Constructing Enterprise Information Network Security Risk Management Mechanism by Ontology

Fong-Hao Liu[1]* and Wei-Tsong Lee[2]

[1]*Information Management Graduated School, National Defense Management College, National Defense University, Taipei, Taiwan 112, R.O.C.*
[2]*Department of Electrical Engineering, Tamkang University, Tamsui, Taiwan 251, R.O.C.*

Abstract

Along with the development of information technology and internet, a lot of modern technology methods and tools are used to management. Therefore, it is an important discussion to information security risk management. In this paper, we buring up an ontology structure of information security risk management, and among them are the ontology-based UPML approach proposed. It is componed of three parts: Domain ontology, Task ontology, and Resolution ontology. This structure is established by Protégé 3.1, and its purpose is adopt ontology technology made early, so that the expert knowledge in intrusion detection, network safety techniques, security policies, etc. can be modeled, stored, shared as well as later queried.

***Key Words*:** Ontology, Information Security, Risk Management, Propose and Revise

1. Introduction

As the prosperous development of information technology and internet, the enterprises change the management of supplier chain into modern technology way. In the past, the communication tools of enterprises are telephone, fax machine, and paper based document. Recently the hottest Electronic Business brought enterprise real-time, much quick, accurate, and integrated information that not only shared by the suppliers but also be used to improve the supplier chain management much better, faster, and just-on-time by making good marketing and sales prediction, decreasing the inventory, enhance competition, improving customer satisfaction.

Because of the globalization of competitive world and the increasing reliance on internet for business transactions, the threat of hackers has seriously affected the enterprise information security for many businesses. For example, where customer data of almost 40 million credit card members was stolen, and potentially exposed to fraud, from one of the payment processors, was probably by far the largest network theft ever made public in the world, exemplifies the urgency.

To counter the threats, organizations spend much resource in deploying and updating multiplex expensive security devices such as firewalls, intrusion detection system and virus protection systems to safeguard sensitive corporate information. The installation of these devices is generally straightforward, compared to what follows, which typically involves establishing an organization-specific security policy & rules to ensure continuous interplay of security requirement analysis and control by experts. This is usually considerably more difficult but essential. Without the latter, an intrusion detection device, for instance, regardless how expensive or feature-rich, can not be made fully effective.

It is for this reason that, using the concepts of ontology technology, this paper seeks to construct a knowledge model that represents a framework which related goals to the control tasks of information security management by analyzing the current accepted information security management standards and practices BS7799

*Corresponding author. E-mail: lfh123@gmail.com

[1]. Then, the ontological domain framework is based platform of Protégé developed by Stanford University. And Jess, an expert system language developed by the Sandia National Lab of New Mexico, is used to present the security management rules that will be used by domain experts when looking for a solution. These security management rules in turn use the associations/relations between knowledge objects in the ontological database for inference. Together the knowledge base and inference rules provide a complete expert system for evaluating information security risks.

2. Concept and Tool of Ontology

In this paper, we will discuss how to use the ontology in systematic construction of the domain knowledge based information security management's goals and tasks captured from the industrial standards. The primary purpose is to enable knowledge sharing among security personnel, which in turn enhances and passes on the experience and knowledge of information security of an organization to safeguard its sensitive data.

2.1 Definition of Ontology

Ontology was proposed by Bunge in 1977 in computer science [2]. The American Heritage Dictionary defines ontology as "the branch of metaphysics that deals with the nature of being." Ontology has a long history in philosophy, in which it refers to the subject of existence. When applied to artificial intelligence, ontology is often used to mean the specification of conceptualization that describes knowledge of a particular domain. Ontology is a collection of concepts, which represent higher level knowledge in the knowledge hierarchy in a given organization [3].

In AI, ontology is a formal description of the sorts of objects, properties of objects, and relations between objects that are possible in a specified domain of knowledge. In other words, ontology is an explicit specification of a conceptualization.

Ontology is often captured in some form of a semantic network – a graph whose nodes are concepts or individual objects and whose arcs represent relationships or associations among the concepts [4].

From the viewpoint of ontology, the world consists of different domains, which are composed of related basic things. These basic things can be reused and shared by means of modifying attributes and relationships, etc. Besides, ontology is easy to understand specific domain because the class hierarchy of ontology is like the way of human beings storing knowledge. Inheritance of the ontology's class improves extensibility as well. Nowadays, ontology is widely used to describe a specific domain's knowledge and to achieve reusability and sharing of knowledge [5,6]. These are the main reasons of ontology's popular application in computer science, knowledge engineering, and information retrieval.

Due to the rapid development of ontology engineering, lots of ontologies are produced and could have overlaps. As a result, integration of ontology has become a research topic and can be classified as merging, alignment, reuse, and use, etc. [7,8].

2.2 Construction of Information Security Ontology

In this paper, Protégé 3.1 is used to establish the ontology of information security knowledge with control goals and control measure elements in BS7799/ISO27001 [1,9] stored at the knowledge base. Protégé 3.1 [10] is one of a series of ontology tools developed by Stanford University with the following features:

(1) Written in Java language and to be operated in internet and across platforms.
(2) Graphic and interactive interface would simplify knowledge management jobs of knowledge engineers and domain specialists.
(3) Hieratical and tree type structure enable the users to browse in the concept class level structure.
(4) Open interface for new plug-ins allows adding knowledge functions.

3. The Architecture of Information Security Risk Management

One of purpose of this paper is to provide subjective domain knowledge to decision-makers for optimal security problem decisions, The topics of systematic knowledge acquisition, representation and sharing have been explored extensively in various knowledge engineering discussions. Among them are the ontology-based UPML approach proposed by Fensel [11] and his colleagues for knowledge conceptualization and representation.

The UPML architecture for describing a knowledge-

based system consists of three mainly different elements (see Figure 1): (1) Task that defines the problem that should be solved by the knowledge-based system; (2) PSM, problem-solving method, that defines the problem solving process of a knowledge-based system; (3) Domain model that describes the domain knowledge. Each of these elements is independently to enable the reuse of task descriptions in different domains, the reuse of problem-solving methods for different tasks and domains, and the reuse of domain knowledge for different tasks and problem-solving methods. Ontology provides the terminology used that in tasks, problem-solving methods and domain definitions. Again this separation enables knowledge sharing and reuse [11]. The UPML have the following advantages:

(1) The ontology of UPML design is flexible, which helps minimize the effort needed to resolve a single but complex problem, thus reducing the overall design complexity.
(2) All major components are functionally independent, which allows for greater reusability and interoperability with knowledge systems of different domains and of different experiences.

Based on the structure of UPML the knowledge needed for information security risk management is divided into 3 major parts. They are, Part 1 "Domain": knowledge acquisition and modeling of organizational data valuation and security flaws and threats; Part 2 "Task": establishing risk rating and measurements; Part 3 "Resolution": using the self-adapting heuristic problem solving method the knowledges are combined to form an ontology designed specifically to minimize organizational information security risks(see Figure 2).

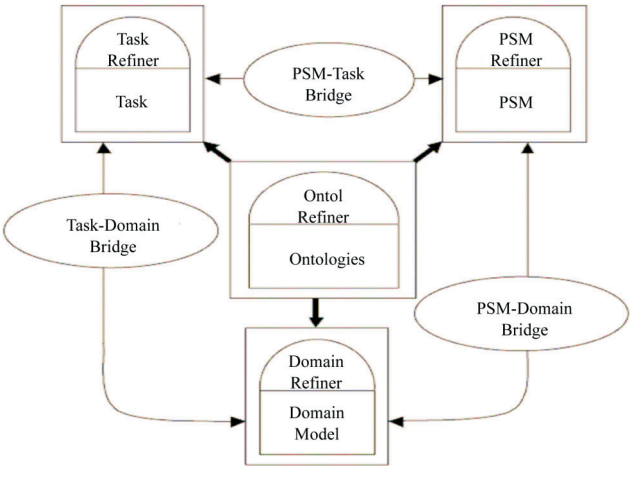

Figure 1. The structure of UPML.

4. Establishment of Information Security Management Knowledge Base

In book Heads Up [12], Kenneth G. McGee proposes a quite good notion. "We are unable to truly prevent the unknown dangers but only to do our best to predict the possible risk based on present situation." Failure of making timely responses to unexpected events is caused by being unable to be aware of the early warning in time. Therefore, to conduct risk management, an information security system systematic covers overall organization should be established and maintained in accordance with information security management standard. With the information security management method, data related to in advanced warning of the risky situations that affect organization operation from achieving its goals would be collected, analyzed, and monitored substantially, and then resolute actions would be taken whenever they are required. That would be an effective way to prevent network disasters.

4.1 Establishment of "Domain" Ontology Knowledge Base

Until recently most organizations' main focus on information security have been on the "availability" when

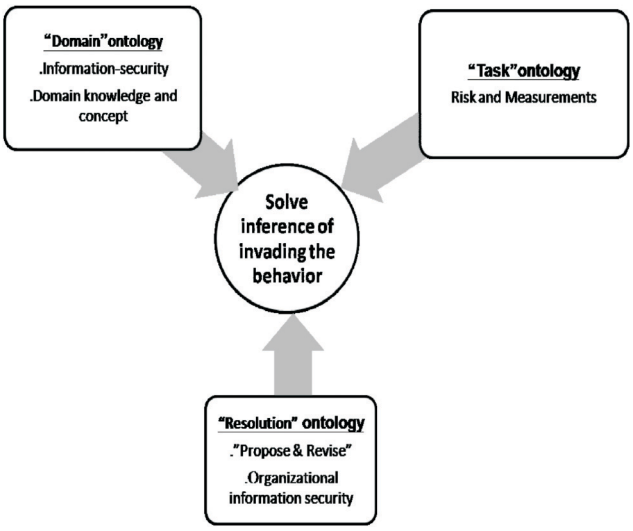

Figure 2. Ontology structure of information security risk management.

conducting electronic business and Supply Chain Management. Learned from the damage of increasing information security threats, many companies recognize that "availability" along is no longer sufficient. Today business transactions must also ensure "confidentiality" and "integrity." To meet this end , BSI (British Standards Institute) have published the BS7799 standards regarding information security management and auditing.

The BS7799 includes eleven control measures with specific requirements on identification of organization assets (see Table 1). The goal is to maintain and ensure that proper protection have been prearranged to those valuable organization asset.

To identify the protected information asset, an organization shall list information assets related to information security, then confirm and evaluate each asset properly. During asset identification, an organization could divide the information asset into seven categories: written documents, software assets, substantial asset, personnel, service, company image and goodwill. Value estimation shall be given to each asset. Asset value can be quantified in the following formula:

Asset value (V) = value of the equipment (tangible value) + organization value affected when the equipment is out of order (intangible or information value) (1)

Based on the formula (1), the assets of an organization can be checked thoroughly and listed in the Protégé knowledge base. In this paper, based on BS7799, confidentiality, integrity, and accessibility of the data have to be put into consideration during the evaluating process of the organization information asset. The analysis of system security threat should be focused on factors of environment, human behaviors, and technology. An organization shall assess its operation, tangibility, personnel and technology, on the respect of the levels of the system security leak they could cause, and reflect the importance accordingly (in five levels with 1 as the least important and 5 the most improvement). Finally, Information related to system security leak has to be established (see Figure 3).

Table 1. 11 control measures in BS7799

1. security policy
2. organization of information security
3. asset management
4. human resources security
5. physical and environmental security
6. communications and operations management
7. access control
8. information systems acquisition, development and maintenance
9. information security incident management
10. business continuity management
11. compliance

4.2 Establishment of "Task" Ontology Knowledge Base

All system impact analyses with their frequency study are required in conducting the Risk Assessment. The Frequency Study evaluates the frequency of impact on the system (e.g. daily, monthly or yearly). The higher impact possibility leads to higher level of risks. After confirmation of the impact and possibility of the impact on the system, one can analyze the overall system risk level. The risk calculation formula is [13]:

$$R = R(PT, PV, I) \quad (2)$$

where R -- risk of the asset under a certain threat.
PT -- possibility of the threat.
PV -- possibility of the leak being used.

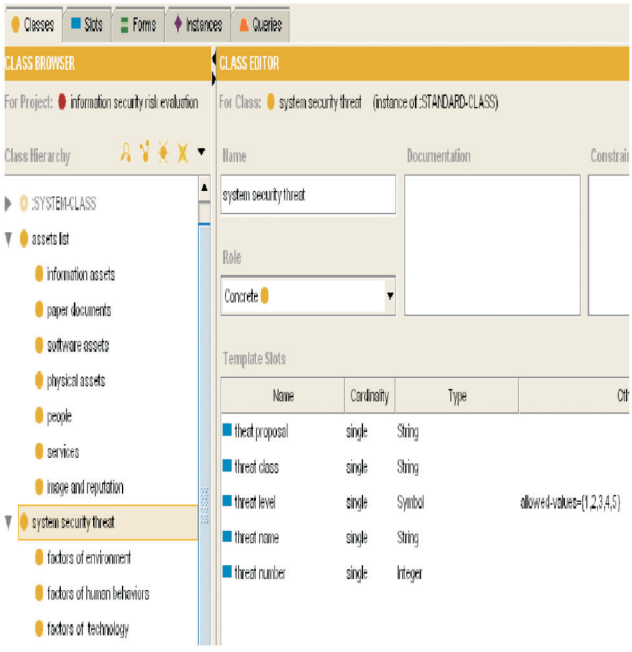

Figure 3. Establish risk management of the "Domain" knowledge in Protégé 3.1.

I -- potential threat impact (I = VX value loss degree CL).

0 < CL value loss degree < = 1 (value of the asset might be completely lost after security incident, i.e, CL = 1. It does cause some affect to the asset value, i.e, CL > 0. To simplify the evaluation procedures, asset value replaces the impact under the threat.)

Risk levels can be measured by different methods. Risk value matrix is used to measure the risk value (see Table 2) with the matrix to verify the risk value regarding the possibility of the threat, possibility of the leak being used, and asset value.

(1) Possibility of the threat is divided into three levels: low, intermediate, high. (0~2)
(2) Possibility of the leak being used into three levels: low, intermediate, high. (0~2)
(3) Qualitative of the asset value under threat is divided into five levels. (0~4)

Provided the case that the possibility of the threat is low, that of the leak being used is intermediate, and asset value is level 3, the risk value of this case is 4 by look up the risk matrix table. Confirming the risk value, area division is used to prioritize the risks (see Table 3).

After verification of the risk levels, the responsive action list of management, operation and technology should be prepared against each confirmed risk impact to minimize the impact by the risk. As eradication of the risks is an unfeasible, alternative of risk avoidance, reduction, transference and acceptance would be added into the list as the reference for decision makers.

At last, establishing the organization information security risk level list would be used to complete implementation of the Task knowledge into the knowledge base in Protégé 3.1 (see Figure 4).

4.3 Establishment of "Resolution Ontology" Knowledge Base

4.3.1 Using the "Propose & Revise" Method to Improve Information Security Risks

The importance of domain ontology lies in it contextual problem solving capabilities. Due to the increasing attentions given to knowledge sharing and reuse, the need to generalize the solutions with respect to the problems they solve is also gaining more momentum. The heuristic problem solving method can generate a rich set of recommendations for corporate policy makers with limited resources.

As an example using the "Propose & Revise" problem solving method in the context of minimizing information security risks (see Figure 5), an organization with limited resources can follow the steps below to perform a feasibility study of recommended solutions and strategies:

Select:

Analyze and prioritize proposed risk reassessment/ readjustment tasks based on urgency, and assign resource requirements to each proposal.

Propose:

A proposed task is only feasible when its resource requirement meets the available resources requirement in the organization.

Table 3. The level of risk divides table

Risk value block	risk level
6, 7, 8	level 1, high risk, priority control
3, 4, 5	level 2, general risk, control properly
0, 1, 2	level 3, low risk, accept

Table 2. Risk value matrix

	PT (possibility of the threat)	Low 0			intermediate 1			high 2		
Asset value (V)	PV (possibility of the leak being used)	low 0	intermediate 1	high 2	low 0	intermediate 1	high 2	low 0	intermediate 1	high 2
	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

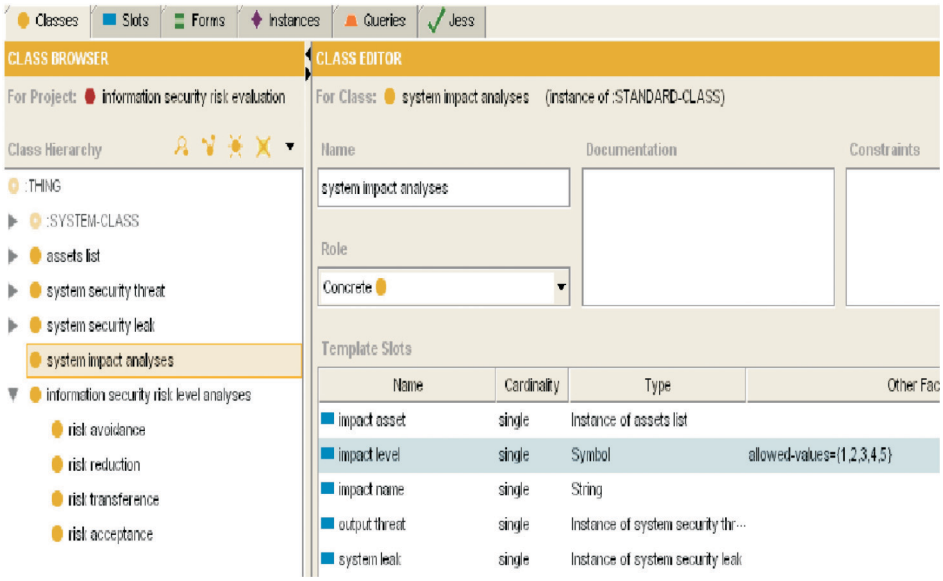

Figure 4. Establish risk management of the "Task" knowledge in Protégé 3.1.

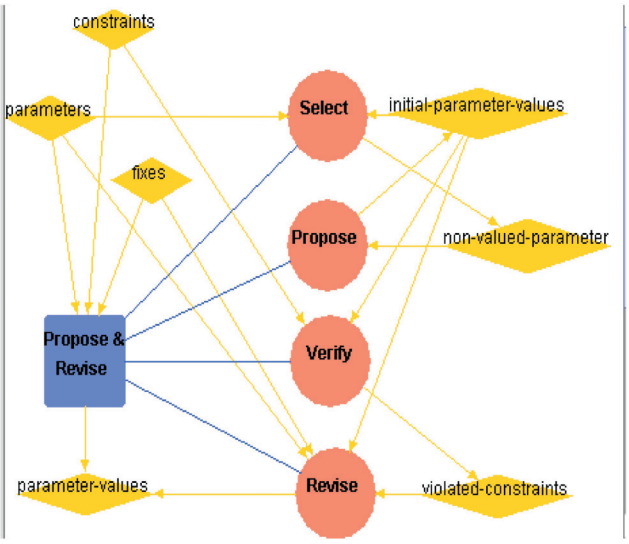

Figure 5. "Propose & revise" the inference and structure chart.

Verify:

Examine the resource requirement of each proposed task in order of priority until one that meets the organizational available resource requirements.

Revise:

Repeat step 3 until the resource requirement of the proposed task in question exceeds the organization's available resource (see the Table 4).

Finally, Jess's rules, which represent methods by which a domain expert uses when developing problem solutions, can be used differently in varying scenarios to give different solutions (see Figure 6).

4.3.2 Compiling Risk Re-Assessment Proposals

Risks associated with various proposals, together with their resource requirements and their priorities, can be measured against organization's established information security risk ratings.

Using the steps mentioned above, the proposals, plus the risk ratings, can be used to establish the information security domain ontology base Protégé 3.1 (see Figure 7), whose data can be queried to provide optimal solution to any organization unit.

5. Conclusion and Future Research

With the advances in information technologies, organizations can now afford to ensure reliable, accurate and complete electronic exchanges between supply chain partners with minimum acceptable risk. Network infrastructure, technology platforms, management policies, as well as security techniques are all-important elements. Although different combinations of these elements can result in different typologies and effectiveness, faced with the ever changing security threats there is really no guarantee that any of these combination can be 100% safe-proof.

Table 4. In the "information security risk" ontology of work rules

Step for compiling the proposal: find all tasks whose resource requirements are lower than available resources afforded by the organization. (*forall* ? *X* (*action*_min_cos *t*? *X*)(business_cos *t*))) Step for analysis & adjustment: from the selected tasks, in order of priority, look for one that requires less resource than what is available, until all available resources have been exhausted. (*exists* ? *X* (⇒ (*risk_ propose_action* ? *X*)(min(*rank* ? *X*))) (*forall* ? *X*(⇒ (*rest_ propose_action* ? *X*) (–(business_cos *t*)(*action*_min_cos *t* ? *X*)))) (*forall* ? *X*(⇒ (*next_ propose_action* ? *X*) (+(*rank* ? *X*)1))) (*next_ propose_action* ? *X* ← (–(*rest*_business_cos *t*)(*action*_min_cos *t* ? *X*))) (*exit* ? *X*(< (*rest*_business_cos *t*)(*action*_min_cos *t* ? *X*)))

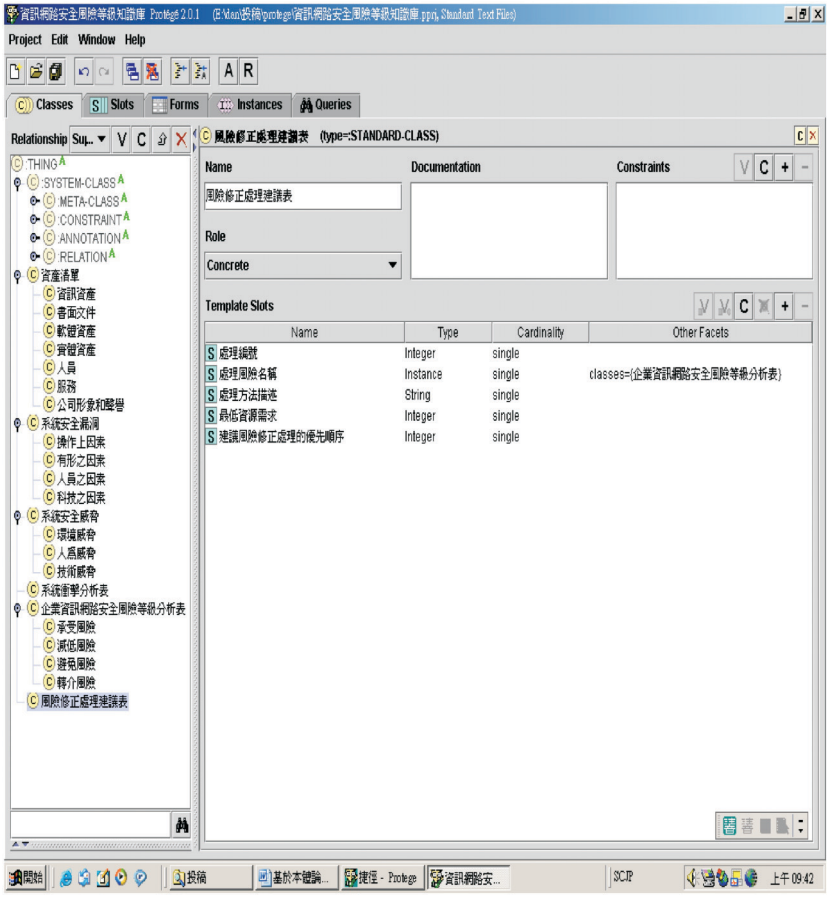

Figure 6. "Problem solving" and "information security risks" task rules.

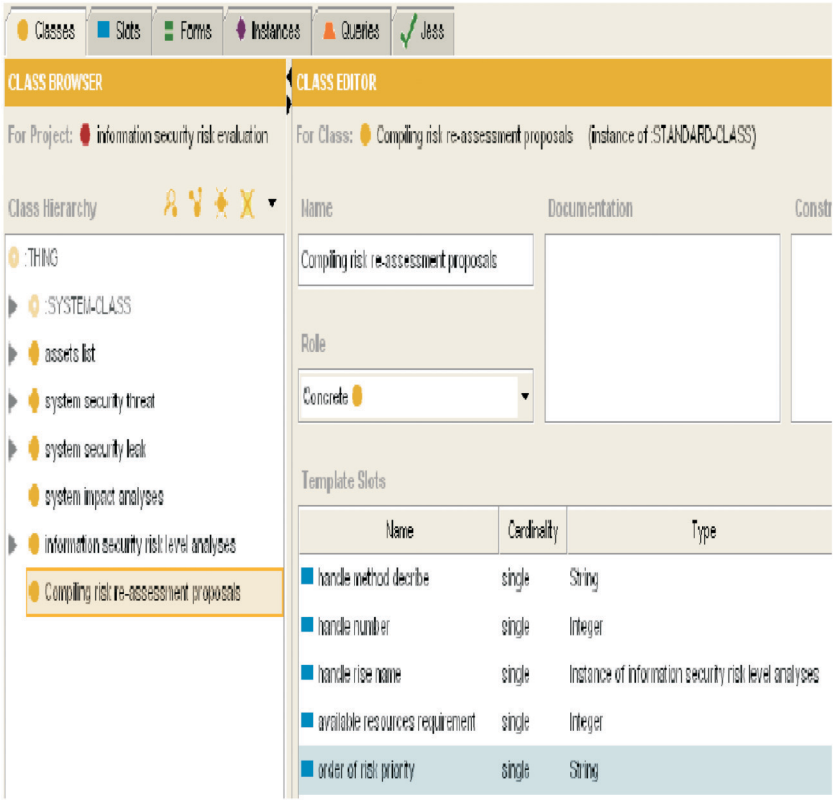

Figure 7. Establish risk management of the problem solving method knowledge in Protégé 3.1.

In order to evaluate the risks and readiness of the typology in meeting an organization's security requirements, this paper's decision to adopt ontology technology was made early so that the expert knowledge in intrusion detection, network safety techniques, security policies, etc. can be modelled, stored, shared as well as later queried. With the addition of risk ratings and associated remedial tasks the security personnel of an organization can repeatedly perform what-if design analysis against the ontology base until a feasible solution, or solutions, is found before the physical implementation commences. This approach has the obvious advantage of shortening the time needed for design, build, operating and testing cycles, not to mention the heightened robustness in network safety once up and running.

The direction of future research is to establish a system that's not only flexible, adaptable and user-friendly with a web-oriented graphical management interface, it must also be extendible, reusable and can integrate easily with other knowledge presentation systems. Given that today's organizations are more and more knowledge-intensive and service-oriented, the need for a collective knowledge base with maximum generality that can be easily developed and effective maintained by the domain experts, and at the same time offers high degree of usability and accessibility to knowledge workers, will undoubtedly give any organization a competitive edge.

References

[1] BSI.BRITISH STANDARD. BS 7799-2 (2002).

[2] Mario Bunge, Ontology: The Furniture of the World. Vol. 3, Treatise on Basic Philosophy (1977).

[3] Swartout, W. and Tate, A., Ontologies, *IEEE Intelligent Systems*, Jan-Feb, pp. 18–19 (1999).

[4] Lu, H.-H. and Liu, F.-H., *An Ontology-Based Architecture Applied to Fault Diagnosis Thesis*, Graduate School of National Defense Information National Defense Management College, National Defense University (2002).

[5] Rudi Studer, V. Richard Benjamins and Dieter Fensel, Knowledge Engineering: Principles and Methods, *Data and Knowledge Engineering*, Vol. 25, pp. 161–197, (1998).

[6] Ekelhart, A., Fenz, S., Goluch, G. and Weippl, E., *Ontological Mapping of Common Criteria's Security Assurance Requirements*, 22nd IFIP TC-11 International Information Security Conference (IFIPSEC'07) (2007).

[7] Fridman Noy, N. and Musen, M. A., *SMART: Automated Support for Ontology Merging and Alignment*, In Proceedings of the Twelfth Banff Workshop on Knowledge Acquisition, Modeling and Management, Banff, Alberta (1999).

[8] Pinto, H. Sofia, Gómez-Pérez, A. and Martins, J. P., Some Issues on Ontology Integration, In Proceedings of IJCAI99's Workshop on Ontologies and Problem Solving Methods: Lessons Learned and Future Trends, pp. 7.1–7.12 (1999).

[9] ISMS, *Information Security Management System*, ISO/IEC 7001 (2005).

[10] The Protégé 3.1 platform was developed by Stanford Center for Biomedical Informatics Research, http://protege.stanford.edu.

[11] Fensel, D., Motta, E., Benjamins, V. R., Crubezy, M. and Decker, S., et al., The Unified Problem-Solving Method Development Language UPML, http://www.cs.vu.nl/dieter/ftp/spool/upml.journal.pdf.

[12] Kenneth G. McGee, Heads Up, Harvard Business School Publishing (2004).

[13] Liang, S.-L., Liu, F.-H. and Lee, W.-T., *The Method and Application of Network Security Management Model Base the View from Vision to Execution*, Department of Information Management of NDUSM, Papers of Master (2005).

Manuscript Received: Jan. 8, 2010
Accepted: Mar. 3, 2010