ISEK: An Information Security Knowledge Graph for CISP Knowledge System

Yuangang Yao, Xing Wang, Xiangjie Meng, Xiaofei Zhang, Bin Li
China Information Technology Security Evaluation Center
Beijing, China
yaoyg@itsec.gov.cn

***Abstract*—As the development of information technology, information security is concerned more by society and industry. One important way to assure the security of information technology is education and training for IT practitioners. In this paper, we propose an information security knowledge graph method for information security training and certification knowledge system, in which security knowledge is described and organized with semantics. It can be used for knowledge organization, architecture presentation and examination in security education and training. To valid the proposed method, we construct the ISEK knowledge graph for CISP knowledge system in China, and use it for knowledge navigation and examination analysis.**

Keywords—information security; knowledge graph; semantic web; ontology; CISP

I. INTRODUCTION

In the information age, information technology is one of the foundations for the industrial, social and economic life. The security of information technology is becoming more and more important for the whole social and economic developments. Information security is a matter of urgent concern. In the information security work, the person is the most important and active factor; personnel information security awareness, knowledge and skills are the important basic elements to guarantee the safe and stable running of information systems.

As the rapidly development of information security, the connotation of information security develops gradually from the initial information confidential to the information integrity, availability, controllability and non-repudiation, and forms the basic theory and implementation technology of security attack, prevention, detection, control, management, evaluation and so on. Currently, The contents of information technology security mainly include equipment security, data security, content security and behavior security[1][2]. On the other side, the security of information systems is affected by system structures, net structures, the software and hardware, etc. Information security knowledge system needs take all these factors into account.

As a result, information security professionals need systematic, comprehensive training and certification of information security knowledge. Professional information security education is needed.

Certified Information Security Professional (CISP) is the highest national certification of information security personnel qualifications in China. It is an important qualification evaluation of information security professionals for network infrastructure and important information systems. CISP is needed for the enterprise information security, information security consulting services, information security evaluation institutions, social organizations, and relevant technical departments. Its basic function is providing technical support for the security of the information systems. According to the work experiences, there are several types of certified information security professionals in China, which are certified information security engineer, certified information security officer, certified information security auditor, etc.

In this context, the key difficulty for information security training and certification is organization and specification of information security knowledge. In this paper we try to organize knowledge nodes in information security education and training, and construct information security knowledge network specification using knowledge graph method.

II. ONTOLOGY

Ontology is defined as a formal, explicit specification of a shared conceptualization, which is shared, conceptualization, explicit and formal[3]. Ontology is organized for sharing between professionals and computer applications. It is abstract description model of concepts and relations for certain domain. Ontology clearly defines the types of all the concepts and constraints between concepts. And based on the formal descriptions of domain knowledge, machines can understand and process knowledge semantically. Ontology is often used to define knowledge schema, such as the Wordnet, OpenCyc, DBpedia, and Freebase[4]. These projects are all ontology-based common knowledge network.

Ontology is also used for educational training in certain domains[5][6]. Macris and Georgakellos propose an ontology model for environmental training, which contains concepts, relations, properties, and related various multimedia in education for sustainable development[7]. Users can search and navigate the knowledge network to understand the relevant knowledge during educational training. Cui et al. propose an

978-1-4673-6537-6/15/$31.00 ©2015 IEEE

ontology-based educational platform architecture for e-learning. With the core educational ontology, the platform can provide concept reusability[8].

III. Information Security Knowledge Graph

Ontology is often referred to as the domain model or concept model. It is a kind of semantic descriptions for sharing domain knowledge. The main elements of ontology are concepts, relations, and attributes. Ontology can be used as knowledge graph model to construct and organize corresponding knowledge network. For CISP, the ontology based information security knowledge graph is abstract descriptions of security concepts and terms and the knowledge instances. Based on information security knowledge graph, knowledge processing methods can use background knowledge to effectively find and understand meaningful domain rules and related knowledge nodes.

According to the CISP education and training knowledge system, we build a fine organized information security knowledge graph to cover the whole knowledge points that should be understood and mastered for security professionals, which is the important basis for the compilation of teaching material, teaching and learning, and examination. The ontology based knowledge graph is constructed based on principles of comprehensiveness and practicability of the knowledge system, which has been considered the current information security conditions and the actual needs of information system.

A. The CISP Knowledge System

The CISP knowledge system has four basic knowledge hierarchies, including knowledge class, knowledge body, knowledge domain, and knowledge subdomain. Fig. 1. Shows the knowledge hierarchies. Knowledge class is the overall division of information security knowledge, which contains five categories of information security knowledge that professionals need to master. Knowledge body is a relatively independent knowledge set from a knowledge class that belongs to the same technology field. Knowledge domain further decomposes knowledge body to form refined knowledge components. Knowledge subdomain is basic elements of knowledge domain that consists of several specific knowledge points. For each knowledge points, there are three degrees to evaluate the learning and mastery of professionals, which are known, understood or mastered.

In CISP knowledge system, there are five knowledge classes including information security assurance overview, information security technology, information security management, information security engineering, and information security standards and regulations. Information security assurance overview introduces the framework, basic principle, and practice of information security assurance. It is the basic knowledge for CISP. Information security technology mainly includes security technology mechanisms of encryption, access control, and audit monitoring, and basic security principles and practices of network, operating systems, databases, and application software, as well as information security defense and software security development technologies and practices. Information security management mainly includes the information security management system construction, information security risk management, security management solutions and other related management knowledge and practices. Information security engineering mainly includes information security related engineering method. Information security standards and regulations mainly include the information security standards, rules and regulations, and policies.

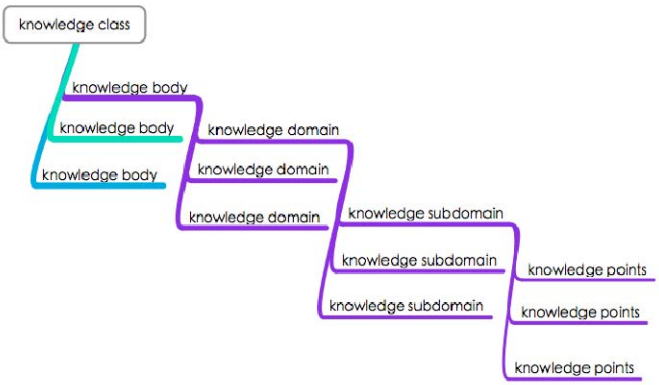

Fig. 1. Hierarchies of CISP knowledge

B. Ontology Constructing

As an initial implementation of information security education ontology, the information security knowledge graph (ISEK) for CISP mainly considers the knowledge architecture and knowledge points in CISP, which means the ontology is an enriched taxonomy structure with simple semantic constrains of information security knowledge. Ontology construction method can be roughly classified as top down and bottom up ones[9]. According to the information security knowledge structures, we propose a top-down ontology construction method to build the ontology semi-automatically. We firstly build five top classes according to knowledge class, and then extract knowledge bodies and knowledge domains and subdomains according to knowledge systems of CISP. Besides the knowledge points of CISP, there are also meta-classes and related classes of information security education and training knowledge, such as the knowledge architecture, professional levels, and certification types. After initial construction processing, we detect ontology consistency using ontology reasoning engine to find and modify the inconsistent knowledge entities, and to merge and redirect reduplicative knowledge entities by renaming and creating constrains and relations. Knowledge entities under subdomains are also detailed in ontology. These entities are associated with meta-classes and related classes. For example, each knowledge entity is associated with a certain professional level for different certification types. In addition, annotations and comments about detail knowledge entities are added after the constructions above. Fig. 2. Shows the ontology constructions steps of ISEK.

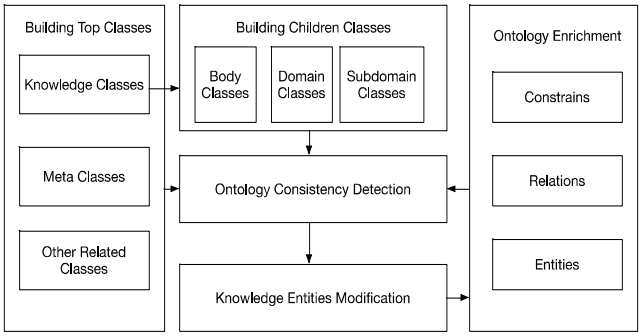

Fig. 2. The ISEK Ontology Construction Processes

C. The Constructed ISEK

According to the proposed constructing method, we build the ISEK ontology. It contains 524 axioms, 313 class axioms including 208 subclass axioms, 118 annotation axioms. The root class of ISEK model is a virtual node to cover all knowledge and metadata of CISP. Corresponding to the CISP knowledge system, the top classes of ISEK are information security assurance overview class, information security technology class, information security management class, information security engineering class, and information security standards and regulations class. The above classes are the main top classes of CISP knowledge. These classes have a sibling class meta-class to describe other related entities about CISP knowledge system, which contains mastery degree class, knowledge architecture class, and certification types class. Mastery degree class has three subclasses to represent the known, understood or mastered of knowledge nodes respectively. The knowledge architecture class describes the knowledge organization architecture of CISP, which contains the four basic knowledge hierarchies knowledge class, knowledge body, knowledge domain, and knowledge subdomain.

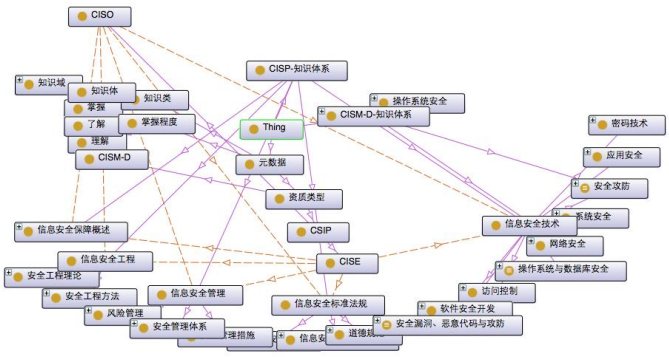

Fig. 3. A partial of the ISEK ontology

For the main classes of CISP knowledge system, the end nodes of them are detailed knowledge entities. They are classified and organized knowledge points of information security. Knowledge entities are also associated with other related classes of ISEK, for example, each knowledge entity is associated with some mastery degree classes and professional level degree descriptions, and some knowledge entity may be related with more than one security topics. Fig. 3. shows a partial of the constructed ontology, including ontology entities and relations.

IV. The Applications

We basically construct the ISEK for CISP education training. It's constructed for knowledge organization, architecture presentation and examination. ISEK is now a knowledge model for CISP knowledge points management. We can easily add, delete and modify knowledge points as the training materials change. And during the CISP training, ISEK is used as the knowledge framework and navigation map for the trainees. They can overview and navigate the CISP knowledge system, and find out the associations between knowledge points. For the CISP certification examination, the ISEK can be used to build exam by organize the exam questions, and analyze the results. Besides the CISP education training, the constructed ISEK can also be used in other work and study scenarios, such as the IT security management.

V. Conclusions

In this paper, we propose an information security knowledge graph method for information security education and training knowledge system. It provides a semantic knowledge organization method for IT security training. The constructed ISEK model covers CISP training and certification knowledge system at several levels, including knowledge class, knowledge body, knowledge domain, and knowledge subdomain of CISP knowledge architecture. And specific knowledge points can be added as the instances of ontology classes. According to the change of CISP training, the ISEK can add, delete, and modify classes and instances of ontology to meet the training demand. The proposed ISEK can be used for knowledge organization, architecture presentation and examination, and further for other IT security scenarios. For the future work, we will add more knowledge entities into the ISEK and associated the knowledge points in ISEK with labeled examination questions.

References

[1] Feng, D.G. 2010. The current information security technology situation in China and abroad. E-government 7:27-33.

[2] Whitman, M.E., and Mattord, H.J. 2010. Principles of information security. Cengage Learning.

[3] Uschold, M., and Gruninger, M. 1996. Ontologies: principles, methods and applications. The Knowledge Engineering Review 11:93-136.

[4] Bordes, A., Weston, J., Collobert, R., and Bengio, Y. 2011. Learning structured embeddings of knowledge bases. In Proceedings of the

Twenty-Fifth AAAI Conference on Artificial Intelligence. San Francisco, California: AAAI Press.

[5] Aroyo, L., and Mizoguchi, R. 2003. Authoring support framework for intelligent educational systems. In U. Hoppe, F. Verdejo, and J. Kay, editors, Proccedings of AI in Education, AIED-200:362– 364. IOS Press.

[6] Mizoguchi, R., and Bourdeau, J. 2000. Using ontological engineering to overcome AI-ED problems. International Journal of Artificial Intelligence in Education 11(2):107–121.

[7] Macris, A.M., and Georgakellos, D.A. 2006. A new teaching tool in education for sustainable development: ontology-based knowledge networks for environmental training. Journal of Cleaner Production 14(9–11): 855-867.

[8] Cui, G., Chen. F., Chen. H., and Li, S. 2004. OntoEdu: a case study of ontology-based education grid system for e-learning. In GCCCE2004 International conference, Hong Kong.

[9] Zhang, H.M., Guo, J.Y., Yu, Z.T., Lei, C.Y., Mao, C.L., and Wang, H.X. 2010. An Approach of Domain Ontology Construction Based on Resource Model and Jena. Third International Symposium on Information Processing:311-315.