other PDAs, tablet PC, and smartphones [2]. Handheld computers have become so popular for business and personal use because of their features such as portability and long battery life. However, the rapid growth of handheld computers has contributed to security problem because most of the handheld computers can connect to the Internet.

According to a website *mysecurecyberspace.com* [3], one of the examples of security problem in tablet PC is security threat. Symantex [4] also reported the increasing intrusion and identity theft on mobile phones in Symantex Intelligent Report, July 2011 edition. Lenny Zeltser [5] said that malware on mobile is distributed by using social engineering and malicious program will be installed in the mobile.

Detecting social engineering attack is not an easy process [6]. Although many detection tools have been introduced to reduce risk from social engineering attacks, the attacks are still increasing every year [7].

Study by Kvedar et al. [8] identified many current techniques to detect social engineering attacks, but the solution is still uncertain because of the unpredictable workings of social engineering attacks.

The purpose of social engineering attacks is to get direct access by using physical or digital access to an organisation's information or information system [9]. According to Peltier [10], the goal of social engineers is to trick people by giving them what they want. Nyamsuren and Ho-Jin [11] defined that social engineering attacks are not only the manipulation of people, but they can also include unauthorised access to physical items or exploitation of any available information.

This paper is structured in four sections as follows: In Section II, previous studies in social engineering attacks and defence mechanism according to their categories are reviewed. In Section III, the methodology used to identify the categories of social engineering attacks and defence mechanism is discussed. Section IV is about the analysis on previous studies that were used to develop the proposed taxonomy. Finally, in Section V, the results and future work for the next research are presented.

II. RELATED WORKS

Previous studies in social engineering attack are very much focused to one particular scope. Moreover, many studies in this area discussed several types of social engineering attacks protection from management perspective. However, technical perspective should also be discussed. The importance of understanding the categories of social engineering attacks is to mitigate this problem from deteriorating as most attacks use advanced technologies and tools. Thus, this section reviews related works in social engineering attacks and defence mechanism for handheld devices.

A. Social Engineering Attacks

Information security threat can be divided into two types namely technical hacking and social engineering attacks. Both types of information security threat give high impact on the security and privacy of the users as the data can be stolen and manipulated for the benefits of the attackers.

The definition of social engineering attacks before 2006 addressed human-based attack that employed psychological skill to gain information. But, in 2006 until recently, Peltier [10], Nyamsuren and Ho-Jin [11], Huber et al. [12], Sandouka

[13], Abraham and Chengalur-Smith [7], Bezuidenhout et al. [14], and Janczewski and Lingyan [15] discovered that social engineering attacks can be categorised into two groups namely human-based social engineering attack and technology-based social engineering attack. This means that social engineering attacks can be done, respectively, by manipulating human psychology and by using computer technology such as pop-up windows, mail attachments, online scam, and vishing [13] [15].

1) Human-Based Social Engineering Attack: Human-based social engineering attack uses person-to-person methods such as impersonating important user, using third party authorisation, utilising in person, dumpster diving and shoulder surfing, creating a sense of urgency, and simple persuasion. Granger [16], Orgill et al. [17], Thornburgh [9], Tiantian [6], Mills [18], and Kvedar et al. [8] discussed those methods and the defence approaches in dealing with physical and human-based social engineering attacks in their studies.

2) Technical-Based Social Engineering Attack: Two experiments were done by Rößlin et al. [19] to get security data using social engineering. The first experiment was to get the log in information for randomly chosen members of a firm and the second experiment was to get access to the firm's mail server from one administrator by using vishing and phishing social engineering attacks.

Maggi et al. [20] wrote a short paper on the status result of data collection system that was developed to examine various types of phishing campaigns. The paper focused on voice channel and analysed instant messages and suspicious emails, and extracted telephone numbers, URLs, and popular words from the content.

Peltier [10], Huber et al. [12], Sandouka et al. [13], Rößlin et al. [19], Abraham and Chengalur-Smith [7], and Bezuidenhout et al. [14] also studied about technical-based social engineering attacks. However, their studies were specific for some technical-based social engineering attacks and did not cover all types of social engineering attacks. In this paper, the outcome taxonomy gives general view about social engineering attacks and defence mechanism in understanding these types of attacks.

B. Defence Mechanism for Social Engineering Attacks

Many researches in this area proposed defence mechanism for social engineering attacks from management perspective such as implementation of policy, standard, and auditing, but researches on defence mechanism from technical perspective are still lacking.

Social engineering attacks are rising every year because it is difficult for a person to be disciplined in applying rule and regulation. Tiantian [6] identified the growing of social engineering attacks because of the difficulties to detect the social engineering attacks, which can affect user privacy and security information.

According to Abraham and Chengalur-Smith [7], malware caused by social engineering attacks can be mitigated if it can

be detected on the machine and blocked from performing its harmful routine.

1) Defence Mechanism from Management

Perspective: Thornburgh [9] suggested to apply policy, procedures, training, awareness programmes, and incident response plans. Peltier [10] also proposed to defend from social engineering attacks using information security architecture such as policies and standard, and vulnerability assessment. Twitchell [21] recommended to put three types of defence into practice namely Education, Training, and Awareness (ETA); back up policy; and auditing. Abraham and Chengalur-Smith [7] suggested that end user security training and other defence technique can be used to reduce social engineering attacks. Moreover, Janczewski and Lingyan [15] recommended to apply a few techniques and also multifactor authentication security policy.

2) Defence Mechanism from Technical Perspective:

Nyamsuren and Ho-Jin [11] suggested to defend from social engineering attacks using technical approaches such as cryptography and encryption, intelligent security systems, and multiple security level. Sandouka et al. [13] recommended to implement Artificial Intelligence (AI) technique because AI has the potential to respond to a large scale of attacks in real time manner and can increase the organisational security. Abraham and Chengalur-Smith [7] also proposed to use e-mail filtering. Janczewski and Lingyan [15] said that physical security and technical control can also be implemented to mitigate these attacks.

III. METHODOLOGY

The aim of this paper is to classify social engineering attacks and how to defend from the social engineering attacks based on their category. The data in this study were retrieved from various databases such as ACM Digital Library, SpringerLink, IEEE Xplore, ScienceDirect, Google, Google Scholar, and Yahoo!.

Using these databases, a statistical analysis on every selected article about social engineering attacks was done to propose taxonomy of social engineering attacks and defence mechanism.

There are three phases involved in this analysis namely planning, analysis, and development. In the planning phase, there are two steps for the preparation before analysis phase. Step 1 is information searching about social engineering using a few databases. Step 2 is identification and collection of data of social engineering category and social engineering attacks. In analysis phase, information that was identified and collected went through two steps as follows:

Step 1: Analysis of social engineering category

Step 2: Analysis of social engineering attacks classification and defence mechanism

The purpose of the first step is to identify the type of attacks whether human-based social engineering attacks or technical-

based social engineering attacks. Classification for the types of attacks was required in this analysis because there are many social engineering attacks that have been identified so far and these will be discussed in the next sub topic. These attacks are hard to countermeasure since the technologies are growing fast and thus it is crucial to classify these attacks.

This paper discusses the preliminary analysis on social engineering attacks by comparing these attacks and finally to propose taxonomy of social engineering attacks and how to defend from social engineering attacks. Figure 1 below, shows the overview of the analysis process.

To propose the taxonomy of social engineering attacks and defence mechanism according to the social engineering categories, analyses on human-based social engineering, technical-based social engineering, defence mechanism in management perspective, and defence mechanism in technical perspective social engineering attack were done. The symbol “√” in the following tables means that that type of attack was discussed in the studies

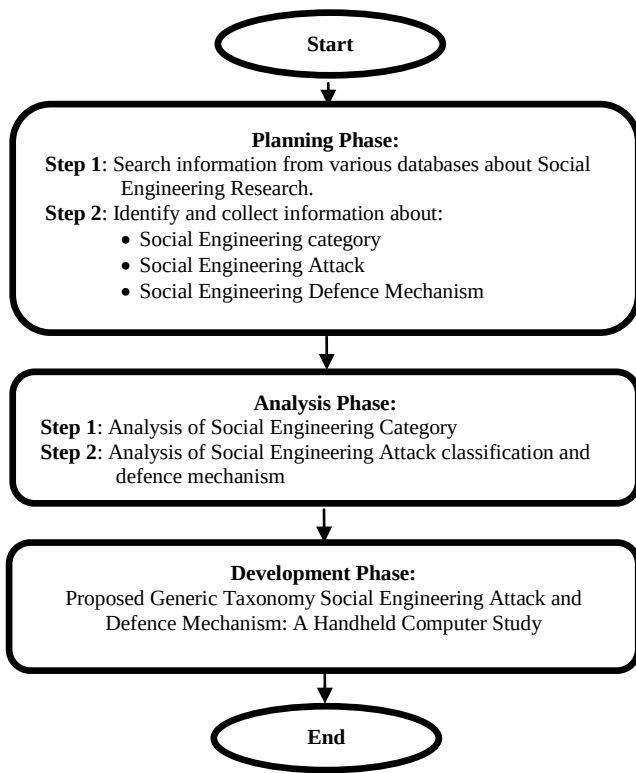


Figure 1. Overview of the Analysis Process

IV. ANALYSIS AND FINDINGS

To propose the taxonomy of social engineering attacks and defence mechanism according to social engineering categories, four analyses on human-based social engineering, technical-based social engineering, defence mechanism in management perspective and defence mechanism in technical perspective social engineering attack were done. The symbol “√” in the following tables means that those types of attack were discussed in the studies.

A. Analysis on Social Engineering Attack

There are several types of human-based social engineering attacks listed in previous studies. Table 1 shows human-based social engineering attacks as studied by Peltier [10], Twitchell [21], Nyamsuren and Ho-Jin [11], Sandouka et al.[13], and Janczewski and Lingyan [15].

TABLE 1. ANALYSIS ON HUMAN-BASED SOCIAL ENGINEERING ATTACKS(ITEM FOUND=√)

Attack \ Researchers	[10]	[21]	[11]	[13]	[15]
Impersonating an Important User	√	√		√	√
Third-Party Authorisation	√			√	
In Person	√				
Dumpster Diving and Shoulder Surfing	√	√	√	√	√
Creating a Sense of Urgency		√			
Simple Persuasion		√			
Reverse Social Engineering					√

Based on Table 1, Impersonating an Important User, Third-Party Authorisation, Dumpster Diving, and Shoulder Surfing show more than one similarity among the studies. Moreover, there were four other types of human-based social engineering attacks discussed in the studies.

For analysis of the technical-based social engineering attacks, the studies were done by Peltier [10], Nyamsuren and Ho-Jin [11], Sandouka et al [13] and Janczewski and Lingyan [15] as listed on Table 2.

TABLE 2. ANALYSIS ON TECHNICAL-BASED SOCIAL ENGINEERING ATTACKS(ITEM FOUND=√)

Attack \ Researchers	[10]	[11]	[13]	[15]
Trojan Horse			√	
Pop-Up Windows	√		√	√
Email	√			√
Software			√	
Web Sites	√			
Signal Hijacking		√		
Network Monitoring		√		
Phishing		√	√	
Spam/Scam Mails			√	√
Instant Messages			√	
Denial of Service (DoS)		√		
Digital Dumpster Diving		√		
Vishing			√	
Theft on Mobile Devices		√		√

As shown in Table 2, there are 14 types of technical-based social engineering attacks covered in the five studies.

B. Analysis on Defence Mechanism for Social Engineering Attacks

An analysis on previous studies on defence mechanism from the management perspective that were done by Abraham and Chengalur-Smith [7], Thornburgh [9], Peltier [10], Twitchell [21] and Janczewski and Lingyan [15] was conducted as

shown in Table 3. From the analysis, it is verified that the management mechanisms are recommended to be used in reducing social engineering risk. Policy is the most frequently suggested mechanism to reduce risk in social engineering attacks.

TABLE 3. ANALYSIS ON DEFENCE MECHANISME IN MANAGEMENT PERSPECTIVE FOR SOCIAL ENGINEERING ATTACKS (ITEM FOUND=√)

Researchers Defense Mechanism	[7]	[9]	[10]	[21]	[15]
Policy		√	√	√	√
Standard			√		
Procedure		√			
Training	√	√		√	
Awareness		√		√	
Incident Response Plan		√			
Vulnerability Assessment			√		
Auditing				√	
Education				√	

Usually, solutions to reduce social engineering risk are from management perspective as shown in Table 3. Sandouka et al. [13] explained that the implementation of security awareness in organisation is very expensive and it needs time for staffs to be trained. The staffs also must be aware of social engineering attacks.

Table 4 lists down the suggested defence mechanisms to defend from social engineering attacks by Abraham and Chengalur-Smith, 2010)[7], Nyamsuren and Ho-Jin [11], Sandouka, et al.[13], and Janczewski and Lingyan[15]. From the analysis on Table 4 below, it is possible to defend from social engineering attacks using the listed mechanisms. Artificial Intelligence (AI) is the most frequently suggested mechanism to reduce risk in social engineering attacks.

TABLE 4. ANALYSIS ON DEFENCE MECHANISME IN TECHNICAL PERSPECTIVE FOR SOCIAL ENGINEERING ATTACKS (ITEM FOUND=√)

Researchers Defense Mechanism	[7]	[11]	[13]	[15]
Cryptography		√		
Encryption		√		√
Artificial Intelligence		√	√	√
Multiple Security Level		√		
Email Filtering	√			
Physical Security				√
Technical Control				√

C. Analysis Social Engineering Attacks on Handheld Computers and Current Defence Mechanism

Table 5 lists down several types of handheld computers that have been attacked by one of technical-based social engineering attacks as shown in Table 2.

TABLE 5. ANALYSIS ON HANDHELD COMPUTER (ITEM FOUND=TYPE OF TECHNICAL-BASED SOCIAL ENGINEERING ATTACK)

Researchers	[22]	[23]	[24]	[25]	[26]
Handheld Computer					
PDA				Vishing	
Palm Pilot		Trojan Horse			
Tablet PC					Phishing
Smartmobile	Trojan Horse		DoS		

Based on Table 5, the researchers have identified the types of attacks that usually attack handheld computers. Table 6 lists down a few studies to overcome such attacks.

TABLE 6. ANALYSIS ON ATTACK DEFENCE MECHANISM FOR HANDHELD COMPUTER (ITEM FOUND=√)

Researchers	[1]	[22]	[23]	[27]	[28]	[29]
Defence Mechanism						
Firewall				√		
SSL					√	
S/MIME					√	
IPsec					√	
Server-Aided Signatures (SAS)						√
Context matching method	√					
Antivirus Software		√				
Digital Signatures			√			

Table 6 shows six defence mechanisms that have been already implemented in the handheld computers. They prove the possibilities to defend from the attack on handheld computers using those mechanisms.

V. RESULT

As a result from the analysis section based on Table 1 and Table 2, it can be concluded that the listed types of attacks are relevant to be included in the taxonomy of social engineering attacks as shown in Figure 2. Table 3 and Table 4 list down the previous studies that studied on the mechanisms to reduce social engineering attacks. Taxonomy of defence mechanism against social engineering attacks has also been developed as shown in Figure 3. Even though there was only one study that discussed that particular type of attack and defence mechanism, it was still relevant to be listed as part of social engineering attacks and mechanism to reduce social engineering attacks.

A. Social Engineering Attack Taxonomy and Defence Mechanism

With reference to Figure 5, the taxonomy of information security threats based on previous studies has been developed. The taxonomy can be used to get clear view about social engineering attacks.

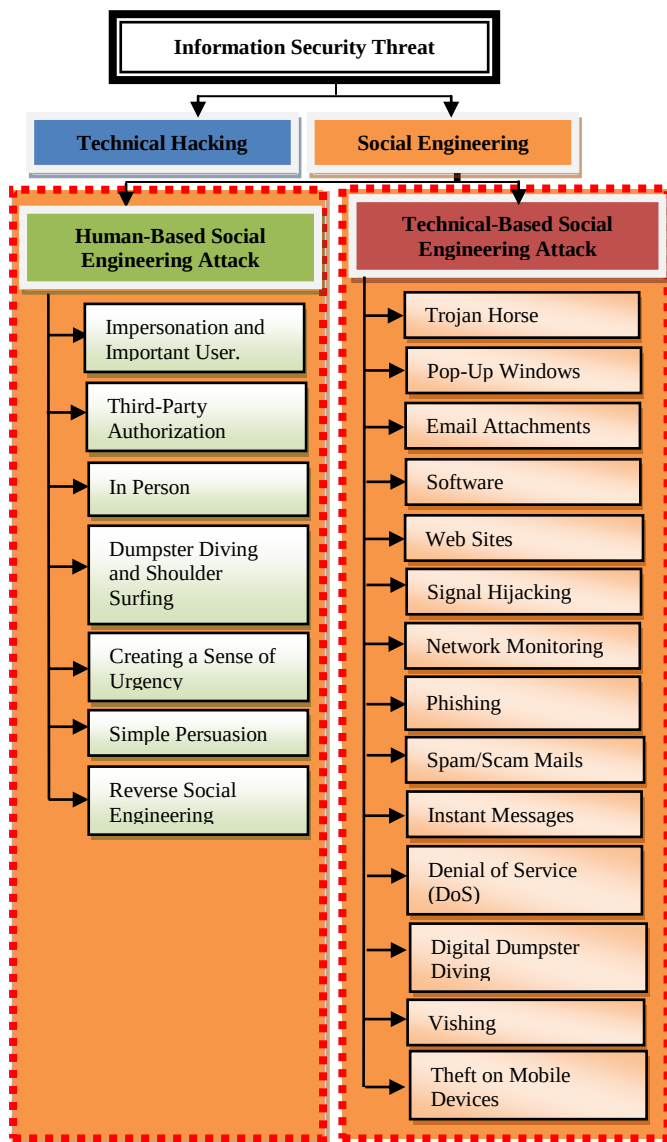


Figure 2. The Proposed Taxonomy of Social Engineering Attacks and Defence Mechanism

By referring Table 3 and Table 4, taxonomy as shown in Figure 3 has also been developed. According to the previous studies on defence mechanism, it can be said that social engineering can be mitigated from two perspectives namely management perspective and technical perspective. Based on the findings, most of the commonly suggested solutions by the previous researchers are from the management perspective for human-based social engineering attacks. Meanwhile, solutions from the technical perspective were for technical-based social engineering attacks.

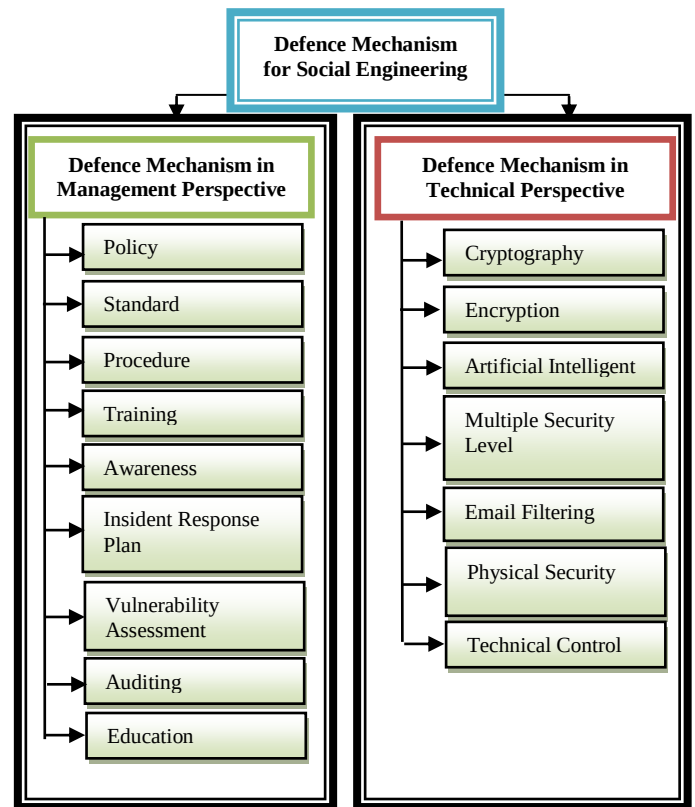


Figure 3. The Proposed Taxonomy of Defence Mechanism for Social Engineering Attacks.

VI. CONCLUSION AND FUTURE WORK

In this study, the researchers reviewed and analysed the social engineering attacks and how to defend from those attacks in certain perspectives. The discussions about defence mechanisms against social engineering attacks in previous studies were more from the management perspective. This paper discusses preliminary analysis on management and technical perspectives. Moreover, generic taxonomy that classifies social engineering attacks and defence mechanism based on suitable categories has also been developed. Taxonomy of social engineering attacks that consists of human-based social engineering attacks and technical-based social engineering attacks, and the defence mechanism has been proposed, which can be categorised into management and technical perspectives. Under these perspectives, a few types of attacks on handheld computers have been listed by comparing the types of social engineering attacks discussed in previous studies. This paper is a preliminary study for future work and it contributes ideas on how to identify types of social engineering attacks. This is because the discussion in this field is still lacking and the types of social engineering attacks are still unclear. As these attacks are still growing, there should be an alternative to mitigate them effectively.

ACKNOWLEDGMENT

The authors would like to thank University Tun Hussein Onn Malaysia (UTHM) for supporting this research.

REFERENCES

- [1] Wen-Chen, H., et al. *Mobile Data Protection Using Handheld Usage Context Matching*. in *Mobile Data Management: Systems, Services and Middleware*, 2009. MDM '09. Tenth International Conference on. 2009.
- [2] Stonemetz, J., K. Ruskin, and R. Prasad, *Handheld Devices Anesthesia Informatics*. 2009, Springer New York. p. 409-424.
- [3] MySecureCyberspace.com (2011) *The Trend of Tablet PCs*.
- [4] Corporation, S., *Symantec Intelligence Report: July 2011*. 2011.
- [5] Zeltser, L. *The Use of Social Engineering by Mobile Device Malware*. 2011 [cited 2011 21 November 2011]; Available from: <http://blog.zeltser.com/post/7641621785/social-engineering-by-mobile-device-malware>.
- [6] 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.
- [7] 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.
- [8] 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.
- [9] 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.
- [10] Peltier, T.R., *Social engineering: Concepts and solutions*. *Information Security and Risk Management*, 2006: p. 9.
- [11] Nyamsuren, E. and C. Ho-Jin. *Preventing Social Engineering in Ubiquitous Environment*. in *Future Generation Communication and Networking (FGCN 2007)*. 2007.
- [12] Huber, M., et al. *Towards Automating Social Engineering Using Social Networking Sites*. in *Computational Science and Engineering, 2009. CSE '09. International Conference on*. 2009.
- [13] Sandouka, H., A.J. Cullen, and I. Mann. *Social Engineering Detection Using Neural Networks*. in *CyberWorlds, 2009. CW '09. International Conference on*. 2009.
- [14] Bezuidenhout, M., F. Mouton, and H.S. Venter. *Social engineering attack detection model: SEADM*. in *Information Security for South Africa (ISSA), 2010*. 2010.
- [15] 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.
- [16] 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>.
- [17] 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.
- [18] 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.
- [19] 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.
- [20] 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.
- [21] 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.
- [22] Munir, K.O.a.Q., *Analysis of Smartphone Worms: A Smart worm for Smartphones*. 2009.
- [23] Freundenthal, M., S. Heiberg, and J. Willemson. *Personal security environment on Palm PDA*. in *Computer Security Applications, 2000. ACSAC '00. 16th Annual Conference*. 2000.
- [24] Li, Y., C. Jing, and J. Xu, *A New Distributed Intrusion Detection Method Based on Immune Mobile Agent*, in *Life System Modeling and Intelligent Computing*, K. Li, et al., Editors. 2010, Springer Berlin / Heidelberg. p. 233-243.
- [25] Mulliner, C., *Security of Smart Phones*, in *Department of Computer Science*. 2006, University of California Santa Barbara: CA.
- [26] Beck, K. and J. Zhan. *Phishing Using a Modified Bayesian Technique*. in *Social Computing (SocialCom), 2010 IEEE Second International Conference on*. 2010.
- [27] Susilo, W., *Securing Handheld Devices*. *Proc. 10th IEEE Int. Conf. Networks*, 2002: p. 349-354.
- [28] P. G. Argyroudis, R.V., H. Tewari, and O. D'Mahony, *Performance Analysis of Cryptographic Protocols on Handheld Devices*. *Proc. 3rd IEEE Int. Symposium on Network Computing and Applications*, 2004: p. 169-174.
- [29] X. Ding, D.M., and G. Tsudik, *Equipping Smart Devices with Public Key Signatures*. *ACM Transactions on Internet Technology*, 2007. 7 no.1.