doi:10.3772/j.issn.1006-6748.2015.02.012

Security analysis of access control model in hybrid cloud based on security entropy①

Che Tianwei (车天伟)②*, Ma Jianfeng*, Li Na**, Wang Chao***
(* The School of Computer Science and Technology, Xidian University, Xi'an 710071, P. R. China)
(** The School of Computer Science and Technology, Northwestern Polytechnical University, Xi'an 710129, P. R. China)
(*** The PLA information Engineering University, Zhengzhou 450001, P. R. China)

Abstract

To resolve the problem of quantitative analysis in hybrid cloud, a quantitative analysis method, which is based on the security entropy, is proposed. Firstly, according to the information theory, the security entropy is put forward to calculate the uncertainty of the system's determinations on the irregular access behaviors. Secondly, based on the security entropy, security theorems of hybrid cloud are defined. Finally, typical access control models are analyzed by the method, the method's practicability is validated, and security and applicability of these models are compared. Simulation results prove that the proposed method is suitable for the security quantitative analysis of the access control model and evaluation to access control capability in hybrid cloud.

Key words: hybrid cloud, security entropy, classificatory access control model, directly unauthorized access, right about access, indirectly unauthorized access

0 Introduction

The key to access control model security proof is to find a recognized and self-evident security axiom, and then based on this security axiom, to deduce, or prove the security assumptions proposed in the model by means of this security axiom, so as to make it more reliable. However, even the proven Bell-La Padula (BLP) model[1,2] can't prove the rationality, completeness and safety of "simple security axiom" and "*-property axiom" that it proposed. So, some scholars point out that the security axioms in BLP cannot completely prove the security of BLP[3]. A complete access control model must clearly tell us which security requirements should be met, which access violation would be prevented, and how to reduce and prove the uncertainty of the access violation that the hybrid cloud allows.

Entropy is a tool of measuring uncertainty, which was originally used in thermodynamics. Shannon introduces it to the information theory, and puts forward the concept of information entropy for disordered degree of information[4]. Since the information entropy theory is proposed, it has been applied in 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].

This study, based on the thought and method that information entropy measures the uncertainty of things, puts forward the concept of security entropy, and by means of it, measures the uncertainty of system's response to access violations, which provides a scientific quantitative method for the safety analysis of classificatory access control model.

1 security entropy

Clouds and large data have become the mainstream mode of service to enhance customer service quality, this service model is facing some security risks such as loss and leakage of user data. In order to meet the access control demand for cloud services, especially the access control requirement for multi-level cloud services to coexist user data of different grades and categories of cloud services at the same time, the access control should be able to support different security strength and support the joint control of different intensities between access control models, which is different

① Supported by the National Natural Science Foundation of China (No. 60872041, 61072066) and Fundamental Research Funds for the Central Universities (JYI0000903001, JYI0000901034).
② To whom correspondence should be addressed. E-mail: tianweiche@163.com
Received on Jan. 28, 2014

from the traditional access control method. A quantitative method is presented for security requirements and security access control model assessment to meet the needs of multi-level cloud security assessment service access control model.

1.1 Definition of security entropy

In the cloud system, when a user sends an access request, the system will respond: to allow or to deny. And this response is the only one. To allow or to deny should not appear simultaneously. In addition, the access request is divided into two types: legal request and illegal request. If the system is seen as a black box, the system will give four kinds of response to user's each access request, that is, "allow legall access"、"refuse legall access"、"allow access violation" and "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 order to comprehensively measure the uncertainty of system's response to various access requests, the security entropy is defined as follows:

Definition 1 (security entropy): If a group of access request $B = b_1, b_2, \cdots, b_q$ is seen as the input, the system's request responses to each access result as the object of study, and variable X as this response results, then the value of X will be :to allow legitimate access, to deny legitimate access, to allow illegal access, and to deny illegal access, which is recorded as a_1, a_2, a_3, a_4 respectively. If Symbol $p(a_i)$ stands for the statistical probability of a_i, the probability space $[X, p(X = a_i)]$ of X will be

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

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

Assigning weight w_i, the impact factor of the system security, for each response result, the greater w_i is, the higher the a_i's influence to system safety is, otherwise the smaller the a_i's influence is. If the distribution of w_i is

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

the security entropy of X will be

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

1.2 The meaning of safety entropy

According to the common sense of information security, response a_2 gives negative effects on the usability of the system, and response a_3 gives negative effects on the confidentiality of the system, while response a_1 and a_4 have less influence on system security. Therefore, if we let w_2, $w_3 \geqslant w_1$, w_4, the meaning of safety entropy in Eq. (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 makes harmful response is.

If $w_2 > 0, w_3 > 0, w_1 = w_4 = 0$, and $w_2 + w_3 = 1$, 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 Eq. (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 Eq. (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, a_3 and a_4 will be 0, and if all input samples are illegal access, a_1 and a_2 will be 0. In order to make the safety entropy reflect the system security accurately, 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 uncertainty of the harmful response that system does is, the more the security of the model is. When the security entropy approaches 0, then the model will achieve the theoretical security.

1.3 Security entropy of different types of illegal accesses

Whether an access is illegal is related to security requirements. According to the access control requirements in national grade of protection standard GB17859-1999[8], illegal access can be classified into three types: directly illegal access, right about access, and indirectly illegal access. The directly illegal 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 word, the one which leads information flow from high class to low class. The indirectly illegal access refers to the one that violates the authorized strategy through information indirect transmission.

For instance, there are two users(s1、s2) and two resourses (o1、o2) in the hybrid cloud, and the relationship of security level is $f(s_1) \triangleright f(s_2) \triangleright f(o_1) = f(o_2)$, the authorized strategy of the system is that "s1 read o2", "s2 read o1", "s2 write o2".

Let us see the following four events: b1: s2 read o1, b2: s2 write o2, b3: s1 read o2, b4: s1 read o1. Because b4 explicitly violates the authorized strategy, b4 is therefore directly illegal access, and the sequence of access b1b2b3 causes the information to flow from s1 into o1, which equals that s1 read o1 indirectly. Therefore b1b2b3 is indirectly illegal access. b1 and b3 cause the information flowing to the violation of the direction made by the system, so b1 and b3 are right about access.

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

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

2 Safety conditions of classificatory access control model

2.1 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:

It is proved that when $H_D(X) = 0$, the event "refuse legal access" and "allow access violation" will never happen, that is, $p(a_2) = p(a_3) = 0$.

The total number of a_i is made as $n_i (i = 1,2,3,4)$, $n_1 + n_2 = s$, $n_3 + n_4 = t$. Because a_1、a_2 and a_3、a_4 are different responses to the same access, $p(a_1) + p(a_2) = s/(s+t)$, $p(a_3) + p(a_4) = t/(s+t)$.

According to the common sense, access requests couldn't be all legal or all illegal, so $s, t > 0$. Because $\sum_{i=1}^{4} p(a_i) = 1$, $p(a_2) \neq 1$, $p(a_3) \neq 1$。

Because $w_2 > 0, w_3 > 0, w_2 + w_3 = 1$, so $w_1 = w_4 = 0$。

End.

Similarly, theorems could be got 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 (indirectly safety of access control model): the access control model has indirect safety, if and only if

$$H_I(X) = -\sum_{i=1}^{4} w_i p(a_i) \log p(a_i) \equiv 0, \text{ in which } w_2 > 0, w_3 > 0, w_2 + w_3 = 1.$$

2.2 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 safety needs of class 2、3、4 information system, the safety theorem of classificatory access control model based on the above security attributes is put forward.

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

3 Analysis of typical access control model based on security entropy

Now, the theory is applied to analyze the security

of typical access control model, verify the practicability of this method, and point out the defect of these access control models.

3.1 Security analysis to HRU model

3.1.1 Direct 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 requests, 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 illegall access $B^- = b_1^-, b_2^-, \cdots, b_t^-$ ($s + t = q$).

Based on the access control matrix, HRU[9] 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 a_4; As long as access behaviors don't disobey the policy, it would be allowed, so the response to any $b_i^+ \in B^+$ is a_1. so $p(a_2) = 0$ and $p(a_3) = 0$.

The statistical probability distribution of responses is

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

Since $H_D(X) \mid HRU \equiv 0$, model HRU can satisfy direct safety.

3.1.2 Mandatory safety

All requests $B = b_1, b_2, \cdots, b_q (q = 2mn)$ are divided into three kinds: requests $B^{\uparrow} = \{b_1^{\uparrow}, b_2^{\uparrow}, \cdots, b_{q/3}^{\uparrow}\}$ that cause information to flow from the low level into the high level, the requests $B^{\downarrow} = \{b_1^{\downarrow}, b_2^{\downarrow}, \cdots, b_{q/3}^{\downarrow}\}$ that causes information to flow from the high level into the low level, and the requests $B^{\leftrightarrow} = \{b_1^{\leftrightarrow}, b_2^{\leftrightarrow}, \cdots, b_{q/3}^{\leftrightarrow}\}$ that cause 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 model HRU judges the legality of the access request, the access request $b_i^{\uparrow}$ and $b_1^{\leftrightarrow}$ does not satisfy the access control matrix. It may be refused or allowed, because of which $p(a_2) \equiv 0$ can not be always deduced.

3.1.3 Indirect safety

Indirectly illegal access is composed of several directly un-illegal accesses, so it can be denoted by $f_i^- = b_{i_1}^+ b_{i_2}^+, \cdots, b_{i_q}^+ (b_{i_1}^+, b_{i_2}^+, \cdots, b_{i_q}^+ \in B^+)$. Because $H_D(X) \mid HUR \equiv 0$, the system will allow every directly un-illegal access in f_i^-. Consequently, f_i^- will be allowed, therefore $p(a_3) > 0$ is deduced.

$H_I(X) \mid HRU > 0$, which shows that the HRU model doesn't satisfy indirect safety.

The above analysis shows that, model HRU satisfies direct safety, and doesn't satisfy mandatory safety and indirect safety.

3.2 Security analysis to BLP

3.2.1 Direct safety and indirect safety

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

3.2.2 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 unright 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

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

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

3.3 Security analysis to RBAC

Model RBAC[9-11] assigns roles for users, and then based on these roles grants authorization. The RBAC's rights management and access control manner are similar to HRU's. so its safety is similar to that of HRU, which is, satisfying direct safety and not satisfying mandatory safety or indirect safety.

3.4 Security analysis to FGBAC

FGBAC[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

$H_D(X) \mid FGBAC = H_M(X) \mid FGBAC = H_I(X) \mid FGBAC \equiv 0$

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, it is concluded the typical model' security and applicability are Table 1

and Table 2.

Table 1 The security of typical access control model

typical access control model	directly safety	mandatory safety	indirectly safety
HUR	satisfy	not satisfy	not satisfy
RBAC	satisfy	not satisfy	not satisfy
BLP	satisfy	satisfy	not satisfy
FGBAC	satisfy	satisfy	satisfy

Table 2 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

In the simulation environment of achieving the RBAC, BLP and FGBAC models, the rationality of this method is tested. In the simulation environment, 30 users and 200 text types of resources have been. Through user behavior simulation program automaticly and randomly generated user access and randomly modified on three models of security rules and procedures, three audit tracking programs are established recording the determination result of each model. the security entropy is calculated according to the execution result shown in Table 3.

Table 3 The security entropy result of typical access model

typical access control model	$H_D(X)$	$H_M(X)$	$H_I(X)$
RBAC	0	0.003	0.027
BLP	0	0	0.0095
FGBAC	0	0	0

4 Conclusion

This study 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 work analyses the typical access control model, verifies the practicability of the method, and concludes the security and application scope of the available models.

Reference

[1] Bell D E, Lapadula L J. Security Computer Systems: Mathematical Foundations and Model. Bedford: Mass Mitre Corp, 1973. 66-79

[2] David E B. Looking back at the bell-La Padula model. In: Proceedings of the 21st Annual Computer Security Applications Conference, Tuscon, USA, 2005. 337-351

[3] Si T G, Tan Z Y, Dai Y Q. A Security Proof Method for Multilevel Security Models. *Journal of Computer Research and Development*, 2008, 45(10): 1711-1717 (in Chinese)

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

[5] Wang G B, Huang H Z, Zhang X L. 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 Y, Wu X P, Ye Q, et al. 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 D M, Ma J F, Wang Y S. 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. Beijing: Standards Press of China, 1999 (in Chinese)

[9] Peter J. Third Generation Computer Systems. *Computer Surveys*, 1971, 3(4): 175-216

[10] Sandhu R S, Coyne E J, Feinstein H L. Role-based access control models. *IEEE Computer*, 1996, 29(2): 38-47

[11] Zhai D G, Xu Z, Feng D G. Violation of static mutual exclusive role constraints in dynamic role transition. *Journal of computer research and development*, 2008, 45(4): 677-683 (in Chinese)

[12] Wang C, Chen X Y, Li N. An access control mode based on information flow graph. In: Proceedings of the International Conference on Computational Intelligence and Security, Sanya, China, 2011. 998-1000

Che Tianwei, born in 1971, He received his Ph. D. in Computer Science and Technology School of Xidian University in 2014. His main research interests include computer architecture, information security, grid computing systems.