Tong ZHANG, Kehe WU, Gang MA, Wei LI

North China Electric Power University

A Network Business Security Model Based on Developed BLP Model in Electric Power Enterprise

***Abstract**. The security defense of Electric Power Information Network should focus on the security of network business running on Intranet. In order to meet the special requirements of network business security in Electric Power Information Network, the access rules of network business between different security levels are researched, and a network business security model based on developed BLP model is proposed. By re-definiting the trusted subjects of BLP model, the network business security model can meet the access rules of network business between diffident security level.*

***Streszczenie.** Analizowano bezpieczeństwo i niezawodność informatycznej sieci wykorzystywanej do kontroli systemów zasilania. Analizowano systemy dostępu do sieci na różnych poziomach bezpieczeństwa. (**Model bezpieczeństwa sieci informatycznej wykorzystywanej do kontroli systemów zasilania**)*

Keywords: Information Security; Network Business Security; BLP Model
Słowa kluczowe: bezpieczeństwo informacji, sieci biznesowe.

I. Introduction

Currently, in practical application, network environment can be simply divided into two types: one is a public information network, such as the Internet, Chinanet and Cernet, which can be able to provide services of information sharing and information exchanging; the other is the Enterprise Internal Information Network (Intranet), such as Electric Power Dispatching Data Network (SPDnet) and Electric Power Integrated Data Network (SPInet) [1,2], which can work as the enterprise businesses' operating and collaborative working platform, as well as the platform of information sharing and information exchanging.

As the platform of information sharing and information exchanging [3], the information systems in public information network mainly focus on the protection of data security and network system security [4,5]. Instead, Enterprise Information System in Intranet is not only the platform for information sharing and information exchanging, but also the platform for Enterprise Production Automation System collaborating with Enterprise Management System [6]. As a result, the security defense of Intranet does not only include data security and network system security, but also include the security of network business in Intranet.

Based on the above analysis and according to the particularity of Intranet security defense, "network business security" concept is proposed. The objects of information security are defined in three aspects — data security, network system security and network business security. The proposal of "Network Business Security" concept provides theoretical basis for security defense of Enterprise Information System.

Electric Power Enterprise Information is a typical kind of Intranet, so the emphasis of security defense is also the network business security. Because of the special position of electric power industry in national economy and social life, electric power information security has special requirements, such as the requirements of ensuring the Automatic Production System absolutely safe. At present, most of Electric Power Enterprise has classified the business security area. Different security area has different defense methods. At the same time, Electric Power Enterprise use the "white list", which can prevent distrustful processes running on the Automatic Production System, in order to ensure the Automatic Production System safe. But because of the requirements of real production and management, information sharing and data transferring between different security area are needed. The BLP [7,8,9] model has regulated the access rules, but because of the requirements of real production and management in Electric Power Enterprise, the BLP model can not apply directly. In order to solve this problem, according to the special requirements of network business security in Electric Power Information Network, depending on the "white list"(trusted subjects) management method, a kind of business security model based on the developed BLP mode is proposed, providing a new kind of theoretical foundation to the Electric Power Information Security.

II. Research on network business security

A. Concept of Network Business Security

Network Business, running on network, refers to enterprise management businesses or controlling processes in Production Automation System. It can be further described as follows:

- Network Business consists of function programs running on network platform, realizing business management processes and production controlling logic in enterprise.
- In network environment, staff work in accordance with logic and rhythm of business management software or in accordance with controlling logic processes, which can constitute the realization of Network Business.
- From computer network system level, Network Business consists of network process sets, data sets and process operation sequence sets.

Based on the analysis of Network Business's concept and features, "Network Business Security" is defined as follows: Network Business Security means the business's reliability, stability and real-time in network, and also means the continuity of business processes as well as business operation's confidentiality and non-repudiation.

Network security can be further described as follows: the integrity of network process sets and data sets, the running reliability and real-time of network process set, and the non-repudiation of processes running and writing operation on data set.

B. Access Rules between different security area in Electric Power Information Network

At present, most of Electric Power Enterprise has classified the business security area. Different security area has different defense methods. But because of the requirements of real production and management, information sharing and data transferring between different security area are needed. In order to protect the confidentiality and integrity of data, the access rules are needed.

The following is the classification of business security area in Electric Power Information Network:

- Dispatching Automation System business, the core business of power grid enterprise, which has requirements of high reliability, high stability, high real-time and non-repudiation of operations, belongs to the Rank Ⅰ businesses security area.
- Dispatching Production Management System businesses, including Waterpower Dispatching Automation System, Electricity Metering System, Electricity Market Transaction system, extended EMS system and so on, are dispatching production auxiliary businesses and belong to Rank Ⅱ businesses security area, which are next to Dispatching Automation System and have requirements of reliability, stability and real-time protection.
- Power grid enterprise management businesses, including businesses of Management System, Power Marketing System, ERP system and so on, which are the main businesses of production command and management decisions, belong to the Rank Ⅲ businesses security area, having requrirements of reliability, stability, and real-time protection.
- Businesses of Comprehensive Management System, Comprehensive Data Integration System, Comprehensive Data Analysis Application in power grid enterprise, which can realize information sharing and decision support, belong to the Rank Ⅳ businesses security area.

The classification of business security area is shown in figure 1.

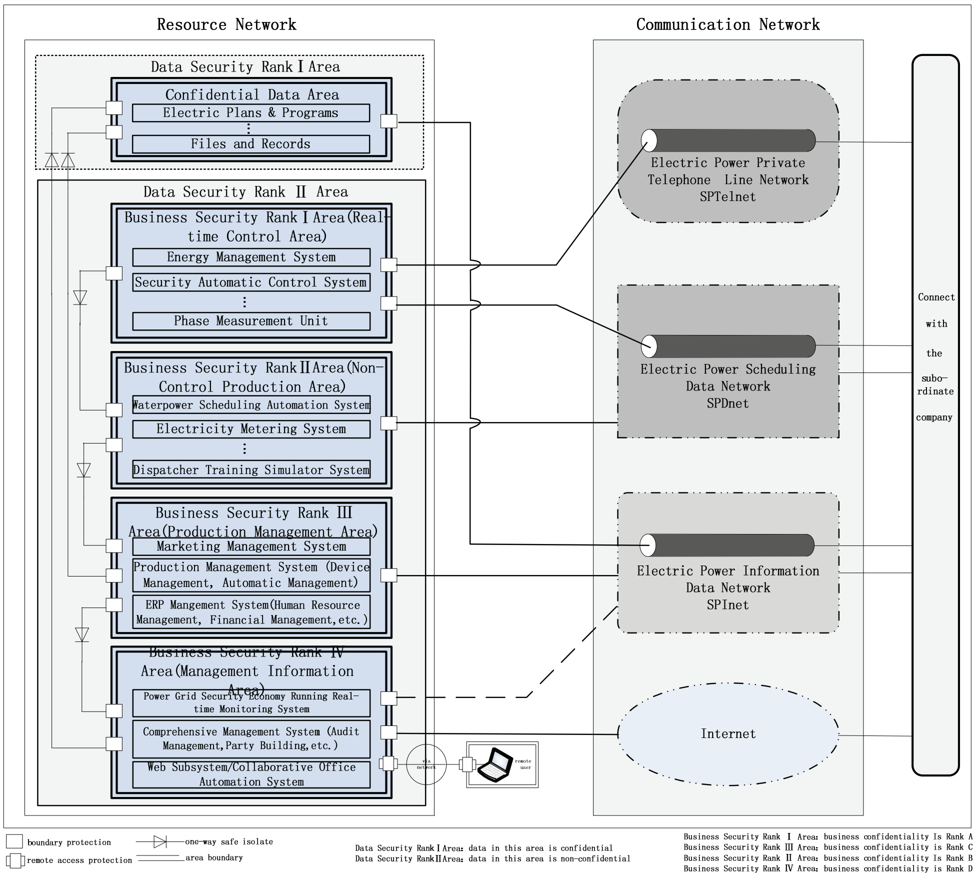
Resource Network
Communication Network
Data Security Rank Ⅰ Area
Confidential Data Area
Electric Plans & Programs
Files and Records
Data Security Rank Ⅱ Area
Business Security Rank Ⅰ Area(Real-time Control Area)
Energy Management System
Security Automatic Control System
Phase Measurement Unit
Business Security Rank Ⅱ Area(Non-Control Production Area)
Waterpower Scheduling Automation System
Electricity Metering System
Dispatcher Training Simulator System
Business Security Rank Ⅲ Area(Production Management Area)
Marketing Management System
Production Management System (Device Management, Automatic Management)
ERP Mangement System(Human Resource Management, Financial Management,etc.)
Business Security Rank Ⅳ Area(Management Information Area)
Power Grid Security Economy Running Real-time Monitoring System
Comprehensive Management System (Audit Management,Party Building,etc.)
Web Subsystem/Collaborative Office Automation System
via network
remote user
Electric Power Private Telephone Line Network SPTelnet
Electric Power Scheduling Data Network SPDnet
Electric Power Information Data Network SPInet
Internet
Connect with the subordinate company
boundary protection
remote access protection
one-way safe isolate
area boundary
Data Security Rank Ⅰ Area: data in this area is confidential
Data Security Rank Ⅱ Area: data in this area is non-confidential
Business Security Rank Ⅰ Area: business confidentiality Is Rank A
Business Security Rank Ⅲ Area: business confidentiality is Rank C
Business Security Rank Ⅱ Area: business confidentiality Is Rank B
Business Security Rank Ⅳ Area: business confidentiality is Rank D

Fig.1. The classification of business security area in Electric Power Information Network

Because of the requirements of real production and management, besides the confidentiality and integrity requirements, access rules between different security areas has special requirements:

- Network business area in lower security rank can not write the one in higher security rank.
- Network business area in higher security rank can write the one in lower security rank.

This paper mainly studys the access control model between different security areas, depending on the "white list"(trusted subjects) management method, a kind of business security model based on the developed BLP mode is proposed. Other research about the network business security will be proposed in future research work.

III. Model of Network Business Security Based on Developed BLP Model

A. BLP Model

Definition 1: The subject set is set S. $S_T \subseteq S$, is the set of trusted subjects. $S=S-ST$, is the set of distrusted subjects.The set O is the object set. The set C is the classification level set. The set K is the category set. The set L is the security level set. $L =\{(C_i ,K_j) \mid C_i \in C \wedge K_j \in K\}$. If $L1 =(C_1,K_1) \in L$, $L_2=(C_2, K_2) \in L$, then $L_1 \geq L_2$ means $(C_1>C_2 \wedge K_1 \supseteq K_2)$ [10,11].

Definition 2: $A=\{r,w,e,a\}$, is the access attribute set. r means "only read", w means "write", a means "only write", and e means "execute"[11].

Definition 3: $V=B\times M\times F\times H$, is the system state set. $B= 2^{(S\times O\times A)}$, is the power of $(S\times O\times A)$. M is the access matrix, is made up of $m_t \in A$, m_t means the access of subject s_i to object o_j. $F \subseteq L_S \times L_O \times L_S$ is the access library function, $\forall f \in (f_s, f_o, f_c)$, f_s is the function which can describe the security level of subject, f_o is the function which can describe the security level of object, f_c is the function which can describe the current security level of subject. H means the hiberarchy of current object.[11]

Any one state of the system $v = (b,M,f,H) \in V$, $b = (s_i, o_j, x) \in B$, $x \subseteq m_t$.

Property 1: Sample Safe property(ss-property): state $v=(b,M,f,H) \in V$, satisfies the sample safe property:

(1) iff for all $(s,o,x) \in b$

- $x = a$ or $x = e$
- $x = w$ or $x = r$, and $f_s(s) \geqslant f_o(o)$

Property 2: *-property: state $v=(b,M,f,H) \in V$, satisfies the *-property:

(2) iff for all $(s,o,x) \in b$

- $x = r \Rightarrow f_s(s) \geqslant f_o(o)$
- $x = a \Rightarrow f_o(o) \geqslant f_s(s)$
- $x = w \Rightarrow f_s(s) \geqslant f_o(o)$

Property 3: Discretionary Safe property(ds-property): state $v=(b,M,f,H) \in V$, satisfies the discretionary safe property.

(3) iff for all $(s_i,o_j,x) \in b$, $x \in m_t$

Definition 4: When state v satisfies the ss-property, *-property and ds-property in the same time, then v is the safe state. The state sequence Z is a safe stae sequence.

iff $t \in T$, for every $t \in T$, and $z \in Z$, v is a safe state.

Definition 5: System is $\Sigma(R,D,W,z_0)$, a safe system:

Iff every state of system $(z_0, z_1, \ldots, z_n)$ is a safe state.

Because the BLP model is too strict, the users are restricted too much. When a user operates the higher level data, he may need to operate the lower level data, but the BLP model doesn't allow the user to "write" the lower level data. However, this situation exists in the production and management of Electric Power Enterprise. For example, the management system in Rank Ⅲ area need the data of non-real production system in Rank Ⅱ area, at the same time, the non-real production system in Rank Ⅱ area need to write the data into the management system in Rank Ⅲ area. Therefore, the BLP model need to be modified to meet the special requirements of Electric Power Enterprise.

B. Network Business Security Model Based on the Developed BLP Model

The trusted subjects in BLP model can escape the restriction of *-property, that means, the trusted subjects can write the lower level objects. Because the "white list" strategy has been used widely in Electric Power Enterprise, and "white list" definite all the trusted processes, in other words, the trusted subjects. Therefore, by re-definiting the trusted subjects of BLP model, the developed BLP model can apply to protect the access between network business in diffident level.

The "white list" is: a list of all trusted processes. The trusted processes in the list is known in Electric Power Enterprise Information System, and is necessary to ensure the business operating normally. No trusted processes will bring threat to the Electric Power Enterprise Information System.

Definition 6: Trusted subjects is the trusted processes in "white list" of Electric Power Enterprise. The "white list" has been checked strictly, ensuring the behavior of trusted subjects credible. At the same time, under the control of safe strategy, the trusted subjects will not destroy the system's confidentiality, and the operation to lower level objects of trusted subjects is credible.

Definition 7: The confidentiality set C is divided into ciphertext set C_1 and plaintext set C_2, $C=C_1 \cup C_2$. C_1 is also divided into "classification ciphertext" C_{1m} (most confidential, classified and confidential) and C_{1p} (private ciphertext); and the levels of all elements in C_1 are higer then the levels of all elements in C_2.

Property 4: *'-property: state $v=(b,M,f,H) \in V$, satisfies the *'-property:

(4) iff for all $(s,o,x) \in b$

- $x = r \Rightarrow f_s(s) \geqslant f_o(o)$
- $x = a \Rightarrow f_o(o) \geqslant f_s(s)$
- $x = w \Rightarrow (\neg \exists o' \in O,\ f_o(o') \leqslant f_o(o) \wedge ((sro') \vee (swo'))) \wedge f_s(s) \geqslant f_o(o)$

So, the developed BLP model can meet the the special access rules between different security areas in Electric Power Enterprise.

C. Discussion of Network Business Security Model

Comparing with the BLP model, the network business security model can apply to meet the access rules between network business in diffident level. The network business security model has the following advantages:

- The "trusted subjects" is defined. Although the BLP model proposed the concept of "trusted subjects", it hadn't specified which subjects are trusted subjects. According to the "white list" in Electric Power Enterprise, the network business security model has defined the "trusted subjects". It has specified that the subjects in "white list" are all the "trusted subjects".
- The network business security model can meet the special security requirements of network business in Electric Power Enterprise. At present, most of Electric Power Enterprise has classified the business security area. Information transmission between different security area is needed. In some special conditions, the business in higher security area will need to write the data in lower security area. BLP model is too strict, so it couldn't meet the special requirements. The network business security model has defined the "trusted subjects" and modified the *-property of BLP model, and it can meet the special requirements.

But the network business security model also has shortcomings. This model isn't proved mathematically, and the property 4(*'-property) is described not exactly. In the future work , the model will be further improved.

IV. Case Study

In this section, we will study a case to illustrate the network business security model.

As shown in figure 1, Electric Power Information Network has been classified into four business security areas. In this case, we discuss the Power Grid Dynamic Monitoring System and Dispatching Management System. Power Grid Dynamic Monitoring System is in the business security rank I area. Dispatching Management System is in the business security rank III area. In the practical condition, businesses in Dispatching Management System should read the data of Power Grid Dynamic Monitoring System. And at the same time, businesses in Power Grid Dynamic Monitoring System should write the data of Dispatching Management System, in order to direct the dispatching management in time.

So, in this case, we define the monitoring business as the subject s_m, and define the dispatching data as the object

o_d,. $b= (s_m ,o_d , x) \in B, x \subseteq m_t$. Because Power Grid Dynamic Monitoring System is in the business security rank Ⅰ area, and Dispatching Management System is in the business security rank Ⅲ area. So, the subject s_m is in rank Ⅰ level, and the object o_d is in rank Ⅲ level. $s_m \in S_{T,}$ is a trusted subject.

When $x = w, f_s(s_m) \geqslant f_o(o_d)$ is true. And $\neg \exists o' \in O, f_o(o') \leqslant f_o(o_d) \wedge ((sro') \vee (swo')))$ is true.

So, $b= (s_m ,o_d , x)$ satisfies the property: $x = w => (\neg \exists o' \in O, f_o(o') \leqslant f_o(o) \wedge ((sro') \vee (swo'))) \wedge f_s(s) \geqslant f_o(o)$.

In this case, the subject s_m and the object o_d satisfy the network business security model. By studying this case, we can prove that the network business security model can meet the business security requirements of Electric Power Information Network.

IV. Conclusion

On the basis of the research on the access rules between different security areas in Electric Power Information Network, according to the defense emphasis of electric power information network, by studying the BLP model, a kind of network business security model based on developed BLP model is proposed. The model has brought the “white list” to the BLP model, and defined the “trusted subjects”. According to the “trusted subjects”, the model has modified the *-property of BLP model. The *'-property of developed model can allow the trusted subjects to write the lower level data. So the network business security model can apply to meet the special security requirements of network business in Electric Power Information Network. The model and research can solve the conflicts between the special access requirements and BLP model access control restriction, and can provide a new kind of theoretical foundation to the Electric Power Information Security.

Acknowledgments:

This work is partially supported by Beijing Engineering Research Center of Electric Information Technology. We would like to thank Ph.D. Hui He and anonymous reviewers for their constructive comments that greatly improved the quality of this paper.

REFERENCES

[1] José E.O. Pessanh, O.R. Saavedr, Julio C.R. Buza, Alex A. Paza, Carlos P. Pomaa. Power system stability reinforcement based on network expansion: A practical case, International Journal of Electrical Power & Energy Systems, 3(2007), No.29,208-216

[2] Nicol, David M.,Davis, Charles M.,Overbye, Tom . A tested for power system security evaluation, International Journal of Information and Computer Security,2(2009),No.3,114-131

[3] DongHui Jiang. Security Offense and Defense Testing and Analysis of LAN, Science&Technology Information, 2009, 125-128

[4] Sahar Selim, Mohamed Hashem, Taymoor M. Nazmy . Intrusion Detection using Multi-Stage Neural Network, International Journal of Computer Science and Information Security, 4(2010), No.8, 14-20

[5] YuanFei Huang, LiYong Ji, LiPing Jin. Investigation of Network Information Security Situation and Hot Issues, Telecommunications Science, 2009, 213-216

[6] XingHua Chen. Enterprise Network Information Security and Countermeasure Study, Agriculture Network Information ,2009, 431-437

[7] Chao Li. Simple Exploration of Network Information Security, Scientific&Technological Information Development and Economic, 2009, 97-101

[8] HongSheng Yan, XueLi Wang, Jun Yang. Computer Network Security and Defense, Electronics Industry Press,2007, 45-49

[9] R.Sandhu, V.Bhamidipati, E.Coyne. The ARBAC97 Model for Role-Based Administration of Roles: Preliminary Description and Outline, Proc. IEEE Symp. Proceedings of Second ACM Workshop on Role-Based Access Control, 1997, 41-49.

[10]WANG Fei, LV Hui-jun, SHEN Chang-xiang. Terminal Categorial Data Protection Based on Trusted Computing, Computer Engineering,2008,133-135

[11]D.E.Bell, L.LaPaDula. Secure Computer Systems: Mathematical Foundations and Model,Technical Report M74～244, Mitre Corp. , Bedford, MA, May 1973.

Authors

Ph.D. Tong Zhang, Control and Computing Engineering School of North China Electric Power University, E-mail:zhtzhangtong@163.com; Prof. Kehe Wu, Deputy Dean of Control and Computing Engineering School, North China Electric Power University, E-mail:epuwkh@126.com; Ph.D. Gang Ma, Control and Computing Engineering School of North China Electric Power University, E-mail:hdmagang@163.com; Associate Prof. Wei Li, Control and Computing Engineering School of North China Electric Power University, E-mail:liwei@ncepu.edu.cn.