A Security Quantitative Analysis Method For Access Control Based on Security Entropy

Tian-Wei Che[1], Jian-Feng Ma[1], Na Li[2], Chao Wang[3]
(Corresponding author: Tian-Wei Che)
School of Computer Science and Technology, Xidian University, Xi'an, Shanxi, China[1]
(Email: tianweiche@163.com)
School of Computer Science and Technology, Northwestern Polytechnical University, Xi'an, Shanxi, China[2]
The information Engineering University, Zhengzhou, Henan, China[3]
(Received May 9, 2014; revised and accepted Jan. 16 & Apr. 21, 2015)

Abstract

This paper has proposed a quantitative analysis method based on security entropy to work out the problem of quantitative analysis in classificatory information systems. Firstly, the security theorems of classificatory information systems have been defined, the uncertainty for the system's determinations on the irregular access behaviors by means of the theory of security entropy have been calculated. Then a security quantitative analysis method has been proposed. By the security method, the typical access control models have been analyzed, security and applicability of these models have been compared. Finally, the method's practicability is validated and has been proved to be suit for security quantitative analysis on access control model and evaluation to access control capability in information system.

Keywords: Access control model, access violations, security entropy, unauthorized access

1 Introduction

Access control is a kind of security technology to achieve the established security strategy. The goal is to prevent users from unauthorized access to information resource. On the basis of the security policy to control user's access behavior, access control capability is directly related to the system access control of information system security attributes such as confidentiality, integrity. Access control is one of the five basic ISO7498-2 security services. There are several forms of unauthorized access in the system, such as explicitly access behavior, indirect access behavior in violation of the access control matrix and other access behavior in violation of information flow. Under normal circumstances, since there are obvious differences to detect these unauthorized access behavior's methods and models, so a problem which we had to face is how to quantify and measure an access control system (or model) for different unauthorized access behavior, in other words, how to calculate the possibility of uncertainty for all kinds of unauthorized access behavior in a system.

Classic access control model mainly has the BLP model, access control matrix model [3, 8], no interference model , RBAC [11] and so on. But research on the model of security measure theory of access control is still insufficient and inadequate, only for a single access to identify behavior is illegal, and fail to prevent unauthorized access behavior indirectly. Even recognized safety higher BLP model [3, 11] also can only prevent information flow from high level security to low security level by the indirect unauthorized access behavior and how to control Effectively indirect unauthorized access behavior to cause the data flow between subject and object in the same security level is powerless.

Due to the lack of safety for quantitative analysis and test method of access control strategy, for the information system managers' selection and application of appropriate access control policy or security mechanism caused confusion and difficulties. Because the information entropy theory has been applied in many fields, so far Information entropy has been successfully introduced it into the quantification analysis of information security risk and event uncertainty [4, 6, 7, 14]. On the basis of the information entropy can be measured the uncertainty things, an access control capability evaluation method is proposed which provides a scientific method for the quantitative analysis of hierarchical security access control model.

2 Weighted Entropy

Information Entropy is the tool to evaluate average uncertainty of event. Its definition is as follows, Let X be discrete random information source, its symbol set be $K : k_i$ $(i = 1, 2, \cdots, q)$, q is size of symbol set, the probability of event k_i is $P(k_i)$, its probability space $[X, p(x)]$ is defined

as:

$$\begin{bmatrix} X \\ P(x) \end{bmatrix} = \begin{bmatrix} k_1 & k_2 & \cdots & k_q \\ p(k_1) & p(k_2) & \cdots & p(k_q) \end{bmatrix}$$

The discrete random information source's information entropy is:

$$H(X) = -\sum_{i=1}^{q} p(x_i) \log p(k_i),$$

where $p(k_i) \geq 0 (i = 1, 2, \cdots, q)$ and $\sum_{i=1}^{q} p(x_i) = 1$.

In real environment, although the stochastic event happened with certain probability, but different event has different value and effect to people, and is of different importance. It is hard to ignore human factors. So, assign a nonnegative real $w_i \geq 0$ $(i = 1, 2, \cdots, q)$ to event k_i, the set of real is called weight of event. Let weight of information source's distribution $[X, w_i]$ be

$$\begin{bmatrix} X \\ w \end{bmatrix} = \begin{bmatrix} k_1 & k_2 & \cdots & k_q \\ w_1 & w_2 & \cdots & w_q \end{bmatrix}$$

Then information resource X's weighted entropy is

$$H_w(X) = -\sum_{i=1}^{q} w_i p(x_i) \log p(k_i).$$

3 Security Entropy

3.1 The Types of Access Security

In the information system, the access request is divided into two types: "legal" and "illegal", and the system's responds to user access request will be "allow" or "deny". So the response will be the four types: k_1 (allow legally access), k_2 (refuse legally access), k_3 (allow access violation) and k_4 (refuse access violation). Obviously, the response can be considered as a basis for judging if a system is good or bad. The more the denial responses to legitimate access gets, the poorer the system availability is. The more the allowable responses to violation access gets, the worse the system's confidentiality is.

In general, illegal access can be classified into three types:

1) Directly legally access;

2) Right about access;

3) Indirectly legally access.

The directly legally 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, in other words, the one which leads information flow from high class to low class. The indirectly legally access refers to the one that violates the authorized strategy through information indirect transmission.

For instance, there is two users (u_1, u_2) and two resources $o_1, o_2)$ in the information system, and the relationship of security level is $f(u_1) \triangleright f(u_2) \triangleright f(o_1) = f(o_2)$, the authorized strategy of the system is that "u_1 read o_2", "u_2 read o_1", "u_2 write o_2".

The following are four events:

1) $b_1 : u_2$ read o_1;

2) $b_2 : u_2$ write o_2;

3) $b_3 : u_1$ read o_2;

4) $b_4 : u_1$ read o_1.

Because b_4 explicitly violates the authorized strategy, b_4 is therefore directly legally access; the Sequence of access $b_1 b_2 b_3$ cause the information to flow from u_1 into o_1, which equals that u_1 read o_1 indirectly. Therefore $b_1 b_2 b_3$ is indirectly legally access. b_1 and b_3 cause the information flowing to the violation of the direction made by the system, so b_1 and b_3 are right about access.

3.2 Definition of Security Entropy

Definition 1. *(Security Entropy) If the whole access requests are seen as the input, the system's request responses to each access result as the object of study, and the variable X as this response results, then the value of X will be: k_1, k_2, k_3, k_4. If the Symbol p_i stands for the statistical probability of k_i, and $p_i \geq 0$ $(i = 1, 2, 3, 4)$, $\sum_{i=1}^{4} p_i = 1$. Let $0 \leq w_i \leq 1$, $\sum_{i=1}^{4} w_i = 1$, the security entropy of X will be*

$$H(X) = -\sum_{i=1}^{4} w_i p_i \log p_i. \quad (1)$$

The w_i is the impact factor of the system security. The greater w_i is, the higher the k_i's influence to system safety is, otherwise the smaller the k_i's influence is. According to the common sense of information security, the response k_2 gives negative effects on the usability of the system, and the response k_3 gives negative effects on the confidentiality of the system, while the response k_1 and k_4 have less influence on system security. Therefore, if we let $w_2, w_3 \gg w_1, w_4$, the meaning of safety entropy in Equation (1) is the average uncertainty of the happened harmful responses. The bigger the value of security entropy is, the more the harmful response uncertainty is; the smaller the value of security entropy is, the less the response uncertainty is. As for the same set of access request, the smaller the security entropy of different access control model is, the less the possibility that model make harmful response is.

If $w_2 > 0$, $w_3 > 0$, $w_1 = w_4 = 0$, and at the same time $w_2 + w_3 = 1$, security entropy is the ground on which the system satisfies usability and confidentiality. If $w_2 = 1$, $w_3 = w_1 = w_4 = 0$, security entropy of Equation (1) will be the ground on which the system satisfies usability. If

$w_3 = 1$, $w_1 = w_2 = w_4 = 0$, security entropy of Equation (1) will be the ground on which the system satisfies confidentiality.

The number of the four responses is related to the number of input samples. If all input samples are legitimate accesses, k_3 and k_4 will be 0, and if all input samples are illegal access, k_1 and k_2 will be 0. In order to make the safety entropy reflect accurately the system security, the input samples must be complete. In addition, the responses are related to the number of input samples. If an input number of the access request is much 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. The smaller the security entropy is, the less the Uncertainty of the harmful response that system do to is, the more the security of the model is. When the security entropy approaches 0, then the model will achieve the theoretical security.

3.3 Security Entropy of Different Types of Illegal Accesses

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

Again, if the legally access is defined as "right about access", the security entropy will be $H_M(X)$: Mandatory security entropy. To "indirectly legally access", the security entropy will be $H_I(X)$: Indirectly security entropy.

4 Safety Theorem

Theorem 1. *(Direct Safety of Access Control Model) Access control model is direct safety, if and only if*

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

in which $w_1 = w_4 = 0$, $w_2 \neq 0$, $w_3 \neq 0$, $w_2 + w_3 = 1$.

Proof. Here we need to prove that when $H_D(X) \equiv 0$, the event "refuse legally access" and "allow access violation" will never happen, that is, $p_2 = p_3 = 0$. Because $w_1 = w_4 = 0$, so

$$H_D(X) = -w_2 p_2 \log p_2 - w_3 p_3 \log p_3.$$

If $H_D(X) \equiv 0$, must be $p_2 = p_3 = 0$. 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*

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

in which $w_1 = w_4 = 0$, $w_2 \neq 0$, $w_3 \neq 0$, $w_2 + w_3 = 1$.

Theorem 3. *(Indirectly Safety of Access Control Model) The access control model has indirectly safety, if and only if*

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

in which $w_1 = w_4 = 0$, $w_2 \neq 0$, $w_3 \neq 0$, $w_2 + w_3 = 1$.

5 Analysis of Typical Access Control Model Based on Security Entropy

Now, we apply the theory to analyze the security of typical access control model, verify the practicability of this method, and point out the defect of these access control model.

5.1 Security Analysis to HRU Model

Directly Safety. Suppose there are m users in the system: $u_1, u_2, \cdots, u_m$, n resources: o_1, o_2, $\cdots$, o_n. Access requests can be divided into read and write atomic request, so there will be $2mn$ access request, which can be expressed respectively by symbol $b_1, b_2, \cdots, b_q$ $(q = 2mn)$. Results of the access can be divided into two kinds: legitimate access $B^+ = b_1^+, b_2^+, \cdots, b_s^+$, and direct legally access $B^- = b_1^-, b_2^-, \cdots, b_t^-$ $(s + t = q)$.

Based on the access control matrix, HRU [6] controls access behaviors. As long as access behaviors disobey the policy, it would be refused. So the responds to any $b_j^- \in B^-$ is k_4. As long as access behaviors don't disobey the policy, it would be allowed, so the responds to any $b_t^+ \in B^+$ is k_1, so $p_2 = 0$ and $p_3 = 0$.

The statistical probability distribution of responses is

$$\begin{bmatrix} X \\ P(x) \end{bmatrix} = \begin{bmatrix} k_1 & k_2 & k_3 & k_4 \\ \frac{s}{q} & 0 & 0 & \frac{t}{q} \end{bmatrix}$$

Since $H_D(X)|HRU \equiv 0$, the model HRU is direct safety.

Mandatory Safety. Divide all requests $B = b_1, b_2, \cdots, b_s$ $(q = 2mn)$ into three kinds: the requests $B^\uparrow = b_1^\uparrow, b_2^\uparrow, \cdots, b_{q/4}^\uparrow$ that causes information to flow form the low level into the high level, the requests $B^\downarrow = b_1^\downarrow, b_2^\downarrow, \cdots, b_{q/4}^\downarrow$ that causes information to flow form the high level into the low level, and the requests $B^\leftrightarrow = b_1^\leftrightarrow, b_2^\leftrightarrow, \cdots, b_{q/2}^\leftrightarrow$ that causes information to flow between the same level. Obviously, request $B^\downarrow$ in the second kind is a right about access.

Because the access control matrix is the base on which the model HRU judges the legality of the access request, the access request $b_i^{\uparrow}$ and $b_1^{\leftrightarrow}$ does not necessarily satisfy the access control matrix. It may be refused or allowed, because of which $p_2 \equiv 0$ cannot be always deduced.

Indirectly Safety. Indirectly illegal access is composed of several directly un-illegal accesses, so it can be denoted by $f_i^- = b_{i1}^+ b_{i2}^+ \cdots b_{iq}^+$, where $b_{i1}^+, b_{i2}^+, \cdots, b_{iq}^+ \in B^+$. Because $H_D(X)|HRU \equiv 0$, the system will allow every directly un-illegal access in f_i^-. Consequently, f_i^- will be allowed, therefore $p_3 > 0$ is deduced.

$H_I(X)|HRU > 0$, which shows that HRU model doesn't satisfy indirectly safety.

The above analysis shows that, the model HRU satisfies directly safety, and doesn't satisfy mandatory safety and indirectly safety.

5.2 Security Analysis to BLP

Directly Safety and Indirectly Safety.] The model BLP uses two methods: DAC and MAC. DAC uses the HRU model, so the directly safety and the indirectly safety of the BLP model coincide with that of the HRU, that is, BLP satisfies directly safety and doesn't satisfy indirectly safety.

Mandatory Safety. The BLP model forbids high level subjects writing low level objects and low level subjects reading high level objects, and prevents the information flowing from high level into low security level. So any right about access $b_i^{\downarrow} \in B^{\downarrow}$ will be refused by BLP, and any un-right about access $b_i^{\leftrightarrow} \in B^{\leftrightarrow}$ and $b_i^{\uparrow} \in B^{\uparrow}$ will be allowed. Consequently, the Probability distribution of BLP's response X is

$$\begin{bmatrix} X \\ P(x) \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ \frac{q}{4} & 0 & 0 & \frac{q}{4} \end{bmatrix}$$

So, $H_M(X)|BLP \equiv 0$, which shows that BLP satisfies mandatory safety.

5.3 Security Analysis to RBAC

The model RBAC [9, 13] assigns roles for users, and then based on these roles grants authorization. The RBAC's rights management and access control manner is similar to HRU's. so its safety is similar to that of HRU, which is, satisfying directly safety and not satisfying mandatory safety and indirectly safety.

5.4 Security Analysis to FGBAC

The FGBAC [5, 10, 12] is the improved BLP, which introduces the information flow graph as a judgment auxiliary tool. In FGBAC, any directly illegal access, right about access and indirectly illegal access will be refused. So

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

It shows that, the model satisfies directly safety, mandatory safety and indirectly safety.

6 Conclusion

According to the characteristics of Information entropy, we introduce the concept of security entropy and provide an access control capability evaluation method for access control quantification analysis of information security risk and event uncertainty.

Acknowledgments

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 under grant JYl0000903001, JYl0000901034. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] D. E. Bell and L. J. Lapadula, *Secure Computer Systems: Mathematical Foundations*, Technical Report M74-244, The MITRE Corporation, Bedford, Massachusetts, 1973.

[2] E. B. David, *Looking Back at the Bell-La Padula Model*, Reston VA, 20191, Dec. 7, 2005. (http://selfless-security.offthisweek.com/papers/looking-back.pdf)

[3] Z. Y. Fu, *Information Theory – Fundamental Theory and Application*, Beijing: Press of Electronics Industry, 2007. (in Chinese)

[4] GB/T 17859-1999, *Classified Criteria for Security*, Beijing: Standards Press of China, 1999. (in Chinese)

[5] Y. Liu, C. C. Chang, and S. C. Chang, "An access control mechanism based on the generalized aryabhata remainder theorem," *International Journal of Network Security*, vol. 16, no. 1, pp. 58-64, 2014.

[6] J. Peter, "Third generation computer systems," *Computer Surveys*, vol. 3, no. 4, pp. 175–216, 1971.

[7] R. S. Sandhu and E. J. Coyne, "Role-based access control models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[8] T. G. Si, Z. Y. Tan and Y. Q. Dai, "A security proof method for multilevel security models," *Journal of Computer Research and Development*, vol. 45, no. 10, pp. 1711–1717, 2008. (in Chinese)

[9] N. Sklavos and O. Koufopavlou, "Access control in networks hierarchy: implementation of key management protocol," *International Journal of Network Security*, vol. 1, no. 2, pp. 103-109, 2005.
[10] C. Wang, X. Y. Chen and N. Li, "An access control mode based on information flow graph," in *Proceedings of the International Conference on Computational Intelligence and Security*, pp.998-1000, 2011.
[11] G. B. Wang, H. Z. Huang and X. L. Zhang, "Risk possibility number – A new model for risk evaluation and prioritization based on maximum entropy theory," *Acta Aeronautica Et Astronautica Sinica*, vol. 30, no. 9, pp. 1684–1690, 2009. (in Chinese)
[12] M. Zareapoor, P. Shamsolmoali, and M. A. Alam, "Establishing safe cloud: Ensuring data security and performance evaluation," *International Journal of Electronics and Information Engineering*, vol. 1, no. 2, pp. 88–99, 2014.
[13] D. G. Zhai, Z. Xu, D. G. Feng, "Violation of static mutual exclusive role constraints in dynamic role transition," *Journal of Computer Research and Development*, vol. 45, no. 4, pp. 677–683, 2008. (in Chinese)
[14] D. M. Zhao, J. F. Ma, Y. S. Wang, "Model of fuzzy risk assessment of the information system," *Journal on Communications*, vol. 28, no. 4, pp.51–56, 2007. (in Chinese)

Tian-Wei 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.

Jian-Feng 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 International 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.