Access Control Capability Assessment Method Based on Security Entropy

Tianwei Che
School of Computer Science and Technology, Xidian University, Xi'an, China
Email:tianweiche@163.com

Jianfeng Ma
School of Computer Science and Technology, Xidian University, Xi'an, China
Email:jfma@mail.xidian.edu.cn

Na Li
School of Computer Science and Technology, Northwestern Polytechnical University, Xi'an , China
Email:tao_lina@163.com

Chao Wang
The Information Engineering University, Zhengzhou, China
Email:wangchao302@sina.com

[1]***Abstract*—In this paper, we propose analysis methods based on security entropy to overcome the problem of quantitative analysis, after going through the study of access control capability assessment for computer information system. At First, we computed the uncertainty how system determine irregular access behavior using the security entropy theory. Next, we defined the security theorem of classificatory information system, and proposed the standard of access control capability. Finally, we analyzed the typical access control models using the methods, and compared security and applicability of them. It proved that the method is appropriate for security quantitative analysis of access control model and for the evaluation of access control capability in information system.**

***Index Terms*—Information entropy; Security entropy; Classificatory access control model; Direct unauthorized access; Right about access; Indirectly unauthorized access**

I. INTRODUCTION

The key to prove the access control model security is to find a recognized and self-evident security axiom, which can be used to deduce or prove security assumptions proposed in the model, so as to make it more reliable. However, even the formally proved BLP model [1,2] can't prove the rationality, completeness and safety of "simple security axiom" and " * - property axiom", which is proposed by BLP model. Therefore, some scholars point out that the security axioms of BLP[3] cannot completely prove the security of BLP. A complete access control model must clearly tell us which security requirements to be met, *what* access violation to be prevented, and how to reduce the uncertainty of the access violation *that* the system allows.

Entropy is the tool for measuring uncertainty, which is originally used in thermodynamics. An American mathematician, Claude Shannon, introduced it to the information theory, and put forward the concept of information entropy for disordered degree of information [4]. Since the information entropy theory is proposed, *it* has been applied to many fields such as Engineering Science and Social Science. Some scholars have successfully introduced it into the quantification analysis of information security risk and event uncertainty [5-7].

In this paper, we put forward the concept of security entropy and measures the uncertainty of system's response to access violations, based on the thought and method where information entropy measures the uncertainty of things, so as to provide a scientific method for the safety analysis of classificatory access control model.

II. SECURITY ENTROPY

A. Definition of Security Entropy

In the information system, when a user sends out an access request, the system will respond in two ways: to allow or to deny. The access request is also divided into two types: legal request or illegal request. If we take the system as a black box, the system will give four kinds of responses to a user's every access request: allow legal access, refuse legal access, allow access violation and refuse access violation. Obviously, the response can be considered as the basis for judging whether a system is

Supported by "National Natural Science Foundation of China (60872041, 61072066)"
Supported by "Fundamental Research Funds for the Central Universities (JYl0000903001, JYl0000901034)"
Email address:tianweiche@163.com

doi:10.4304/jcp.9.12.2804-2808

good. The more denial responses legal access gets, the poorer availability the system has.

In order to comprehensively measure the uncertainty of a system's response to various access requests, the security entropy is defined as follows:

Definition 1 (security entropy): If a group of access request like $B = b_1, b_2, ..., b_q$ is seen as the input, and the system's request responses to each access result is taken as the object of study and the variable X as the response results, then there will be four values for X: allow legal access, ~~to~~ deny legal access, allow illegal access, and deny illegal access, which are recorded as a_1, a_2, a_3, a_4 respectively. If we use Symbol p(ai) to represent statistical probability of ai, then the probability space [X, p(X=ai)] of X will be

$$\begin{bmatrix} X \\ P(x) \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ p(a_1) & p(a_2) & p(a_3) & p(a_4) \end{bmatrix}$$

$$p(a_i) \geq 0 \ (i=1,2,3,4), \sum_{i=1}^{4} p(a_i) = 1 .$$

We assign a weight w_i, the impact factor of the system security, for each response result. The greater w_i is, the higher a_i's influence on system safety will be, and vice versa. If the distribution of w_i is

$$\begin{bmatrix} X \\ w \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ w_1 & w_2 & w_3 & w_4 \end{bmatrix} , \quad 0 \leq w_i \leq 1 , \quad \sum_{i=1}^{4} w_i = 1 ,$$

The security entropy of X will be:

$$H(X) = -\sum_{i=1}^{4} w_i p(a_i) \log p(a_i) \qquad (1)$$

B. The Meaning of Safety Entropy

Based on common sense of information security, the response a_2 gives negative effects on the usability of the system, and the response a_3 gives negative effects on the confidentiality of the system, meanwhile the response a_1 and a_4 has less influence on system security. Therefore, if we let $w_2, w_3 \square w_1, w_4$, the meaning of safety entropy in formula (1) will be the average uncertainty of harmful responses occurring. The bigger value security entropy has, the higher uncertainty a harmful response will occur. On the other hand, the smaller value security entropy has, the lower uncertainty a harmful response will occur. As for the same set of access request, the smaller the security entropy of different access control model is, the less possibility model will make harmful response.

If we make $w_2 > 0, w_3 > 0, w_1 = w_4 = 0$, and at the same time $w_2 + w_3 = 1$, then security entropy can be used to judge whether the system satisfies usability and confidentiality. If $w_2 = 1, w_3 = w_1 = w_4 = 0$, security entropy of formula (1) can be used to judge whether the system satisfies usability. If $w_3 = 1, w_1 = w_2 = w_4 = 0$, security entropy of formula (1) can be used to judge whether the system satisfies confidentiality.

The number of the four responses is related to the number of input samples. If all input samples are legal access, then a3 and a4 will be 0. If all input samples are illegal access, the a_1 and a_2 will be 0. In order to make the safety entropy accurately reflect the system security, the input samples must be complete. In addition, the responses are related to the number of input samples. If the input number of the access request is much way more than others, the response will be distorted.

Therefore, when security entropy is calculated, the input samples (access requests) must be complete and its probability distribution must be uniform.

When the security entropy is smaller, there will be less uncertainty of harmful response to the system, hence the security of the model becomes better. When the security entropy approaches 0, the model will achieve the theoretical security.

C. Security Entropy of Different Types of Illegal Accesses

Whether an access is illegal or not is related to security requirements. According to the access control requirements from National Grade of Protection Standard GB17859-1999[8], illegal access can be classified into three types: direct legal access, right about access, and indirect legal access. The "direct legal access" refers to explicitly violating the authorized strategy such as the access control matrix and so on.

The "right about access" refers to the one which leads to violating information flow direction that the system stipulates, or in other words, the one which leads information flow from higher class to lower class. The "indirect legal access" refers to the one that violates the authorized strategy through information indirect transmission.

For instance, there are two users(s_1、s_2) and two resources (o_1、o_2) in the information system, and the relationship between each security level is $f(s_1) \triangleright f(s_2) \triangleright f(o_1) = f(o_2)$. The authorized system strategy is that "s_1 reads o2", "s2 reads o1", "s2 writes o2".

Let's see the following four events: b1: s2 reads o1,b2: s2 writes o2,b3:s1 reads o2,b4:s1 reads o1. Since b4 explicitly violates the authorized strategy, b4 is therefore "direct legal access"; the sequence of access b1b2b3 causes the information to flow from s1 to o1, which equals ~~that~~ to s1 reading o1 indirectly. Therefore b1b2b3 is "indirect legal access". b1 and b3 causes the information flowing to the violation in the direction stipulated by the system, so b_1 and b_3 is "right about access".

For different types of legally access, the meaning of (1) is different. If the legal access is defined as "direct legal access", then the security entropy of (1) is called "direct security entropy" being recorded as $H_D(X)$.

Again, if the illegal access is defined as "right about access", then the security entropy of (1) is called "mandatory security entropy" recorded as $H_M(X)$. If the legal access is defined as "indirect legal access", then the security entropy of (1) is called "indirect security entropy"

recorded as $H_I(X)$.

III. Safety Conditions Of Classificatory Access Control Model

A. Security Attributes Based On Security Entropy of Safety

$$H_D(X) = -\sum_{i=1}^{4} w_i p(a_i) \log p(a_i) \equiv 0,$$

$w_2 > 0, w_3 > 0, w_2 + w_3 = 1$。

Theorem 1 (direct safety of access control model): Access control model has direct safety, if and only if

$$H_D(X) = -\sum_{i=1}^{4} w_i p(a_i) \log p(a_i) \equiv 0, \text{ in which}$$

$w_2 > 0, w_3 > 0, w_2 + w_3 = 1$。

Prove:

Here we need to prove that when $H_D(X) = 0$, the event "refuse legal access" and "allow access violation" will never happen, that is, $p(a_2) = p(a_3) = 0$.

We mark the total number of ai as ni(i=1,2,3,4), $n_1 + n_2 = s$, $n_3 + n_4 = t$, since a1, a2, a3 and a4 are different responses to the same access, $p(a_1) + p(a_2) = s/q$, $p(a_3) + p(a_4) = t/q$.

Based on common sense, access requests can't be all legal or all illegal, so $s, t > 0$. Since $\sum_{i=1}^{4} p(a_i) = 1$, $p(a_2) \neq 1, p(a_3) \neq 1$.

Since $w_2 > 0, w_3 > 0, w_2 + w_3 = 1$,so $w_1 = w_4 = 0$.

End.

Similarly, we can get theorems as follows:

Theorem 2 (mandatory safety of access control model): the access control model has mandatory safety, if and only if

$$H_M(X) = -\sum_{i=1}^{4} w_i p(a_i) \log p(a_i) \equiv 0, \text{ in which}$$

$w_2 > 0, w_3 > 0, w_2 + w_3 = 1$.

Theorem 3 (indirect safety of access control model): the access control model has indirect safety, if and only if

$$H_I(X) = -\sum_{i=1}^{4} w_i p(a_i) \log p(a_i) \equiv 0, \text{ in which}$$

$w_2 > 0, w_3 > 0, w_2 + w_3 = 1$.

B. Safety Theorem of Classificatory Access Control Model

Symbol Θ_2 represents class 2 access control model, Θ_3 represents class 3 access control model, and Θ_4 represents class 4 access control model.

Now, according to the safety needs of class 2, 3 and 4 information system, we put forward the safety theorem of classificatory access control model based on the above security attributes.

Theorem 4 (safety of classificatory access control model): Class 2 access control model Θ_2 satisfies safety needs, if and only if $H_D(X) | \Theta_2 \equiv 0$,in which $w_2 > 0, w_3 > 0, w_2 + w_3 = 1$;Class 3 access control model Θ_3 satisfies safety needs, if and only if $H_D(X) | \Theta_2 \equiv 0$ and $H_M(X) | \Theta_3 \equiv 0$,in which $w_2 > 0, w_3 > 0, w_2 + w_3 = 1$;Class 4 access control model Θ_4 satisfies safety needs, if and only if $H_D(X) | \Theta_4 \equiv 0$、$H_M(X) | \Theta_4 \equiv 0$ and $H_I(X) | \Theta_4 \equiv 0$,in which $w_2 > 0, w_3 > 0, w_2 + w_3 = 1$;

IV. Analysis Of Typical Access Control Model Based On Security Entropy

Now we apply the theory to analyze the security of typical access control model, in order to verify the practicability of this method, and to point out the disadvantages of each access control model.

A. Security Analysis to HRU MODEL

(1) Direct safety

Suppose there are m users in the system: $u_1, u_2, \ldots, u_m$, and n resources: $o_1, o_2, \ldots, om$, then access requests can be divided into reading and writing atomic requests; and there will be 2mn access request requests, which can be expressed respectively with symbol $b_1, b_2, \ldots, b_q$ (q=2mn). Results of the access can be divided into two types: legal access $B^+ = b_1^+, b_2^+, ..., b_s^+$, and direct legal access $B^- = b_1^-, b_2^-, ..., b_t^- (s + t = q)$.

Based on the access control matrix, HRU[9] controls access behaviors. As long as access behaviors disobeys the policy, it will be refused. So the responds to any $b_j^- \in B^-$ is a_4;As long as access behaviors obeys the policy, it would be allowed. Thus ~~so~~ the responds to any $b_i^+ \in B^+$ is a_1, and so $p(a_2)$=0 and $p(a_3)$=0.

The statistical probability distribution of responses is

$$\begin{bmatrix} X \\ P(x) \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ \frac{s}{q} & 0 & 0 & \frac{t}{q} \end{bmatrix}$$

Since $H_D(X) | \text{HRU} \equiv 0$, the model HRU can satisfy direct safety.

(2) Mandatory safety

Suppose we divide all requests $B = b_1, b_2, ..., b_q (q = 2mn)$ into three kinds: the request $B^{\uparrow} = \{b_1^{\uparrow}, b_2^{\uparrow}, ..., b_{q/3}^{\uparrow}\}$ that causes information to flow from low level to high level, the request $B^{\downarrow} = \{b_1^{\downarrow}, b_2^{\downarrow}, ..., b_{q/3}^{\downarrow}\}$ that causes information to flow from high level to low level, and the request $B^{\leftrightarrow} = \{b_1^{\leftrightarrow}, b_2^{\leftrightarrow}, ..., b_{q/3}^{\leftrightarrow}\}$ that causes information to flow between the same levels. Obviously, request $B^{\downarrow}$ in the second kind is a "right about access".

Since the model HRU judges the legality of the access request by visiting the access control matrix,

the access request $b_i^{\uparrow}$ and $b_1^{\leftrightarrow}$ *does* not necessarily satisfy the access control matrix, and it may be refused or be allowed, so $p(a_2) \equiv 0$ can not be always deduced.

(3) Indirect safety

"Indirect illegal access" is composed of several direct non-illegal accesses, so it can be denoted as $f_i^- = b_{i_1}^+ b_{i_2}^+ ... b_{i_q}^+ (b_{i_1}^+, b_{i_2}^+, ..., b_{i_q}^+ \in B^+)$. For $H_D(X) \mid \mathrm{HUR} \equiv 0$, the system will allow every direct non-illegal access in f_i^-. Consequently, f_i^- will be allowed, therefore $p(a_3) > 0$ is deduced.

With $H_I(X) \mid \mathrm{HRU} > 0$, it shows that HRU model doesn't satisfy indirect safety.

Through analysis we can conclude that the model HRU satisfies direct safety, but it doesn't satisfy mandatory safety and indirect safety.

B. Security Analysis to BLP

(1) Direct safety and indirect safety

The model BLP uses two methods: DAC and MAC. DAC uses the HRU model, so the direct safety and the indirect safety of the BLP model coincide with that of the HRU, which means BLP satisfies direct safety but doesn't satisfy indirect safety.

(2) Mandatory safety

The BLP model forbids high level subjects writing low level objects and vice versa, and prevents the information flowing from high level into low security level. Therefore any "right about access" $b_i^{\downarrow} \in B^{\downarrow}$ will be refused by BLP, and any non "right about access" $b_i^{\rightarrow} \in B^{\leftrightarrow}$ and $b_i^{\uparrow} \in B^{\uparrow}$ will be allowed. Consequently, the probability distribution of BLP's response X is

$$\begin{bmatrix} X \\ P(x) \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ \frac{2q}{3} & 0 & 0 & \frac{q}{3} \end{bmatrix}$$

So $H_M(X) \mid \mathrm{BLP} \equiv 0$, and it shows that BLP satisfies mandatory safety.

C. Security Analysis to RBAC

The model RBAC[9,10] assigns a role for the user, and then grants authorization based on these roles . The RBAC's rights management and access control manner are similar to HRU's. Thus its safety is similar to that of HRU, which satisfies direct safety but not mandatory safety and indirect safety.

D. Security Analysis to FGBAC

The FGBAC[12] is the improved BLP, which introduces the information flow graph as a judgment auxiliary tool. In FGBAC, any "direct illegal access", "right about access" or "indirect illegal access" will be refused. So

$$\begin{aligned} & H_D(X) \mid \mathrm{FGBAC} \\ &= H_M(X) \mid \mathrm{FGBAC} \\ &= H_I(X) \mid \mathrm{FGBAC} \\ &\equiv 0 \end{aligned}$$

It shows that the model satisfies direct safety, mandatory safety and indirect safety.

According to the above safety analysis of the typical access control model, and in the light of the safety needs of 2, 3 and 4 class systems, we conclude the typical model' security and applicability as below:

TABLE I
THE SECURITY OF TYPICAL ACCESS CONTROL MODEL

typical access control model	direct safety	mandatory safety	indirect safety
HUR	satisfy	not satisfy	not satisfy
RBAC	satisfy	not satisfy	not satisfy
BLP	satisfy	satisfy	not satisfy
FGBAC	satisfy	satisfy	satisfy

TABLE II
THE APPLICABILITY OF TYPICAL ACCESS CONTROL MODEL

typical access control model	Scope of application
HUR	Class 2
RBAC	Class 2
BLP	Class 3
FGBAC	Class 4

V. CONCLUSION

This paper puts forward the concept of "security entropy" for measuring uncertainty of system's response to access request, and proposes its security theorems based on security entropy. The theory can be widely applied to security analysis of access control mode and system.

Based on the theory,this paper analyses the typical access control model, verifies the practicability of the method, and concludes the security and application scope of the available models.

ACKNOWLEDGMENT

The research in this paper is supported by National Natural Science Foundation of China via grants numbers 60872041, 61072066 and Fundamental Research Funds for the Central Universities (JYl0000903001.JYl0000901034).

REFERENCES

[1] BELL D E,LAPADULA L J. Secure Computer Systems: Mathematical Foundations[R]. Technical Report M74-244,The MITRE Corporation, Bedford, Massachusetts, 1973.

[2] David Elliott Bell, Looking Back at the Bell-La Padula Model[J]. Reston VA, 20191,December 7,2005.

[3] Si Tian-Ge, Tan Zhi-Yong, and Dai Yi-Qi A Security Proof Method for Multilevel Security Models[J]. Journal of Computer Research and Development, 2008,45(10): 1711-1717 (in Chinese).

[4] FU Zu-yun. Information theory—basic theory and application[M]. BEIJING: Publishing House of Electronics Industry,2007 (in Chinese).

[5] Wang Guibao,Huang Hongzhong,Zhang Xiaoling. Risk Possibility Number--A New Model for Risk Evaluation

and Prioritization Based on Maximum Entropy Theory. ACTA AERONAUTICA ET ASTRONAUTICA SINICA. 2009,30(9):1684-1690 (in Chinese).
[6] Fu Yu,Wu Xiao-Ping ,Ye Qing,Peng Xi. An Approach for information Systems Security Risk Assessment on Fuzzy Set and Entropy-Weight. ACTA ELECTRONICA SINICA. 2010,38(7):1490-1494(in Chinese).
[7] Zhao Dong-Mei,Ma Jian-Feng, Wang Yue-Sheng. Model of fuzzy risk assessment of the information system. Journal on Communications. 2007, 28(4):51-56(in Chinese).
[8] GB/T 17859-1999. Classified criteria for security [S]. BEIJING: Standards press of china,1999 (in Chinese).
[9] P. Denning, Third Generation Computer Systems[J], Computer Surveys. 1971,3(4):175-216.
[10] Sandhu R S, Coyne E J, Feinstein H L. Role-based access control models[J]. IEEE Computer, 1996,29(2):38-47.
[11] Haibo Gao, Wenjuan Zeng, Xiaohong Deng. The Design and Simulation of a New Dynamic Credit and Role based Access Control Strategy. Journal of Computer .2014,Vol 9,No.2 :506-510.
[12] Bailing Liu. Efficient Trust Negotiation based on Trust Evaluations and Adaptive Policies. Journal of Computer.2011, Vol 9,No.1:222-227.
[13] Wang Chao, CHEN Xing-yuan, LI Na. An access control mode based on information flow graph[C]// Proceedings of the International Conference on Computational Intelligence and Security. SANYA, CHINA,2011,998-1000.
[14] Huawang Shi, Wanqing Li. Risk Assessment for Construction Projects Contracting Based on Unascertained Sets. Journal of computers.2011,Vol6,No.11:2446-2453.

Tianwei Che was born in Xi'an, Shaanxi Province of China in 1971. He received the master degree in computer network and information security from the Information Engineering University, Zhengzhou, China in 2003. He is current Ph.D. candidate studying at School of Computer Science and Technology, Xidian University, and his supervisor is Prof. Jianfeng Ma. His main research interests include computer architecture, information security, and cloud computing.

Jianfeng Ma was born in Xi'an, Shaanxi Province of China in 1963. He received his Bachelor of Science degree from the Department of Mathematics at the Shaanxi Normal University in July 1985; obtained his Master of Engineering degree in computer software from the Department of Computer software from the Department of Computer Science and Technology, Xidian University in March 1988. He earned his Doctorate of Engineering in communication and electronic system from the Department of Information Engineering, Xidian University. His major research fields include computer architecture, cryptology, information security, cloud computing and system survivability.

He is Inside-school specially appointed professor; advisor of Ph.D candidates of computer system architecture and cryptology; director of the Ministry of Education /Ministry of Information Industry Key Laboratory of Computer Network and Information Security; dean of the School of Computer Science and Technology; outstanding returned student of Shaanxi province.

Prof. Ma has published 7 books, and more than 200 research papers in journals and international conferences. In addition, Prof. Ma is the committee members of ernational Journals.

Na Li was born in Xi'an, Shaanxi Province of China in 1972. She received the master degree in computer network and information security from the Information Engineering University, Zhengzhou, China in 2004. She is currently Ph.D. candidate studying at School of Computer Science and Technology, Northwestern Polytechnical University, Xi'an, China. Her main research interests include computer information security and software Engineering.

Chao Wang was born in Zhengzhou, Henan Province of China in 1975. He received his Ph.D. degree in network and information security from the Information Engineering University, Zhengzhou, China in 2003. He works now as the associate professor in the Information Engineering University. He has published 3 books, and more than 10 research papers in journals and international conferences. His main research interests include computer architecture, information security, cloud computing.