CHAPTER III

MATERIALS AND METHODOLOGY

3.0 INTRODUCTION

This chapter explains the material and methodology adopted in this study. Mainly, materials depend on publications. Methodology of developing stages consists of eight stages for developing ontology on social engineering. This chapter also provides a brief summary of some ontology editors.

3.1 MATERIALS

The knowledge resources used for developing the social engineering ontology consisted of publications related to social engineering from selected databases from 2001 to 2014. The publications will mainly be related on several aspects of social engineering such as types, potential threats, techniques of human based, techniques of technical based, awareness, and attacks countermeasures. In addition, ontology applications for construction and visualization is going to use protégé.

3.2 RESEARCH METHODS

The social engineer attacker targets everyone - from users of phones, social networking sites, email, to banks, and a variety of businesses activities. Discussion should focus on security weaknesses in order to prevent or mitigate social engineering attacks. Substantially, there are two kinds of weaknesses that create a gap to social engineering attacks. Insufficiency of security awareness for an organization's employees simplifies most social engineering attacks. In other words, people do not have an awareness of how to behave adequately to attack situations. Insufficient security plans and not applying procedures also simplify an attack.

Social engineering awareness must cover not only training and educating staff about phishing and different internet security, but also, significantly, not giving information or secret details to unauthorized people to receive them and the detection and prevention of physical social engineering attacks. If a social engineer can get inside the physical perimeter, then, that will allow him to access the network security perimeter and less control to bypass.

Suppose that, a particular company were attacked by one or more social engineering techniques which could be, for example, unawareness of its employees about these techniques. And suppose that this attack led to disclosure of sensitive operational company information, along with a huge number of passwords, unintentionally giving social engineers the ability to paralyze the company in spite of good security measures. A similar result could happen for any company. The study

concludes with comprehensive social engineering taxonomy to mitigate and reduce the social engineering threats.

3.2.1 DEVELOPING STAGES

The ontology in this research will be developed based on stages as suggested by Noy and McGuinness (2000). They suggested the following steps are to be followed in order to develop ontology.

a) Determine the domain and scope of the ontology.

The scope of the ontology in this study are as listed below:

- ✓ What are the types of social engineering?
- ✓ What are the threats of social engineering?
- ✓ What are the types of human-based social engineering attack?
- ✓ What are the types of technical-based social engineering attack?
- ✓ What are the countermeasures for social engineering attacks?

b) Consider reuse.

If there is an ontology available from a third party, it can be used as a useful starting point. If there are none available, researchers have to develop an ontology from scratch.

c) List key terms

All the terms that are likely to appear in the ontology can be listed out. The relations among the classes and the properties of the classes and instances in the ontology may also be listed out.

d) Define taxonomy

After the identification of key terms, these terms must be organized in a taxonomic hierarchy. This social engineering ontology will use the top-down approach. Social Engineering is the main root class. Subclasses of this root are Types (Human-based attacks and Technical-based attacks), Threats, and Countermesures. Under these subclasses, many more subclasses are going to be defined.

e) Define the properties of the classes.

Properties define the relationships between two objects. For example, different object properties are used in the ontology. Whereas, data properties is added in the ontology.

f) Define the facets of a class

Facets of a property describe the value type. For example, consider the property Has_Direct_Interaction.

g) Define instances

Individual instances of the classes are created in the ontology. This ontology organizes sets of instances.

h) Implementation in Protégé.

3.2.2 PROTÉGÉ (*http://protege.stanford.edu*)

Protégé is one of the open source and ontology editors, in addition to a knowledge base framework. It is free for all users. So, this tool supports modeling ontologies for web clients and / or desktop users. Ontolegies through this tool can be developed in different types of formats such as OWL, XML schema and RDF. It is a flexible base for application development, and also for rapid prototyping, because it is based on Java, and provides a plug and play environment according to extensible. Protégé serves developers, corporate, government, and academic users for knowledge in different areas. It can be downloaded from the following site: (*http://protege.stanford.edu/download/download.html*).

Web protégé is also a product of Stanford, it is an open source, lightweight but it is used for developing web ontology. The web protégé is more similar to the protégé environment but it is used for web applications. It allows users to collaboratively develop ontologies in a distributed way; supports OWL 2 ontologies and users can upload OBO Format ontologies and edit them collaboratively. It has a content management system. So this ontology can also be made for web also for the broader usage of ontology.

3.3 CONCLUSION

In this chapter a description of used materials is given, all selected publications from the database are covered from 2001 to 2014. Whereas the research methodology based on stages as suggested by Noy and McGuinness (2000), in addition to employ these stages according to the methods adopted by previous studies. Among the various reviewed ontology editors, Protégé is chosen to implement social engineering ontology. Because it is free, open source and easy to use, allows class definition, hierarchy of classes, and easy to construct relationships between classes and properties with the help of diagrams. The main difference is that it supports tool builders, domain specialists, and knowledge engineers. Additional support can be received by consulting others.