Dynamic Access Control Model based on User Trust for Radio and Television Monitoring System

Wenqing Shi
School of Information Engineering
Communication University of China
Beijing, China
shiwenqing32@foxmail.com

Pei Tian
School of Information Engineering
Communication University of China
Beijing, China
tianpei@263.net

***Abstract*—The authority management module is an important part of the broadcast TV monitoring system. In order to ensure that the important and key functions of the system are implemented by the users who meet the requirements, this paper introduces the static trust value and dynamic trust value based on the original access control model of the monitoring system, and proposes a dynamic access control model based on user trust. Static trust value and dynamic trust value are derived from Bayesian estimation theory. The model uses the user's role and static trust value as the basis for obtaining permissions, and then calculates the user's dynamic trust value in real time in combination with user behavior and device state, and grants the user specific permissions in the actual operation. Finally, an application example and the model security analysis are given. The results show that the model can realize dynamic authorization and satisfy the principle of least privilege.**

Keywords—access control; level of trust, bayesian estimation theory, dynamic authorization, radio and television monitoring

I. INTRODUCTION

Radio and television transmitting station is responsible for radio and television transmitting task. The monitoring system of transmitting station is the brain of the whole station, and access control is the portal of the monitoring system, which is one of the key strategies for resource allocation and information protection of the system. As a complex information system, large-scale network has complex system properties, usually unable to implement the overall survivability strategy and unified management. For example, the backbone of Internet has no global policies in consideration, the reason is that it does not exist a global management. Therefore, simple network survivability structure does not apply to open complex systems. Large-scale network survivability mainly considers the system as a whole to provide the critical services survivability. The theories and methods of large-scale network survivability should be investigated and proposed from the essential characteristics of large-scale network as an open complex system.

Strict authentication and restricting users' access to and use of system resources can effectively prevent unauthorized users from maliciously destroying related transmission devices, which is of great significance for ensuring the integrity of broadcast TV programs and the security of devices and lines. The current broadcast television monitoring system adopts the traditional Role-Based Access Control (RBAC) mode. The basic principle of RBAC is to add a role layer between the user and the access rights, to separate the user and the authority, grant the permission to the role instead of directly granting the subject, and the subject obtains the object operation authority through the role assignment to realize the authorization. RBAC is also a popular access control model in information systems, but it has the following defects: (1)The authorization policy of BAC is static and fixed. (2)When RBAC is faced with the increase of users, it is not flexible and easy to cause role diffusion problems. (3)The RBAC mode does not comply with the principle of least privilege. In RBAC mode, after a user obtains a role, he has all the rights of the role, and the number of uses is not limited. This is easy to cause abuse of rights and cannot effectively curb malicious behavior of users.

Therefore, it is of great practical significance to study and optimize the rights management model to make up for the shortcomings of the static authorization strategy and improve its flexibility. This is not only about whether radio and television signals can be transmitted accurately, whether the program can be broadcasted according to the scheduled time, but also related to the personal safety of the related staff and the safety of radio and television facilities.

In order to ensure the security of the system and strictly control the terminal behavior of the access process, this paper proposes a User Trust Based Dynamic Access Control (UT-DAC) model based on user trust. UT-DAC introduces static trust value and dynamic trust value. The trust value is calculated based on Bayesian estimation theory. The UT-DAC can realize dynamic access control.

II. DYNAMIC ACCESS CONTROL MODEL BASED ON USER TRUST

In UT-DAC model, static trust value and dynamic trust value are introduced as the basis of access and operation. In the actual access process, the model will adjust the dynamic trust value according to the user's IP address, login location, login time and other attributes. Only when the user's two trust values meet the access requirements can the user obtain the final authorization. The structure diagram of UT-DAC model is shown in Fig. 1.

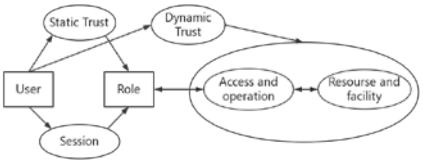

Fig. 1. The structure of User Trust Based Dynamic Access Control Model

A. Basic Concepts

Concept 1. User: The user is the subject of accessing system resources, and the user set is represented by U={$user_1$,$user_2$,...,$user_n$}.

Concept 2. Resource and facility: Object accessed by the subject, resource and facility is represented by O={object1,object2,...objectn}.

Concept 3. Access Operation: A collection of various operations performed by the subject on resource and facility, and access operation is represented by AO={op_1,op_2,...,denial}.

Concept 4. Role: Users have a role in the department or organization, and the operations they perform match the functions of the roles they play, and each role has the corresponding function.

Concept 5. Session: Session is the user's mapping of roles. When the user activates the assigned role, a session is established.

Concept 6. Trust: According to the related information of the subject and its context, the trust relationship of the resource is determined.

In the UT-DAC model, the trust value of the user subject is divided into a static trust value and a dynamic trust value, and the static trust value is recorded as TS and the dynamic trust value is recorded as TD.

Concept 7. Trust Level: The correspondence between trust index and trust level is given by the project expert, and the trust degree is divided into five levels, as shown in Table I.

TABLE I. TRUST INDEX AND TRUST LEVEL

Trust index	Trust Level
(0.9,1]	Level1
(0.8,0.9]	Level2
(0.7,0.8]	Level3
(0.6,0.7]	Level4
(0,0.6]	Level5

B. User trust calculation

Bayesian estimation theory can introduce posterior information based on prior information and sample information, which is closer to the actual situation. When calculating the user trust, take the user's possible behavior as a hypothesis, and set the probability that the user will operate on the system to obey uniform distribution U(0,1), that is, prior information. This assumption is a Bayesian hypothesis, and the user history access record is used as sample information to infer the user's future behavior information, that is, the posterior information.

In this paper, the factors affecting user trust are divided into two categories: static trust value TS and dynamic trust value TD. The trust values are all in [0, 1], which can be calculated based on the user's basic information and dynamic information. W_{TS} and W_{TD} are the corresponding preset weights. If there are W_{TS}, $W_{TD} \in [0,1]$ and $W_{TS}+W_{TD}=1$.Then, the user's trust T(u) is shown in Equation (1).

$$T(\mathrm{u}) = TS(u)W_{TS} + TD(u)W_{TD} \tag{1}$$

1) Static trust value

In this paper, the probability that the user's next visit is successful is taken as the static information value of the user. The information of the user's previous access to the system is taken as sample information, and the static trust value is calculated by Bayesian estimation theory. The higher the probability of successful access next time, the more credible the user is.

First, assume that a user accesses the system, the user requests access to the system, and the result is represented by $|,|$ is expressed as Equation (2).

$$o = \begin{cases} 1 & \text{successfulaccess} \\ 0 & \text{failed access} \end{cases} \tag{2}$$

In the event t, a binary group R^t is used to represent the history of the user's access to the system. o^t=(s,f),where s represents the total number of successful visits by the user in the event t, and f represents the total number of failed accesses. o^t will update each time the user visits.The total number of user accesses is n=s+f, and the probability of successful user access is θ ,$0 \leqq \theta \leqq 1$.p(s)= θ ,p(f)=1-θ .Then s/θ satisfies the binomial distribution, $s/\theta \sim b(n, \theta)$, that is, Equation (3).

$$P(s/\theta, n) = \binom{n}{s}\theta^s(1-\theta)^{n-s}, s = 0.1....,n \tag{3}$$

From this, the posterior distribution of θ can be obtained from Bayesian. The joint distribution of s and θ is obtained according to Equation (3).

$$\mathrm{h}(s,\theta) = \binom{n}{s}\theta^s(1-\theta)^{n-s}, s = 0,1,...,n, 0 \le \theta \le 1 \tag{4}$$

Marginal distribution of s is shown in Equation (5).

$$m(s) = \binom{n}{s}\int_0^1 \theta^s(1-\theta)^{n-s}d\theta = \binom{n}{s}\frac{\Gamma(s+1)\Gamma(n-s+1)}{\Gamma(n+2)} \tag{5}$$

Finally, the posterior distribution of θ is obtained and shown in Equation (6).

$$\pi(s/\theta) = \frac{h(s,\theta)}{m(s)} = \frac{\Gamma(n+2)}{\Gamma(s+1)\Gamma(n-s+1)}\theta^{s-1}(1-\theta)^{n-s+1} \tag{6}$$

So θ /s~Be(s+1,n-s+1),its posterior expectation is estimated to be Equation (7).

$$\hat{\theta}_B = E(\theta/s) = \frac{s+1}{n+2} \tag{7}$$

That is Equation (8).

$$TS(u) = \hat{\theta}_B = E(\theta / s) = \frac{s+1}{n+2} \tag{8}$$

Therefore, the higher the success rate of the user interaction, the higher the static trust value, and the more credible the user is.

2) Dynamic trust value

There are four factors in the dynamic trust value, namely:

IP address (ip). In general, the system user only logs in to the system through the fixed network to perform corresponding operations. If the IP address used by the user changes or is not a common IP, the user is suspicious.

Login location (location). The system is divided into a PC end and a mobile terminal. Mobile terminal can be used in a larger area. However, in general, the use range is fixed. If the system login location is not in the usual range, the user is suspicious.

User login time (time). Under normal circumstances, the user would normally access the system at a fixed time period, such as working time or specified time. If the user suddenly accesses the system in the early morning, the behavior of the user is suspicious.

Exceptional operation (exception).Under normal circumstances, the user will perform routine operations on the system. For example, turn on the transmitter before the program is transmitted and read the log records before coming off duty. If a user closes the transmitter during the broadcast of a program or frequently checks the contents of the database, such irregular operations performed by the user indicate that the user's behavior is suspicious.

When the user registers, these factors are recorded as factor[4]={ip, location, time, exception}, the initial value is 0, and the corresponding number of occurrences is expressed as t[4]={t1, t2, t3, t4 }.

When the user accesses the system and performs the operation, if the factor i changes, set factor[i]=1, t[i]=t[i]+1.After the values of factor[i] and t[i] are determined, then the dynamic trust value is calculated. The dynamic trust value TD is equal to the sum of factor[i] and its weight product, that is, Equation (9).

$$TD = \sum_{i=1}^{4} \omega_i \, factor[i] \tag{9}$$

$$\omega_i = \frac{t[i]+1}{\sum_{i=1}^{4} t[i] + 4}, \sum_{i=1}^{4} \omega_i = 1 \tag{10}$$

Use ω_i to indicate the weight of each factor. When a factor does not change, in order to avoid the weight of this factor is 0, use the above formula to calculate the weight of each factor.

C. Model authorization process

According to different trust levels, users can perform different operations. The operation authorization process is as shown in Fig. 2.

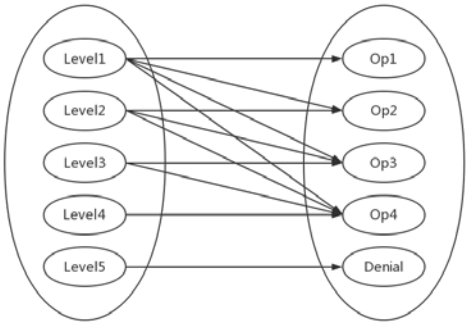

Fig. 2. Model authorization process

D. Model operation mechanism

The operation mechanism of the model is shown in Figure 1.

(1) The user u accesses the system and the system calculates a static trust value TS according to the basic information of the user u, and assigns a corresponding role to the u.

(2) User u collects dynamic information of u during the operating system process and calculates dynamic trust value TD.

(3) According to the trust value level conversion table, obtain the trust level of the user u.

(4) Determine whether the user's trust level can meet the resource operation requirements, and if the requirements are met, provide authorization to the user. If the requirements are not met, the user is denied authorization.

III. EXAMPLE OF APPLICATION

In the monitoring system of radio and television transmitter station, some resources are only accessible by some employees, and some operations are only accessible by some employees. Moreover, the time and place and network environment where each person is allowed to access are also different, which requires a flexible dynamic constraint rule. Some constraint rules of the system are as follows:

Constraint 1: the director and administrator of the station can access resource R, while the ordinary duty officer has no access qualification to resource R.

Constraint 2: the access rights of different personnel to R are restricted by time, place, network environment and other factors. The administrator can read and modify the resource R within the company, and can only read it outside the company, and cannot modify it. The Director can read and modify the resources anywhere.

Constraint 3: The attendant can turn the transmitter on or off, but the transmitter cannot be turned off directly during the broadcast of the program and needs to be approved by the leader.

In the case of combining the above constraints, the user can obtain the final authority on the resource.

Example 1 Administrator A's computer and account password were stolen. Criminals attempted to tamper with the resource R information through the login system outside the launch pad. After logging in to the system, because the login location is not in the station control center, the network

is not a common IP, and the login time is In the early morning, the behavior was abnormal. The system calculated that the account TS was 0.5 and the TD was only 0.01, which refused to provide services, thus ensuring information security.

Example 2 The attendant B logs in to the system on a certain day. According to the basic information of B, the system obtains its TD of 0.5. In the process of B acquiring system information, the system obtains its TS as 0.4, B can read and modify the resource R, and enters in B. After the transmitter management module, the program is currently being broadcast, and the system gets its TS to be 0.15, refusing to provide it with the right to turn off the transmitter.

IV. Model Safety Analysis

The security analysis of the model is shown.

(1) Dynamic authorization. Through the real-time calculation and judgment of the user dynamic information, after obtaining the trust value of the user, according to the trust level conversion table, the dynamic allocation and real-time updating of the user rights can be realized.

(2) Support the principle of least privilege. The user's dynamic trust value is updated in real time during the operation, and the user's access rights do not exceed the permissions required to complete the work.

V. Conclusions

In the case of dynamic changes in user behavior, the traditional broadcast control system access control mode presents many drawbacks.

By introducing the concept of static trust value and dynamic trust value, combined with the traditional RBAC access control mode, this paper proposes a trust-based dynamic access control model, so that the process of user acquisition of rights is not only related to the role, but also to the user's current dynamic information. The device status is associated with the analysis and judgment of the user operation through model calculation and analysis, which can effectively avoid the malicious behavior and misoperation of the subject.

In the future work, it is necessary to study the factors, classifications and calculations that affect the user's trust value, and hope to propose a more comprehensive and reasonable method.

References

[1] C.L. Zhou, Automatic Monitoring Technology for Broadcast and Television. Beijing, China Radio Film & TV Press, 2009.

[2] Y.B. Wang, Overall monitoring of media information security. Beijing, Communication University of China press, 2006.

[3] D.D. Sun, Y. Zhao, B. Lang, “Two Level Access Control Model of Distributed Services Based on RBAC,” Computer Engineering and Applications, vol. 26, pp. 119-122, 2006.

[4] R.Ferraiolo, R.Kuhn, “Role-Based Access Controls,” In Proceedings of the 15th National Computer Security Conference, pp. 554-563, 1992.

[5] R.Sandhu, “Role-Based access control Models,” IEEE Computer, vol. 29, issue 2, pp. 38-47, 1996.

[6] R.Sandhu, V.Bhamidipati, E.Coyne, “The ARBAC97 model for role-based administration of roles: preliminary description and outline,” RBAC '97 Proceedings of the second ACM workshop on Role-based access control, pp. 41-50, 1997.

[7] D.Ferraiolo, R.sandhu, S.gavrila, “Proposed NIST Sandard for Role-Based Access Control,” ACM Transactions on Information and System Security, vol. 4,issue 3, pp. 224-274, 2001.

[8] R.N Su, Y.P. Zhang, Z.K. He, et al, “ Trust-Based Fuzzy Access Control Model Research,” In International Conference on Web Information Systems and Mining, vol. 5854, pp. 393-399, 2009

[9] L.L. Zhao, S. Liu, J.S. Li, H.C. Xu, “A Dynamic Access Control Model Based on Trust,” In the 2nd Conference on Environmental Science and Information Application Technology, vol. 1, pp. 548-551, 2010.

[10] L.S. Zhang, “TAAC: A trust-aware access control model,” In the 2nd International Conference on Computer Engineering and Technology, vol. 7, pp. 489-492, 2010.

[11] H.F. Xing, B.L. Cui, L.L Xu,“An Mixed Access Control Method based on Trust and Role,” In the 2nd IITA International Conference on Geoscience and Remote Sensing, vol. 1, pp. 552-555, 2010.