A TWO LEVEL TRUST ASSESSMENT IN WEB SERVICES ACCESS

Shamila E.S.[1], Ramachandran V.[2]

[1]Research Scholar, Sathyabama University, [2]Professor, Anna University, Chennai.
E-mail: :shamieeshiv@gmail.com

ABSTRACT

In web service technology the hazard of security is growing, such as the problem of access control. Recently, trust management is considered as an effective approach for enhancing web services security. In this paper, we focus on a two-level trust evaluation based access control system for web service environment. The model considers direct trust and recommended trust comprehensively between domains. This system is dynamic and can realize access control across domains by evaluating the comprehensive trust correctly and effectively. This trust model has a good performance even though under the condition of malicious recommendations by malicious domains that the percentage of secure access is high.

Keywords Trust, Webservice, Access control

I. INTRODUCTION

A web service is defined by the W3C as "a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-process able format".

Access control which is to restrict the use of resource is an important safeguard in security. An **access control system** is a system which enables an authority to control access to areas and resources in a given physical facility or computer-based information system. An access control system, within the field of physical security, is generally seen as the second layer in the security of a physical structure.

Access control is, in reality, an everyday phenomenon. A lock on a window is essentially a form of access control. A PIN on an ATM system at a bank is another means of access control. The possession of access control is of prime importance when persons seek to secure important, confidential or sensitive information and equipment.

Trust [2] is a complex subject relating to an entity's belief in honesty, trustfulness, competence and reliability of another entity.

Trust Services are a set of professional assurance and advisory services based on a common framework (that is, a core set of principles and criteria) to address the risks and opportunities of IT. However, most of the existing trust evaluation models are built based on the direct experiences and recommendations of other entities whose recommendations are known to be reliable. Here in this paper we proposed to compute every entity's trust degree and reputation value, and set a threshold of trust degree for every entity to restrict access.

II. A SECURED TRUST ENVIRONMENT IN WEB SERVICE

An access requester sends a request of resource access to the Access Control Management Center(ACMC) in local domain. The Access Control Management Center of user domain delivers the request and sends the requester's trust weight to the Access Control Center of resource domain. The Direct Trust Module calculates the direct trust vector. Because the direct trust vector is often used, it can be calculated beforehand and stored to a Database. The Trust Reasoning Module gets the trust vectors of the user domain from all other domains and calculates the recommended trust vectors by trust reasoning. Then the Access Control Management Center calculates the comprehensive trust remark of the access request domain by second level trust evaluation. The Access Authorization Module awards an access certificate to the access requester if the request is permitted after decision-making. The access requester accesses the resource and the resource provider records the related access information for the next evaluation.

A trust based access control in Web Services, which proposed to compute every entity's trust degree and reputation value, and set a threshold of trust degree for every entity to restrict access.

The trust management center will update entities' trust degree and reputation value after every transaction by the feedback from entities which participate in the transaction.

This method can easily calculate trust degree between entities and the feedback mechanism will restrict the behavior of entities very well. But the representation of trust is excessively precise which does not confirm to the attribute of trust.

- The core of the Trust Evaluation Based Access Control contains three modules in Access Control Center.
- Direct trust Module is used to calculate direct trust between domains by first level trust evaluation.
- Trust reasoning Module is used to calculate the recommended trust.
- Access Authorization module is used to receive request and make decision of authorization.

A. The Elements of Trust Assessment for Access Control

The domain in web service is the organization of entities which have independent management policy.

There are four main elements of direct trust evaluation for access control in web service:

(i) Reliability of Behavior (RB)

The reliability of behavior of entity means that the behavior of entity in transaction accords with the behavior that was agreed before transaction started.

(ii) Ability of self-Protection (AP)

If an entity is lack of ability of self-protection and intruded by virus or Trojan horse, the entity may make bad behavior out of control.

(iii) Responsibility of Management (RM)

The responsibility of management means that the behavior of entity in transaction accords with the local trust weight recommended by the entity's domain before transaction starts.

(iv) Success ratio of Transactions (ST)

The success ration of transactions from entity E in domain X to domain Y means that the ratio between the number of successful transactions and the total number of transactions from entity E in domain X to domain Y.

B. Trust Assessment

Direct trust refers to a situation in which two individuals have established a trusting relationship between themselves. The vector $b = (b1, b2, b3, b4, b5, b6)$ is a trust evaluation vector which considers four kinds of elements omprehensively and bi represents the degree of the remark of vi. And b can be calculated by the following formula,

$$b = wo\,R = (b_1, b_2, \ldots, b_6)$$

where

$$b_1 = \overset{4}{\underset{i=1}{v}}(w_i \cdot r_y), j = 1, 2, \ldots 6$$

v means the operation of getting maximum.

(i) Trust Reasoning

In this section we are calculating the recommended trust vector. Trust reasoning is used to calculate recommended trust, and this paper only considers one-level trust reasoning. For instance, there are three domains named A, B and C. So the trust evaluation vector of A to C from B's recommendation is $bABC$, which can be calculated as follows:

$$b_1^{ABC} = \frac{\overline{b}_k^{AB} \cdot \overline{b}_1^{BC}}{1 + (1 - \overline{b}_j^{AB})\,(1 - \overline{b}_j^{BC}}, j = 1, 2, \ldots, 6$$

C. Trust Evaluation

we have to calculate the comprehensive trust remark and to make decisions based on the result. The vector of trust weight for trust evaluation between domain A and B is

$$w = (\overline{T}_{AB}, \overline{T}_{AX_1}, \ldots, \overline{T}AN_{n-2})$$

where

$$\overline{T}_{AB} = \frac{T_{AB}}{T_{AB} + \sum_{i=1}^{n-2} T_{AX_1}} \cdot \overline{T}_{AX_1} = \frac{T_{AX_2}}{T_{AB} + \sum_{i=1}^{n=2} T_{AX_1}}$$

$$j = 1, 2, \ldots n-2$$

Then, the comprehensive trust vector $b = (b1, b2, b3, b4, b5, b6)$ can be calculated by the formula 1. Finally, the comprehensive trust remark of b is vj, which is determined by the maximum membership degree principle:

$$v_j j = \{ i \mid \max i < 6 (b_1) \}\}$$
$$1 \leq$$

III. ARCHITECTURE AND WORK FLOW OF ACCESS CONTROL

The architecture of our proposed model is given in the figure 1.

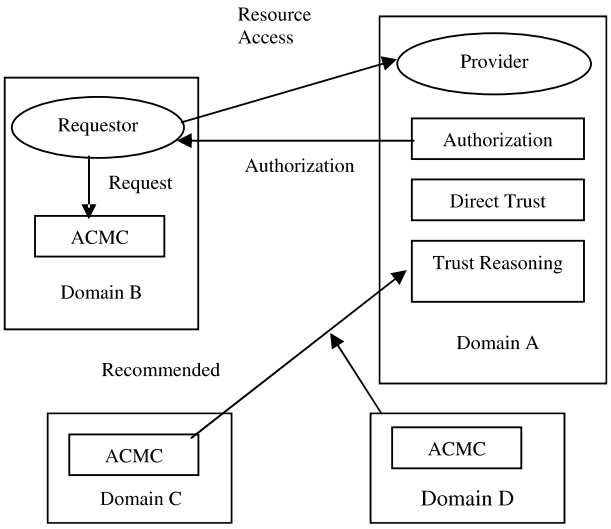

Fig. 1. Architecture of Access Control System

The working flow of access control is summarized as follows:

1. An access requester sends a request of resource access to the Access Control Management Center in local domain.
2. The Access Control Management Center of user domain delivers the request and sends the requester's trust weight to the Access Control Center of resource domain.
3. (a) The Direct Trust Module calculates the direct trust vector. Because the direct trust vector is often used, it can be calculated beforehand and stored to a Database.

   (b) The Trust Reasoning Module gets the trust vectors of the user domain from all other domains and calculates the recommended trust vectors by trust reasoning.
4. Then the Access Control Center calculates the comprehensive trust remark of the access request domain by second level trust evaluation.
5. The Access Authorization Module awards an access certificate to the access requester if the request is permitted after decision-making.
6. The access requester accesses the resource and the resource provider records the related access information for the next evaluation.

IV. IMPLEMENTATION

In this section, we describe scenario to evaluate of our model. To simplify the experiments, we assume that service X requested by service requestor A, which has obtained identities authentication by objects authorities, and direct trust vector, recommended Trust Vector and comprehensive trust vector was calculated. The implementation was done through dot NET for online shopping. The screenshots are as follows

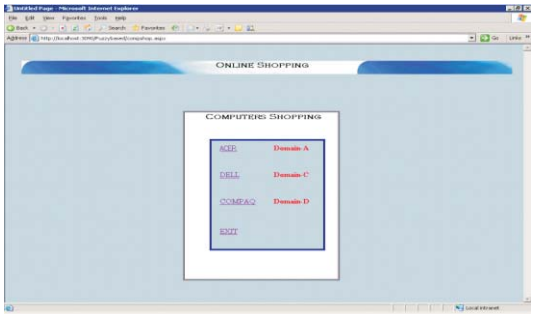

Fig. 2. Domain

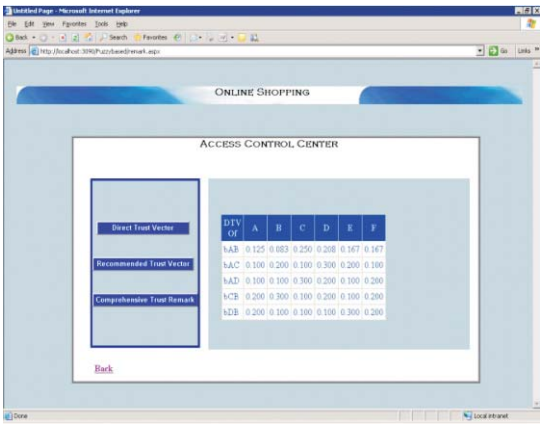

Fig. 3. Direct Trust Vector

This trust model has a good performance even though under the condition of malicious

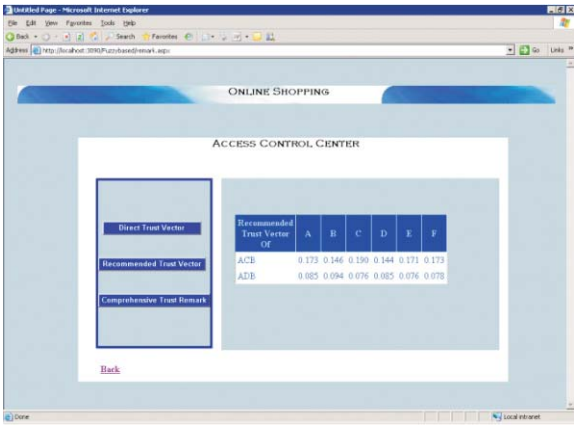

Fig. 4. Recommended Trust Vector

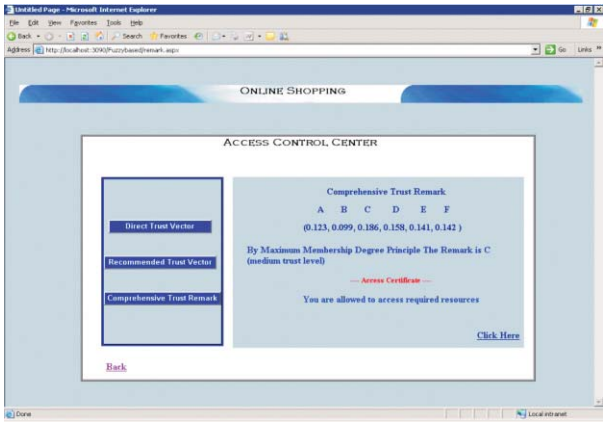

Fig. 5. Comprehensive Trust Vector

recommendations by malicious domains that the percentage of secure access is above 80% when the percentage of malicious domains is below 40%.

V. CONCLUSION

This paper presents a two-level trust assessment based access control scheme for interdomain in web service environment and the model considers direct trust and recommended trust comprehensively between domains. So this scheme is dynamic and can realize access control across domains by evaluating the comprehensive trust correctly and effectively.

VI. REFERENCES

[1] Trusted Computing Group [EB/OL]. http://www.trustedcomputinggroup. org/home. 2005.

[2] Maheswaran F.A. and Maheswaran M., 2002 “Evolving and managing trust in grid computing systems”, Proceedings of the 2002 IEEE Canadian Conference on Electrical Computer Engineering.

[3] Chuang Lin, and Xuehai Peng, 2005 “Research on trustworthy network”, Chinese Journal of Computers, Vol.28, No.5, pp. 751-758.

[4] Miao Liu, Wei Zhang, Huailiang Liu, 2007 “Specification of access control policies for web services”, CIS workshops 2007 International conference on computational intelligence and security,PP.476- 479.

[5] Blaze M., Feigenbaum J., Lacy J., 1996 “Decentralized Trust Management”, Proc. of the 1996 IEEE Symp. on Security and Privacy, Washington: IEEE Computer Society Press, pp. 164-173.

[6] Yi Chen, Junzhou Luo, Xudong Ni, 2008 “A Fuzzy Trust Evaluation Based Access Control in Grid Environment”, In Proceedings of the The Third ChinaGrid Annual Conference, 978-0-7695-3306-3/08.

[7] A Flexible Trust Model for Distributed Service Infrastructures, Zhaoyu Liu, Stephen S. Yau, Dichao Peng, Yin Yin, 2008 In Proceedings of the 11th IEEE Symposium on Object Oriented Real-Time Distributed Computing (ISORC), 978-0-7695-3132-8/08.

[8] Ali Shaikh Ali, Simone Ludwig A., Omer F.Rana, 2005 “A Cognitive Trust-Based Approach forWeb Service Discovery and Selection”, In the proceedings of Third European Conference on Web Services (ECOWS’05) 0-7695-2484-2/05.

[8] Xudong Ni and Junzhou Luo, 2007 “A Trust Aware Access Control in Service Oriented Grid Environment”, The 6th International Conference on Grid and Cooperative Computing.