CHAPTER V

DISCUSSION AND CONCLUSION

5.0 INTRODUCTION

In this chapter, discussion, explanation and analyzing of results that have been obtained by the process of development of social engineering ontology, which contained compilation, collection of related terms on social engineering, and implementation with comparison of previous studies in the same field.

5.1 DISCUSSION

First of all, development of any ontology depends on reuse consideration, if there was no ontology to be used as a starting point; the researcher needs to construct a new one. In this study, it was taken into consideration that there were previous studies which discussed the development of social engineering taxonomy, but no ontology construction was found. Therefore, the process of development passed through three main steps for social engineering ontology development can be listed as follows:

5.1.1 EXTRACT RELEVANT TERMS

It was necessary to overcome hurdles throughout the process of collecting and extracting related terms on social engineering. What has been extracted was derived from many publications. Previous studies focused on influences of social engineering rather than focusing on its techniques. Therefore, the terms have been compiled from different areas depending on a lot of literature review (discussed in Section 2.3.2). During the searching process, the researcher tried to cover the specified scope and used a variety of related keywords by using various search engines.

The collected terms are extracted based on publications on social engineering to build a taxonomy block for the proposed ontology. Furthermore, the previous developed taxonomy is also involved in this study such as, taxonomy of (Cik Feresa, et.al, 2011) (discussed in chapter 2).

5.1.2 COLLECT EXTRACTED TERMS

This phase focuses on identification of category the attack belongs, because there are many techniques identified by other researchers, which have been classified in a general form of social engineering attacks. Mainly, this study adopted two categories of social engineering attacks, such as **1- Human-based attacks** and **2- Technical-based attacks**. Both categories contain many techniques of attack. Similarities in techniques also adopted with clarifying difference aspects between them.

5.1.2.1 HUMAN-BASED ATTACKS

Social engineering related terms that have been added to this category depend on the techniques that need interaction with humans. Mostly, techniques of this category are using face-to-face impersonation or over the phone to release sensitive information. These techniques are categorized under human-based attacks (discussed in chapter 1).

5.1.2.2 TECHNICAL-BASED ATTACKS

Social engineering related terms that have been added to this category, depend on the techniques that use computer software and target users of computer systems. Mostly, techniques of this category are using technical scams to retrieve the desired information. These techniques are categorized under Technical-based attacks and also discussed in (chapter 1).

5.1.3 ONTOLOGY DEVELOPMENT

For the implementation of ontology on social engineering, Protégé open software is used for construction according to its advantages such as;

1. Facilities of editor, for example, construction of classes, properties and restrictions creation, in addition to facilities of ontology reuse.

2. In case of adoption for another ontology design platform, Protégé can provide the same interface for constructed ontology and the adopted one.
3. Give opportunity to export to different format such as OWL and RDF.
4. Support different ways of graph view, and good display for classes and their relationships.
5. Graphs provided by Protégé are suitable for purposes of presentation.

Through the process of transformation knowledge model into knowledge representation language, the developed ontology model for the social engineering consists of three sub classes which describe the main branches for social engineering developing process. Such as:

1. *Types* class: contains two others sub-classes (Human-based attacks and Technical-based attacks).
    a) Human-based attacks: contains all instances of targeting and represent direct interaction with victims.
    b) Technical-based attacks: contains all instances of targeting computer systems and their users.
2. *Threats* class: created to involve instances of potential threats and vulnerabilities that caused by social engineering attacks.
3. *Countermeasures* class: involve instances that represent methods and techniques to avoid social engineering attacks.

The relationships can be either used to describe relation between instances of two classes or instances of classes and resource description framework schema (RDF).

In social engineering ontology, the relationships are divided into six types of relations as follows:

1. Affect_Individual: represents the relationship between *Threats* instances that affect individuals and *Types* class.
2. Affect_Organization: represents the relationship between *Threats* instances that affect organization facilities and *Types* class.
3. Countermeasures_to_People_Attacks: represents the relationship between instances of *Human-Based_Attacks* and *Countermeasures* classes.
4. Countermeasures_to_Tech_Attacks: represents the relationship between instances of *Technical-Based_Attacks* and *Countermeasures* classes.
5. Has_Direct_Interaction: represents the relationship between instances of *Human-Based_Attacks* class and other instances in *Types* class.
6. Has_Indirect_Interaction: represents the relationship between instances of *Technical-Based_Attacks* class and other instances in *Types* class.

Of course the need of these relations is to associate one individual with one another among ontology classes. For example, *Countermeasures_to_Tech_Attacks* relationship associated between the individuals *Security_culture* of *Countermeasures* class and *Phishing* of *Technical-Based_Attacks* class.

5.1.4 THREATS AND VULNERABILITIES

As long as social engineering attacks are still prevalent everywhere, the threats will continue to affect individuals and organizations. Social engineers will start creating a list which contains potential targets considering some factors such as;

a) Where he can get appropriate access into the target,
b) Volume of resistance, determine aware of victim in order to determine which suitable technique to be used, and
c) availability of information, that's why social engineer supports search method in information gathering depending on social networking sites.

Most previous studies show that, the use of the same password across multiple services make users' passwords more likely to be disclosed. On the other hand, and as would be expected, employees and public users who had awareness and training courses are less to share passwords.

A threat of social engineering targeting many aspects and the primary motivation is financial gains. For this reason, many of studies refer to the rise in theft of credit cards and confidential data of customers. These attacks are costly, particularly in organizations where they target their systems and sensitive information, secure data, database and harvest passwords, trade secrets, workstations and lead to the sabotage of networks and the breakage of physical security control. Social engineering techniques target new employees and make them the most susceptible to

its impacts due to lack of sufficient awareness and training. Therefore, experts stress the need for proactive training in order to avoid attacks that target new employees.

5.1.5 COUNTERMEASURES AND PREVENTION

Because social engineering techniques are in rapid progress, it is difficult to absolutely prevent this art of hacking by technical methods only. The task of prevention starts from getting users and organization employees to know about the danger of these attacks and implement effective security measures. Through a review of previous studies, countermeasures can be categorized in three categories as follows:

a) Physical security: Assets included in this category must be well-protected and monitored, such as physical entry and exit points to all organization facilities, taking into account the importance of securing the entries to workstations and resources. This category needs provisions of equipment such as video surveillance, biometric access devices, automatic locked gates, and sign-in sheets for strangers.

b) Personal security: It is never easy to fully protect individuals against social engineering attacks, but it is not impossible. However, there are several procedures that can be adopted to avoid attacks. The most important factor is awareness. Raising awareness between systems' users and all organization's employees in addition to regular training courses is crucial. A person should not give any random contact

confidential information over the phone or online except after verifying their identity. All employees must know that, username and password should not be requested by technicians. It is necessary to protect user passwords and make it difficult to guess and use different usernames and password for each service. Furthermore, users must remove their information from any public database such as People Finders sites.

c) Digital security: Multiple security measures must be employed by systems administrators in order to make any social engineering attack as difficult as possible. At the least, implementing security baselines according to organization security requirements such as password policy, firewalls policy, email filtering, multi factor authentication, an efficient encryption mechanism, caller ID technology, access control, and raising the system level of security should be undertaken, in addition to keeping all scanners updated.

5.2 CONTRIBUTIONS

This thesis supports the process of knowledge sharing by focusing on development of ontology on social engineering. Development of social engineering ontology contributes in knowledge sharing for academic purposes equally among researchers on social engineering. This is achieved by collecting related terms on social engineering from publications and developing social engineering taxonomy. Concrete contributions of this research can be summarized as follows:

a) Extract social engineering terms from compiled related publications from 2001 through 2014 in addition to describing motivations that make social engineers attack.

b) Develop a collection of social engineering related terms (Taxonomy), and give some ideas on how to identify social engineering types and how to categorize each and every technique according to the types.

c) The thesis describes methodology that should be followed in ontologies construction. Furthermore, it presents implementation steps for social engineering ontology by using Protégé 4.2 editor.

d) Construct ontology for social engineering with surrounding how to create its classes and properties and the relationships among them. There is also the possibility to use this ontology as a starting point or to be merging with one another.

e) Social engineering ontology focus on three aspects such as, types and this represented in human-based attacks and technical-based attacks, potential threats of social engineering and countermeasures.

5.3 LIMITATIONS

Research objectives provided in this research have been achieved by compiled related publications, developed taxonomy and developed ontology. But none of these have worked at levels that are desirable, according to unavoidable limitations, such as

the study time being very limited because there was not enough space between the needed time to sit for the subjects and doing the thesis as much as possible at the same time. Second, it was planned for the process of compilation of a related publication on social engineering to cover more than the current related publications, but this also faced the same constraint mentioned above. Third, design and implementation phases needed more time in order to give a level of confidence and certainty at each step in all of the stages.

5.4 SUGGESTION FOR FUTURE RESEARCH

What has been presented in this research is also scalable. Therefore, future research could be built upon; first, by adding more countermeasures that are commensurate with the evolution of social engineering attacks. Second, a future ontology should be able to include more relationships between classes and instances. Third, developed taxonomy presented in this thesis should make it possible to classify a large range of social engineering attacks. Fourth, as most of the previous studies have suggested, the most effective defense to prevent or mitigate social engineering attacks are awareness and training; for more enhancements, a search for a new approach is needed. Furthermore, it is better to add "attacks scenarios" to increase the awareness level about social engineers, behaviors and their techniques in order to give a complete scope of these attacks. Fifth, OWL properties also can be enriched by using properties characteristics.

In the future research the main domain presented in this ontology "Social engineering" can be extended to involve scenarios of the two types' techniques (human-based and technical-based), so this requires deep analysis from a different perspective which may enhance knowledge and make ontology more efficient.

5.5 CONCLUSION

In the modern day, social engineering has been widely used in society for building relationships and interacting with others for a long period of time. In this study, the researchers reviewed and analyzed the social engineering attacks in specific view. Some researchers of social engineering attacks have classified the attacks based on the human-based social engineering attacks and technical-based social engineering attacks. Basically, Social Engineering attacks vulnerabilities in what is deemed to be common sense. In order to build a knowledge sharing based on the analysis, we need to associate terms with the concepts and relations in the ontology. As a result of this study, social engineering attacks have been categorized under two categories, human-based attacks and technical-based attacks. Both of the two categories are contained 57 attack techniques. The most dangerous threat presented is stealing sensitive information and passwords, where the essential countermeasure is users' and employees' awareness. The developed ontology in this study can be reused for future work as a starting point to build a larger ontology, or it can be merged with another one.