An Improved Authorization Model in Trust Network

Xianming Gao[1(✉)], Xiaozhe Zhang[1], Baosheng Wang[1], and Huiting Shi[2]

[1] School of Computer, National University of Defense Technology, Changsha 410073, China
{gxm9000,xiaozhe,baosheng}@163.com

[2] School of Mechanical Science and Engineering, HUST, Wuhan 430074, China
huiting@163.com

Abstract. Though traditional authorization models can ensure the security of equipment, they don't offer promise both for good quality of service and for strong system robustness. Therefore, this paper presents a semi-distributed authorization model which splits the single decision point into two roles: core-authorization decision point and sub-authorization decision point. In this model, several decision points can provide authorization service for one and the same equipment. The experimental results prove that this model can effectively reduce authorization service time and has some marked advantages on system robustness.

Keywords: Authorization model · Decision point · Centralized/distributed model · Quality of service · System robustness

1 Introduction

At present, the existing mature technologies are usually based on the access control mechanisms provided by third-party to build a safe and reliable network environment [1, 2]. Most access control mechanisms use the centralized authorization models including the sole decision point, to control the access requests from equipment. Unfortunately, the continuous expansion of target network and the increasing amount of equipment, which results in the sharp decrease of quality of service and poor system robustness. Specially, when several equipment concurrently send requests for access, the subsequent requests have to wait to be disposed until the decision point completes the anterior requests, which substantially increases the authorization service time. In order to enhance the quality of service, some research communities proposed the semi-distributed authorization models [3, 4], which have several decision points being only responsible for disposing the access requests in the corresponding area. In the same way, this model can't provide normal authorization service for equipment in some areas, when one or some decision points have a single point of failure.

Therefore, the traditional authorization models cannot meet practical requirements in terms of quality of service and system robustness. So, this paper presents a semi-distributed authorization model, which adopts the hierarchical multi-decision point mode, and spits the decision point of traditional centralized authorization model into one core-authorization decision point and multiple sub-authorization decision points. This model supports for several sub-authorization decision points to dispose the access

J. Tian et al. (Eds.): SecureComm 2014, Part II, LNICST 153, pp. 10–16, 2015.
DOI: 10.1007/978-3-319-23802-9_2

request of one and the same equipment. So this model still can provide authorization service for equipment, even though some decision points encounter system halted. At last, the experimental results show that authorization service time of proposed model is only 58 % of traditional centralized authorization model when this model deploys five sub-authorization decision points. At the same time, it also can enhance its system robustness by increasing the number of SADPs.

2 Related Works

Many studies have been carried out by industries to ensure the security of equipments. Attempts that solving this problem have resulted in the development of access control mechanism as follows.

For an illustrative purpose, five typical access control mechanisms are presented: Cisco's Network Admission Control (NAC) [5], Microsoft's Network Access Protection (NAP) [6], Juniper's Unified Access Control (UAC) [7], Huawei's Endpoint Admission Defense (EAD) [8], TOPSEC's Trusted Network Architecture (TNA) [9]. We analyze these mechanisms in terms of distributed/centralized, system robustness, authorization service time, and network scale, as shown in Table 1.

Table 1. Comparison of typical access control mechanisms

Technology	Distributed/ centralized	System robustness	Service time	Network scale
NAC	Centralized	Poor	Poor	Medium and small-sized
NAP	Centralized	Poor	Poor	Medium and small-sized
UAC	Centralized	Poor	Poor	Medium and small-sized
EAD	Semi-distributed	Weak good	Weak good	Medium
TNA	Centralized	Poor	Poor	Medium and small-sized

However, these technologies have some lacks in system robustness, quality of service and network scale. Therefore, some research communities propose multiple decision-points model [3, 4], which splits the global authorization strategies into several subsets and issues these subsets to corresponding decision point that only providing authorization service in the defined area.

3 System Overview

The traditional centralized authorization model or semi-distributed authorization model cannot provide normal authorization service, when the failure of network devices or links occurs. Meanwhile, the traditional centralized authorization model also has poor quality of service. Therefore, we propose new authorization model to solve these above problems.

3.1 Design

The decision point in traditional authorization model is a dedicated server, which is equipped to provide authentication service. As illustrated in Fig. 1, our proposed model uses one CADP and multiple SADPs to cooperate the overall functions.

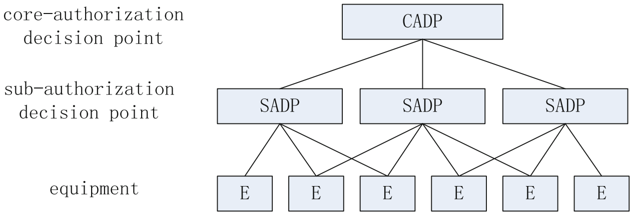

Fig. 1. Proposed authorization model architecture

CADP is the most critical component, which not only provides authorization service, but also is responsible for the planning and distribution of authorization strategies. And SADP only provides authorization service, which can be deployed in network devices rather than in dedicated servers, because SADP is just a special function (or protocol), similar with other routing protocols (such as OSPF, RIP, BGP and so on).

This model splits one decision point into multiple decision points, so how to ensure the consistency of authorization strategies between CADP and SADPs is the primary problem. In startup, CADP stores the global authorization strategies and SADPs don't store any strategy. Only when SADP completes the registration from CADP, CADP will issue the corresponding authorization strategies to this SADP, while CADP sends keeping alive messages to SADPs. If CADP or SADPs can't receive keeping alive messages from others, SADP will clean out authorization strategies, and CADP will cancel the authorization service to make SADP to re-register. On the other hand, the operation of authorization strategies can only be done in CADP, and SADP can get the newest authorization strategies from CADP.

An important feature of this model is that several SADPs can provide authorization service for one and the same equipment, which is the biggest different from other traditional authorization models. Even if an individual SADP has a single of failure, this model is still able to respond to access requests. In this paper, we also define DP trust that refers to the number of decision points providing authorization service for one and the same equipment.

3.2 Data Flow

This authorization service uses client/server authorization mode, which is consistent with traditional authorization system. After SADP completes registration from CADP and obtains authorization strategies, it is able to provide authorization service for network devices. The data flow in this model is as shown in Fig. 2.

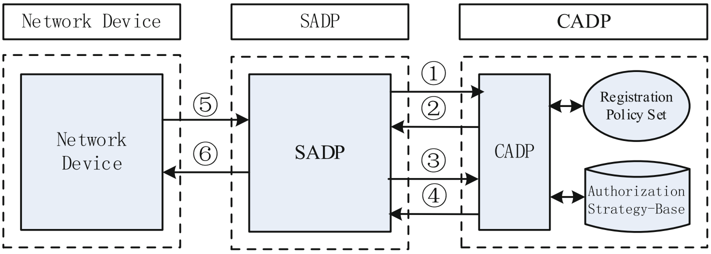

Fig. 2. Data flow

The processing of authorization service in this model is as follows:

(1) In startup, equipments stay in un-accessed status, and firstly send access requests;
(2) After receiving requests, CADP verifies equipment identity, determines whether to allow this equipment to connect based on its Authorization Strategy-Base. At last, it will return the decision to this equipment.
(3) After the equipment receives response from CADP, it will adopt next action based on this response: if it's positive, the equipment sends registration request to CADP; otherwise, it won't adopt any action.
(4) After receiving the request, CADP verifies equipment identity and decides whether to deploy SADP on this equipment based on Registration Policy Set: If it's positive, CADP will issue corresponding authorization strategies to this equipment; Otherwise, CADP ignores this registration request.
(5) Non-accessed equipment sends access request to the defined SADP.
(6) After receiving request, SADP verifies equipment identity, determines whether to allow this equipment to access to the target network, and returns the decision.

4 Simulation and Analysis

This section validates the superiority of ND-OSDAM based on CERNET topology in terms of authorization service time and system robustness.

4.1 Experimental Environment

In order to verify the real performance, this part uses CERNET topology to set up experimental environment, as shown in Fig. 3. CERNET includes 37 nodes and 46 edges, which further contains 8 core-nodes and 8 backbone edges. Every node (except for core-node) has a three layer of complete ten-ary tree, which make network topology include 3227 nodes and 3236 edges.

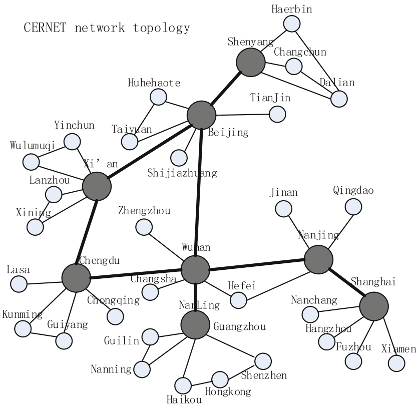

Fig. 3. CERNET topology

Our authorization model, compared with traditional authorization models, can deploy multiple decision points. In order to further analyze the impact of the number of decision point on authorization performance, this paper sets five scenes including different number of SADP, as shown in Table 2. For example, S.2 indicates that two SADPs are deployed respectively in Wuhan and Xi'an.

Table 2. Five scenes

Scene ID	Number of SADP	Location of decision points
S.1	SADP = 1	Wuhan
S.2	SADP = 2	Wuhan, Xi'an
S.3	SADP = 3	Wuhan, Xi'an, Beijing
S.4	SADP = 4	Wuhan, Xi'an, Beijing, Nanjing
S.5	SADP = 5	Wuhan, Xi'an, Beijing, Nanjing, Chengdu

4.2 Authorization Service Time

Authorization service time refers to the time between access request sent by equipment and the equipment having accessed to target network, which is an important indicator to measure the performance of authorization model. To compare the difference between our proposed model and traditional authorization models in terms of authorization service time, this paper uses five scenes in Table 2 to verify that our model has a shorter authorization service time, as shown in Fig. 4.

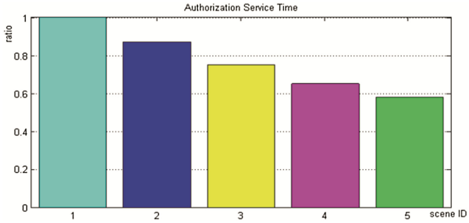

Fig. 4. Authorization service time

Compared with traditional authorization model only having one SADP, our model has a shorter authorization service time. When the number of SADP is two, authorization service time can be reduced by approximate 14 %; when the number is five, authorization service time is only 58 % of traditional authorization model. As the number of SADP increases, authorization service time continually reduces. Thus, our model can greatly reduce the authorization service time, especially, in large-scale network.

4.3 System Robustness

System robustness is an important index to evaluate the feasibility of the authorization system. We adopt the DP trust to measure the system robustness of our model.

Compared with traditional authorization model, our model can support several SADPs to provide authorization service for one and the same equipment, which avoids access requests not to be responded when some SADPs are in invalid. This part calculates the DP trust of every device, as shown in Fig. 5.

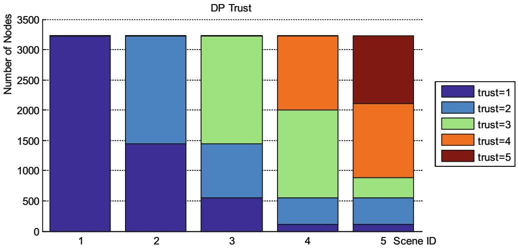

Fig. 5. DP trust

DP trust of each device in traditional centralized authorization model is just one. In our model, DP trust is usually more than one, which is related with the number of SADPs. For example, when it deploys four SADPs, the number of devices is only about 100 of which value of DP trust is one. As the number of SADPs increases, the range of DP trust gradually expands, as well as the value of DP trust continually rises.

DP trust is just one in traditional centralized authorization model. When decision point has a single point of failure, the system cannot provide authorization service for network devices. Even if some SADPs have a single point of failure, our model also offers multiple SADPs to increase the DP trust. It proves that our model has better system robustness than traditional authorization models.

5 Summary and Outlook

Existing mature technologies use access control mechanism to ensure the security of equipment and build a safe, reliable and controllable environment. However, most authorization systems use centralized authorization mode, which does not meet practical requirements in terms of quality of service and system robustness. Thus, this paper presents a new model to solve these problems and to verify the validity of our model.

Acknowledgement. This work is supported by Specialized Research Fund for the Doctoral Program of Higher Education of China (20114307110006) “Research on Technology of Network Quality of Service based on Network Virtualization”.

References

1. Liu, A.X., Chen, F., Hwang, J.H., et al.: Designing fast and scalable xacml policy evaluation engines. IEEE Trans. Comput. **60**(12), 1802–1817 (2011)
2. Marouf, S., Shehab, M., Squicciarini, A., et al.: Adaptive reordering and clustering-based framework for efficient XACML policy evaluation. IEEE Trans. Serv. Comput. **4**(4), 300–313 (2011)
3. Kohler, M, Brucker, A.D.: Access control caching strategies: an empirical evaluation. In: Proceedings of the 6th International Workshop on Security Measurements and Metrics, p. 8. ACM (2010)
4. Hilliker, J.: Speculative authorization. In: Second EECE 512 Mini-Conference on Computer Security, p. 9 (2007)
5. Oliveira, L.M.L., Rodrigues, J.J.P.C., Neto, C., et al.: Network admission control solution for 6LoWPAN networks. In: 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 472–477. IEEE (2013)
6. Arkko, J., Eronen, P., Tschofenig, H., et al.: Quick NAP-secure and efficient network access protocol. In: Proceedings of 6th International Workshop on Applications and Services in Wireless Networks (ASWN 2006), pp. 163–170 (2006)
7. La Padula, L.J.: Formal modeling in a generalized framework for access control. In: Proceedings of Computer Security Foundations Workshop III, pp. 100–109. IEEE (1990)
8. Yuyang, Z., Linxian, Z.: The feasibility of endpoint admission defense in the reconstruction of network security. J. Lishui Univ. **2**, 018 (2007)
9. Huangguo, Z., Lu, C., Liqiang, L.: Research on trusted network connection. Chin. J. Comput. **33**(1), 706–717 (2010)
10. CERNET topology: http://www.edu.cn/20010101/21585.shtml