An Action Based Access Control Model for Multi-level Security

Mang Su[1], Fenghua Li[2], Guozhen Shi[3] and Li Li[3]

[1]*National Key Laboratory of Integrated Services Network, Xidian University, Xi'an, Shaanxi 710071, China*
[2]*Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100195*
[3]*Department of Electronic Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China*
sm1222@163.com, lifenghua@iie.ac.cn, sgz@besti.edu.cn, lili103@besti.edu.cn

Abstract

The new computing modes, such as mobile computing, distributed computing, cloud computing and ubiquitous computing, etc., have brought about diversification and open features to the expression, exchange and access of computer network information. The multi-level security management is widely used in operation systems and information management systems. Focus on the multi-level security problem in various network environments, this paper defines the security identity, environment and temporal state of object, based on the ABAC (Action Based Access Control), and shows the security level, access scope and the demand of environment and temporal state of accessing subject, then proposes a multi-level security access control mechanism .Finally, an application example is given.

Keywords: *multi-level security; access control; action; security level; structured document.*

1. Introduction

With the development of information technology, the communication network has already become an isomerous, open, distributed computing system, which also supports mobile computing. New computing modes, such as distributed computing, mobile computing, cloud computing and ubiquitous computing, have appeared, meeting people's ever increasing demand for personalized service on open connection, determining the diversification and openness features of information spread in an open network environment. The access control technology is used for management and access authorization of the shared data. It is one of the core technologies to ensure the security of information system. An access control model is used to unambiguously express and analyze the access control strategy used in an information system, which prevent unauthorized accessing and data divulging by monitoring user's behavior. With the development of the research of access control, several access control models have appeared such as autonomous access control model, mandatory access control model, role-based access control model, task-based access control model, access control for distributed environment and cross-domain, spatiotemporal attribute based access control and security attribute based access control, etc..

Multi-level Security [1, 2] mainly focuses on analyzing, management and access authorization of information, which ensure information on different security levels can only be accessed to by users with corresponding permission. Besides, those access control models above manage the authorization mainly based on the elements like the role, the temporal state and environmental state of the subject, tend to ignore the abstraction and description of the object. And they cannot meet the demand of multi-level information management. Meanwhile, The multi-level security access control models existing usually base on mandatory access control model, without considering comprehensive factors of the subject like its temporal and environmental state, which make its management lack of flexibility and generality. As a result,

it is a significant issue that how to combine the multi-level security model and the current multi-element access control mechanism in research on the field of access control nowadays.BLP[3]and Biba [4] models protect the confidentiality and integrity, performing mandatory access control strategy. Multi-level security models are widely used in operating systems, databases and large information management system, such as J-S model [5] based on classical BLP model and multi-level security model VMAC [6] based on view, etc..

This paper mainly focuses on the issues above. In this paper, the description of object in the ABAC model will be extended. The concept of object security attribute will be added. The definition of the subject-object security level will be given. And Action Based Access Control Model for Multi-level security will be proposed. This model can meet the demand of objectified and fine-grained access control of structured documents in the multi-level security information system.

2. Action based Access Control for Multi-level Security

2.1. Action based Access Control Model

The above models have taken into account temporal and location related with access control on the characters distributed computing and mobile computing. But all of them have not analyzed the environment of the role in detail, including physical positions, hardware platforms, operation systems and networks. Ref [7] presents an Action Based Access Control model (ABAC) as shown in Figure 1.

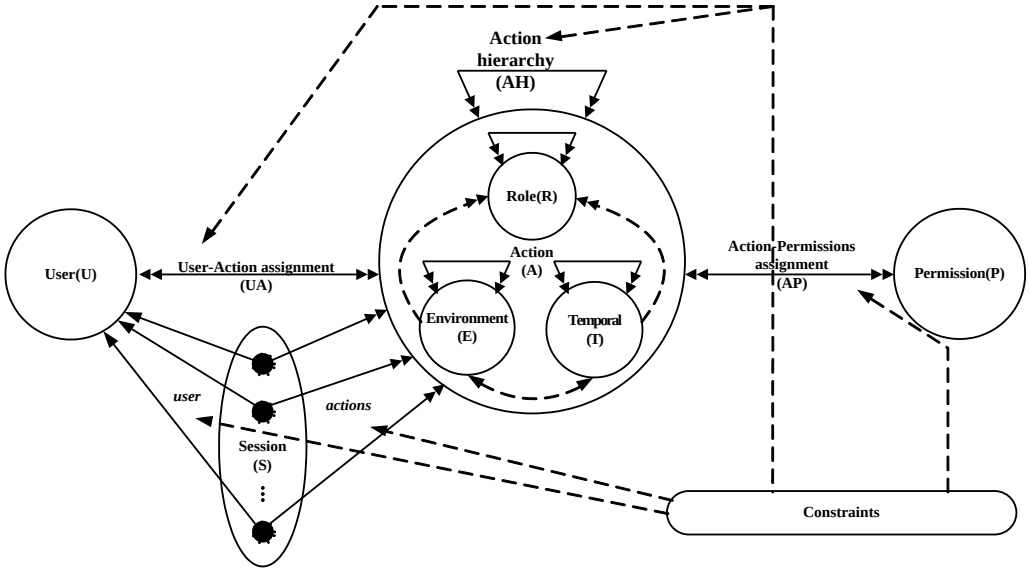

Figure 1. Action based Access Control Model

The Model describes abstractly role, environment, temporal and is suitable to the information management for distributed computing and mobile computing. But this model doesn't define and describe the situation of multi-level security problem. In order to solve this problem, the security security-level and scope of subject and object will be defined.

2.2. Action based Access Control Model for Multi-level Security

Based the definitions of ABAC, environment state and temporal state of subject, the security identity for both of subject and object , the environment state and temporal state for

object will be described for multi-level security management. Security identity including the security level and scope is defined to show the level of subject or object and the scope for access or being access. For example, some detailed information of department finance will be only accessed by the related person. The environment state and temporal state have direct influence on operation. Operation to the object with certain level will be deceived by the environment of temporal of subject. Different physical position, device and time of subject need to be taken into account when assigning the operation to objects.

To meet the system requirements of access control for multi-level, The Role of User is extended as follow:

R=[RV|RS]

RV shows the level of the user in such information system. RS shows the scope of the user, which can be similar with the ID of department.

Also the security identity is described further as follow:

V=[VC|VS]

VC shows the level of the object in such information system. VS shows the scope of the department in which the user can access this subject.

Referring to NIST RBAC[8] and ABAC(Action Based Access Control) [7] structure, the structure for Action Based Access Control Model for Multi-level security is shown as in Figure 2. If a user requires to access an object, the system will get the role, environment and temporal state of this user, and the security identity, environment and temporal state of the object, then decide the whether the user has the permission of operation.

The ABAC model has the following components:

- U, A, P, S, O (users, actions, permissions and sessions, object), where A=(R, T, E) is a complex variable determined by the mutual influence of R, T, E, and R, T, E are roles, temporal states and environmental states respectively.
- OPS, type of operation to object;
- UA⊆U×A, a many-to-many user-to-action assignment relation;
- AP⊆A×P, a many-to-many action-to-permission assignment relation;
- AH⊆A×A, an action hierarchy on A, also written as $\geqslant$;
- actions: $S \rightarrow 2^A$, a function mapping each session s_i to a set of actions , and session has the permissions .
- user: $S \rightarrow U$, a function mapping each session s_i to the single user(s_i)(constant for the session's lifetime);

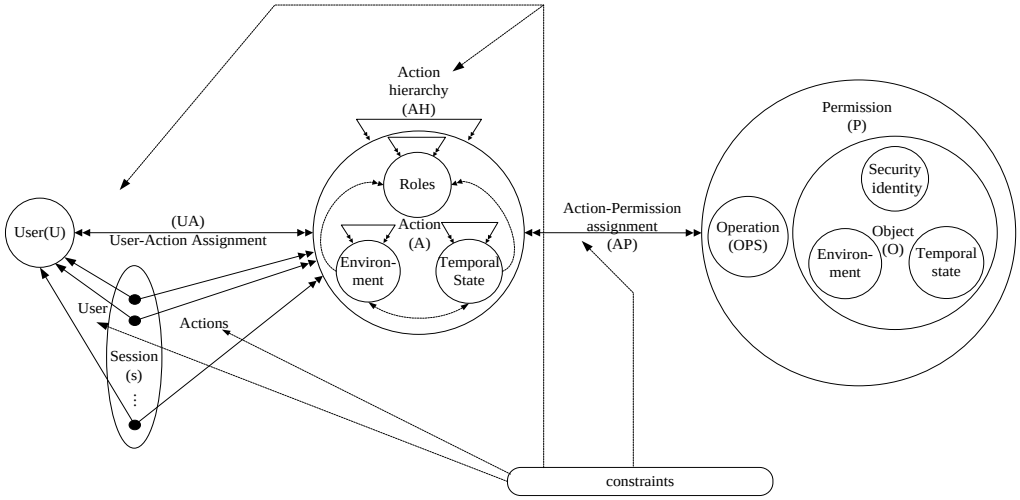

Figure 2. Action based Access Control Model for Multi-level Security

3. An Example

Object: document of the company (DC), which includes four objects, O_A, O_B, O_C and O_D;
User: general manager C;
Department A: Manager A_0, Staff A_1, A_2, A_3;
Department B: Manager B_0, Staff B_1.
Security level is divided into 4 levels. The relationships between users and levels are shown in Table 1.

Table 1. User Security Level Definition

Level	User
1	C
2	A_0、B_0
3	A_1、A_2、B_1
4	A_3

User R can be described as follows:

$R_C = (1,C), R_{A_0} = (2,A), R_{B_0} = (2,B), R_{A_1} = (3,A), R_{A_2} = (3,A), R_{B_1} = (3,B), R_{A_3} = (4,A)$

According to the definition of security level, security identify of a certain object is described as follows:

$V_1 = (i,(C)), V_2 = (i,(AC)), V_3 = (i,(BC)), V_4 = (i,(ABC)), (i = 1\ldots4)$, i identifies the lowest security level of subject, which allows accessing.

The object is defined as follows:

Taking the Structured document as an example, it contains the sub document. The resources of the company are stored in the Cloud data centre.

O_C: important information of the company, which is only permitted to access by manager C;

O_A: internal stuff of department A, which only department B and general manager C can access; O_D: public resource of the company;

Operation type: *OPS*=<*read, write, modify, delete*> respectively means reading, writing, modifying and deleting. To be convenient, in the chart below, the above operation is abbreviated as <*r, w, m, d*>. *E* is expressed as [*EL*|*EP*], in which $EL=\{el_1,el_2\}$={internal, on business}, $EN=\{ep_1,ep_2\}$={desktop computer, mobile equipment} ; temporal state $T=\{t_1, t_2\}$={work, after work}. Provided the access control strategy needs to meet the security demand in Fig. 3, the certain relationships are described as Fig.3. In this Figure, temporal information can be gat from the NTSC.

This model can realize fine-grained access control to the object according to user's security levels, action category, environmental state and temporal state, etc... If user U takes the role of general manager C, during working hours, using laptop computers inside the company to send an access request "modify" to the object O_A, then the description of the user's action A is $c' = ((1,C),(el_1,ep_1),t_1)$. According to the object and the user's request, the relative description $c = ((1,C),(el_1,ep_1),t_1) \cup (1,AC),(el_1,ep_1),t_1); c' \in c$. Then, the user U can get the access permission of modify. If the user U send out the same request when on business, the description $c'' = (1,C),(el_1,ep_1),t_1); c'' \notin c$, and the returned result will be "fail".

For users with the same security levels, this mechanism controls the access category of subject according to the demand of object. For a example, if user U with the role B_0 sends a request of write on O_A , during working hours, using laptop computer, then its description $c_{B_0} = ((2,B),(el_1,ep_1),t_1)$, the set of description $c = (((1,C),(el_1,ep_1),t_1)) \cup ((1,AC),(el_1,ep_1),t_1)) \cup ((1,AC),(el_1,ep_2),t_1)))$, $c_{B_0} \notin c$, the returned result will be "fail".

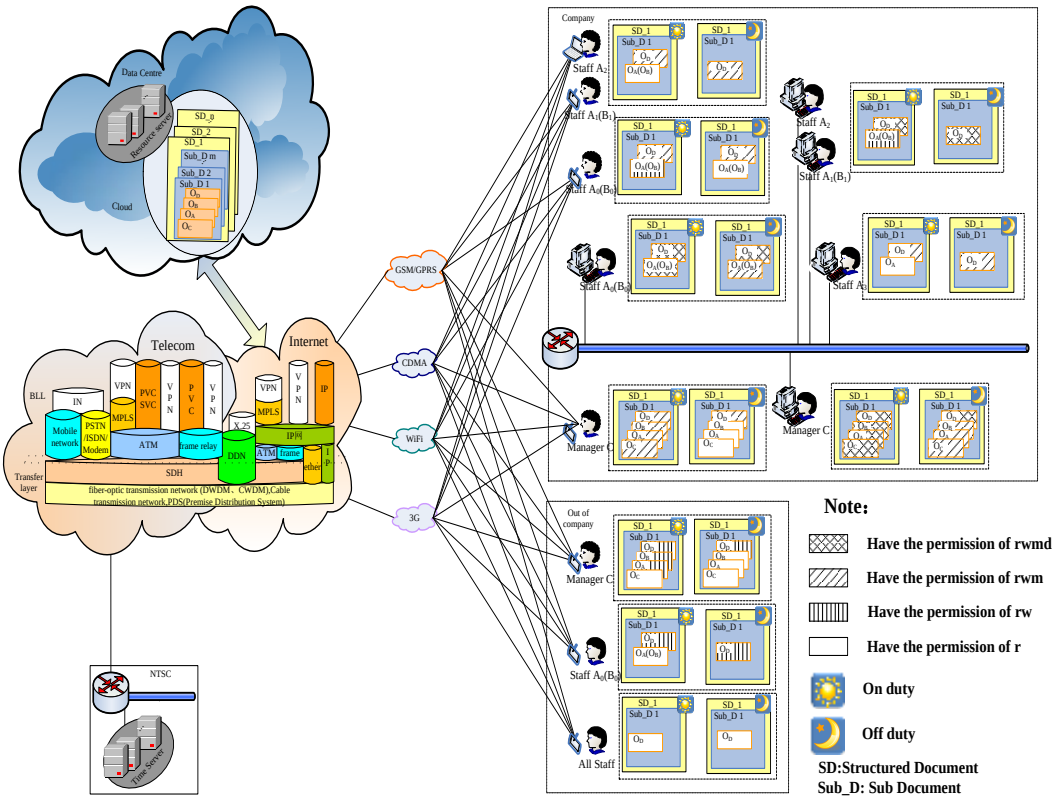

Figure 3. Multilevel Security System Authorized Schemes

Table 2. Permission for Figure 3

Object	Security identity		Environment		Temporal	OPS
	Security Level	Scope	Location	Platform		
O_C	1	C	el_1	ep_1	t_1	*rwmd*
	1	C	el_1	ep_2	t_1	*rwm*
	1	C	el_2	ep_2	t_1	*rw*
	1	C	el_2	ep_2	t_1/t_2	*r*
$O_A(O_B)$	1	C	el_1	ep_1	t_1	*rwmd*
	2	AC(BC)	el_1	ep_1	t_1	*rwm*
	2	AC(BC)	el_1	ep_2	t_1	*rw*
	3	AC(BC)	el_1	ep_1	t_1	*rw*
	3	AC(BC)	el_1	ep_2	t_1	*r*
	4	AC(BC)	el_1	ep_1	t_1	*r*
	1	AC(BC)	el_2	ep_2	t_1	*rw*
	1	AC(BC)	el_2	ep_2	t_2	*r*
	2	AC(BC)	el_2	ep_2	t_1	*r*
O_D	4	ABC	el_1	ep_1	t_1	*rwmd*
	3	ABC	el_1	ep_1	t_2	*rwmd*
	4	ABC	el_1	ep_2	t_1/t_2	*rwm*
	3	ABC	el_2	ep_2	t_1/t_2	*rw*
	4	ABC	el_2	ep_2	t_1/t_2	*r*

The paper built an experimental environment to test and prove the conclusions as shown in Figure 4, including the DHCP Server which is running on the Windows Server 2003. Three IP

domains have been set, which are VLAN 1, VLAN 2, VLAN 3. The addresses are 172.16.66. 200-172.16.66.210, 172.16.66.110-172.16.66.126, 172.16.66.135-172.16.66.145. Subnet mask is 255.255.255.224. In this experiment, we define PC1, PC2, PC3 and PC4. All of them can get IP automatically.

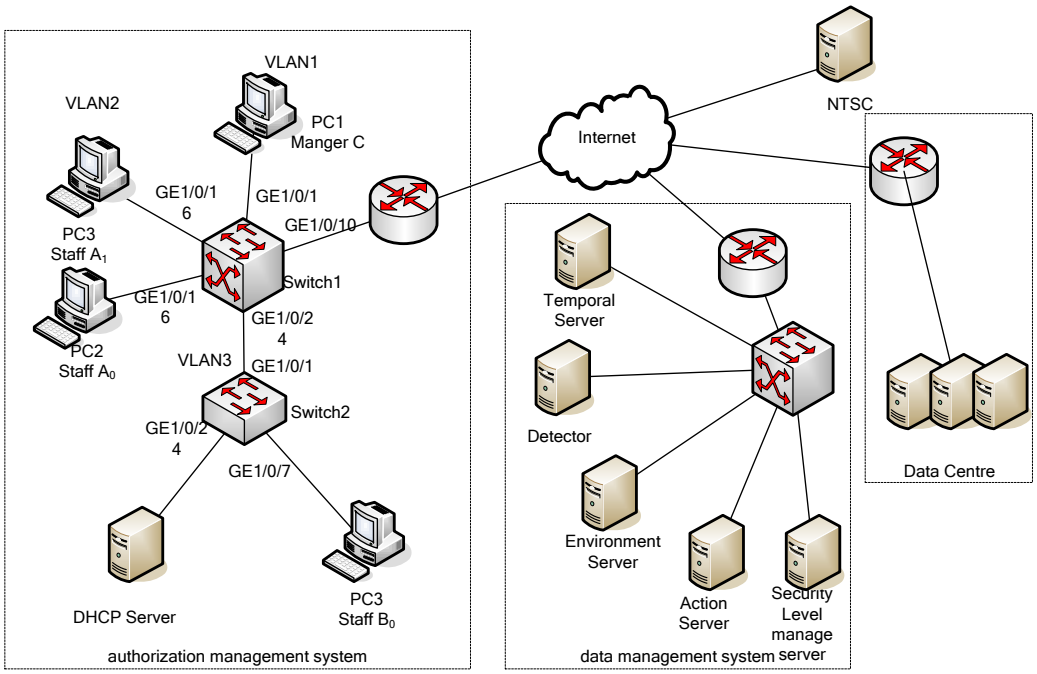

Figure 4. The Network Topological Structure Experimental Environment

When a user needs to access the structured documents, the environment server gets the user name and software information and sends the requirement to detector for the network location. Then the temporal server gets the temporal state from the NTSC. All of the information above will be set to the action server. Finally, the action server and security level server will return the response of the access requirement. The experiment used the Microsoft Visual Studio 2005 to implement.

4. Conclusion

The computer network has been gradually developing to multi-mode, such as ubiquitous computing, mobile computing and cloud computing. Accessing and viewing methods has been developing from a single form to various, such as plant equipment, mobile equipment and handheld equipment. The expression, exchanging and accessing of information have presented features of diversity and openness.

Existing access control models fail to realize fine-grained management on object and to considering multi-level security demand. This paper mainly focuses on access control model and mechanisms. Firstly, the concept of security identity of subject and object is introduced, including security level and access scope, and the description of environment and temporal state are also given. Then, combined with Action Based Access Control model, a new access model based on action and multi-level security is proposed. This new model can meet the demand of multi-level access control in pervasive networks. Finally, a multi-level security management example is given.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (No.61170251), the Key Program of Scientific and Technology Research of Ministry of Education (No.209156), the Beijing Natural Science Foundation (No.4102056), and the Major Science and Technology Project of Press and Publication – Research and Development Project on Digital Rights Protection (No.GXTC-CZ-1015004/05).

References

[1] Department of Defense: Department of Defense Standard, DOD 5200．28．STD：Department of Defense Trusted Computer System Evaluation Criteria(Orange Book), Washington DC: Department of Defense **(1985)**.

[2] J. Campbell, The Future of Multi-Level Secure (MLS) Information Systems **(1998)**.

[3] D. E. Bell, "Looking Back at the Bell-LaPadula Model", Proceedings of the 21st Conference On Annual Computer Security Applications, **(2005)** December Washington, DC, USA.

[4] K. J. Biba, "Integrity Considerations for Secure Computer Systems", MTR-3153 **(1977)**.

[5] S. Jajodia and R. Sandhu, "Toward a Multilevel Secure Relational Data Model", Information Security: An Integrated Collection of Essays, **(1995)**.

[6] Z. Yan, Y. Zhao and B.Wen, "A View-Based Multilevel Security Model", 43(z3) **(2006)**.

[7] F. H. Li, W. Wang, J. F. Ma and M. SangJae, "Action-based access control model", 07, 17(3) **(2008)**.

[8] R. Sandhu, E. Coyne, H. Feinstein, et al., "Role-based access control models", 2,29 **(1996)**.

Authors

Su Mang is pursuing the Ph.D. degree in Xidian University, China. Her research interests include network security and system security. (E-mail:sm1222@163.com)