Towards an Ontological Model Defining the Social Engineering Domain

Francois Mouton, Louise Leenen, Mercia Malan, H. Venter

Towards an Ontological Model Defining the Social Engineering Domain

Francois Mouton[1], Louise Leenen[1], Mercia M. Malan[2], H.S. Venter[3]

[1]Defence Peace Safety & Security, Council for Industrial and Scientific Research, Pretoria, South Africa

moutonf@gmail.com, lleenen@csir.co.za

[2]University of Pretoria, Information and Computer Security Architecture Research Group, Pretoria, South Africa

malan747@gmail.com

[3]University of Pretoria, Computer Science Department, Pretoria, South Africa

hventer@cs.up.ac.za

Abstract The human is often the weak link in the attainment of Information Security due to their susceptibility to deception and manipulation. Social Engineering refers to the exploitation of humans in order to gain unauthorised access to sensitive information. Although Social Engineering is an important branch of Information Security, the discipline is not well defined; a number of different definitions appear in the literature. Several concepts in the domain of Social Engineering are defined in this paper. This paper also presents an ontological model for Social Engineering attack based on the analysis of existing definitions and taxonomies. An ontology enables the explicit, formal representation of the entities and their inter-relationships within a domain. The aim is both to contribute towards commonly accepted domain definitions, and to develop a representative model for a Social Engineering attack. In summary, this paper provides concrete definitions for *Social Engineering*, *Social Engineering attack* and *social engineer*.

Key words: Bidirectional Communication, Compliance Principles, Indirect Communication, Ontology, Social Engineering Attack, Social Engineering Attack Ontology, Social Engineering Definitions, Social Engineering History, Taxonomy, Unidirectional Communication

1 Introduction

Social Engineering (SE) is focused on the exploitation of a human in order to gain unauthorised access to information and falls under the umbrella of the Information

Security spectrum. Humans are the focal point of most organisations but they also pose a risk to their organisations. An organisation's sensitive information places them at risk if it falls in the wrong hands. Examples of sensitive information are the secret recipe that gives the Kentucky Fried Chicken meals their distinctive flavour or the personal banking information of clients.

Although organisations usually employ advanced technical security measures to minimise opportunities for unauthorised individuals to gain access to that information, it is vital that they consider the risk of their staff members falling victim to SE attacks. Humans often react emotionally and thus may be more vulnerable than machines at times. An organisation with sensitive information's biggest threat is not the technical protection, but the people who form the core of the organisation. Attackers have realised that it is easier to gain unauthorised access to the information and communications technology infrastructure of an organisation through an individual, rather than trying to penetrate a security system.

In a 1995 publication, the authors Winkler and Dealy posit that the hacker community has started to define SE as "the process of using social interactions to obtain information about a victim's computer system." [1]. The most popular definition of SE is the one by Kevin Mitnick who defines it as "using influence and persuasion to deceive people and take advantage of their misplaced trust in order to obtain insider information" [2].

An individual may be at the risk of exposing his or her own personal information to a social engineer. It is also the case that more and more individuals are exposed to electronic computing devices as the costs of these devices are decreasing drastically. Electronic computing devices have become significantly more affordable during the past few years and due to this nearly everyone has access to these devices. This provides the social engineer with more victims to target using skillfully crafted SE attacks.

Social engineers use a variety of techniques to manipulate their victims with the goal of extracting sensitive information from them. The title of Kevin Mitnick's book, *The art of deception: controlling the human element of security*, suggests that SE can be seen as an art of deception [2].

Various articles define SE and give descriptions of an SE attack. The definitions are diverse and often reflect one aspect of an approach relevant to a particular research project. Commonly agreed upon definitions that include all the different entities in SE are required. The purpose of this paper is to craft definitions and develop an ontological model for SE. Several papers, each with a different view on SE, have been studied and analysed to develop this model.

An ontology is a technology that allows for a formal encoded description of a domain and allows for the representation of semantic information: all the entities and their inter-relationships can be defined and represented. It also has powerful reasoning capabilities [3]. The ontological model presented in this paper will be implemented in future to provide an SE ontology.

The rest of this paper is structured as follows. Section 2 provides a background on different existing SE definitions and proposes more structured definitions for terms within the domain of SE. Section 3 discusses some existing taxonomies for the SE domain. Section 4 expands on the definitions provided in section 2 by providing an

SE attack classification model as well as an ontological model for SE attacks. Section 5 concludes the paper by providing a summary of the contributions.

2 Defining Social Engineering

The earliest literature that the authors found on SE is an article by Quann and Belford (1987) [4]. According to these authors SE, whilst still in its infancy, is seen as "an attempt to exploit the help desks and other related support services normally associated with computer systems" [4]. SE was later described as "trickery and deceit, also known as Social Engineering", according to Kluepfel (1989) [5, 6]. Even in one of the most prominent hacker magazines, the 2600: The Hacker Quarterly[1], the term *Social Engineering* was not widely used. One of the articles entitled, "Janitor Privileges", explains in great detail how to perform an SE attack, however the term *Social Engineering* is never mentioned in the article [8].

The following definitions of SE illustrate that there exists no single, widely accepted definition:

- "a social/psychological process by which an individual can gain information from an individual about a targeted organization." [9]
- "a type of attack against the human element during which the assailant induces the victim to release information or perform actions they should not." [10]
- "the use of social disguises, cultural ploys, and psychological tricks to get computer users to assist hackers in their illegal intrusion or use of computer systems and networks." [11, 12]
- "the art of gaining access to secure objects by exploiting human psychology, rather than using hacking techniques." [13, 14]
- "an attack in which an attacker uses human interaction to obtain or compromise information about an organization or its computer system." [15, 16, 17, 18]
- "a process in which an attacker attempts to acquire information about your network and system by social means." [19, 20]
- "a deception technique utilized by hackers to derive information or data about a particular system or operation." [21, 22, 23]
- "a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures." [24]
- "a hackerâ€™s manipulation of the human tendency to trust other people in order to obtain information that will allow unauthorized access to systems." [25, 26]
- "the science of skilfully manoeuvring human beings to take action in some aspect of their lives." [27, 28]
- "Social Engineering, in the context of information security, is understood to mean the art of manipulating people into performing actions or divulging confidential information." [29]

[1] A magazine which was established by Emmanuel Goldstein in mid January 1984 and contains articles regarding the undergound world of hacking. The individuals publishing in this magazine are mostly individuals who are already facing several charges regarding computer related crimes. [7]

- "the act of manipulating a person or persons into performing some action." [30, 31]
- "using subversive tactics to elicit information from end users for ulterior motives." [32]
- "using influence and persuasion to deceive people and take advantage of their misplaced trust in order to obtain insider information." [2, 33, 34, 35, 36]
- "the use of social disguises, cultural ploys, and psychological tricks to get computer users to assist hackers in their illegal intrusion or use of computer systems and networks." [37]

These definitions specify different ideas as to what SE involves. Two of these definitions specifically focus on gaining information from an organisation [9, 15, 16, 17, 18]. Several of the definitions define SE as the manipulation and persuasion of people in order to get information or to persuade someone to perform some action. Furthermore, some of the definitions are formed around gaining access to computer systems and networks. The only element that all of these definitions have in common is that a human is exploited in order to gain some unauthorised information or perform some action.

The authors of this paper propose the following definitions:

- *Social Engineering*: The science of using social interaction as a means to persuade an individual or an organisation to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity.
- *Social engineer* (noun): An individual or group who performs an act of Social Engineering.
- *Social engineer* (verb): To perform an act of Social Engineering. When the verb is used in the Past Perfect form, it means a successful Social Engineering attack has occurred. For example, "The target may not know that he or she has been social engineered."
- *Social Engineering attack*: A Social Engineering attack employs either direct communication or indirect communication, and has a social engineer, a target, a medium, a goal, one or more compliance principles and one or more techniques.

Section 4.2 elaborates more on these definitions. Apart from the several definitions available for SE, there are also various taxonomies which try to encapsulate SE and the structure of an SE attack. In existing literature, a few taxonomies were proposed to provide some structure to the domain of SE. All of these taxonomies have inherent flaws in them and these flaws are discussed in the following section.

3 Existing Taxonomies

Several taxonomies are studied and discussed in this section: Harley [38], Laribee [39], Ivaturi & Janczewski [40], Mohd et al. [41] and Tetri & Vuorinen [42].

3.1 Harley

Harley [38] is one of the first articles to present a taxonomy for the SE domain, and in fact proposes two different taxonomies. The first one defines the following SE techniques and related attacks: Masquerading, Password stealing, Dumpster diving, Leftover, Hoax Virus Alerts and other Chain Letters, Spam and Direct Psychological Manipulation. This taxonomy mixes social compliance principles with techniques.

The second taxonomy defines seven user vulnerabilities: Gullibility, Curiosity, Courtesy, Greed, Diffidence, Thoughtlessness and Apathy. Even though these vulnerabilities are mostly the reasons why individuals are susceptible to SE attacks, they do not specify an SE attack as such. The same SE attack can be performed using more than one of the mentioned vulnerabilities, which clarifies that these vulnerabilities are not the unique establishment of what an SE attack entails. Vulnerabilities of a human, not limited by the seven mentioned above, lead to the susceptibility of an attack.

3.2 Laribee

Laribee [39] identifies two different models, namely a trust model and an attack model. According to Laribee, SE is complex and typically requires multiple communications and targets. The two models are meant to be applied, individually or together, at various times to attain each individual attack goal [39]. The trust model describes how the social engineer establishes a trustworthy relationship with the target, whilst the attack model describes how a social engineer performs an information gathering attack. The attack model is limited to four techniques: deception, manipulation, persuasion and influence. In the attack model the social engineer is only able to use one of these techniques. Furthermore, after the technique has been performed, the attack model feeds into the trust model where the aim is to build a trustworthy relationship.

These models are problematic because not all SE attacks require a continuous relationship since there is not always the need to build a trustworthy relationship with the target. A social engineer generally uses a combination of compliance principles and techniques to perform a single SE attack.

3.3 Ivaturi & Janczewski

Ivaturi & Janczewski [40] classify an SE attack to be either *person-person* or to be *person-person via media*. *Person-person* is when there is direct communication involving a human, whereas *person-person via media* involves some medium used to communicate. The medium can be text, voice or video. Person-person attacks involve impersonation. Different techniques are described.

This taxonomy contains a well-defined structure for different SE techniques, as well as the types of attacks in which they are used. It is very similar to the structure of the direct communication part of our model, as further on proposed in section 4.1. Their study only focuses on direct communication and does not further elaborate on a scenario where indirect communication can be used for an SE attack.

3.4 Mohd et al.

Mohd et al. [41] classify an SE attack as being either human-based or technical-based. Human-based attacks apply some techniques that are combined to form an attack, such as “in person” and “simple persuasion”. The one technique cannot be used without the other. The items they regard as types of attacks are techniques that form a single attack, rather than being used separately as individual attacks.

Their technical-based attacks are mediums used within an SE attack such as “Email, Software, Web sites”. Another example is “Denial of Service” which is not an SE attack; it is an attack on a service and brings down a system instead of extracting information from it. The latter effect is the aim of an SE attack.

In summary, the Modh et al. model describes techniques used in SE attacks instead of depicting an SE attack as a whole.

3.5 Tetri & Vuorinen

Tetri & Vuorinen [42] studied several papers on SE and critically analysed them in order to present an overview of SE. They defined three main dimensions of SE: persuasion, fabrication and data gathering.

Persuasion involves getting someone to comply with an inappropriate request. The paper identifies two features of persuasion: *Direct interaction* and *active engagement between the intruder and the target* [42]. Fabrication involves techniques such as impersonation and using a false identification document to deceive victims into thinking the attacker is someone else. Data gathering is the process of gaining information from the target.

The authors of this paper agree with Tetri & Vuorinen’s description of persuasion although it can be seen as a compliance principle from a psychological perspective. The definitions of fabrication and data gathering on the other hand, are techniques aimed at aiding an SE attack rather than being a phase of an SE attack.

The authors take these taxonomies into account and attempt to improve on these ideas by identifying three different subcategories of an SE attack, as well as, to develop a structured SE attack ontological model. The next section firstly proposes the Social Engineering Attack Classification and then proposes an ontological model for an SE attack.

4 Ontological Model

In this section the authors motivate and present an ontological model for SE. Subsection 4.1 discusses a classification of an SE attack based on the type of communication that is employed. In subsection 4.2 a broader view is provided which defines the different parts of an SE attack.

4.1 Social Engineering Attack Classification

An SE attack, as depicted in Figure1, can be divided into two main categories: An indirect attack and a direct attack.

An indirect attack refers to an incident where a third party medium is used as a way of communicating. Third party mediums typically include physical mediums such as flash drives, pamphlets or other mediums, such as web pages. Communication occurs through third party mediums when a medium is accessed by a target, without direct interaction with the social engineer.

A direct attack is an incident where two or more people are involved in a direct conversation. This conversation can either be one-sided or two-sided. Due to this, this type of attack is further classified into two ways of communicating: Bidirectional or unidirectional communication.

Bidirectional communication is when two or more parties take part in the conversation, in other words, a two-way conversation occurs. Each party consists of an individual, a group of individuals or an organisation. A popular example of an attack in this category is an impersonation attack, where the social engineer impersonates the target in order to gain access to something which the target has access to.

Unidirectional communication is a one-sided conversation where the social engineer communicates with the target, but the target has no means to communicate back with the social engineer. This is normally done through some communication medium such as bulk e-mails or short message service (SMS). An example of a popular attack in this category is an e-mail phishing attack sent from the attacker to the target.

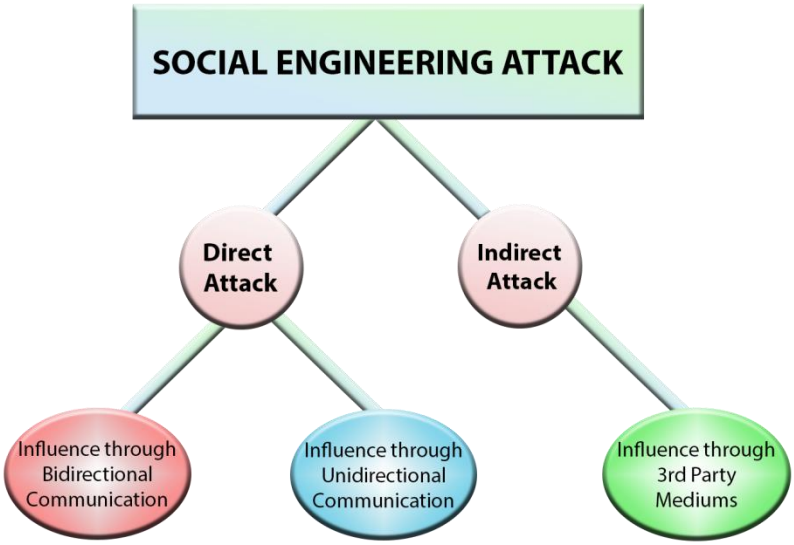

Fig. 1. Social Engineering Attack Classification

The rest of this subsection explains the different categories, bidirectional communication, unidirectional communication and indirect communication, in more

detail with an example of each. Each example discusses the various parts of an SE attack, as defined in section 2: a social engineer, a target, a medium, a goal, one or more compliance principles and one or more techniques. Compliance principles are principles used by the attacker, aided by different techniques, in order to persuade the target, through some medium, to comply with a request.

Bidirectional communication (Figure 2) is defined as a two-way conversation between two people. In the bidirectional communication category, the social engineer can either be an individual or a group of individuals. The target of the attack can be an individual or an organisation. The mediums that are frequently used for bidirectional communication are e-mail messages, face-to-face conversations or telephone conversations. Any compliance principle, technique and goal can be used in combination with a bidirectional communication medium.

An example of an SE attack that uses *bidirectional communication* is one where a social engineer attempts to influence a call centre agent into divulging sensitive information regarding a specific client. In this example, both the attacker and the target are *individuals*. *Pretexting* is used as the technique for this attack because the social engineer impersonates the client whose information the social engineer wishes to obtain. The compliance principle used in this example is *authority*, because the client impersonated by the social engineer acts as if he or she has authorised access to the information. The goal of the attack is to gain *unauthorised access* to the client's sensitive information.

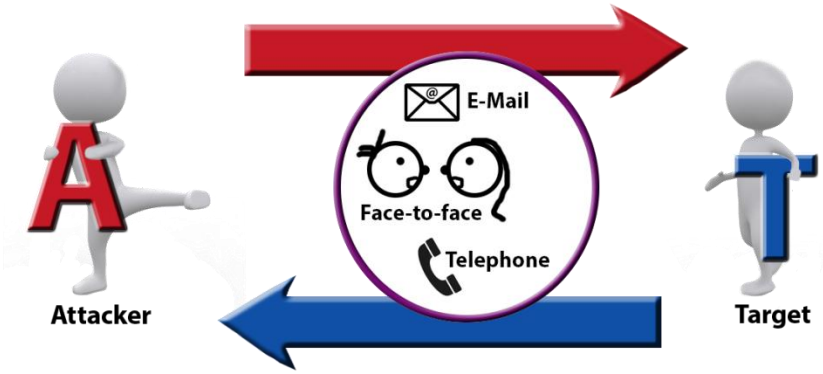

Fig. 2. Bidirectional Communication

Unidirectional communication (Figure 3) is very similar to bidirectional communication, except that the conversation only occurs in one direction: From the social engineer to the target. The social engineer and the target can either be an individual, a group of individuals or an organisation. The mediums that are frequently used for unidirectional communication are one-way text messages, e-mails or paper mail messages. Any compliance principle, technique and goal can be used in combination with unidirectional communication.

An example of an SE attack that uses *unidirectional communication* is an e-mail phishing attack where the target places an online order at some online store and waits for delivery of the item. The phishing e-mail is masked as an e-mail from the online store informing the target that a limited offer is available relating to the order. The target recognises the link between the e-mail and his order and clicks on the infected link. The target is specifically chosen. *Phishing* is the SE technique used for this attack and *scarcity* is the compliance principle. Since the e-mail states that it is a limited offer, the target feels that he or she has to explore this limited opportunity before it becomes unavailable. The infected link gives the social engineer *unauthorised access* to the target's computer.

Fig. 3. Unidirectional Communication

Finally, there is **indirect communication** (Figure 4) which is defined as communication through a third party medium. The social engineer and the target can be either an individual, a group of individuals or an organisation. The mediums that are frequently used for indirect communication are pamphlets, flash drives and web pages. Any compliance principle, technique and goal can be combined with indirect communication.

An example of an SE attack that uses *indirect communication* is when a social engineer leaves an infected flash drive lying around in a specifically chosen location with the intention of it being picked up by the target. The infection vector on the flash drive opens up a backdoor on the target's computer when inserted into the computer, allowing the social engineer unauthorised access to the computer. In this example the social engineer, as well as the target, are *individuals*. The technique used for this attack is known as *baiting* because a physical object is left in visible view of a target. The success of the attack relies on the curiosity level of the target. The compliance principle used is *social validation*, which states that someone is more willing to comply if they are performing some action they believe to conform to a social norm. The target may feel socially obliged to attempt to find the owner of the lost flash drive. This leads to the target plugging the flash drive into his or her computer which then activates the backdoor and unknowingly grants access to the social engineer. The goal of the attack is *unauthorised access* to the target's computer.

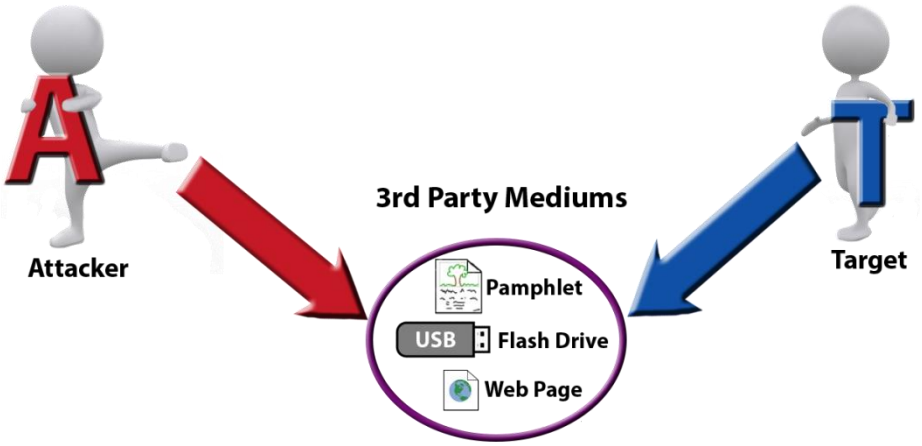

Fig. 4. Indirect Communication via 3rd Party Medium

4.2 Social Engineering Attack Ontological Model

The model that is presented in this section has been compiled from various other taxonomies and the authors' classification of SE attacks. The purpose of this ontological model is not just to define the domain but also to form the foundation for an ontology for SE attacks. Our argument is that a taxonomy is too limited to define SE and SE attacks sufficiently. An ontological model provides additional structure to fully define this domain. According to Van Rees (2003), a taxonomy is a hierarchical structure to aid the process of classifying information, while an ontology is a well-defined set of definitions that create a taxonomy of classes and the relationships between them. Van Rees also states that "an ontology resembles both a kind of taxonomy-plus-definitions and a kind of knowledge representation language." [43].

It is clear from the other taxonomies discussed previously, that their authors tend to mix techniques, compliance principles, mediums and phases of an attack. Our ontological model represents each entity of an attack as well as the relationships between entities.

An ontology allows a formal, encoded description of a domain: All the relevant entities, their attributes and their inter-relationships can be defined and represented in a machine-readable model. Gruber (1993) defines an ontology as "formal, explicit specification of a shared conceptualisation." [44]. Noy and McGuinness define an ontology as: "…a common vocabulary for researchers who need to share information in a domain …includes machine-interpretable definitions of basic concepts in the domain and relations among them." [45]. Ontologies have automated reasoning facilities that enable the derivation of new information from the facts contained in an ontology.

The model is based on our definition of an SE attack as depicted in Figure 5. We defined a *Social Engineering attack* (Section 2) to have:

- one Social Engineer;

- one Target;
- one or more Compliance Principles;
- one or more Techniques;
- one Medium; and
- one Goal.

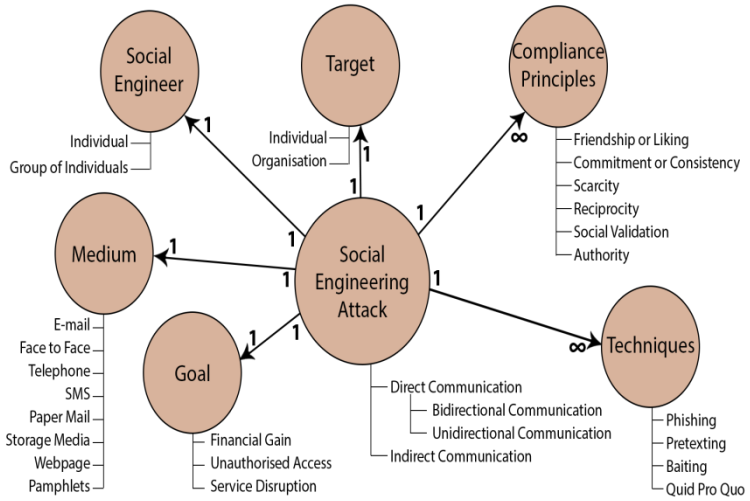

Fig. 5. An Ontological Model of a Social Engineering attack

Each of the six entities is represented as a different class in the model. The subclasses of each class are shown in Figure 5. For example, the *Social Engineering Attack* class has two subclasses: *Direct Communication* and *Indirect Communication*. In turn *Direct Communication* has two subclasses: *Bidirectional Communication* and *Unidirectional Communication*.

The model, in its current state, provides the building blocks to further expand the model into a full ontology. As a future task, when the ontology is built from this model, additional relationships between these classes can be developed and described in detail. One example of a relationship between two classes is *performsAttack* between the *Social Engineer* class and the *Target* class. Our model partially represents our definition of *Social Engineer* (Section 2): *An individual or group who performs an act of Social Engineering*. The latter part of the definition requires representation of the verb *social engineer* and will be presented in the ontology as the relation *performsAttack*.

Further development of the ontology will be performed as future research.

5 Conclusion

Organisations usually employ advanced technical security measures to minimise opportunities for unauthorised individuals, however, every organisation has

employees who are likely to be susceptible to SE attacks. As electronic computing devices becomes more prevalent, the group of individuals who can be targeted by Social Engineering is increasingly significantly. These reasons motivate why SE is such an important field of research. Although SE is a discipline that enjoys increasing attention, it is still not well defined. This paper provides an overview of several definitions from the literature and shows that many researchers define SE to suit their specific topic of research.

In order for the field of Social Engineering to mature, it is required to have commonly accepted domain definitions. Based on all of the definitions and existing taxonomies that have been examined, this paper proposes both a Social Engineering Attack Classification as well as a Social Engineering Attack Ontological Model.

The Social Engineering Attack Classification divides an SE attack into two classes: a direct attack and an indirect attack. The direct attack is further subdivided into an attack utilising bidirectional communication and an attack utilising unidirectional communication. The indirect attack class is further defined as an attack utilising third party mediums as a communication platform.

The Social Engineering Attack Ontological Model expands on the Social Engineering Attack Classification by providing six entities of an attack as well as the relationships between these entities. This model currently represents the definition of an SE attack and partially represents the definition of a social engineer.

In summary, this paper is able to provide definitions for several terms within the domain of Social Engineering. The most important of these terms are Social Engineering and Social Engineering attack. The first one is defined as: *The science of using social interaction as a means to persuade an individual or an organisation to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity*. The latter term is defined as: *A Social Engineering attack employs either direct communication or indirect communication, and has a social engineer, a target, a medium, a goal, one or more compliance principles and one or more techniques*.

Additional work is required to fully develop the ontological model. This includes the expansion of classes as well as the relationships between classes. In future work it is also required to represent the different phases of an SE attack.

References

1. Winkler, I.S., Dealy, B.: Information security technology? ...don't rely on it: A case study in social engineering. In: Proceedings of the 5th Conference on USENIX UNIX Security Symposium - Volume 5. SSYM'95, Berkeley, CA, USA, USENIX Association (1995) 1–1
2. Mitnick, K.D., Simon, W.L.: The art of deception: controlling the human element of security. Wiley Publishing, Indianapolis (2002)
3. Uschold, M., Gruninger, M.: Ontologies and semantics for seamless connectivity. ACM Special Interest Group on Management of Data **33**(4) (December 2004) 58–64
4. Quann, J., Belford, P.: The hack attack - increasing computer system awareness of vulnerability threats. In: 3rd Applying Technology to Systems; Aerospace Computer Security Conference, United States, American Institute of Aeronautics and Astronautics (December 1987) 155–157

5. Kluepfel, H.: Foiling the wiley hacker: more than analysis and containment. In: Security Technology, 1989. Proceedings. 1989 International Carnahan Conference on. (1989) 15–21
6. Kluepfel, H.: In search of the cuckoo's nest [computer security]. In: Security Technology, 1991. Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on. (1991) 181–191
7. Goldstein, E.: The Best of 2600, Collector's Edition: A Hacker Odyssey. Wiley Publishing, Inc., Indianapolis, IN (2009)
8. Voyager: Janitor privileges. 2600: The Hacker Quarterly **11**(4) (Winter 1994) 36–36
9. Thornburgh, T.: Social engineering: the "dark art". In: Proceedings of the 1st annual conference on Information security curriculum development. InfoSecCD '04, New York, NY, USA, ACM (2004) 133–135
10. Nohlberg, M.: Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks. PhD thesis, Stockholm University (2008)
11. Abraham, S., Chengalur-Smith, I.: An overview of social engineering malware: Trends, tactics, and implications. Technology in Society **32**(3) (2010) 183 – 196
12. Erbschloe, M.: Trojans, worms, and spyware: a computer security professional's guide to malicious code. Butterworth-Heinemann (2004)
13. Boshmaf, Y., Muslukhov, I., Beznosov, K., Ripeanu, M.: The socialbot network: when bots socialize for fame and money. In: Proceedings of the 27th Annual Computer Security Applications Conference. ACSAC '11, New York, NY, USA, ACM (2011) 93–102
14. Boshmaf, Y., Muslukhov, I., Beznosov, K., Ripeanu, M.: Design and analysis of a social botnet. Computer Networks **57**(2) (2013) 556 – 578 <ce:title>Botnet Activity: Analysis, Detection and Shutdown</ce:title>.
15. Kvedar, D., Nettis, M., Fulton, S.P.: The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition. Journal of Computing Sciences in Colleges **26**(2) (December 2010) 80–87
16. McDowell, M.: Cyber security tip st04-0141, avoiding social engineering and phishing attacks. Technical report, United States Computer Emergency Readiness Team (February 2013)
17. Cruz, J.A.A.: Social engineering and awareness training. Technical report, Walsh College (2010)
18. Culpepper, A.M.: Effectiveness of using red teams to identify maritime security vulnerabilities to terrorist attack. Master's thesis, Naval Postgraduate School, Monterey, California (September 2004)
19. 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. InfoSecCD '09, New York, NY, USA, ACM (2009) 139–141
20. Doctor, Q., Dulaney, E., Skandier, T.: CompTIA A+ Complete Study Guide. Wiley Publishing, Indianappolis, Indiana (2007)
21. Hamill, J., Deckro, R.F., Jr., J.M.K.: Evaluating information assurance strategies. Decision Support Systems **39**(3) (2005) 463 – 484
22. Joint Chiefs of Staff: Information assurance: Legal, regulatory, policy and organizational legal, regulatory, policy and organizational considerations. Technical Report Fourth Edition, Department of Defense, Pentagon, Washington (August 1999)
23. Hamill, J.T.: Modeling information assurance: A value focused thinking approach. Master's thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio (March 2000)

24. Braverman, M.: Behavioural modelling of social engineering-based malicious software. In: Virus Bulletin Conf. (2006)
25. Åhlfeldt, R.M., Backlund, P., Wangler, B., Söderström, E.: Security issues in health care process integration? a research-in-progress report. In: EMOI-INTEROP. (2005)
26. Granger, S.: Social engineering fundamentals, part i: Hacker tactics (December 2001)
27. Schoeman, A., Irwin, B., Richter, J.: Social recruiting: a next generation social engineering attack. In: Uses in Warfare and the Safeguarding of Peace. (2012)
28. Hadnagy, C.: Social Engineering: The Art of Human Hacking. Wiley Publishing, Inc. (2010)
29. Espinhara, J., Albuquerque, U.: Using online activity as digital fingerprints to create a better spear phisher. Technical report, Trustwave SpiderLabs (2013)
30. Nemati, H.: Pervasive Information Security and Privacy Developments: Trends and Advancements. First edition edn. Information Science Reference (July 2010)
31. McQuade, III, S.C.: Understanding and managing cybercrime. Prentice Hall, Boston, MA (2006)
32. Spinapolice, M.: Mitigating the risk of social engineering attacks. Master's thesis, Rochester Institute of Technology B. Thomas Golisano College (2011)
33. Lenkart, J.J.: The vulnerability of social networking media and the insider threat new eyes for bad guys. Master's thesis, Naval Postgraduate School, Monterey, California (2011)
34. Bezuidenhout, M., Mouton, F., Venter, H.: Social engineering attack detection model: Seadm. In: Information Security for South Africa. (2010) 1–8
35. Mouton, F., Malan, M., Venter, H.: Development of cognitive functioning psychological measures for the seadm. In: Human Aspects of Information Security & Assurance. (2012)
36. Mouton, F., Malan, M.M., Venter, H.S.: Social engineering from a normative ethics perspective. In: Information Security for South Africa. (2013) 1–8
37. Kingsley Ezechi, A.: Detecting and combating malware. Master's thesis, University of Debrecen, Hungary (June 2011)
38. Harley, D.: Re-floating the titanic: Dealing with social engineering attacks. In: European Institute for Computer Antivirus Research. (1998)
39. Laribee, L.: Development of methodical social engineering taxonomy project. Msc, Naval Postgraduate School, Monterey, California (June 2006)
40. Ivaturi, K., Janczewski, L.: A taxonomy for social engineering attacks. In Grant, G., ed.: International Conference on Information Resources Management, Centre for Information Technology, Organizations, and People (June 2011)
41. Mohd Foozy, F., Ahmad, R., Abdollah, M., Yusof, R., Mas' ud, M.: Generic taxonomy of social engineering attack. In: Malaysian Technical Universities International Conference on Engineering & Technology, Batu Pahat, Johor (November 2011)
42. Tetri, P., Vuorinen, J.: Dissecting social engineering. Behaviour & Information Technology **32**(10) (2013) 1014–1023
43. Van Rees, R.: Clarity in the usage of the terms ontology, taxonomy and classification. CIB REPORT **284**(432) (2003) 1–8
44. Gruber, T.R.: A translation approach to portable ontology specifications. Knowledge Acquisition - Special issue: Current issues in knowledge modeling **5**(2) (June 1993) 199–220
45. Noy, N.F., McGuinness, D.L.: Ontology development 101: A guide to creating your first ontology. Technical report ksl-01-05, Stanford Knowledge Systems Laboratory (March 2001)