Research on Knowledge Representation Methods of Network Information Security

Yan Junya, Yang Sen

Business College of Shanxi University,

Keywords: network security; information security; knowledge representation

Abstract: This paper starts from the classification of the knowledge hierarchy of network information security, on the basis of researching the knowledge of database system. It combines the inherent features of the knowledge on network information security, and the objects, forms and contents, focuses on methods of knowledge representation on network information security, and analyzes the advantages of knowledge representation methods of network information security and the practical applications.

1. Introduction

As the development of network and the increasing of information, information technology has not only propelled the society forward constantly, but also promoted the development of humankind; information security also has been an important factor that influences the safety of a nation, such as economic safety, political safety, defense safety, cultural security and so on. Therefore, it is necessary to do some early preventive strategies, and to construct knowledge system of the network information system by artificial intelligence and knowledge engineering, and then the system can integrate and systematize the knowledge of network information security, and provide effective support for the knowledge base management of information security. This thesis starts from the classification of the knowledge hierarchy of network information security, on the base of researching the knowledge of database system, it combines the inherently features of the knowledge about the network information security, and the objects, the methods and the contents, so as to lay a solid foundation for constructing and managing the knowledge base system..

2. The Knowledge Hierarchy of Network Information Security

As the constant emergence and development of network information security, it becomes more important to research the classification of network information security. In view of the importance, immaturity and complexity of the development of network information security, we should explore the knowledge system of network information security from multiple perspectives. First of all, from the perspective of application, to provide a complete knowledge system about network information security to the different users; second, from the perspectives of different users, such as government, enterprise, the publics and so on, to provide different users with different knowledge about network information security; third**,** from the perspective of social education and ideology, for the ordinary people, the unhealthy contents on the network will hinder the stability of society and the development of human beings, this phenomenal must be controlled; by integrating the relevant knowledge on network information security, it is very important to build a user-oriented knowledge system whose main contents is about network information security and it is also supplemented by other knowledge classifications, so as to form a relative integral knowledge system of network information security that can meet the needs of all aspects.

3. Knowledge Base System

During the process of constructing the knowledge system of information security, according to the different ways of getting the original knowledge, the main ways of getting the knowledge about

network information security are specialist, government, enterprise, documents, and internet etc. people can organize these knowledge about network information security together, and then, represent these knowledge by means of knowledge representation, construct the knowledge base, manage the knowledge, so that people could accumulate, sort, share, and reuse the knowledge, finally, they can easily find out the relevant knowledge, which can lay a solid foundation for construction and management of the knowledge system about network information security. The structure of knowledge base system is shown as Chart 1 blow.

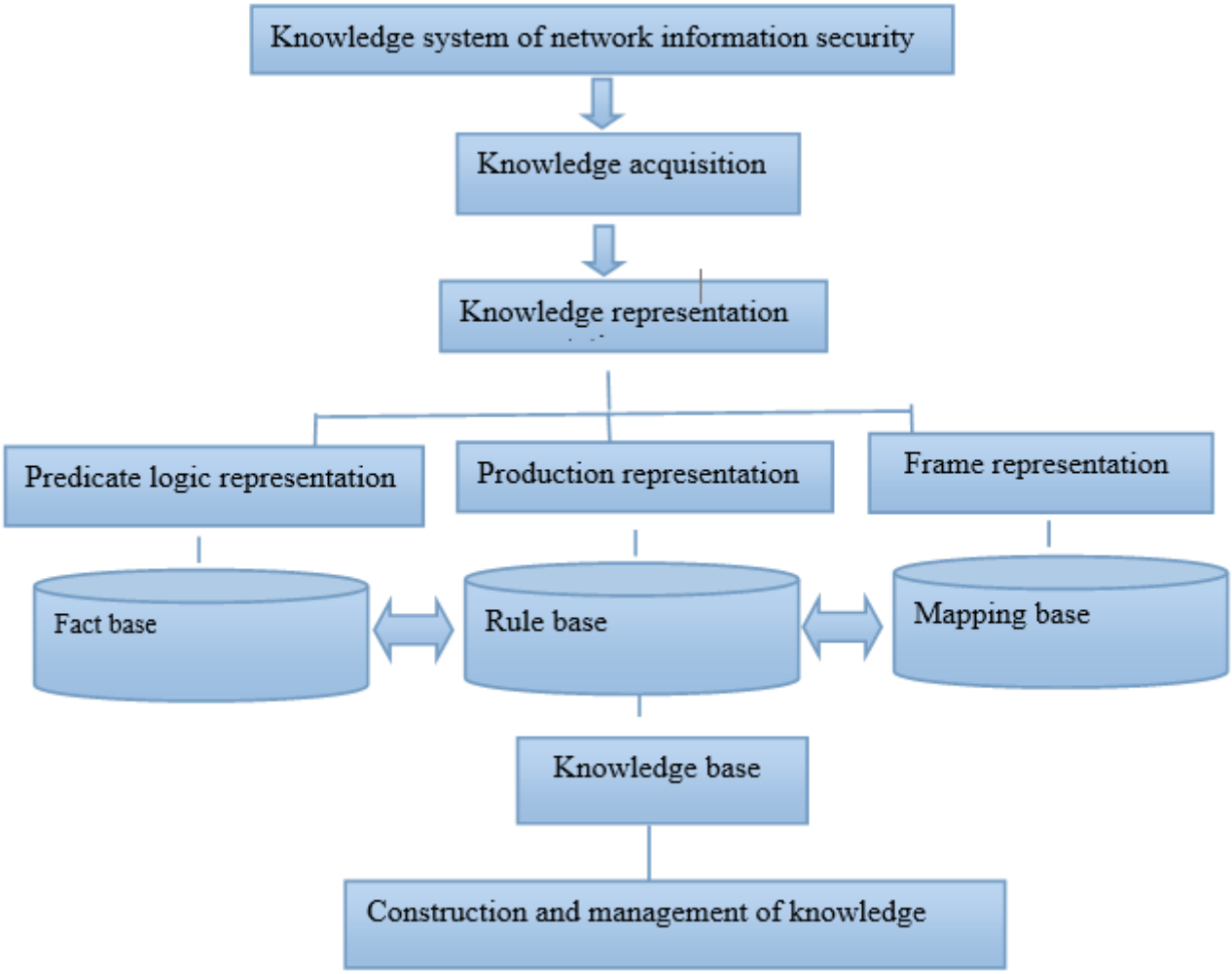

Chart 1. Structure of knowledge base system

4. Forms of Knowledge Presentation

Knowledge representation is not only one of the key researching issues of artificial intelligence, but also one of the important step of developing the knowledge system of network information security. Knowledge representation is the process of knowledge symbolization; it organizes the knowledge of network information security together, prepares the knowledge map and encodes the knowledge in the knowledge base, so as to encode it into an appropriate data structure. Considering the inherent features of the knowledge about network information security, and the object, mode and contents of the knowledge system, this thesis mainly researches how to organize the knowledge such as the physical and natural security risk, security risk of information system, the security precaution, standard system management, and emergency response of network information security, etc. as a whole by means of Predicate Logic Representation, Production Representation, and Frame Representation.

(1) To represent knowledge by means of Predicate Logic Representation would formally represent the physical, natural, and the system-inherent security risk knowledge, which is represented by the form of natural language, by means of adding predication and function, so as to

acquire the relevant logical formula, further more, the knowledge could be indicated in the form of internal codes, and then it could be inferred accurately, and it constitutes an information entity. The predicate logic representation has a clear and uniform stipulation on simply explaining complex things, and it can effectively separate knowledge from the procedure of dealing with knowledge, and make the structure more clear.

Predicate logic is equivalent to function representation in mathematics.

Its defining proposition is shown as below:

P: User identity interception, camouflage, replay attacks occur in information system; data interception; usurpation; virus; denial of service; disorder the code maliciously; file loss of database, operating system damage, system source file leak, system administrator password leak, etc.

Q: Improper security configuration of system; bug of the system; system privilege levels are too little, password is short and simple.

R: Information security incidents involving the network and information system of the important departments of a company, or key website or other network and information systems, related to local social affairs or economic operations, which have been severely impacted to a large extent.

W: Defending in depth by some technologies such as firewall, intrusion detection system, bug scanning system, antivirus system, data backup, and host protection, etc.

Knowledge represent by Predicate Logic Representation: $(\forall x)(P \wedge Q \rightarrow R) \rightarrow W$, $\forall(x)$ is universal quantifier.

(2) Application of Production Representation could clarify the safety precautions, the relationship between the knowledge of emergency response, it has a certain logical structure, so it could make the knowledge of network information system be an organized whole with prerequisite and conclusion, and provide knowledge guarantee for the construction of the knowledge system about network information security. Production Representation are usually used to represent the knowledge representation with causality, its basic form is: P→Q or IF P THEN Q, in this form, P is the prerequisite of Production Representation, Q is a set of conclusions or actions。

(3) Frame Representation is a kind of data structure that combines some declarative knowledge of the network information security, such as standard management system, with the procedural knowledge of the network information system, and applies the frame as the basic knowledge organization unit, so as to restore all the knowledge about a special event or object. It represents the inner relationship of the category message of the network information security by the form of slot, and establishes the whole framework which represents the knowledge about network information security, so that the structural relationship of the knowledge can be revealed clearly. It is convenient to supply and revise the knowledge later, and reduce the redundancy of knowledge, so as to guarantee the homogeneity of the knowledge system about network information security. Safety precaution of network information security includes some security policies and laws, tools and software of safety precaution, technology of network information technology and so on; they are all the subordinate slots of the frame of network information security.

Table 1. Frame representation of network information security prevention

Frame: Network Information Security Prevention (Frame Name)		
Policies and lows of network information security (Slot Name)	Tools and software of network information security	Technology of network information Security
Policies of network information security Laws of network information Security	TCP/IP tool Port&Bug Scanning Sniffer Password cracking tool	Digital authentication technology Cryptology intrusion detection system firewall

By the application of the knowledge representation forms listed above, people can easily find out the relevant information about network information security, so that it lays a good foundation for

the decision inference and final result in the design of knowledge system about network information security.

5. Conclusion

Except these methods of knowledge representation, there are some other methods of knowledge representation. For example, the representation base on Petri Net, the representation base on Fuzzy Logical Algorithm, the representation base on Relation Schema, the representation base on Event Correlation Diagram, the representation base on Decision Table, and the representation base on Problem Reduction, etc.. These different methods of representation are fit for representing the different kinds of problems. The complexity of the real world causes that the systematic knowledge of a certain academic realm can not be expressed accurately with a single knowledge representation method. Therefore, many expert system builders adopt the hybrid knowledge representation method that relate to various methods of knowledge representation, so as to improve the accuracy of knowledge representation and the validity of reasoning.

Acknowledgement

Foundation item[1]: Key research and development project of the Shanxi Science and Technology department. (Number:201603D321112)

Foundation item[2]: 2016 Shanxi Provincial Information Fund Project (Research of Network Information Security Support Service Based on Knowledge Engineering)

References

[1] Xu Baoxiang, Ye Peihua. Research on Methods of Knowledge Representation [J]. Information Science, 2007.5:690-694.

[2] Shang Fuhua, Li Xiang, Gong Miao. Research on Knowledge Representation Based on Fuzzy Frame Production and Its Inference [J]. Computer Technology and Development, 2014.7:38-42.

[3] Zhu Wenbo, Li Aiping, Liu Xuemei. Research on Knowledge Representation Based for Stamping Process on Ontology [J]. China Mechanical Engineering [J], 2006 17(6):616-622

[4] Liu Jianwei, Yan Lufeng. A Comparative Study of Knowledge Representations [J]. Computer Systems & Applications, 2010, 20(3):242-246.

[5] Li Haigang, Yin Wanling. A Comparative Study of Knowledge Representation Methods for New Product Development [J]. Studies in Science of Science, 2009, 27(2):176-179.

[6] Xi Sumei. Research on Methods of Knowledge Representation Based on Petri Net [J]. Shandong University, 2009.7: 15-30.