Time-Space Trust in Networks

Shunan Ma[1], Jingsha He[2] and Yuqiang Zhang[1]

[1]College of Computer Science and Technology
[2]School of Software Engineering
Beijing University of Technology, Beijing 100124, China
msn1679@126.com, jhe@bjut.edu.cn

Abstract. Trust is part of our daily life and thus can be used as a mechanism for providing security in computer networks. In this paper, we consider the time and space nature of trust, and propose the concept of time-space trust which includes two factors: time and place, and compute a value for trust.

Keywords: trust, security, time, space

1 Introduction

Trust is a part of our daily life and thus can be used as a tool to reduce the complexity of making access decisions, which can be accomplished by using trust to provide security [1]. In recent years, many researchers have applied trust to the dynamic environments. Trust models have been proposed to control anonymity, unpredictability and uncertainty [2-5]. The concept of trust is originally derived from social sciences and is defined as the degree of subjective belief about the behaviors of a particular entity [6]. Blaze first introduced the notion of "trust management" and identified trust as a separate component of security services in networks [7]. In recent years, many researchers have also applied trust to solving network security problems in which measurement of trust relationship between entities in networks has become a key issue. However, the application of classic mathematics functions to compute trust values often leads to inaccuracy. The reason is that trust has the nature of subjectivity and fuzziness.

In this paper, we consider the time and space nature of trust, and propose the concept of time-space trust which includes two factors: time and place, and compute a value for trust.

2 Trust Computation

Trust is very subjective that reflects one body's subjective expectation on another body's future actions based on their previous exchanges. Trust exhibits three characteristics: dynamism, subjectivity and ambiguity. Every user has a particular

trust value towards others at a certain point of time or during a certain period of time. The trust value changes as a result of interactions with others.

Given each factor of trust, suppose every factor's trust value is T_0, T_1, …, T_{n-1}, respectively, and the weight of each factor is W_i, trust value can be computed as: $T = \sum_{i=0}^{n-1}(W_i \times T_i)$. For different application, factors of trust can be set specifically. In addition, trust computation consists of two parts: determine each factor's trust evaluation method to get each factor's trust value and each factor's weight allocation.

To reflect dynamicity of trust in an open environment, we compute trust with two factors introduced above as follows:

$$T = \alpha_1 T_1 + \alpha_2 T_2 \quad \text{in which} \quad \alpha_1 + \alpha_2 = 1 \tag{1}$$

In this paper, we can define the weights of time and space is 0.5.

According to an object's property and a subject's behavior history information, we can establish tables for the time and place of the trust evaluation rules. For example, the trust value of a subject who accesses a recreation resource during work hours is lower than that during spare time. For accessing educational resources, trust value of a subject whose IP address belongs to an educational network is higher than that to a non-educational network.

According to the property of each resource, time can be divided into n periods. For each time period $[t_i,t_j]$, we formulate corresponding trust interval $[T_i,T_j]$, which means that when a subject accesses the resource at time t, if $t_i \le t \le t_j$, then randomly generate a trust value $T \in [T_i,T_j]$. To avoid denial of access to an object in high crime periods, we use the following method. For each time period $[t_i,t_j]$, when the number of accesses reaches a certain value, count the total access number m and fraud number k and the fraud probability in this period is p=k/m. Then, randomly generate a trust value T_x at time x where $T_x \in [T_i,T_j]$. The trust value of time factor is then

$$T = T_x \times (1 - p). \tag{2}$$

According to the time attribute of resources, trust evaluation table for the time factor is shown in Table 1.

Table 1. Trust evaluation table for the time factor.

Time period	$[t_0,t_1)$	$[t_1,t_2)$	$[t_2,t_3)$	…	$[t_{n-1},t_n)$
Trust interval	$[T_0,T_1)$	$[T_1,T_2)$	$[T_2,T_3)$	…	$[T_{n-1},T_n)$
Fraud probability	p_0	p_1	p_2	…	p_{n-1}

We use IP addresses as the place factor. Subjects can be classified according to the property of an object. For example, subjects can be classified into subjects in the same

subnet, domain, important service segment and general service segment. We then formulate the trust evaluation intervals. For each network segment, when the length of access time reaches a certain number, we count the fraud probability in this network segment. For a given IP address, we can use Formula (2) to compute the trust value of the IP factor. Trust evaluation table for the IP factor is shown in Table 2.

Table 2. Trust evaluation table for the IP factor.

IP address	Same subnet	Same segment	Important service	⋯	General service
Trust interval	$[T_0,T_1)$	$[T_1,T_2)$	$[T_2,T_3)$	⋯	$[T_{n-1},T_n)$
Fraud probability	p_0	p_1	p_2	⋯	p_{n-1}

4 Conclusion

In this paper, we considered the time and space nature of trust, proposed the concept of time-space trust which includes two factors: time and place, and computed a value for trust.

References

1. Fan, T., Guo, H.: Attributed Based Access Control of Collaborative Design Systems. Advanced Materials Research, Vol. 267, 80--85 (2011)
2. Nagarajan, A.: Dynamic Trust Enhanced Security Model for Trusted Platform based Services. Future Generation Computer Systems, Vol. 27, No. 5, pp. 564--573 (2011)
3. Alboaie, L., Vaida, M.F.: Trust and Reputation Model for Various Online Communities. Studies in Informatics and Control, Vol. 20, No. 2, pp. 143--156 (2011)
4. J. Jiang, H. Bai and W. Wang, "Trust and cooperation in peer-to-peer systems". Springer-Verlag, pp. 371-378, 2004.
5. F. Feng, C. Lin, D. Peng and J. Li, "A Trust and Context Based Access Control Model for Distributed Systems". Proc. 10th IEEE International Conference on High Performance Computing and Communications, pp. 629-634, Washington, 2008.
6. Cook, K.S. (editor): Trust in Society, Russell Sage Foundation Series on Trust, Vol. 2 (2003)
7. Blaze, M., Feigenbaum, J., Lacy, J.: Decentralized Trust Management. In: IEEE Symposium on Security and Privacy, pp. 164--173 (1996)