CHAPTER IV

RESEARCH RESULTS

4.0 INTRODUCTION

In this chapter, the social engineering ontology is an ongoing process to compile relevant publications related to social engineering from 2001 to 2014 and to develop its taxonomy. All data and social engineering terms that have been reviewed from previous studies will be collected and described in this section. This process of results contains three steps which are, a) Compilation of related publications on social engineering, b) Collection of related terms on social engineering, c) Implementation in Protégé.

4.1 COMPILATION OF RELATED PUBLICATIONS ON SOCIAL ENGINEERING

As mentioned in these study chapters, the social engineering ontology aims to compile related publications on social engineering from selected databases. This study aims to develop a collection of related terms (taxonomy) based on the extraction of publications related on social engineering, in order to facilitate information and knowledge sharing as well as knowledge reuse on social

engineering. In order, to achieve the first objective which is, the compilation of related publications on social engineering, this requires a deep review of previous studies associated with social engineering. The review is going to include the previous study based on objectives of this study.

Throughout the phase of data gathering, and applying to suggested phases proposed by Noy and McGuinness (2000), it is necessary to say that the gathering of data and domain and scope determination are closely connected to each other to bank up an effective search operation.

Table 1 reflects the phase of data gathering considering the keywords that are supposed to be used in the search process. It's important to use a variety of related keywords in different search engines, in try to include all previous studies concerning with this study such as, social engineering and its types, techniques , taxonomy, countermeasures, etc. A major search engine used in the data collection phase is *Google Scholar*. As can be seen from Table 1, most of the studies cover social engineering categories in detail such as, its fundamentals, the most used techniques, types of attacks, threats and awareness including employees training programs.

TABLE 1: Publications on Social Engineering

No	Keywords used	Search engines/ databases used	Citation	Category	Sub-category
1	Social Engineering	Google Scholar	Granger (2001). "*Social Engineering Fundamentals*". Retrieved on 7 March 2014, from http://www.cwu.edu/~tiddr/Courses/Archive/ACCT565/WebQuests/04SocialEngineering/04SocialEngineeringWebQuest.pdf	Social Engineering	Types of Social Engineering
2	Kinds of Social Engineering.	Google Scholar	Guenther (2001). "*Social Engineering Security Awareness Series*". Retrieved on 18 March 2014, from http://www.iwar.org.uk/comsec/resources/security-awareness/social-engineering-generic.pdf	Social Engineering	Awareness
3	Social Engineering Tactics	Google Scholar	Allen (2006). "*Social Engineering A Means To Violate A computer system*". Retrieved on 18 March 2014, from https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529	Social Engineering	Social Engineering Tactics
4	Social Engineering countermeasures	Google Scholar	Robert et al (2011). Social Engineering "*The Neglected Human Factor for Information Security Management*". Retrieved on 7 May 2014, from http://www.unm.edu/~xinluo/papers/IRMJ2011.pdf	Social Engineering	Techniques and Countermeasures
5	Taxonomy of Social Engineering	Google Scholar	Marcus Nohlberg (2008). "*Securing Information Assets-Understanding, Measuring and Protecting against Social Engineering Attacks*". Retrieved on 7 May 2014, from http://privat.bahnhof.se/wb810999/Nohlberg_Thesis.pdf	Social Engineering	S.E attacks

TABLE 1 (Continued)

No	Keywords used	Search engines/ databases used	Citation	Category	Sub-category
6	Taxonomy of Social Engineering	Google Scholar	Stergiou (2013). "*Social Engineering and Influence*". Retrieved on 7 May 2014, from http://pure.ltu.se/portal/files/43754945/LTU-EX-2013-43692742.pdf	Social Engineering	Influences
7	Social Engineering Techniques	Google Scholar	Hasan, et.al (2010). "*Social Engineering Techniques For Persuasion*". Retrieved on 7 May 2014, from http://airccse.org/journal/graphhoc/papers/0610jgraph2.pdf	Social Engineering	Techniques
8	Social Engineering Terms	Google Scholar	Alan and Roderic (2006) "*Social Engineering and Crime Prevention in Cyberspace*". Retrieved on 6 July 2014, from http://eprints.qut.edu.au/7526/1/7526.pdf	Social Engineering	Terms
9	Social Engineering Terms	Google Scholar	Lech Janczewski and Lingyan Fu (2010) " *Social Engineering-Based Attacks: Model and New Zealand Perspective*". Retrieved on 6 July 2014, from http://www.proceedings2010.imcsit.org/pliks/36.pdf	Social Engineering	Terms
10	Social Engineering Human-Based	Google Scholar	Gupta and Agrawal (2012). " *A Survey On Social Engineering And The Art Of Deception*". Retrieved on 7 May 2014, from http://ijiet.com/wp-content/uploads/2012/08/5.pdf	Social Engineering	Human-based
11	Social Engineering Terms	Google Scholar	Ivaturi and Janczewski (2012)."*A Typology Of Social Engineering Attacks – An Information Science Perspective*" Retrieved on 6 July 2014, from http://www.pacis-net.org/file/2012/PACIS2012-066.pdf	Social Engineering	Terms

TABLE 1 (Continued)

No	Keywords used	Search engines/ databases used	Citation	Category	Sub-category
12	Social Engineering	Google Scholar	Maan and Sharma (2012). "*Social Engineering: A Partial Technical Attack*" Retrieved on 8 July 2014, from http://ijcsi.org/papers/IJCSI-9-2-3-557-559.pdf	Social Engineering	Terms
13	Social Engineering Taxonomy	Google Scholar	Greitzer et al (2014). "*Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits* " Retrieved on 8 July 2014, from http://www.ieee-security.org/TC/SPW2014/papers/5103a236.PDF	Social Engineering	Taxonomy
14	Social Engineering Attack Methods	Google Scholar	Irani et al (2010) "*Reverse Social Engineering Attacks in Online Social Networks*" Retrieved on 10 July 2014, from https://www.iseclab.org/papers/irani_dimva.pdf	Social Engineering	Methods
15	Social Engineering	Google Scholar	Gulati (2003)."*GIAC Security Essential (GSEC) Certification Practical Assignment*". Retrieved on 17 March 2014, from http://123seminarsonly.com/Seminar-Reports/021/55172071-The-Threat-of-Social-Engineering-and-Your-Defense-Against-It.pdf	Social Engineering	Types of Social Engineering
16	Social Engineering Attack Methods	Google Scholar	Spinapolice (2011) "*Mitigating the Risk of Social Engineering Attacks*" Retrieved on 10 July 2014, from https://ritdml.rit.edu/bitstream/handle/1850/14666/MSpinapoliceThesis11-15-2011.pdf?sequence=1	Social Engineering	Methods
17	Social Engineering	Google Scholar	Kee (2008) "*Social Engineering: Manipulating the source*" Retrieved on 10 July 2014, from http://www.sans.org/reading-room/whitepapers/engineering/social-engineering-manipulating-source-32914	Social Engineering	Social Engineering

TABLE 1 (Continued)

No	Keywords used	Search engines/ databases used	Citation	Category	Sub-category
18	Social Engineering	Google Scholar	Mandy (2005) " *Social Engineering: Information Bandits*" Retrieved on 10 July 2014, from http://www.giac.org/paper/gsec/4202/social-engineering-information-bandits/106723	Social Engineering	Social Engineering
19	Social Engineering	Google Scholar	Gragg (2002) " *A Multi-Level Defense Against Social Engineering* " Retrieved on 10 July 2014, from http://www.sans.org/reading-room/whitepapers/engineering/multi-level-defense-social-engineering-920	Social Engineering	Social Engineering
20	Social Engineering	Google Scholar	Lieu (2002). " *Social Engineering – Attacking the Weakest Link* " Retrieved on 10 July 2014, from http://www.giac.org/paper/gsec/2082/social-engineering-attacking-weakest-link/103563	Social Engineering	Social Engineering
21	Social Engineering Types	Google Scholar	Heary (2009)."*Top 5 Social Engineering Exploit Techniques*". Retrieved on 18 March 2014, from http://www.pcworld.com/article/182180/top_5_social_engineering_exploit_techniques.html	Social Engineering	Exploit Techniques
22	Social Engineering	Google Scholar	Chan (2006) " *Social Engineering*" Retrieved on 10 July 2014, from http://uwcisa.uwaterloo.ca/Biblio2/Topic/Olivia_Chan_Social_Engineering.pdf	Social Engineering	Social Engineering
23	Social Engineering Taxonomy	Google Scholar	Cheung (2012) "*Social engineering*" Retrieved on 14 July 2014, from http://uwcisa.uwaterloo.ca/Biblio2/Topic/ACC626%20Social%20Engineering%20A%20Cheung.pdf	Social Engineering	Social Engineering Types

TABLE 1 (Continued)

No	Keywords used	Search engines/ databases used	Citation	Category	Sub-category
24	Human-based Social Engineering Techniques	Google Scholar	Algarni and Xe (2013). " *Social Engineering in Social Networking Sites: Phase-Based and Source-Based Models*" Retrieved on 15 July 2014, from http://www.ijeeee.org/Papers/278-A0046.pdf	Social Engineering	Models
25	Human-based Social Engineering Techniques	Google Scholar	Arief and Besnard (2003) " *Technical and Human Issues in Computer-Based Systems Security* " Retrieved on 15 July 2014, from http://homepages.cs.ncl.ac.uk/budi.arief/home.formal/Papers/TR790.pdf	Social Engineering	Technical and Human Issues
26	Social Engineering Tactics	Google Scholar	Whitaker (2009)."*Top 10 Social Engineering Tactics*". Retrieved on 18 March 2014, from http://www.informit.com/articles/printerfriendly/1350956	Social Engineering	Social Engineering Tactics
27	Social Engineering	Google Scholar	Heikkinen (2006) "*Social engineering in the world of emerging communication technologies*" Retrieved on 15 July 2014, from http://www.cs.tut.fi/~sheikki/docs/WWRF-Heikkinen-SocEng.pdf	Social Engineering	Social Engineering
28	Social Engineering Taxonomy	Google Scholar	Twitchell (2009). "*Social Engineering and its Countermeasures*". Retrieved on 6 May 2014, from http://www.igi-global.com/chapter/social-engineering-its-countermeasures/21344	Social Engineering	Taxonomy

TABLE 1 (Continued)

No	Keywords used	Search engines/ databases used	Citation	Category	Sub-category
29	Social Engineering Types	Google Scholar	Buetler (2009) " *Social engineering test cases*" Retrieved on 16 July 2014, from http://www.csnc.ch/misc/files/publications/Social_Engineering_V2.0.pdf	Social Engineering	Social Engineering
30	Social Engineering Attack Types	Google Scholar	Tovstukha and Laaneots (2013) " *Prevention Strategies For Social Engineering*" Retrieved on 16 July 2014, from https://courses.cs.ut.ee/MTAT.03.246/2013_spring/uploads/Main/essay07.pdf	Social Engineering	Social Engineering
31	Social Engineering Attack Types	Google Scholar	Cazier and Botelho (2007). " *Social Engineering's Threat to Public Privacy*" Retrieved on 16 July 2014, from http://www.isy.vcu.edu/~gdhillon/Old2/secconf/secconf07/PDFs/51.pdf	Social Engineering	Social Engineering Threats

Despite the scarcity of publications on social engineering, however, one of the research process constraints was that some researches need a paid membership to be able to read and download information. However, in the end, that was not an obstacle to collect comprehensive articles on social engineering categories and subcategory, because the same publications can be obtained using other's free access sites.

4.2 COLLECTION OF RELATED TERMS (TAXONOMY) ON SOCIAL ENGINEERING

There are different types of classifications of social engineering attacks based on literature review. For example, Guenther (2001) categorized these attacks into human-based and computer-based. This is the most popular classification used out of reviewed related topics. But, some prefer to use analogous terms such as person-to-person instead of human-based and technical-based for the second attack type. Some respect the use of those prospective terms depends on the analysis of the social engineering process, because it requires multiple stages of implementation. Where some of these types' techniques are used in phase of data gathering about victims before attack implementation. For example (dumpster diving, shoulder surfing, mail-out and forensic analysis) are techniques used to gather information as a preliminary phase before social engineering attack is achieved, (Allen, 2006).

Table 2 shows the different techniques used in the two types of social engineering attacks depending on what are listed in literature reviews in Chapter 2. Current literatures discussed and distinguished techniques that need face-to-face

interaction or that implemented via media such as penetrate people by using technology in general.

In human-based techniques, Table 2 reflects more than one similarity through reviewed studies such as by Phone, dumpster diving, impersonation, tech support, shoulder surfing, direct approach, important user, social engineering in reverse, on-line social engineering, persuasion, spying and eavesdropping, third-party authorization, piggyback rides, pharming, pretexting and tailgating. On the other side, groups of a unique technique are given by individual researchers. Furthermore, the most common threats presented by these studies are sensitive information of an organization, and stealing user names and passwords and so on. The main countermeasure factors that have resulted until now are awareness and employee training because this kind of attack is primarily aimed at human weaknesses.

Technical-based techniques showed that most of them have similarity based on the previous studies except to three of the techniques such as social (engineer) networking, bogus surveys and key-ghost. Recent findings of technical based threats differed between sabotage network, deploying viruses and malicious, and stealing user IDs and passwords. Whereas, countermeasures of technical-based attacks also focus on awareness, in addition to other security mechanisms that are applied in an organization as implementing security baseline requirements.

TABLE 2: Related Terms (Taxonomy) on Social Engineering

Type of Social Engineering Attack	Type of Technique	Threats	Countermeasures	References
Human-based	**By Phone**	Sensitive information	Train employees	(Granger 2001) , (Nohlberg, 2008) , (Gupta and Agrawal, 2012) , (Alan and Roderic, 2006) , (Maan and Sharma, 2012), (Kee, 2008), (Gragg, 2002) , (Chan D Lieu, 2002), (Buetler, 2009), (Cazier and Botelho, 2007).
	Dumpster Diving	Organization data security.	Keep all trash in secured, monitored areas.	(Granger, 2001), (Gulati, 2003), (Guenther, 2001), (Allen, 2006), (Twitchell, 2009) , (Luo et.al, 2011), (Nohlberg, 2008), (Gupta and Agrawal, 2012) , (Hasan, et.al, 2010) , (Alan and Roderic, 2006) , (Janczewski and Lingyan Fu, 2010) , (Spinapolice, 2011) , (Kee, 2008) , (Lieu, 2002) , (Chan, 2006) , (Cheung 2012) , (Algarni and Xe 2013) , (Buetler, 2009) , (Tovstukha and Laaneots, 2013) , (Cazier and Botelho, 2007).

TABLE 2 (Continued)

Type of Social Engineering Attack	Type of Technique	Threats	Countermeasures	References
Human-based	**On-Line Social Engineering**	Harvest passwords	Don't repeat the use of one simple password	(Granger, 2001) , (Luo et.al, 2011) , (Gupta and Agrawal, 2012) , (Janczewski and Lingyan Fu, 2010)**.**
	Persuasion	Sensitive Information	Require all guests to be escorted.	(Granger, 2001) , (Gupta and Agrawal, 2012) , (Kee, 2008) , (Algarni and Xe 2013) , (Heikkinen, 2006) , (Cazier and Botelho, 2007)**.**
	Impersonation (Quid Pro Quo)	Passwords	Don't type in passwords with anyone else looking.	(Granger, 2001), (Gulati 2003), (Guenther, 2001), (Twitchell, 2009) , (Gupta and Agrawal, 2012), (Janczewski and Lingyan Fu, 2010) , (Greitzer et.al, 2014) , (Spinapolice, 2011) , (Gragg, 2002), (Chan, 2006), (Cheung 2012), (Arief and Besnard, 2003) , (Heikkinen, 2006) , (Buetler, 2009) , (Tovstukha and Laaneots, 2013).

TABLE 2 (Continued)

Type of Social Engineering Attack	Type of Technique	Threats	Countermeasures	References
Human-based	**Conformity**	Individual Settings	Shred important and sensitive data.	(Granger, 2001).
	Direct approach	ID and Password	Documented and Security Policy.	(Gulati, 2003), (Whitaker, 2009).
	Spying and Eavesdropping	ID and Password	Training on Security Policy	(Gulati, 2003), (Nohlberg, 2008), (Alan and Roderic, 2006), (Mandy, 2005).
	Questionnaire	Sensitive Information	Awareness	(Janczewski and Lingyan Fu, 2010).
	Tech Support	Access permission - Database	Passwords are never spoken over the phone	(Gulati 2003), (Guenther, 2001), (Whitaker, 2009), (Allen, 2006), (Gupta and Agrawal, 2012), (Alan and Roderic, 2006).
	Support Staff	Valuable information – confidential file	Awareness	(Gulati 2003), (Gupta and Agrawal, 2012).
	The Voice of Authority	Password – Accessing the system	Identity Management policy	(Gulati 2003), (Gupta and Agrawal, 2012), (Gragg, 2002).

TABLE 2 (Continued)

Type of Social Engineering Attack	Type of Technique	Threats	Countermeasures	References
Human-based	**Important User**	Sensitive Information	Awareness & Training	(Guenther, 2001), (Allen, 2006), (Alan and Roderic, 2006).
	Third-party Authorization	Access permission	Caller ID technology	(Guenther, 2001), (Olivia Chan, 2006), (Cheung 2012), (Arief and Besnard, 2003).
	In Person	Sensitive Info	Awareness	(Guenther, 2001) , (Chan, 2006) , (Cheung 2012).
	Shoulder Surfing	Password – Phone-card numbers	Awareness & Training	(Guenther, 2001), (Allen,2006), (Twitchell, 2009) , (Luo et.al, 2011) , (Gupta and Agrawal, 2012) , (Alan and Roderic, 2006) , (Janczewski and Lingyan Fu, 2010), (Greitzer et.al, 2014) , (Spinapolice, 2011) , (Kee, 2008) , (Mandy, 2005) , (Chan, 2006) , (Cheung 2012) , (Algarni and Xe 2013), (Heikkinen, 2006) , (Tovstukha and Laaneots, 2013).
	Familiarity Exploit	Secure area	Training and awareness	(Heary, 2009).
	Creating a hostile situation	Access control- Secure area	Personnel training and awareness programs	(Heary, 2009).

TABLE 2 (Continued)

Type of Social Engineering Attack	Type of Technique	Threats	Countermeasures	References
Human-based	**Gathering and Using Information**	Sensitive Information	Training and awareness	(Heary, 2009).
	Get a Job There	Sensitive Information	Personnel training and awareness programs	(Heary, 2009), (Arief and Besnard, 2003).
	Reading body language	Organization Secrets	Personnel training and awareness programs	(Jamey, 2009).
	Sex Sells	Sensitive Information	Awareness	(Jamey, 2009), (Whitaker, 2009).
	Social Engineering in Reverse	Sabotage a network - Stealing confidential data	Training and Awareness	(Whitaker, 2009), (Allen,2006), (Twitchell, 2009) , (Nohlberg, 2008) , (Stergiou, 2013) , (Gupta and Agrawal, 2012) , (Hasan, et.al, 2010) , (Alan and Roderic, 2006) , (Janczewski and Lingyan Fu, 2010) , (Greitzer et.al, 2014), (Irani et.al, 2010) , (Spinapolice, 2011) , (Kee, 2008) , (Mandy, 2005) , (Gragg, 2002) , (Algarni and Xe 2013) , (Heikkinen, 2006) , (Buetler, 2009).
	Piggyback Rides	Bypassing physical security control	Awareness – follow security policy	(Whitaker, 2009) , (Masan, et.al, 2010), (Maan and Sharma, 2012).
	Personal stake- Phishing	Bank account or password	Training and awareness	(Andrew Whitaker, 2009) , (Budi Arief and Denis Besnard, 2003).

TABLE 2 (Continued)

Type of Social Engineering Attack	Type of Technique	Threats	Countermeasures	References
Human-based	**Neuro-linguistic programming**	Company's secrets	Training and awareness	(Andrew, 2009).
	Get smashed	Trade secrets – passwords - get into a building	Training and awareness	(Andrew, 2009).
	Mail-outs	Individual / organization information	Education/ Awareness	(Allen, 2006).
	Forensic analysis	Individual / organization information	Education/ Awareness	(Allen, 2006).
	Helpless user	Organization's systems	Physical security	(Allen, 2006), (Alan and Roderic, 2006).
	Asking for Favors	Passwords	Training and awareness	(Twitchell, 2009), (Gragg, 2002).
	Cold Calling	Unauthorized access	system level security- awareness	(Twitchell, 2009).
	Contriving Situations	Data files	Educate/Awareness	(Twitchell, 2009).
	Giving out free software – Reward	Organization's systems	Security policy	(Twitchell, 2009), (Arief and Besnard, 2003).
	Photography	Trade Secrets	Security policy	(Allen, 2006).
	Pharming	ID and Password	Training on Security Policy	(Twitchell, 2009), (Spinapolice, 2011), (Alan and Roderic, 2006).
	Pretexting	Sensitive Information	Awareness	(Twitchell, 2009), (Luo et.al, 2011) , (Nohlberg, 2008), (Stergiou, 2013) , (Greitzer et.al, 2014) , (Spinapolice, 2011), (Tovstukha and Laaneots, 2013).

TABLE 2 (Continued)

Type of Social Engineering Attack	Type of Technique	Threats	Countermeasures	References
Human-based	**Reconnaissance**	Physical Access	Physical security	(Twitchell, 2009).
	Simple Requests	Individual / organization information	Education/ Awareness	(Twitchell, 2009).
	Surveys	Sensitive Information	Awareness	(Twitchell, 2009) , (Heikkinen, 2006).
	Tailgating	Bypassing physical security control	Awareness – follow security policy	(Twitchell, 2009) , (Maan and Sharma, 2012), (Mandy, 2005) , (Heikkinen, 2006) , (Tovstukha and Laaneots, 2013).
	Theft	Confidential Information	Awareness	(Twitchell, 2009) , (Nohlberg, 2008) , (Mandy, 2005).
	Fear	Sensitive Information	Awareness/ Training	(Stergiou, 2013), (Hasan, et.al, 2010).
	Diffusion of responsibilities	Sensitive Information	Awareness/ Training	(Stergiou, 2013).
	Chance of ingratiation	Sensitive Information	Awareness/ Training	(Stergiou, 2013).
	Guilt	Sensitive Information	Awareness/ Training	(Stergiou, 2013).
	Overloading	Sensitive Information	Awareness/ Training	(Stergiou, 2013).

TABLE 2 (Continued)

Type of Social Engineering Attack	Type of Technique	Threats	Countermeasures	References
Technical-based	**Trojan horse**	Workstations - Network	Physical technical solutions to eliminate or reduce unauthorized physical access	(Gulati, 2003), (Twitchell, 2009), (Stergiou, 2013), (Greitzer et.al, 2014), (Spinapolice, 2011) , (Chan, 2006) , (Arief and Besnard, 2003).
	The popup window	ID – Password - System	Operating procedures to limit vulnerabilities.	(Gulati, 2003), (Guenther, 2001), (Stergiou, 2013), (Alan and Roderic, 2006), (Janczewski and Lingyan Fu, 2010), (Lvaturi and Janczewski, 2012), (Maan and Sharma, 2012).
	Fake Mail and Attachments	Viruses– Worms- clog mail systems – Malicious code	Always update scanners - Limit data leakage	(Guenther, 2001), (Allen,2006) , (Nohlberg, 2008) , (Hasan, et.al, 2010) , (Janczewski and Lingyan Fu, 2010) , (Maan and Sharma, 2012) , (Kee, 2008) , (Lieu, 2002) , (Cheung 2012) , (Heikkinen, 2006) , (Buetler, 2009).
	Spam, Chain Letters and Hoaxes	Loss of productivity – Network resources	Always update scanners	(Guenther, 2001), (Masan, et.al, 2010), (Lvaturi and Janczewski, 2012), (Algarni and Xe, 2013).

TABLE 2 (Continued)

Type of Social Engineering Attack	Type of Technique	Threats	Countermeasures	References
Technical-based	**Websites**	E-mail address and password	Training and Awareness	(Guenther, 2001), (Allen,2006) , (Nohlberg, 2008) , (Lvaturi and Janczewski, 2012) , (Greitzer et al, 2014) , (Gragg, 2002) , (Chan, 2006) , (Cheung 2012) , (Heikkinen, 2006) , (Cazier and Botelho, 2007).
	Social (Engineer) Networking	Sensitive Information	Awareness	(Whitaker, 2009).
	(Catch Me a Vish) SMS cell phone vishing	Credit card	Awareness	(Whitaker, 2009), (Alan and Roderic, 2006), (Lieu, 2002).
	Bogus Surveys	E-mails	Awareness	(Alan and Roderic, 2006).
	KeyGhost	ID- Passwords	Awareness	(Chan, 2006).
	Spyware and Malicious software	Personal Information	Security culture	(Alan and Roderic, 2006), (Janczewski and Lingyan Fu, 2010), (Lvaturi and Janczewski, 2012), (Cheung 2012).

TABLE 2 (Continued)

Type of Social Engineering Attack	Type of Technique	Threats	Countermeasures	References
Technical-based	**Phishing**	Financial / personal information	Security culture	(Allen,2006), (Twitchell, 2009) , (Luo et.al, 2011) , (Nohlberg, 2008) , (Stergiou, 2013) , (Alan and Roderic, 2006) , (Janczewski and Lingyan Fu, 2010), (Lvaturi and Janczewski, 2012) , (Maan and Sharma, 2012) , (Greitzer et.al, 2014) , (Spinapolice, 2011) , (Mandy, 2005) , (Chan, 2006), (Algarni and Xe 2013) , (Heikkinen, 2006) , (Buetler, 2009) , (Tovstukha and Laaneots, 2013) , (Cazier and Botelho, 2007).

4.3 DEVELOPMENT PROCESS OF SOCIAL ENGINEERING TERMS (TAXONOMY)

4.3.1 INTRODUCTION

This section describes the process of developing social engineering taxonomy in terms of terminology analysis and classifies them according to hierarchy relationship. As will be shown here, subclasses that resulted from social engineering main root, as well as other members that have hierarchical relationship inherited of sub-classes.

4.3.2 DEVELOPMENT PROCESS

FIGURE 3: Social Engineering main and sub- classes.

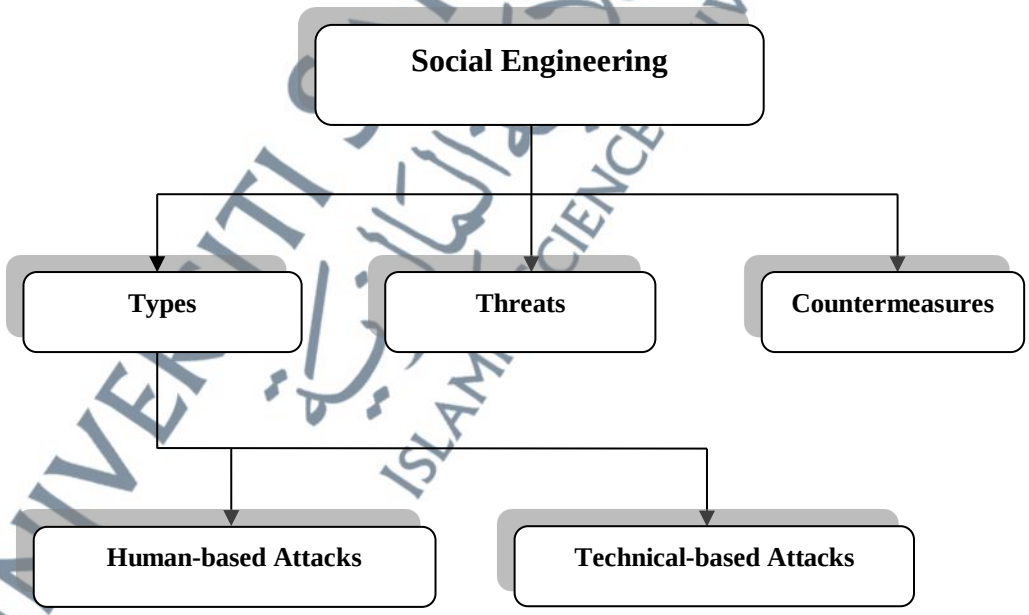


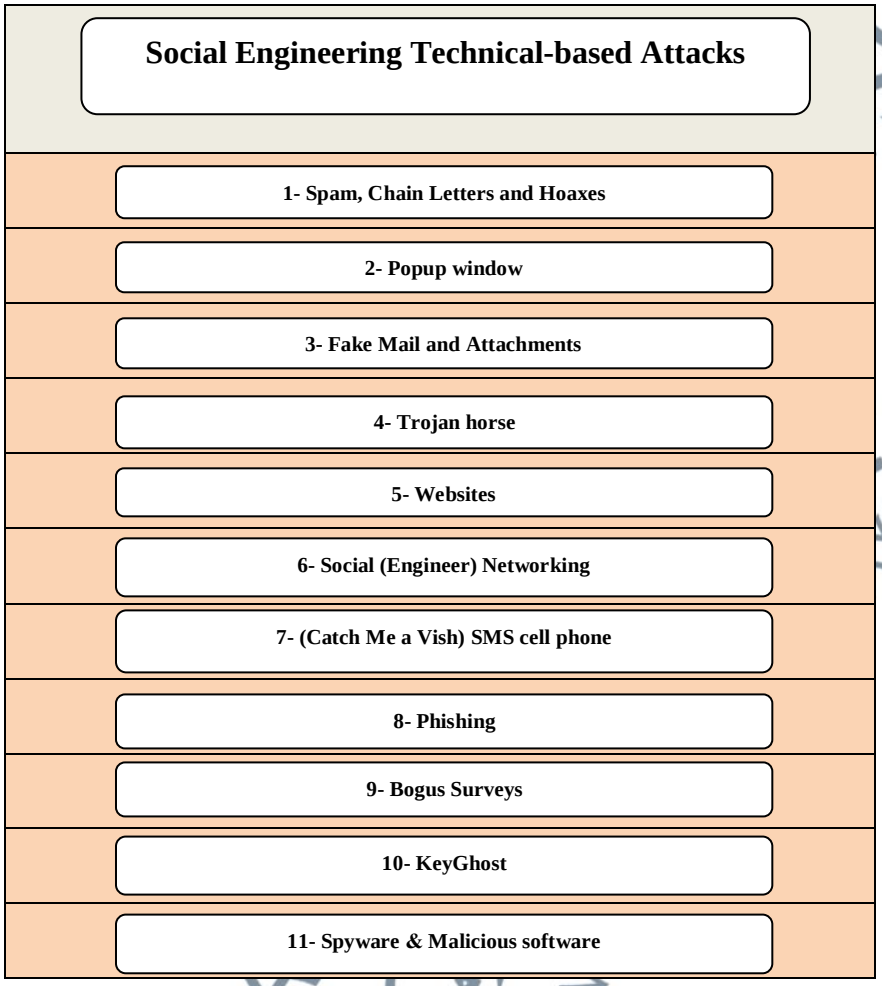
Figure 3 shows the hierarchy of proposed social engineering ontology which is going to be implemented by Protégé software. The main class of this proposed ontology is "Social Engineering" which contains three sub-classes listed under it. These sub-classes are ***a) Types*** of social engineering techniques; ***b) Countermeasures*** to avoid social engineering attacks; and potential ***c) Threats*** that threaten humans, secure area and sensitive information.

Basically, human-based attacks and technical-based attacks are also two sub-classes listed under "Types" sub-class and Social engineering's main root. These two sub-classes, human-based and technical-based, contain many members which reflect the techniques of social engineering attacks which are implemented by social engineers, whether they were using these methods directly to attack the victims or to gather information about them to discover their vulnerabilities, as a preliminary stage before attack implementation.

FIGURE 4: Social Engineering Human-based Taxonomy.

With reference to Figure 4, which is based on the literature review to develop a comprehensive list of terms (taxonomy) of social engineering attacks, it became clear that the most techniques are used, with direct communication with the victims. While on the other side there is a group of techniques used to manipulate the victim via media. The list of human-based key terms consists of by phone, dumpster diving, on-line social engineering, persuasion, impersonation, conformity, questionnaire, spying and eavesdropping, tech support, support staff, the voice of authority, important user, third-party authorization, in person, shoulder surfing, familiarity exploit, creating a hostile situation, gather & use Information, get a job there, reading body language, sex sells, reverse social engineering, piggyback rides, personal stake- phishing, NLP, get smashed, mail-outs, forensic analysis, helpless user, asking for favors, cold calling, contriving situations, free software – reward, photography, pharming, pretesting, reconnaissance, simple requests, surveys, tailgating, theft, fear, diffusion of responsibilities, chance of ingratiation, guilt, and overloading.

FIGURE 5: Social Engineering Technical-based Taxonomy.



In contrast to person-to person interaction, Figure 5, shows manipulation via media represented by technical-based attack which consists of key terms which are, spam, chain letters and hoaxes, popup window, fake mail and attachments, trojan horse, websites, social (engineer) networking, (Catch Me a Vish) SMS cell phone, phishing, bogus surveys, keyghost, and spyware & malicious software.

FIGURE 6: Social Engineering Threats.

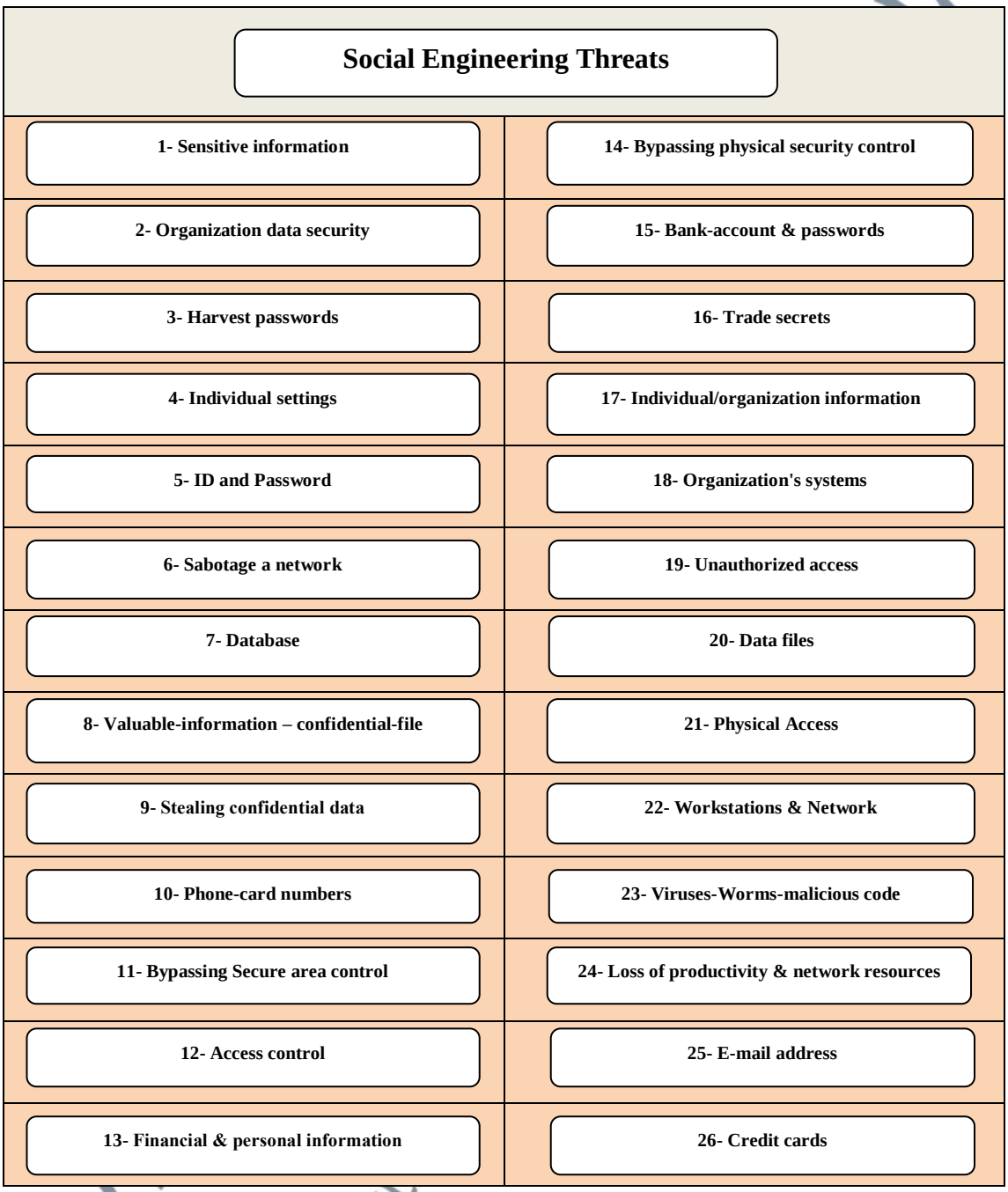
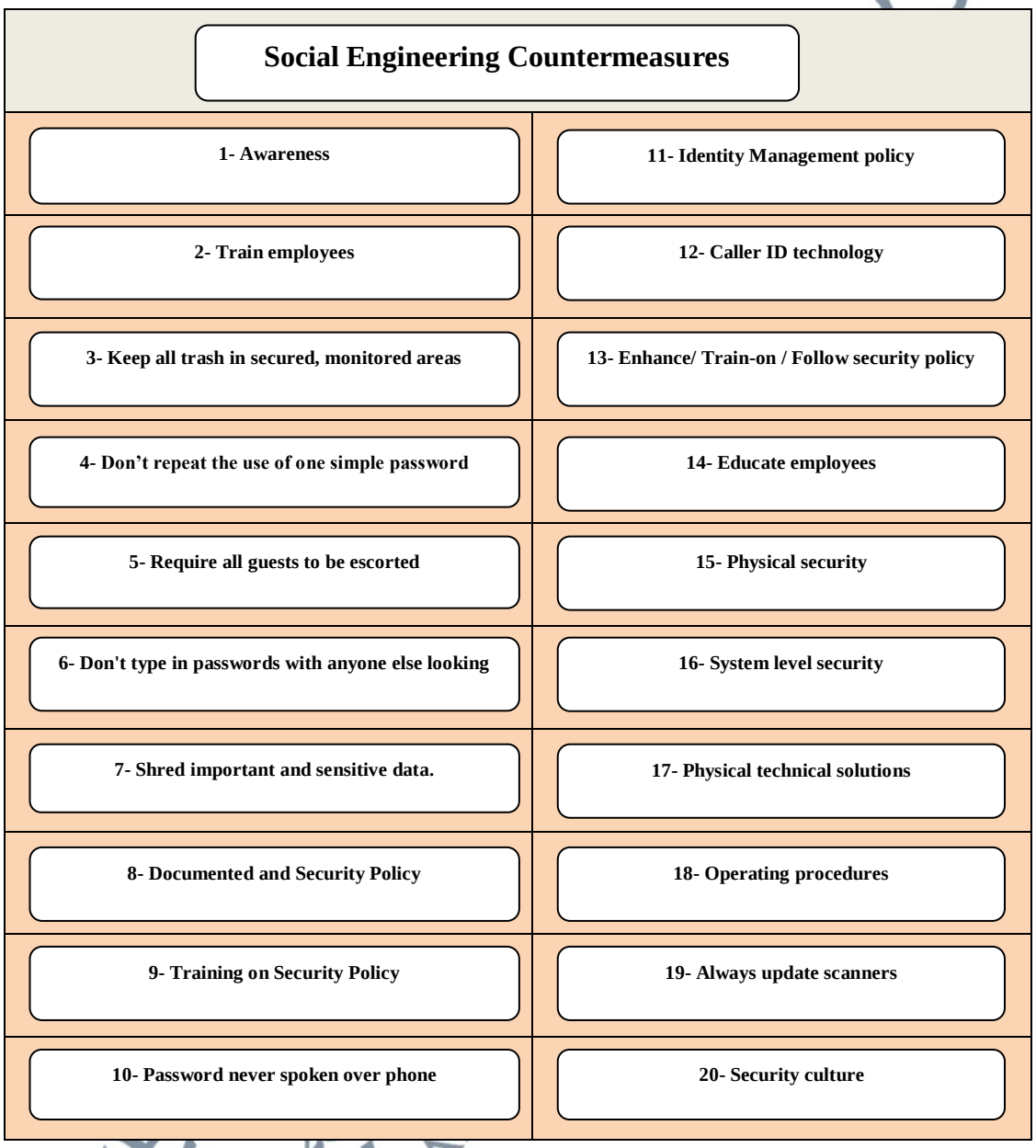


Figure 6 shows the most threatening aspects that are directly or indirectly affected by social engineering attacks. These threats vary depending on the target of social engineers. Targets can be represented by, Sensitive information, Organization

data security, harvest passwords, individual settings, ID and password, access permission, database, valuable-information/ confidential-file, phone-card numbers, bypassing secure area control, access control, sabotaging a network, stealing confidential data, bypassing physical security control, bank-account & passwords, trade secrets, individual/ organization information, organization's systems, unauthorized access, data files, physical access, workstations & network, viruses-worms-malicious code, loss of productivity & network resources, e-mail address, credit cards, and financial & personal-information.

The next figure 7, represents countermeasures that are considered as defense lines against social engineering attacks. As urged in previous studies, avoidance of social engineering threats can be implemented through these methods which are, awareness, training employees, keeping all trash in secured, monitored areas, not repeating the use of one simple password, requiring all guests to be escorted, not typing in passwords with anyone else looking over your shoulder, shredding important and sensitive data, documented and security policy, training on security policy, passwords never being spoken over the phone, identity management policy, caller ID technology, enhance/ train-on / follow security policy, educating employees, physical security, System level security, physical technical solutions, operating procedures, always updating scanners, and security culture.

FIGURE 7: Social Engineering Countermeasures.



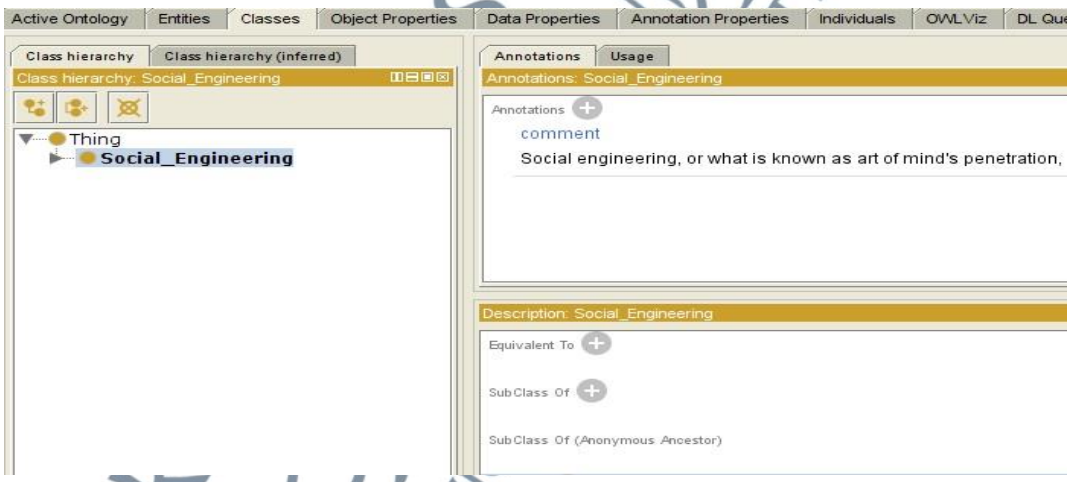
4.4 IMPLEMENTATION IN PROTÉGÉ 4.2

4.4.1 INTRODUCTION

This study used Protégé 4.2 as a tool of developing the ontology. The resulting development process enabled the proposed social engineering ontology to contain tree sub-classes categorized under social engineering main root which is sub-class of OWL: Thing.

4.4.2 IMPLEMENTATION

Figure 8: Top Level Social Engineering Taxonomy.



As it can be seen from the Figure 8, the ***Social_Engineering*** is the main class of implemented ontology. Also Figure 9 shows that, the middle level of social engineering sub-classes which are ***Types*** including (***Human-Based_Attacks*** and ***Technical-Based_Attacks***), ***Countermeasures*** and ***Threats***.

FIGURE 9: Middle Level Social Engineering Taxonomy.

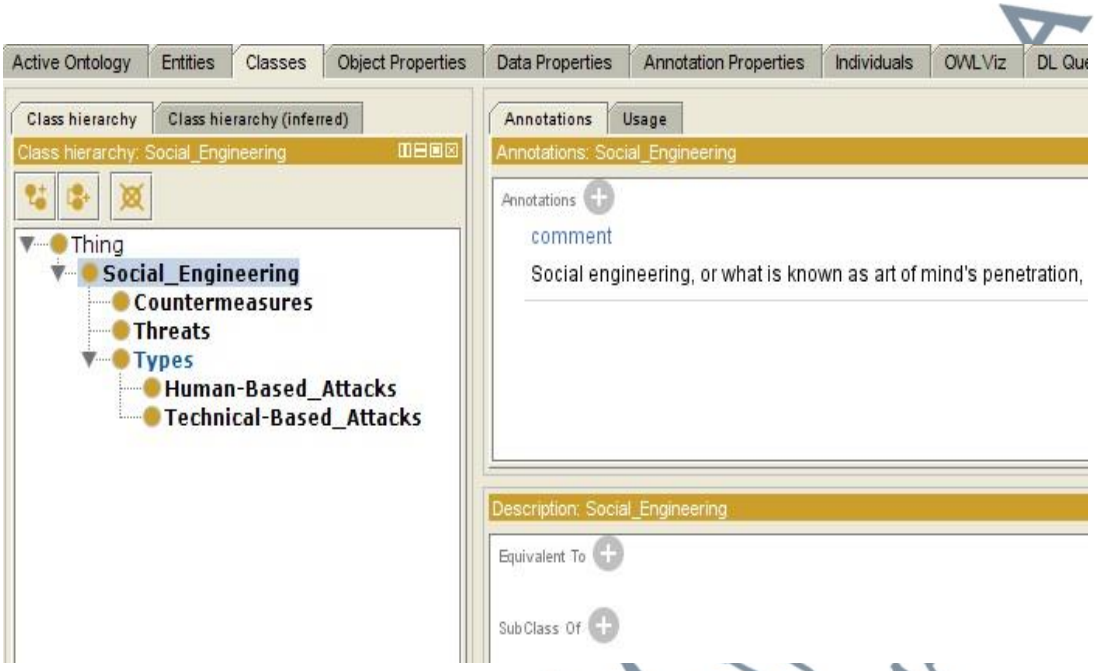
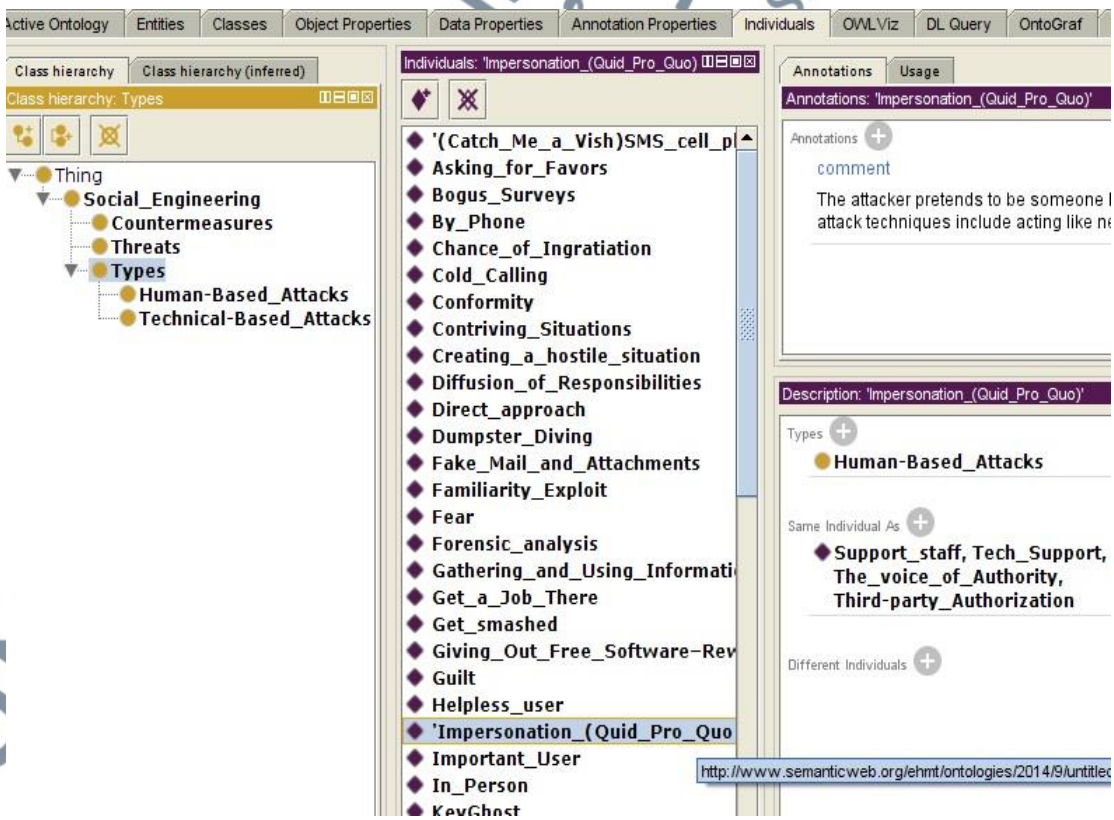


FIGURE 10: Individuals "Facts" of Social Engineering Taxonomy.



Individuals of the sub-class are also individuals of the main class of that sub-class. Figure 10 shows that, all individuals of ***Human-Based_Attacks*** and ***Technical-Based_Attacks*** as they two sub-class of ***Types*** class. Furthermore, the description of any individual is clear if it is 'same individual as' another one or not. For example, the member ***Impersonation*** is the same individual as *Support_staff*, *Tech_Support*, *The_voice_of_Authority*, and *Third-party_Authorization*.

FIGURE 11: Sample of class and its individuals.

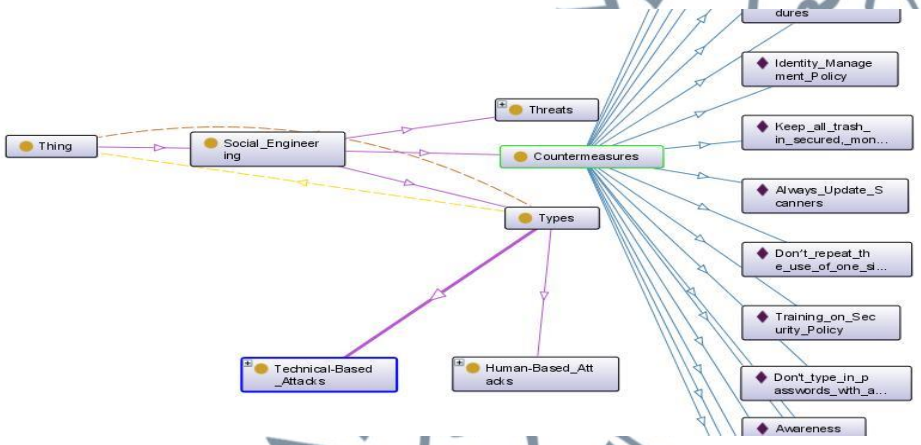


Figure 12: Object property of Social Engineering Taxonomy.

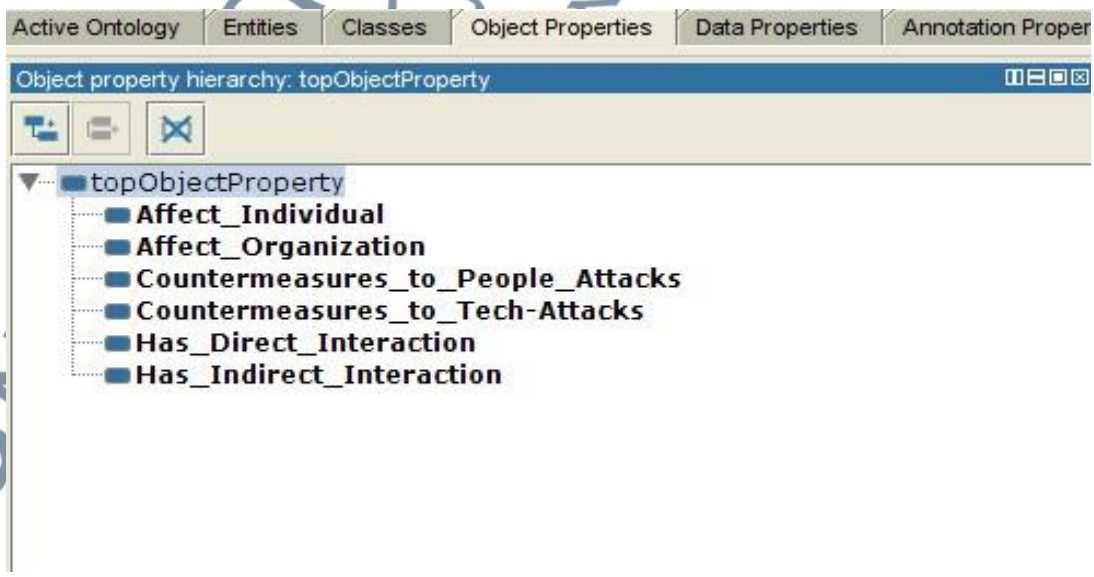


Figure 12 shows that, the list of object property of social engineering taxonomy. These object properties reflect the relationships between individuals of different classes in the ontology. For example, ***Affect_Organization*** represents the relationship between Threat's members and members of social engineering tactics as shown in Figure 13 that, the threat of *Physical Access* affect organization by *Reconnaissance* and *Get-smashed* attacks.

FIGURE 13: Sample of Relationship view.

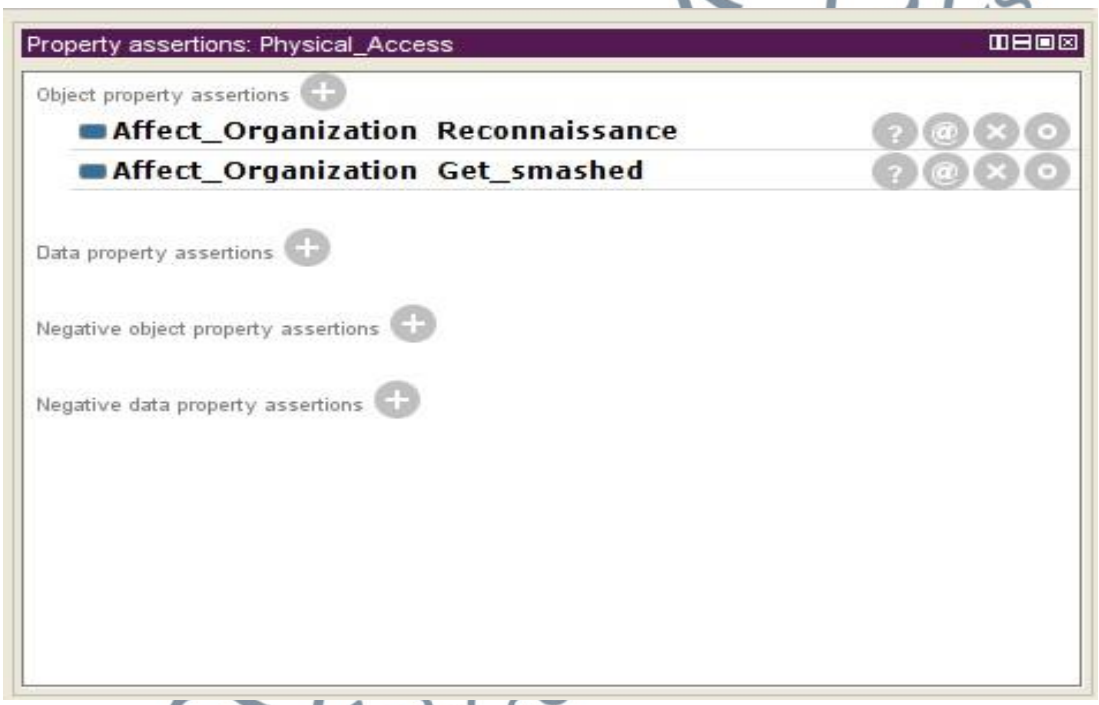
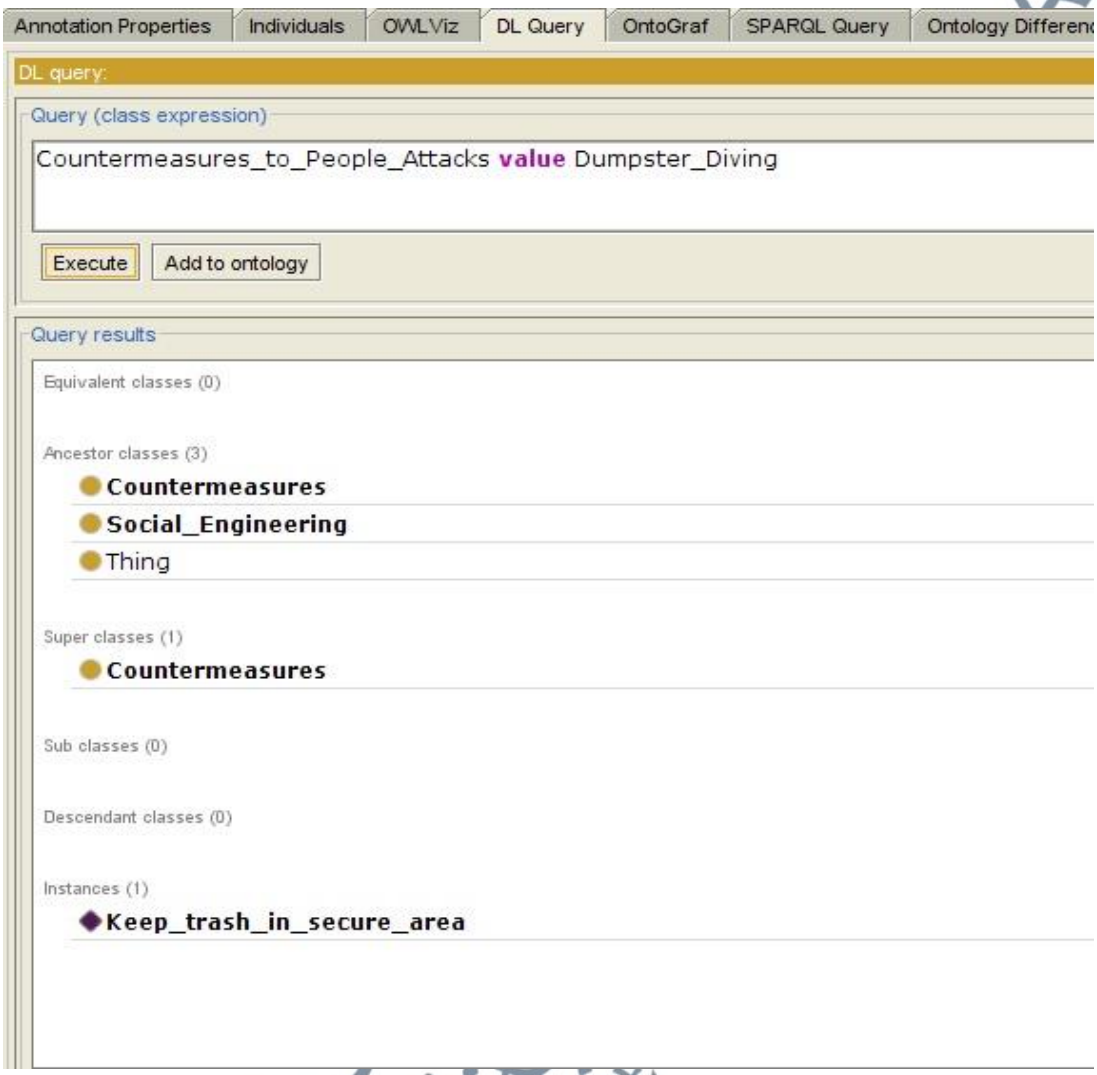


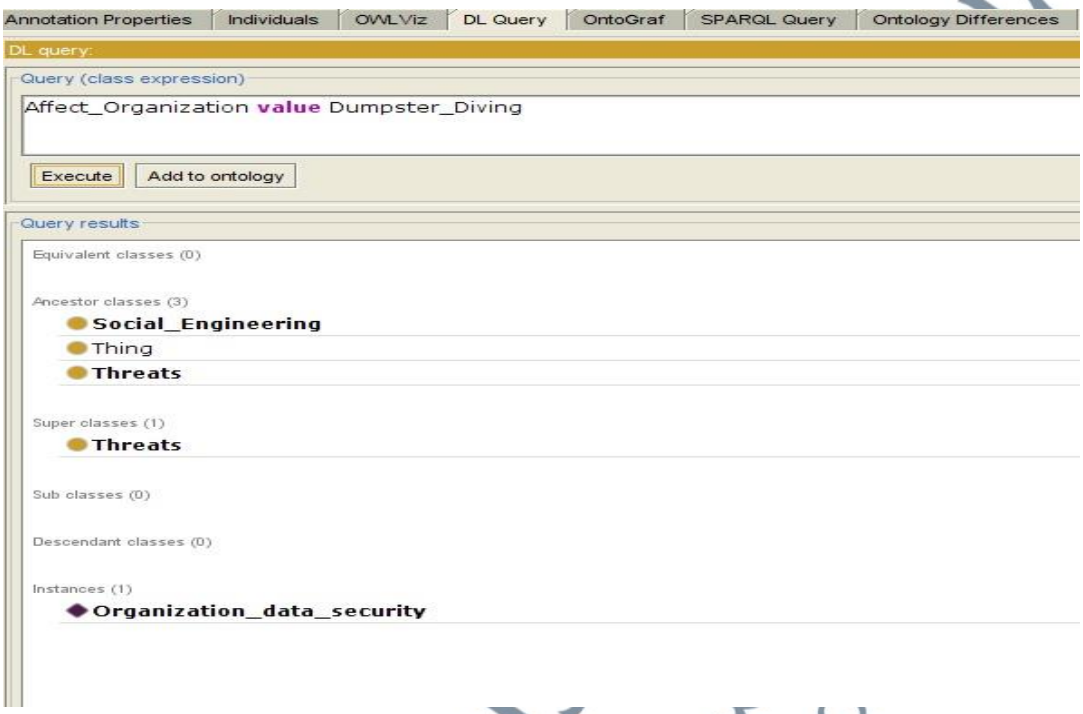
FIGURE 14: Sample of DL Query (1).



Referring to the Figure 14, it shows the result of queries whenever they were given to the DL Query tab. For example, querying about ***countermeasures_to_People_Attacks*** relationship for ***Dumpster_Diving*** instance will result in the command to "*Keep trash in secure and monitored area*".

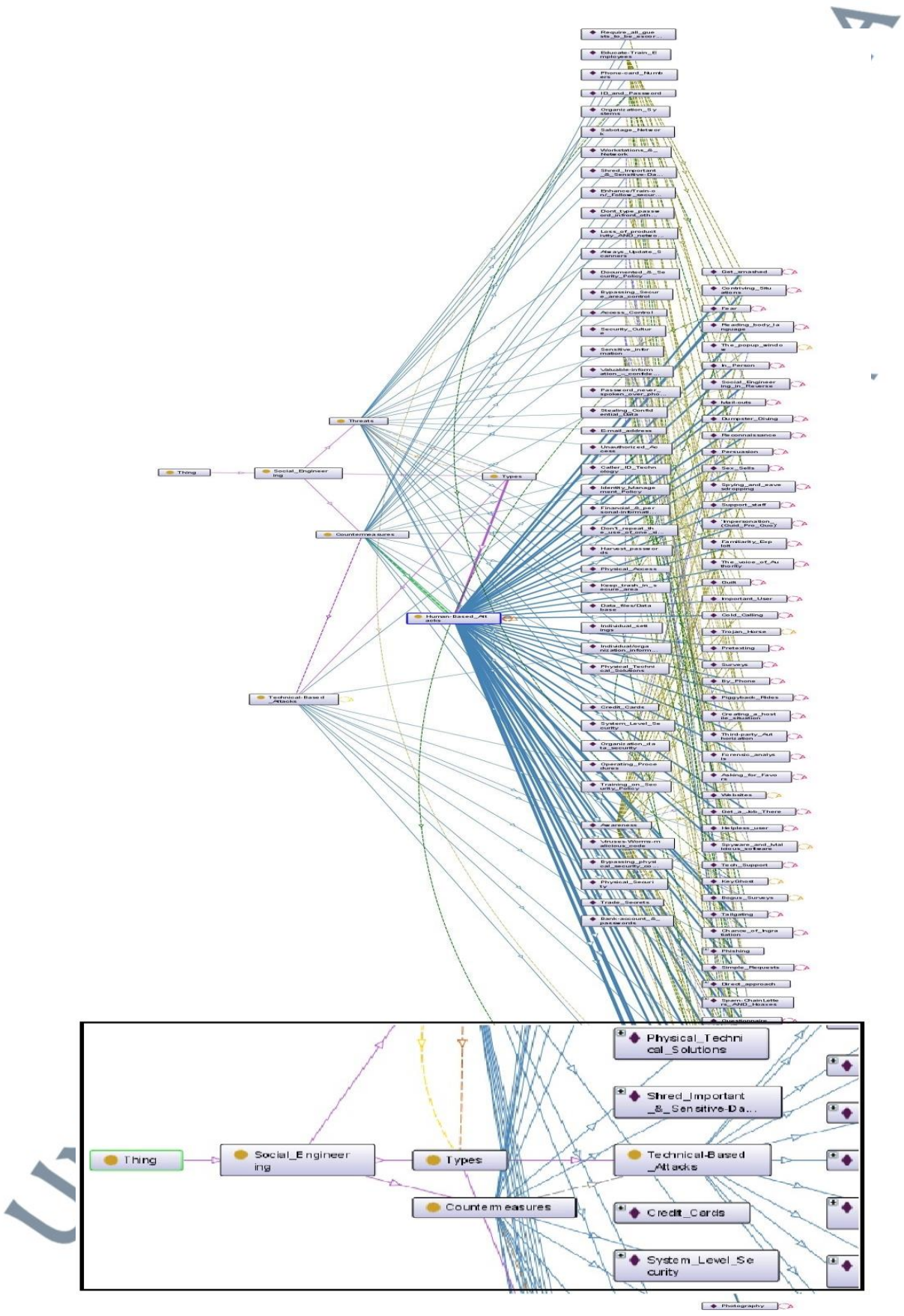
On the other side, querying about same member "***Dumpster_Diving***" with the relationship ***Affect_Organization*** will result the type of threats, which is "*Organization data security*" as shown in the next Figure 15.

FIGURE 15: Sample of DL Query (2).



The next figure (all class hierarchy) for social engineering ontology is shown in Figure 16, which allows us to visualize the whole ontology which includes 3 classes under one social engineering main class. Since the rest of the sub-classes which are 2 sub-classes are categorized under type class.

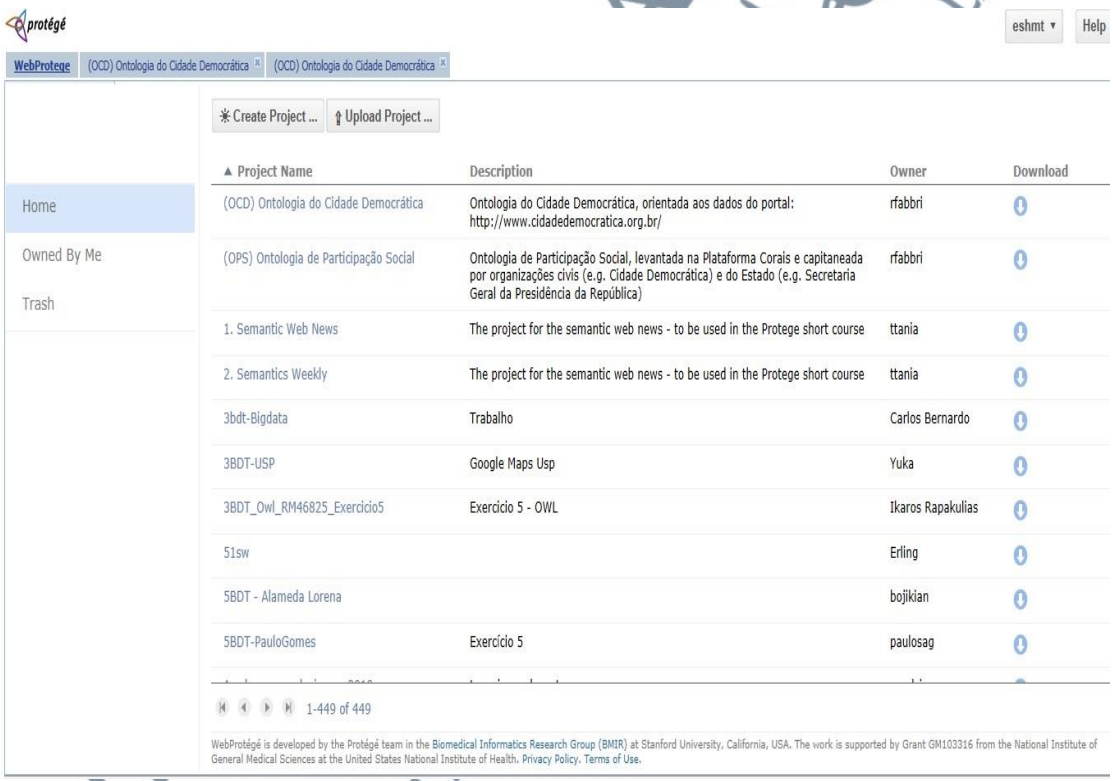
FIGURE 16: Example of Social Engineering class hierarchy.



4.4.3 OWL VISUALIZATION BY WEBPROTÉGÉ

WebProtégé is an open and free tool for creating, managing, analyzing, and visualizing RDF/OWL descriptions. The general information about this online software is given under the methodology in chapter 3. There are various ontologies under the project name in the home page of the WebProtégé software. After the registration step, and a login, creating a new project is the next step to start using Web Protégé (Figure 17).

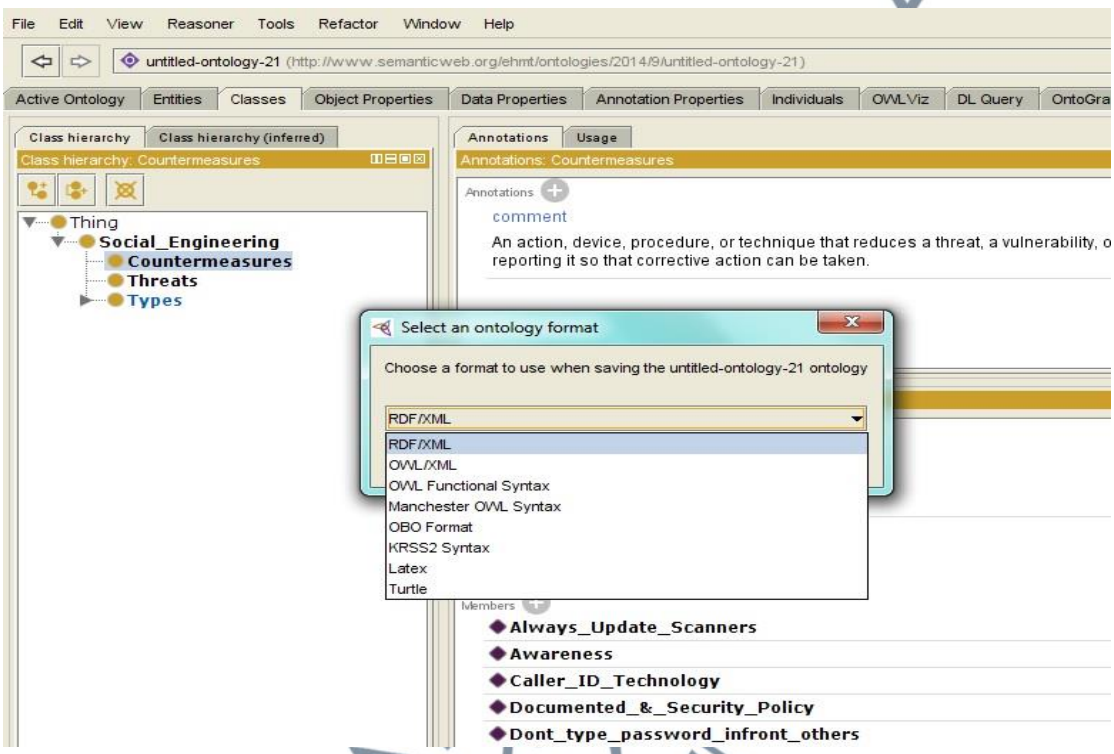
FIGURE 17: WebProtégé home page.



The next step is uploading the ontology that is already created in Protégé. The "Social_Engineering" domain ontology, generated by Protégé, is used and uploaded to the site to visualize the class structure and relations. WebProtégé requires the ontology to be in the RDF/XML format instead of an OWL/XML format. Because the

"Social_Engineering" domain ontology is saved in Protégé with OWL/XML format, it was saved as an RDF/XML format in order to use it under the tool (Figure 18).

FIGURE 18: Selection of an ontology format.



Under the "Home" tab in WebProtégé, the ontology can be uploaded using the "Upload Project" option as shown in Figure 19. Ontology is saved as RDF/XML format is uploaded as "File". The project name is "*Social_Engineering*" and the project description is "Social engineering ontology".

FIGURE 19: WebProtégé uploading ontology.

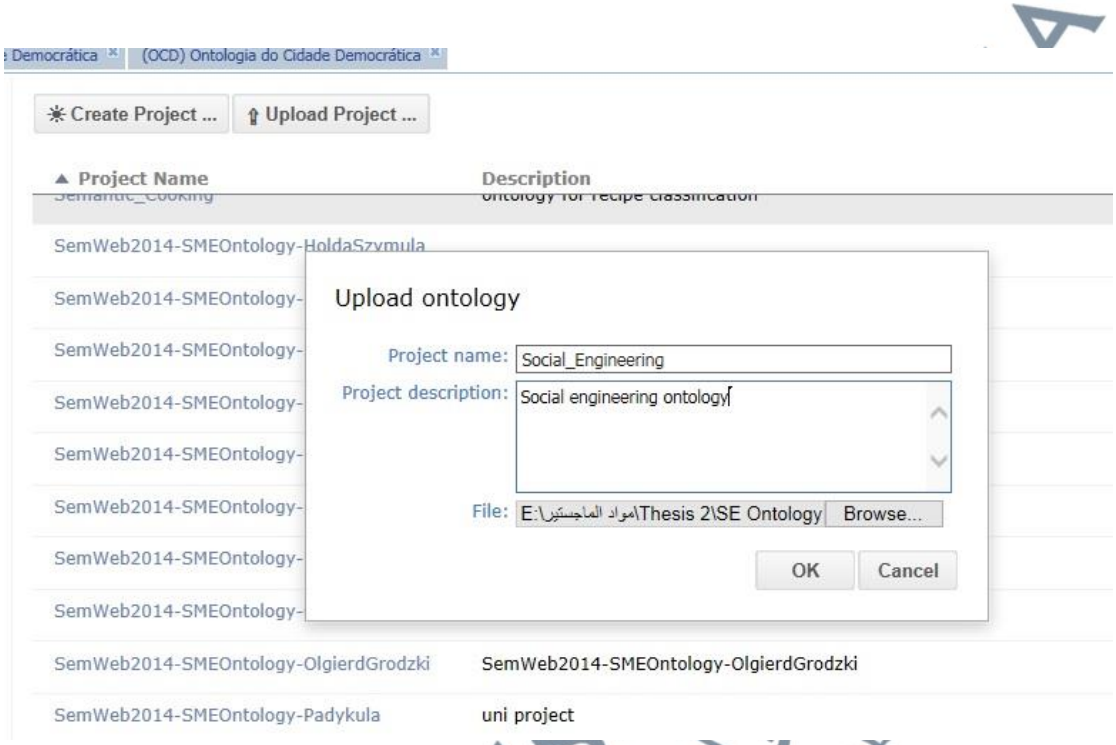


Figure 20 shows that the social engineering ontology has been uploaded successfully to the WebProtege.

FIGURE 20: Ontology uploaded successfully.

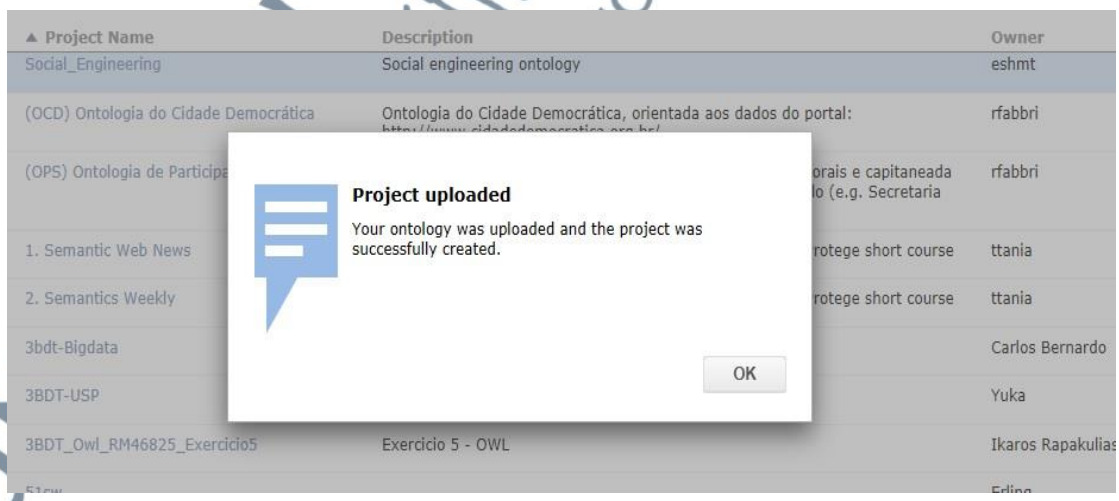


Figure 21 shows the contents of the "*class description for social engineering*" tab, which includes information about the contents, which are listed as "Display Name", "IRI", "Annotations", and "Property". They are all uploaded from the ontology which was created in Protégé.

FIGURE 21: Class description for social engineering ontology.

After the uploading process, the domain ontology is ready to use in *WebProtege*. The general view looks like Protégé as it is displayed in Figure 22. "Classes", "Properties", "Individuals", "Changes By Entity", "Project Dashboard" tabs are located on the left side of this figure.

FIGURE 22: General view after uploading ontology.

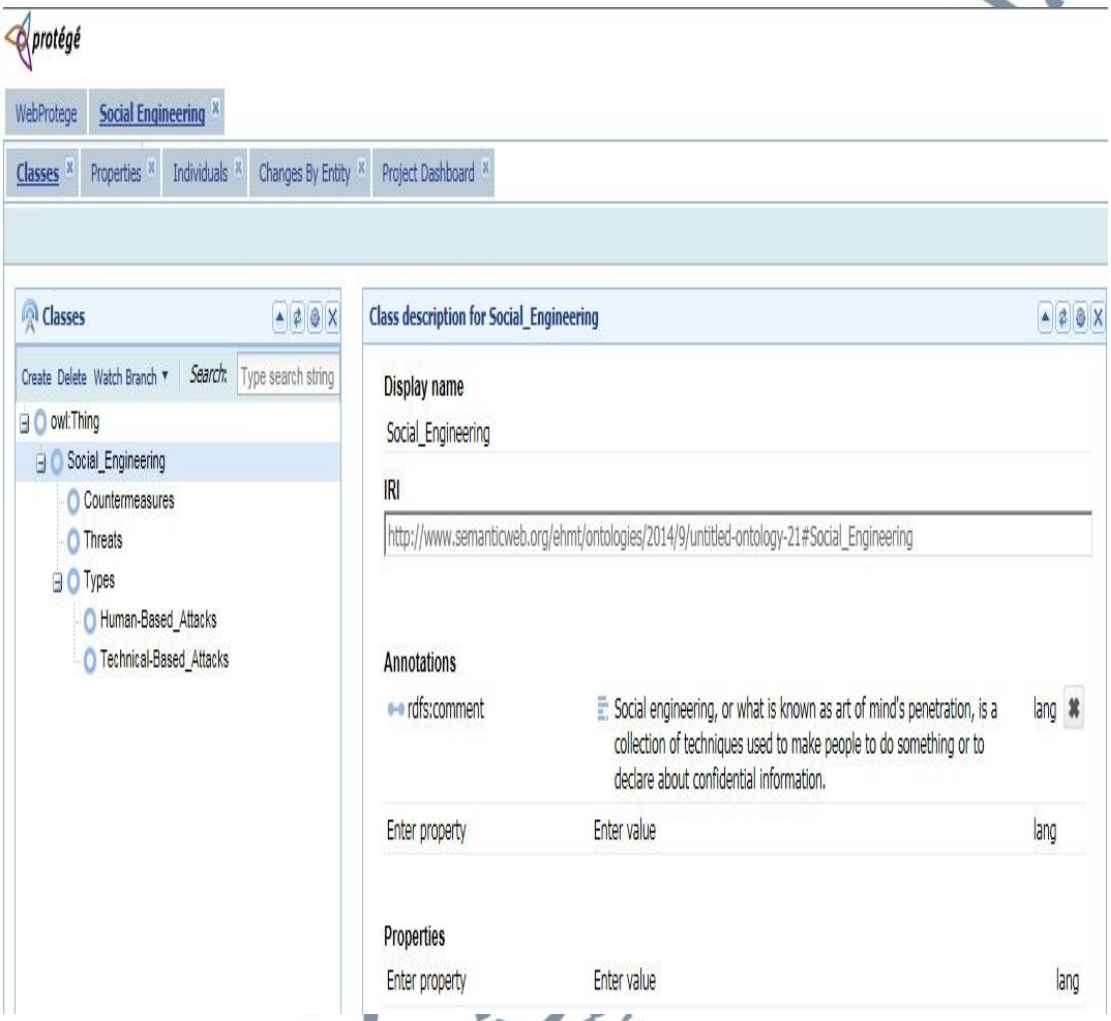
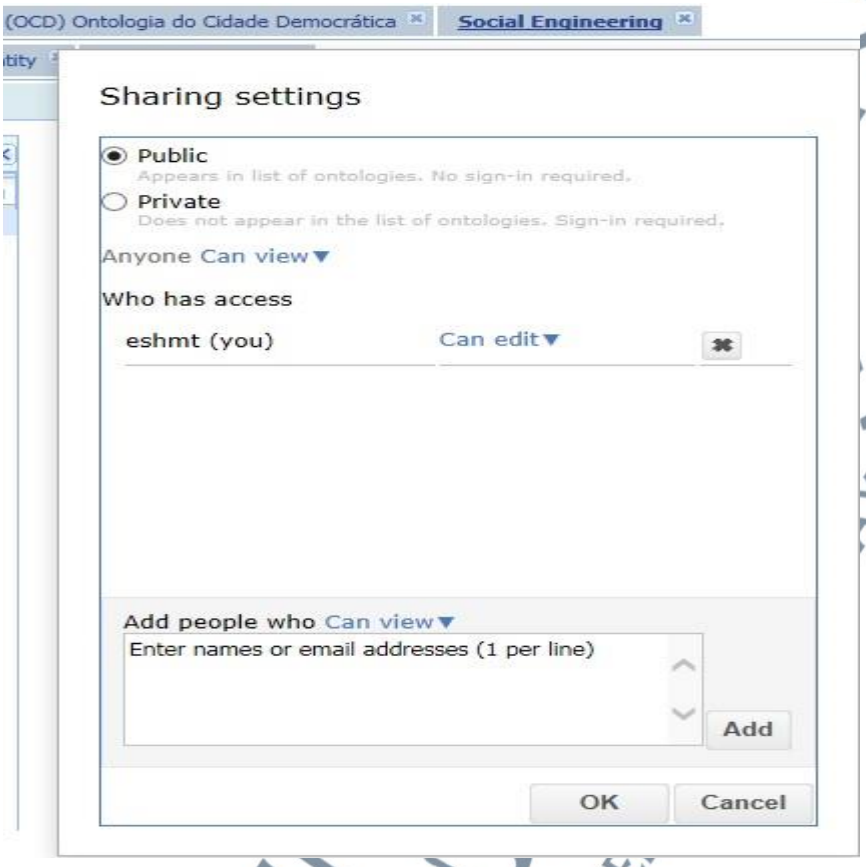


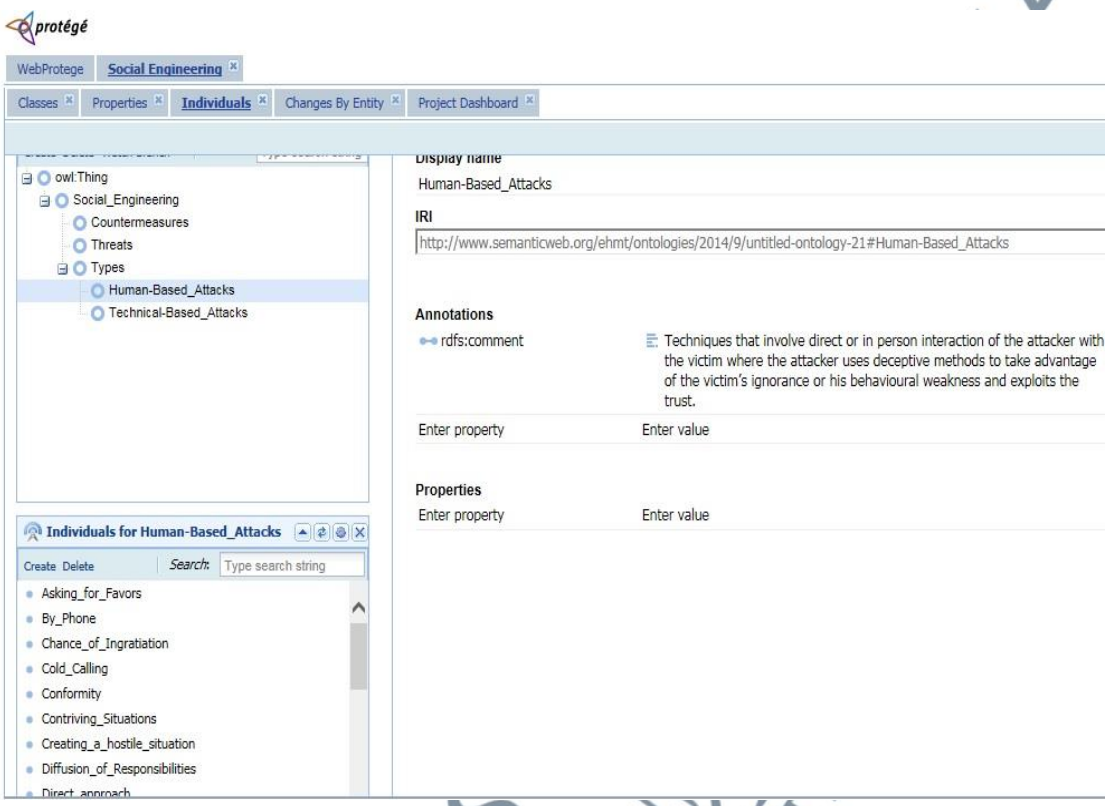
Figure 23 shows the sharing settings under the "share" tab. Public option is used in order to make social engineering ontology in a public sharing for interested users.

FIGURE 23: Sharing settings as a public option.



The next figure 24 provides an example, including individuals from the social engineering ontology. Classes, properties, and individuals can be viewed separately in the visualization.

FIGURE 24: WebProtégé social engineering individuals view.



4.5 CONCLUSION

In summary, techniques of social engineering attacks grow in an evolutionary process, and some of these techniques have plurality in names. But, in both types, human- based and technical-based, there are unique terms according to current reviews, which reflect that there is progress in offensive techniques of social engineering. With reference to Table 1, there are two types of social engineering attacks, human-based and technical-based. Under these two categories, human-based contains more of the attack techniques compared with the technical based. There is a variety of social engineering threats but, mostly it is targeting sensitive information of

an organization and individuals. On the other side, awareness is classified as an important defense line against social engineer attacks in addition to employee training and keeping security baseline mechanisms.

Through its implementation process, Protégé is used as an open source and ontology editor tool. It's a flexible base for application development and for rapid prototyping as it's based on Java. After the creation of a social engineering main root, all sub-classes are defined, and object properties are also defined. In addition all members of lists and sub-lists are defined.

After the implementation process, the developed social engineering ontology format was converted from OWL/XML to the RDF/XML format and uploaded to the public users on web protégé. It can be downloaded from *http://webprotege.stanford.edu/#Edit:projectId=03277414-c1b3-43eb-807f-626dc37-fc02d.*