Enterprise Network Business Process Incompatible Vulnerability Detection Method Based on FPN Model*

Yan Huaizhi
Beijing Key Laboratory of Software Security Engineering Technology
School of Software Engineering, Beijing Institute of Technology
Beijing, China
yhzhi@bit.edu.cn

Ye Wenwen**
Beijing Key Laboratory of Software Security Engineering Technology
School of Software Engineering, Beijing Institute of Technology
Beijing, China
two_ye@hotmail.com

Abstract—**This paper proposes a kind of enterprise network business process characteristics, gives the definition of incompatible vulnerability, analyzes the formation mechanism of incompatible vulnerability. Then, we establish the FPN mapping model of incompatible vulnerability, propose an incompatible vulnerability detection method based on the FPN, and constructs the incompatible vulnerability detection system that can effectively detect the enterprise network business incompatible vulnerabilities.**

Keywords-FPN; business process; incompatibility vulnerability; vulnerability detection

I. INTRODUCTION

With the rapid development of the manufacturing industry of information technology, manufacturing enterprises, especially manufacturing enterprises with large complex equipment, their internal organization and the interaction of both internal and external have become more and more complex. At the same time, the requirements for the rapid response of the enterprises, which were brought by the competition, should also require enterprises to use a fast and effective method to reduce product cycle, improve product quality, and improve product design costs. All aspects of enterprise management already have the application with related technologies, such as ERP systems and PDM systems. Increasingly complex business processes running on the enterprise's network, which brought a series of vulnerabilities because of the inconsistencies in resource sharing of the business process and security requirements, these incompatible vulnerabilities have become the major hidden danger of enterprise network security and reliable operation.

Most of the traditional enterprise network information security concerned about the operating system, network and application software security vulnerabilities, such as buffer overflow and less concerned about the vulnerabilities which caused by the inconsistencies between the resource sharing of the business process and security requirements. Currently, there still has a lack of effective analysis and detection methods for this kind of security issues.

In order to solve these above problems, this article proposes a new model based on the FPN incompatible vulnerabilities of business process from the perspective of the characteristics of collaborative combined with the general workflow technology. Using workflow primitives to describe collaborative processes and the incompatible vulnerabilities in collaborative processes are the conflicts and gaps between the business processes or inside the business process. Therefore, as for static workflow diagrams, using FPN net modeling techniques can describe static workflow diagrams as a Petri net system wherein for workflow concurrency characteristics can be a good simulation , then use the reachable marking graph theory of Petri nets and other methods to detect the incompatible vulnerabilities that may arise.

II. MECHANISM OF THE ENTERPRISE BUSINESS PROCESS INCOMPATIBILITY VULNERABILITY

A. *Integration of the causes of incompatibility vulnerability*

In this article, enterprise business process incompatible vulnerability is generally defined as: the major hidden danger which caused by the inconsistencies in resource sharing of the business process and security requirements, including some exclusive states which are inconsistent and unstable between the numbers of interrelated objects. These objects include design objects, design goals, the product development process, developers and resources with a variety of physical or functional entities of a certain structure and associated attribute information. In the process of the actual enterprise network business, there is impossible to avoid conflicts, incompatible vulnerability can only be to avoid in a certain extent, to minimize all kinds of incompatible vulnerability caused by human.

B. *Classification of incompatibility vulnerability*

According to the objects involved in incompatible vulnerability, it can be divided into the following three categories:

The incompatible vulnerability of the security policy: The different business process participants are not the same design requirements and objectives of the security requirements of the network as others. The performance of this vulnerability is that the network security policy is not able to meet all the requirements of various business process and has a contradictions and antagonistic relationship.

* Supported by the Project of National Ministry (No.A2120110006), BIT Basic Research Fund.

**Corresponding author (email: two_ye@hotmail.com)

The incompatible vulnerability of the resources: in the actual business process applications, resources are limited, the needs of different business processes on the same kind of material resources inconsistencies will cause incompatible vulnerability, or the different processes needed the same participant to complete also results in incompatible vulnerabilities. If multiple logic activities, which can be, performed simultaneously share the same data may cause data access conflicts, this data access conflicts may come from parallel internal activities within one business process, may also come from activities from different business process instances, and even between the different instances of the same business process. This data access conflicts will result in the incompatible vulnerability of the resources.

Because the collaborative design and development process are totally different with traditional business development process which is the multi-participant collaboration through the same platform, showing parallel characteristics that different participants may mutually do the exclusive operations at the same time which causes the incompatible vulnerability. On the other hand, the execution of a process maybe require all previous activities completed, so that there will be uncoordinated and bring it into conflict affecting the system's business process executions.

III. Knowledge Expression of the Incompatibility Vulnerability

A. *Knowledge expression of the enterprise networks business process*

Expression of the business process knowledge converts specific business processes of the enterprise network to a computable knowledge model. Expression of business process applications uses XML-based process description language, which realizes the standardized format description of the enterprise network business processes and completes the abstract expression of the business process. Specifically including the business processes' start and termination conditions, constitute a process activities as well as activities flow control rules, users need to complete the task, the application may be invoked, business flow reference relationship, as well as all the business flow data defined. The use of formal language, you can describe the processes and activities connected to each other to achieve business objectives and strategies set, portrayed documents, information or tasks between different executions completely or partially automatically passed, the process of implementation.

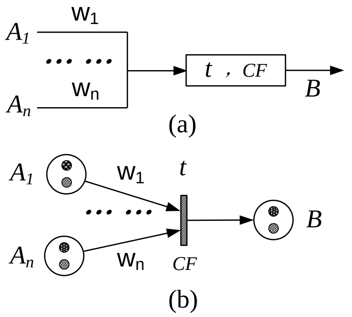
B. *Expression method of the incompatibility vulnerability based on the FPN*

According to the business security requirements of the system input and a number of business process information in its formal description. A description module of the business process gives a formal representation of the control flow and data flow in the business process. Using the Petri-net based reasoning technology, according to the established business process incompatible vulnerability knowledge base for validation, and finally get the business process application incompatible vulnerability.

Because of the uncertainty of detecting knowledge and rules caused by the complexity of the enterprise network and its application, which makes the decision fusion has become very complex, difficult to analyze and understand. Uncertain vulnerability Knowledge Representation and Reasoning of the most important is the relations generated rules and reasoning synthetic rules. Uncertainty divided into two levels: The uncertainty of knowledge (The weight of evidence and rule credibility) and reasoning processes, the latter is the former's reaction in the dissemination process. The key lies in the choice of the knowledge base structure and reasoning strategies. Compared with the binary logic, giving the detection of vulnerabilities conclusion is more in line with the actual situation. Weighted fuzzy production rules can be intuitive and simple to represent fuzzy knowledge and have well consistent with formal logic. Therefore, this paper uses fuzzy Petri net (FPN) model for knowledge representation and reasoning. The representation, which uses the knowledge based on fuzzy Petri nets, is easy to describe and deal with parallel reasoning, effectively solve the problems caused by traditional production rules: matching conflict, combinatorial explosion etc. , and can easily use the Petri net analysis tool to verify the knowledge base of structural errors.

1) *The FPN description of weighted fuzzy rules*

FPN is a model of knowledge by combining fuzzy theory and Petri nets, formal definition of the four-tuple: FPN = {P, T, U, W}, where P is the finite set of library, T is the change limited collection, U is the proposition finite set, W is a fuzzy multiple collections, and represent the connection strength of the library to transition.



(a)

(b)

Figure 1. The basic rules of reasoning unit and its FPN representation.

Figure 1 (a) shows the reasoning unit of basic rules. The activation of the rules corresponding to FPN transition, the premise proposition and conclusions proposition corresponding to the library; uncertain weights corresponding to the input intensity, the credibility of the corresponding output intensity; same variables in the rule base corresponding to the same library, the same operation corresponding to the same changes. According to this, it is easy to complete the construction of FPN, shown in Figure 1 (b).

2) *The FPN description of conversion process*

Using the FPN to express vulnerability knowledge, giving the definition, knowledge representation model of

FPN, and then convert the vulnerability knowledge into the corresponding rules for each base type, obtaining the expression of the corresponding FPN model, while using the FPN reachability graph to verify the structural errors of knowledge base. We can format that information after system access to information from the network environment, and then save the sequence of events in the (fuzzy) facts library. The fuzzy-rule-base is made up of the uncertain production vulnerabilities rules, describing the similar rules in a formally unified way, and finishing the static configuration through knowledge acquisition.

The specific configuration is given in Figure 2:

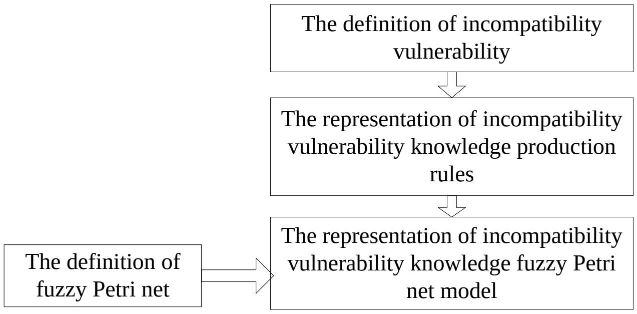

The definition of incompatibility vulnerability
The representation of incompatibility vulnerability knowledge production rules
The definition of fuzzy Petri net
The representation of incompatibility vulnerability knowledge fuzzy Petri net model

Figure 2. Uncertainty vulnerability knowledge description process base on FPN.

The definition of incompatible vulnerability gives an incompatible vulnerability semantic description and definition. Production rules extract the characteristics of the incompatible vulnerability, using the production rules to represent the incompatible vulnerability. FPN model represents the incompatible vulnerability knowledge automate convert into a reasoning FPN model of production rules.

IV. Detection Based on the FPN the Incompatibility Vulnerability

In this paper the fuzzy knowledge base and uncertainty reasoning mechanisms to detect framework design. Using fuzzy inference technology to detect vulnerabilities, solve the uncertainty from the information acquisition process uncertainty caused by noise, incomplete and other factors, using fuzzy theory to solve the vulnerability of knowledge fuzzy uncertain problems. On this basis, achieving further integration based on the FPN vulnerability knowledge representation of uncertainty reasoning and incompatibility vulnerability knowledge base checksum. FPN reasoning is a process that running in its initial condition, the dynamic behavior of the system implemented by the changes of network system identification which caused by the transfer points. First, the data file is transferred to the knowledge base given by the experts and initialization, and then match the facts with the fact base facts and rules premise. If the match is successful, you can trigger corresponding changes of the fact. Cycle following the above steps and traverse the entire fact base to complete the reasoning. In practical application, it should also consider the preservation of the fact and logic "non" and specific issues such as the number of restrictions. The uncertain inference machine determine whether the rule is activated according to the the fuzzy premise match, the confidence of the rule and the threshold value. Finally it will give the decision and its credibility value.

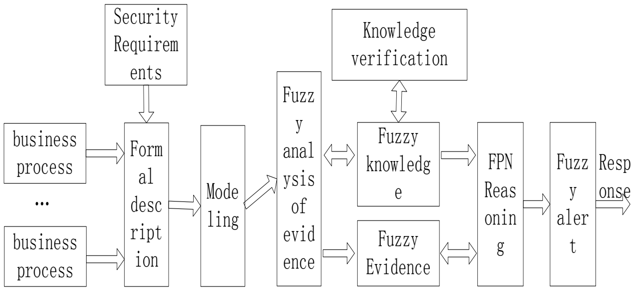


Figure 3. uncertainty vulnerability detection process base on FPN

Fuzzy rule libraries, fuzzy facts libraries as well as uncertain inference machine are the core of the fuzzy inference, epitomizes the detection mechanism and performance of the system. FPN's fuzzy features are used to express the uncertainty of production rules. Using the method that dynamic matching fuzzy knowledge base and FPN can achieve real-time parallel reasoning, greatly enhance the information processing capacity and scope of application of the active defense system. Moreover, it can find knowledge redundancy in the rules library and facts library, the fact that the library rules of conflict as well as the case of circular reasoning easier. FPN can concentrate on describing similar rules, making information abstraction of reasoning process, a higher degree of integration, and effectively solve the problem of the model expansion that makes the model more concise and intuitive.

V. Conclusion

Due to the increasing scale of the enterprise network, the incompatible vulnerability caused by inconsistent business processes resource sharing and security needs, running on a variety of business processes are increasingly complex, which seriously affect the security of enterprise networks and reliable operation.

Combining with the general business process technology, this paper proposed a new FPN model that based on the business process incompatible vulnerability, offered the definition of incompatible vulnerability incompatible, and analyzed the formation mechanism of the incompatible vulnerability. We realized the FPN mapping model of incompatible vulnerability, and proposed the incompatible vulnerability detection method based on the FPN, and built the incompatible vulnerability detection system, which can effectively detect the enterprise networks business process incompatible vulnerability according to this model.

This paper used the fuzzy knowledge representation and reasoning method, but in the actual testing process, fuzzy knowledge should be assigned through experience. In addition, our future work would pay attention to figure out how to obtain the fuzzy knowledge through machine learning methods.

ACKNOWLEDGMENT

This work was supported by the Project of National Ministry under the Grant No.A2120110006 and BIT Basic Research Fund.

REFERENCES

[1] Haibo Ma, Guangleng Xiong, Tao Li, etc. Integrated solution for the conflict in collaborative design[J]. High Technology Letter, 2001, (01) :61-65(In Chinese).

[2] Zifang Wu, Xiansheng Qin, Run Wang, etc. Concurrent engineering constraint management research[J]. Journal of Northwestern Polytechnical University, 2001,19(1):110-113(In Chinese).

[3] Tao Li, Guangleng Xiong. Conflicts arbitration strategy based optimization algorithm [J]. Chinese Journal of Computer, 2002,25(1):57-62. (In Chinese).

[4] Xiaofei Qu. Bargaining game based multiplayer multi-objective strategy[M]. Dalian University of Technology Press, 1998:93-98.Ni, Q.. Privacy-aware role-based access control[J]. ACM Transactions on Information and System Security (TISSEC).2010,13(3): 1-31(In Chinese).

[5] Wensheng Xu, Guangleng Xiong, Peisi Zhong. Negotiation Approach in parallel engineering standards Satisfaction Evaluation Space[J]. Computer Integated Manufacturing Systems, 2001,7(9):60-63(In Chinese).

[6] Xiang Li, Dongzhe Wang, Xionghui Zhou, etc. Conflict resolution in collaborative design process[J]. Aeronautical Manufacturing Technology, 2001,1:32-35(In Chinese)

[7] Klein M. Conflict Resolution in Cooperative Design[A]. Progress in Engineering-Artificial Intelligence in Engi-neering Design. Computational Mechanics[C]. 1993:17-19.

[8] Min Li,Youdong Yang,Jie Li,et al.A preliminary study on synchronized collaborative design based on heterogeneous CAD systems[A].Computer Supported Cooperative Work in Design[C],The 8th International Conference on 26-28 May 2004, Vol.2:22-27.

[9] SHARE : A Methodology and Environment for Collabora-tive Product Development[EB/OL]. http://gummo.standford.edu/html/SHARE/share.htm.

Lander S E. Issues in multiagent design systems. IEEE Expert, 1997.

[10] Serigio N,Fabio N.A Concurrent Engineering Decision Mode:Management of the Project Activities Information Flows[R].Int.J.Prodection.Economics，1988.

[11] Bo Sun, Rongguo Zhang, Yanyan Wang, Rong Wang. Fuzzy collaborative design conflict resolution method [J]. Computer Engineering and Applications, 2009(3)