CHAPTER I

INTRODUCTION

1.1 INTRODUCTION

Ontology is the study of the concepts of knowledge within any domain which might be relevant. In information sciences, it involves the use of methods to control human behavior in order to achieve certain utility.

Ontological analysis will make the structure of knowledge simpler. Without ontology, the terms cannot represent knowledge. Thus, an effective knowledge representation of a system of terminologies requires ontological analysis of a given domain.

Ontology is an explicit specification of a conceptualization (Gruber, 1993). In a hierarchy structured from top to bottom, under domain there are a set of terms for describing a certain domain and this relationship consists of a foundation for a knowledge base. In a system, concepts are provided by ontology in an organizational framework allowing for knowledge reasoning. Basically, ontology is known as a medium of human expression and a man-made tool to communicate with machines. Presently, ontology is one of the most interesting components for knowledge management, especially in terms of retrieval efficiency and knowledge sharing. Its ability to access knowledge through varieties of relationship between concepts serves well the need of users who want to access required information and knowledge, in a

world so rich of information like now, more efficiently and comprehensively (Gruber, 1993).

Relational databases are often used as a basis for persistent storage of ontologies to facilitate rapid operations such as search and retrieval, and to utilize benefits of relational databases management systems such as transaction management, security and integrity control. On the other hand, there appear more and more OWL files that contain ontologies.

There are two basic techniques for storing ontologies, (Astrova et al, 2007). The first technique is to use file systems for storing ontologies in flat files, and the second technique is to use database management systems (DBMS) for storing ontologies in databases. There are several options for storing ontologies in databases; e.g. relational, object or object-relational. Storing ontologies in relational databases is less straightforward than storing ontologies in object or object-relational databases, because relational database management systems do not support inheritance. However, relational database management systems have significant advantages over object or object-relational database management systems. In particular, relational database management systems provide maturity, performance, robustness, reliability, and availability.

The database schema of a database system describes in formal language the structure supported by the database management system (DBMS). It refers to the organization of data as a blueprint of how a database is constructed. A semantic mapping from a database schema to an ontology defines a semantic relationship

between the schema and the ontology. Therefore, once a semantic mapping from a schema to an ontology has been created, it is important and necessary to automatically, at least to some extent, maintain the validity of the semantic relationship when the schema and ontology evolve (Yuan and Topaloglou, 2008).

Social engineering is an important topic to protect systems from the threat of intervention of hackers or other intruders, whereby, if exploited, it might provide access to the internal infrastructure of an organization, which can lead to disastrous outcomes.

Many people know about the ontology of social engineering; through automatic systems have been implemented by these means, in order to be aware by social engineering vocabulary, and to avoid leaking of sensitive information for people who don't have authorized access. But if social engineering is still one of the best ways to access private information by bypassing the security policies, in that case, all knowledge is insecure in the absence of a good security policy.

Therefore, this research aims to compile relevant publications on social engineering from selected databases as well as to develop a collection of related terms (Taxonomy) on social engineering based on the extraction of multiple publications related to social engineering. This research also aims to develop ontology to facilitate information and knowledge sharing as well as knowledge reuse on social engineering.

1.2 RESEARCH PROBLEM

The research problem is how, in the present society, to secure information exchanging and knowledge sharing among people, which is a most important activity. However, many problems are faced within the area of knowledge sharing and knowledge reused due to the diversity of multiple knowledge sources and online sabotage operations. Currently, knowledge sharing between entities is achieved in a very ad hoc fashion, lacking of an appropriate understanding of the meaning of the data. Ontologies can potentially solve these problems by facilitating the knowledge sharing and reusing the data.

Ontology defines what exists in a domain and how they relate with each other to form common vocabulary for researchers who need to share information in a domain.

The problem in knowledge sharing of information, reusing and updating of the existing ontology is the major justification for the ontology development. By developing ontology, it is possible to develop a common understanding of the structure of information among people or software agents.

Information on social engineering is scattered everywhere. It is not easy to search and find relevant information on social engineering. Through ontology, all these different sources of information can be aggregated and published .The users and agents can use this aggregated information to answer user queries or as input data to other applications.

Furthermore, duplication in research topics might occur if researchers are not aware of what other researchers on this kind of duplication exist. This potential problem has established a real reason to develop ontologies without having to re-invent the wheel and introduce standards to allowing interoperability.

1.3 RESEARCH OBJECTIVES

The main objective of the study is to develop the ontology to facilitate knowledge sharing and knowledge reusing, which are related to social engineering. The following research objectives are proposed to fulfill the main specific objectives that are mentioned in the following points:

a) To compile related publications on social engineering published from 2001 – 2014 from selected databases.
b) To develop a collection of related terms (taxonomy) on social engineering which is based on the extraction of heterogeneous publications related to social engineering.
c) To develop ontology to facilitate information and knowledge sharing as well as knowledge reusing on social engineering.

1.4 RESEARCH QUESTIONS

The research problem defines the objectives, and can therefore be divided into three successive main research questions as follows:

a) How to compile relevant publications on social engineering published from 2001 – 2014 from selected databases

b) How to develop a collection of related terms (taxonomy) on social engineering based on the extraction of heterogeneous publications related to social engineering.

c) How to develop ontology to facilitate information and knowledge sharing as well as knowledge reusing on Social Engineering.

1.5 SCOPE AND LIMITATION OF THE RESEARCH

In this study the extraction of key terms and related terms on insider and outsider threats are mainly related on several aspects of social engineering such as 1) types, 2) threats, 3) human-based social engineering attacks, 4) technical-based social engineering attacks, and 5) countermeasures. Basically, the researcher aims to create an ontology of social engineering on a minimum requirement basis based on publications published from 2001 to 2014 from selected databases. The challenges in developing this ontology will be to extract the knowledge from the various sources and to determine the notions of different kinds such as classes, entities, relationships between them and properties of things. This is a one-man show project due to limitation of time and resources, therefore, the extraction of information might not be wholly based on the printed materials related to social engineering.

1.6 RESEARCH SIGNIFICANCE

Different publications contain a variety of details about the social engineering. It is, therefore, necessary to have an obvious theoretical perception of the types of social engineering, as well as the manipulation process, in order to classify incidents, understand their elaboration, and devise mitigation techniques. Through ontology all the information about threats and secure methods can be cumulated, shared and published. The researchers from various fields can use this information to contribute to the existing research or create new research findings. This research study could provide knowledge sharing for potential users or researchers who have interest about methods of social engineering. Further, the developed ontology would be beneficial to researchers and the research community in the field of security and technology, as this study would provide the necessary information on social engineering. This would indirectly encourage the sharing of knowledge on social engineering among the researchers and public users. In the future, this study could provide baseline information for ongoing and future research related to social engineering.

Furthermore, in the future, other users will reuse this ontology if a larger model needs to be developed or built; this existing ontology could be integrated into a larger ontology. The existing ontology can also be updated.

1.7 DESCRIPTION OF THE RESEARCH PROCESS

The work on this thesis started out with a literature study, in which the aim was to compile and collect relevant publications on social engineering. The focus was on using *"Google Scholar"* search engine and select publications relevant to social

engineering categories such as attacks, threats, techniques, etc. Also, the focus was on publications generated by universities and international conferences.

Within the literature study, social engineering types and their characteristics were also investigated. The objective was to try to find what is specific in such publications, e.g. how many categories exist for social engineering attacks, what are the threats of social engineering attacks, what are countermeasures for social engineering, and which are the requirements when looking at the ontology development methodologies?

The next step in the research process was to select the ontology development methodologies found during the literature study. Noy and McGuinness (2000) construction methodology was used (as discussed in chapter 3).

1.8 TERMINOLOGY

Ontology: Knowledge representation as a set of concepts related to a particular domain as well as conceptual relationships between them. These concepts can be used to represent the domain. Ontology is created in machine readable languages of RDF, XML and OWL.

Semantic Web: This is a special form of ontology on the web and allows machines to process incoming knowledge on the World Wide Web, as well as to connect and interpret it to help humans for interpretation.

Social Engineering: This is a collection of techniques used to make people to do something or to declare about confidential information. It is here defined as a way to gain valuable information about the system from people in general, where attackers using little owned information to win the confidence of his victim, this trust, leads the victim to provide sensitive information to the attacker through which can be discovered the properties of the system.

Asking for Favor: This technique is used by skilled hackers who gain information slowly by asking for favors through ordinary conversations.

By Phone: This social engineering involves impersonation through phone. The attacker uses a phone to trick the victim and provides him with necessary information.

Chance of Ingratiation: It is quite similar to the principle of reciprocation, but there is no tangible benefit given to the victims, they are merely led to believe that complying will allow them to get some kind of benefit in the future.

Cold Calling: Tactics for social engineering cold calling. This has become notable after a given attacker admits where he would play recorded calls and explains his thought process on what he was doing to get passwords through the phone.

Conformity: Social engineers could use this technique with a group of people or individuals by convincing a certain user that all users have been giving the same requested information, in case the hacker pretending to be an IT manager. This attitude alleviates the stress on the individual user.

Contriving Situation: The social engineer will search for a mark or something that allows him to be a fellow employee and plays on the victim's background.

Creating a Hostile Situation: Pretending to have a heated phone conversation to make others avoiding you as well as you seems to be angry at something. Because it is normal that people would withdraw from those kinds of people.

Diffusion of Responsibility: A method which is used to convince victims that they are not responsible for the taken action. But they act as a part of group that has established a consensus for common goals.

Direct Approach: There are many situations that allow social engineer to use a direct approach such as simply calling and directly asking a simple question or receiving information through conversations.

Dumpster Diving: Looking for helpful documents by sorting through a company's trash. Sometimes social engineers may take computer equipment such as memories or old hard drives and use forensic analysis to retrieve information.

Familiarity Exploit: Method to lower the guard of others by making you familiar and normal to those you want to exploit their help. This technique is a cornerstone and one of the most effective modes of social engineering.

Fear: Psychological principle of fear is introduced by work-man (Social engineer). He recognizes that he cannot act alone and can only be used in conjunction with an authoritative source.

Forensic Analysis: Used when a social engineer obtains old computer equipment such as DVD/CDs, hard-drives, floppy disks, memory sticks, then tries to extract information that might be of use about an individual/ organization.

Gathering and Using Information: Some researchers have classified this method as an initial phase before an attack is implemented. It is merely a way to make social engineering successful and an easy way to attack a victim depending on what you have got.

Get a Job There: Just get a job at a social engineer's target and grab all the information he can.

Get Smashed: Way of knowing whether the victim attends wine bars. Social engineers can extract sensitive information from a victim while he is drunk. Also he may pay for his drink to drink a lot. lose consciousness and expose sensitive things to his attacker.

Giving out Free Software: Software is given out as a gift but in fact, it has a trojaned version which has replaced the original source code. The software looks like it does what it's supposed to do, but it includes an extra code to bypass the security.

Guilt: A way to play at the basic instincts of the victims, social engineering attackers can leverage guilt to persuade the victim to assist them.

Helpless User: A social engineer pretends to be somebody who is helpless. This technique is used to shift from one department to another one or to get access to a network station under the pretext of learning.

Impersonation: Often the social engineer pretends to reincarnate roles of others. In this technique, the attacker may act like a service provider, administrator of network or anyone in authority to manipulate other employees.

Important User: An attacker pretending to be a senior manager or anyone with important tasks.

In Person: In-person social engineering involves having the hacker pretend to be repairman offering to help other employees.

Mail-Out: Participate in a survey that offers enticements and promise with prizes after completion of survey in order to gather information about an individual or organization by enticing him/his staff.

Nero Linguistic Programming (NLP): is a psychological tool used by social engineers to manipulate people that, when done right, is highly successful. NLP deals with a person's neurological processes, language, and learned behavior responses.

Online Social Engineering: Make emails, online chat sessions or reliance on any methods that a company may use in interacting with customers in order to gather information or persuade others.

Overloading: Refers to actions taken by a social engineer which aims at flooding the victim with information. This is done in order to force the victim to concentrate on absorbing information, not on evaluating it.

Personal-stake Phishing: A social engineer uses a dummy website such as a banking site or an online shopping site to ask someone by email to enter there and insert his ID and password to do something necessary. The attacker may use same logo and trademark in order to appear as a real website.

Persuasion: This is a basic social engineering method, which depends on psychological triggers. It requires a convincing and smooth-talking attitude with a person; it is very simple but can be very effective.

Pharming: This technique is similar to phishing but a social engineer can use Domain Name System (DNS) cache poisoning which makes DNS redirect the user to a spoofed site. This is contrasted with phishing, where a user needs to open a fake email or to click on a false link.

Photography: Tricks to taking photographs used by social engineer when he is targeting any building, in order to have a sensible thing to do.

Piggyback Rids: Basically in this kind of attack, authorized person provides access to social engineer through a secured door. Maybe he stays outside the building with some employees for smoking, then follows behind them into the building appearing as a legitimate employee.

Pretexting: It is an act of creating and using a fabricated scenario (pretext) to disclose sensitive information about the target. This method requires serious planning.

Questionnaires: An information gathering method.

Reading Body Language: An experienced social engineer will read and respond to the victim's body language. This is one of the most powerful connections S.E can make with his victims: smiling at the right times, breathing when they breathe, adapting to their emotions, being polite and friendly enough to gain their confidence, but not going so far as to seem inauthentic. Once the attacker has established a comfort level with the victims, he is free to exploit them.

Reconnaissance: Considered as one of the war techniques, which is watching the target and gathering information about when, where and how they do things.

Sex Sells: It could be to build trust or exploit by using human attraction for getting someone interested in you and giving them the impression that the feelings are reciprocated.

Shoulders Surfing: Looking over a user's shoulder to capture a username and a password that a user is typing into the computer.

Simple Request: A social engineer can make a simple request to be dealt with by a victim without the others feeling or thinking about what he is doing.

Social Engineering in Reverse: Tactics done by a social engineer to make a legitimate user ask him for help and, depending on the hacker, to solve his technical problems. Social engineers carry out this attack through three steps:

a) First, the attacker damages a victim's equipment.
b) He then advertises himself in the role of authority, to solve the victim's problem.
c) He then convinces the victim that, he is able to solve such these problems to make the victim depend on him for any problem and ask him for help.

Spying and Eavesdropping: Social engineers may place themselves at a known location, 'over lunch' for employees of a particular company, to be able to overhear their chat about company tasks.

Support Staff: Social engineer posing as a network technician and requests him to access to workstation to fix problems.

Surveys: A way of gathering information. Occasionally, questions seem to be innocuous but they could disclose interesting information or data about a company's

tasks or its members, where the social engineer could use them later for building manipulative relationships.

Tailgating: Sometimes also called piggybacking, a way to get access to the facilities, for example, a social engineer can gain access through a locked door or security gate at the same time with one who has access permission. So he uses the facilities as an authorized person. He could wear the uniform and interact with company's employees as one of them.

Tech-Support: In this technique, a social engineer uses a series group of tricks by pretending to be a technical support or system engineer; by this tactic he could extract useful information. Perhaps when he asks for a user's password, in order to be able to fix some problems in a user account.

The Voice of Authority: A social engineer pretends to represent someone in a company position of authority, and uses its contact number to then pull out information from their users.

Theft: Social engineer could take others' property without their permission. This theft could involve information about the company, customer records, or equipment.

Third Party Authorization: The social engineer may have obtained the name of someone in the organization who has the authority to grant access to information.

Catch Me a Vish (SMS/ Cell Pone Vishing): The phone version of phishing.

Social Engineer networking: A social engineer uses social networking sites (Facebook, Twitter, etc) to find out a lot of information about the victim. People use these sites to post their information, photos and a lot of what they like to do. So this could provide plenty of data for an attacker.

Bogus Survey: Social engineers use this type of survey by placing it in the mail with the lure of a cash prize, then using this information to build a relationship or to implement an attack.

Fake Mails and Attachment: This attack is implemented by using e-mails. The attacker sends a group of useless emails to harm a victim's operating system or uses an attachment to install malicious code to get access into a victim's system.

Key-Ghost: A device attached to the keyboard which in turn captures everything typed on the keyboard. (Some researchers classified this technique as human-based attacks).

Phishing: Social engineers using technology to present themselves to be from a legitimate organization and usually they use emails (for example from a bank). They may request from victims to confirm their account or to enter their username and password then, they can use these to illegally access the website whenever they want.

Spam- Chain Letters and Hoaxes: This technique depends on what the social engineer wants to spread. It does not cause permanent damage, but can result in a loss of productivity by targeting resources of a valuable network.

Spyware and malicious Software: This kind of malicious software is used to steal personal information such as username and password and theft of credit cards by using key-logger.

Popup Windows: Counterfeit windows used by hackers asking users to re-enter their usernames and passwords after notifying them that the internet connection has dropped out. If the user responds to this false window, then his details can be redirected to the hacker.

Trojan horse: An attachment sends by email to deploy a warm or a virus through the entire network. This can be done when the attacker sends this attachment to a certain unsuspecting user, then he opens it. Examples for these attachments are "I Love You" and "Anna Kournikova".

Websites: Websites can be used on a large scale of social engineers. For example, they may give victims promises for nothing and request them to register in a certain site; usually some victims use the same user name and password in many sites. This allows hackers to try the username and password that they have procured to get access for example, to the target account of their victim.