Action Based Access Control Model for Multi-level Security (MLS)*

Mang Su[1], Fenghua Li[2], Guozhen Shi[3], 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, China;
[3]Department of Electronic Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China)
{sm1222@163.com;lfh@iie.ac.cn;sgz@besti.edu.cn;lili103@besti.edu.cn}

Abstract. 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

Multi-level Security[1] 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. BLP [2] and Biba [3] 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 [4] based on classical BLP model and multi-level security model VMAC [5] based on view, etc.

This paper mainly focuses on the new requirement for access control. The description of object in the ABAC model will be extended. The definition of the subject-object security level will be given. And Action Based Access Control Model

* Foundation: The National Natural Science Foundation of China (No.61172051);The Key Program of Scientific and Technology Research of Ministry of Education (No.209156);The Beijing Natural Science Foundation (No.4102056);The Major Science and Technology Project of Press and Publication - Research and Development Project on Digital Rights Protection (No. GXTC-CZ-1015004/05)

for Multi-level security will be proposed, which can meet the demand of objectified and fine-grained access control for multi-level security of structured documents.

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 do not analyze the environment of the role in detail, including physical positions, hardware platforms, operation systems and networks. Ref [6] presents an Action Based Access Control model (ABAC). 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:

$$R=[RV|RS] \quad (1)$$

RV shows the level of the user in the 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:

$$V=[VC|VS] \quad (2)$$

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

Referring to NIST RBAC [7] and ABAC (Action Based Access Control) [6] structure, the structure for Action Based Access Control Model for Multi-level security is shown as in Fig.1.

3 Conclusion

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.

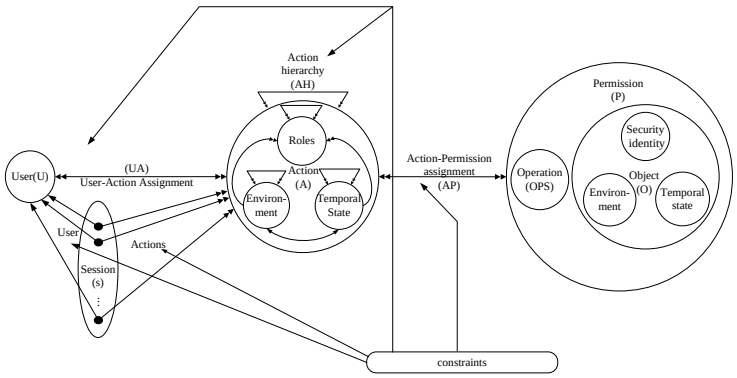

Fig. 1. Action Based Access Control Model for Multi-level security

References

1. The Future of Multi-Level Secure (MLS) Information Systems. 1998. http://csrc.nist.gov/nissc/1998/ proceedings/panelF3.pdf.
2. Bell, D.E.: Looking Back at the Bell-LaPadula Model. In Proceedings of the 21st Conference On Annual Computer Security Applications. Washington, DC, USA: IEEE Computer Society. 2005, 12. 337 - 351.
3. K J Biba, K.L.: Integrity Considerations for Secure Computer Systems. MTR-3153, The Mitre Corporation, 1977, 04.
4. Jajodia, S., Sandhu, R.: Toward a Multilevel Secure Relational Data Model. Information Security: An Integrated Collection of Essays. IEEE Computer Society Press, 1995: 461-491.
5. Yan, Z., Zhao-hua, Y., Wen-yang, B.: A View-Based Multilevel Security Model. Journal Of Computer Research and Devlopment. 2006, 43(z3): 267 - 270(in Chinese).
6. Li, F.H., Wang, W., Ma, J.F., et al: Action-based access control model. Chinese of Journal Electronics, 2008, 07, 17(3): 396 - 401.
7. Sandhu, R., Coyne, E., Feinstein, H., et al: Role-based access control models. IEEE Computer, 1996, 29(2): 38-47.