Analysis of Trust-based Access Control Using Game Theory

Jingsha He[1*], Shunan Ma[2,3] and Bin Zhao[1]

[1]*School of Software Engineering, Beijing University of Technology*
Beijing 100124, China
[2]*College of Computer Science, Beijing University of Technology*
Beijing 100124, China
[3]*Institute of Information Engineering, Chinese Academy of Sciences*
Beijing 100093, China

jhe@bjut.edu.cn

Abstract

Access control is an important security mechanism that is used to limit user access to information and resources and to prevent malicious users from making unauthorized access. Traditional access control models are well suited for centralized and relatively static environments in which information about subjects and objects are known in priori, but they can hardly meet the needs of open and dynamic network environments. Access control in open network environments must therefore adapt to dynamic addition and deletion of subjects and objects. In this paper, we use game theory to analyze trust-based access control to help compute trust values that involve several factors. By viewing access control as a game played between the requester and the provider entities, we can develop strategies that would motivate subjects to make honest access to objects continuously to get the most payoffs.

Keywords: *Access Control; Trust; Game Theory; Network Environments*

1. Introduction

Trust is an important aspect of decision making for Internet applications and also influences the specification of security policies [1]. Trust is a part of our daily life and thus can also be used as a tool to deal with the complexity of making decisions in access to network information and resources, which can be accomplished through using trust to provide security. In recent years, many researchers have applied trust to deal with various problems in dynamic environments. As part of the effort, trust models have been proposed to control anonymity, unpredictability and uncertainty [2]. However, there may be more than one or a few factors that can affect trust, such as attributes associated with entities, time, network conditions and the behavior history of entities.

Access control is a prime means in network security, for it is used to constrain access to critical information and resources in computer systems and networks that need to be protected. When a user entity issues a request for access to a piece of information or resource, access control performs necessary checks and makes an authorization decision regarding whether to grant or to deny the request based on established access control policies.

* The corresponding author (email: jhe@bjut.edu.cn).

Access control has gone through several phases of development in the past, resulting in at least three major types: discretionary access control (DAC) [3], mandatory access control (MAC) [4] and role-based access control (RBAC) [5]. All these models are essentially based on user identities in which each subject and each object is identified by a unique name and access control is based on successful identification and authentication of a subject before an access control decision is made based either directly on the identity of the subject in the cases of DAC and MAC or indirectly on a role to which the subject is assigned to in the case of RBAC. Since they are all identity-based in nature, DAC, MAC and RBAC are effective primarily in closed and relatively static environments such as organizations that deal with a set of known users who access a set of known resources and services within the organizations.

Traditional access control models do not work well in open, dynamic network environments such as the Internet. This is because not enough information about the entities that interact with one another and the resources to be accessed is always known in advance. Thus, it is almost impossible to predefine access permissions for an entity. Thus, since all the major traditional access control models rely on successful authentication of predefined users, they become unsuitable for open, dynamic network environments. Access control in these environments must dynamically adapt to dynamic addition and deletion of entities.

In this paper, we propose a method for the construction and computation of trust values as the basis for access control. We then apply game theory to analyzing trust-based access control to develop strategies that would motivate a subject to make honest access to an object continuously, which would contributes to enhancing the effectiveness of access control in the protection of information and resources in open network environments. Our trust computation and game theory based analysis show that trust-based access control is feasible and effective strategies can be established for the design of highly secure access control mechanisms.

The rest of this paper is structured as follows. In the next section, we review some related work in access control and in trust management and applications. In Section 3, we propose a method and the procedure for the evaluation and computation of trust values by involving several factors for access control to information and resources in open network environments. In Section 4, we analyze our trust-based access control using game theory in which we view access control as a game played by the resource requester and the resource provider in order to derive effective strategies that would motivate the requester to behave in an honest manner in making continuous access to the same resource. Such strategies are very important in the design of access control mechanisms in addition to the traditional design involving mostly access condition checks. Finally, we conclude this paper in Section 5 in which we also discuss some future work.

2. Related Work

Trust models have been developed to control anonymity, unpredictability and uncertainty in network communications [6]. The concept of trust is originated from social sciences and is defined as the degree of subjective belief about the behaviors of a particular entity [7]. Blaze first introduced the notion of “trust management” in which he also identified trust as a separate component of security services in networks [8]. A fuzzy trust model proposed for Grid computing integrated history factors and new evidence in calculating trust [9]. In recent years, many researchers have also applied

trust to solving access control problems in which measurement of trust relationships between entities in networks has become a key issue.

Access control is a security mechanism that allows owners of information and resources to define, manage, and enforce access conditions for each protected resource. Most major access control models that have been developed and widely used, *i.e.*, the DAC, the MAC and the RBAC models, are aimed at special environments and are mostly suitable for closed and relatively static organizational settings. Therefore, They are not well suited for use in open and dynamic network environments due to the lack of flexibility and efficiency.

Semantic access control (SAC) [10] is a new kind of access control model in which machine reasoning is used at a semantic level to determine whether to let requests go through according to the semantic descriptions of policies, requests, resources and other entities. Compared to traditional access control, SAC is more scalable, more applicable to dynamic environments with heterogeneous and complex access criteria. But the foundation of SAC is based on semantic web technologies, thus making it difficult to be applied in all access control fields. Management of access control for distributed environments to support dynamic collaboration is discussed in [11], in which along with the development of ontology and semantic web, context-based access control was designed. Different from the traditional access controls, context-based access control examines context as the key for access control, *i.e.*, the context of a requestor is examined to decide whether to grant to the requestor the requested access permissions.

With the research of trust, some researchers have thought about the application of trust in access control. In [12], a method was proposed to incorporate the concept of trust into RBAC to apply trust to access control. The concept of access control based on trust levels was discussed [13] in which a role-based access control model was proposed that assigns roles to users based on their trust levels. In [14], a trust and context based access control model (TCAC) was proposed to extend the RBAC model with trust and context. In the model, only when the user's trust level is not lower than the trust threshold and the context information satisfies the limit in access control policy, will the user be given some roles, which leads to access permissions for the user. More work has been done in trust-based access control [15], which uses trust on the requestor as the key for access control. The owner of resource gives access permissions to the requestors whom he/she trusts. In all the work proposed above, although trust has been introduced into access control models, it didn't take into account many factors that affect trust.

3. Trust Computation

Trust is very subjective, which reflects someone's subjective expectation on someone else's future actions based on their previous experiences. In general, trust changes dynamically according to the behavior of users. Every user has a particular trust evaluation towards others at a certain point of time or during a certain period of time. Trust value will change as the result of interactions between users. In this paper, we compute the trust value by considering several factors as follows.

Static factors include ID, IP and the domain of entity. We use the notation T1(attribute) as the attributes for trust evaluation.

The meaning of behavior credibility speculation is that we can predict an entity's credibility of future behavior based on its behavior in the past. We use T2(t_i, behavior) to denote the influence of the entity's behavior to trust evaluation at time t_i.

We compute an entity's trust degree based on external factors such as the trust evaluation of neighboring nodes to the present node. We use T3(C, t, B) to denote trust evaluation of a neighboring node C on present node B at time t.

T4(other behavior) denotes the influence of other on-going interactions on the trust evaluation of node B.

Network communication environment also affects trust evaluation of node A on node B, which may include bandwidth and channel security. We use T5(A, B) to denote the influence of network environment to trust evaluation.

To show the dynamic nature of trust in open network environments, we use the following formula to compute a trust value:

$$T(A,B) = \frac{a}{n}\sum_{i=1}^{n} T_1(attibute_i) + \frac{\beta}{n}\sum_{i=1}^{n} T_2(t_i, behavior_i) + \frac{\phi}{n}\sum_{i=1}^{n} T_3(C_i, t_i, B) + \frac{\gamma}{n}\sum_{i=1}^{n} T_4(otherbehavior_i) + \mu T_5(A,B) \quad (1)$$

in which

$$\alpha + \beta + \varphi + \gamma + \mu = 1 \quad (2)$$

The values of $\alpha, \beta, \varphi, \gamma, \mu$ are given as a set of optimal weights which reflects the dynamic and uncertainty of trust in a distributed dynamic environment, where $\alpha, \beta, \varphi, \gamma, \mu \in [0,1]$ and $\alpha + \beta + \varphi + \gamma + \mu = 1$.

In this paper, we define the scoring standard for each static attribute of an entity as follows. For any static attribute that can affect trust evaluation between entities, we suppose that the attribute has m possible cases. Trust interval is then divided into m disjoint subinterval in which every case of the attribute corresponds to a subinterval of the trust. The scoring standard above can also be adapted to the evaluation of network communication condition. Table 1 shows an example of the scoring standard for the IP attribute in which the trust interval is A=[-10,10].

Table 1. Scoring Standard for the IP Attribute

IP Attribute	Same Segment	Same Domain	Neighboring Domain
Subinterval	[8,10]	[6,8]	[3,6]

We define the scoring standard for behavior speculation as follows. According to interaction results between entities, the behavior history can be divided into k possible cases, such as trusted, hostile and attempted hostile and so on. Every case of k corresponds to a subinterval of trust. Table 2 shows an example of the scoring standard for an entity's history behavior speculation in which the trust interval is A=[-10,10].

Table 2. Scoring Standard for Behavior Speculation

History behavior	Trusted	Hostile	Attempted Hostile
Subinterval	[8,10]	[-10,0]	[0,8]

Generally speaking, access behavior has time characteristics. According to access behavior history, we then establish the relationship between the time factor and trust. We divide access time into four periods: frequent, moderate, rare and impossible. Table 3 shows an example of trust values that correspond to the access time.

Table 3. Trust Interval Corresponding to Time

Access time	Frequent	Moderate	Rare	Impossible
Trust interval	[0.8,1]	[0.5,0.8)	[0.2,0.5)	[0,0.2)

We consider network conditions as a factor which would affect trust computation. Network conditions mainly include bandwidth and channel security. We divide network conditions into four general cases: very safe, safe, moderate and dangerous. An example of network conditions that correspond to trust values is shown in Table 4.

Table 4. Trust Intervals Corresponding to Network Conditions

Network condition	Very safe	Safe	Moderate	Dangerous
Trust interval	[0.9,1]	[0.6,0.9)	[0.3,0.6)	[0,0.3)

Weight allocation to each factor is a multiple attribute decision problem. There are several weight allocation methods, such as information entropy method, multi-objective optimization method and fuzzy aggregation method. In this paper, the weights of these four factors are each initialized to 1/4, which means an equal allocation. The information and subjects' trust and access feedback results are considered as sample information and stored in files. When the sample reaches a certain number, then we use information entropy weight allocation method [16] to calculate the weight for each factor.

Following is the procedure in which the information entropy method is used:

(1) Determine the sample information which needs to be dealt with and extract every factor's data.

(2) Establish the fuzzy similarity relationship.

(3) Use the fuzzy equivalence closure method to derive a fuzzy equivalence matrix and then determine the classification number of factors.

(4) Determine the mutual information content of each factor at every confidence level.

(5) According to the information content of factors, determine their weight value.

For access control, every object entity will build and maintain its own history access record table to store subject entities' access behavior history to provide support for

future behavior trust computation. The history access record table includes: subject, access time, access behavior, and trust value. Every factor's weight and the calculated trust value will also be stored in files.

The formula that we have proposed for trust computation includes factors such as entities' IP attribute, time, behavior history, and network conditions, which can primarily describe the dynamism and the uncertainty of trust in open and dynamic network environments.

4. Analysis of Access Control as a Game

4.1. The Game Theory

Game theory is a field of applied mathematics that can be used to describe and analyze interactive situations to make decisions for players in the interactive situations [17]. It provides an analytical tool to predict the outcome of complex interactions among rational entities, where rationality requires strict adherence to a strategy based on perceived or measured results. Game theory has been widely used in many applications in economics, political science, biology, and sociology. The first application of game theory in engineering and computer science happened in early 1990s [18].

Game theory describes the decision scenarios of two or more players as games in which each player chooses actions to bring the best possible payoffs for the player while anticipating the rational actions from other players [19]. Game is a precise description of the strategic interactions that include the constraints and payoffs that the players can take, but says little about what actions the players might actually be taking. Generally speaking, a game includes four basic elements.

(1) Player: a basic entity in a game that is tasked with making choices for certain actions. A player can represent a person, a machine, or a group of individuals in a game.

(2) Strategy: a plan of actions in the game that a player can take during game play.

(3) Order: the sequence of chosen strategies by the players.

(4) Payoff: the positive or negative reward to a player for a given action he/she takes in the game.

4.2. Access Control as a Game

Access control in open network environments can be viewed as a game that is played between the resource requestor and the resource owner. From the perspective of the resource owner (or the subject), getting access permissions is the payoff while from the perspective of the resource owner (or the object), maintaining the security of the resource over a long period of time is the payoff.

To simplify the strategy space of a game, we classify a subject's access behavior as either honest access or malicious access. Meanwhile, an object is a resource with an associated permission. Object then becomes a logical concept. For example, if a file in the physical concept has two permissions: read and write, the file can be logically divided and viewed as two logical objects: read file and write file. Therefore, the strategies for the object have two choices: permit access and deny access, which can simplify the strategy space in the game and improve the efficiency of decision-making.

When applying game theory to analyzing trust-based access control, the four elements of the game can be as follows:

(1) The players in access control are the subjects and the objects in the open network environments.

(2) The strategies of a subject are honest behavior and malicious behavior. The strategies of an object are permit access and deny access.

(3) According to the process of access to a resource, after the subject makes an access request, the object needs to assign some access permission to the subject first and then the subject performs access to the resource. Therefore, the object is the earlier player, and the subject is the later player.

(4) After the subject carries out the honest or malicious strategy, the subject gets the benefit or the loss.

In a dynamic game, there is a close relationship between players' strategies and their behavior trust. Therefore, trust is a key issue in dynamic games. In trust-based access control, the trust of an object on a subject depends on the subject's history of access behavior. There are many trust evaluation methods, in which direct trust and recommendation trust are used to denote the subject's information, and access feedback mechanism or reputation are used to denote the impact of subjects' history access information for trust evaluation.

In dynamic games with incomplete information, two important key factors that influence the game result are the order of the game and whether players know each other's information. In a trust-based access control game, the object is the earlier player. Namely, the order of the game is determinate.

There are two types of important information in a game: prior information and payoff information. In a game process, players amend the prior information by observing the game result. After the amendment, the prior information becomes posterior information. Through continuous amendment of information, the game can reach the equilibrium. Moreover, information amendment is an important difference between dynamic games and static games.

We can see from above that game theory can be readily applied to analyzing trust-based access control in which the recommendation trust and direct trust in trust evaluation can be viewed as prior information while the access feedback can be viewed as posterior information. In trust-based access control, the trust value for a subject affects permission assignment and the trust value and assigned access permission for the subject is the payoff information. In general, game-related information in trust-based access control can be described using Figure 1.

To motivate a subject to make access to a resource in an honest manner, we design a constraint mechanism as follows: if a subject makes access to an object in a malicious manner, it will never be allowed to access the same object again. If the subject makes access to an object in an honest manner, a discount of rate σ ($\sigma \in (0,1]$) will be used to denote the increase of payoff during the next honest access by the same subject.

The strategy that a subject selects to make a malicious access in order to get more payoffs is:

$$Q = S_c\_Income - S\_Income \tag{3}$$

The subject's potential loss is that it will never be allowed to access the same object again. Meanwhile, the expected payoff for the subject to continuously make honest access can be expressed as follows:

$$W = S\_Income + S\_Income \cdot \sigma + S\_Income \cdot \sigma^2 + S\_Income \cdot \sigma 3 \ldots = \frac{S\_Income}{1-\sigma} \quad (4)$$

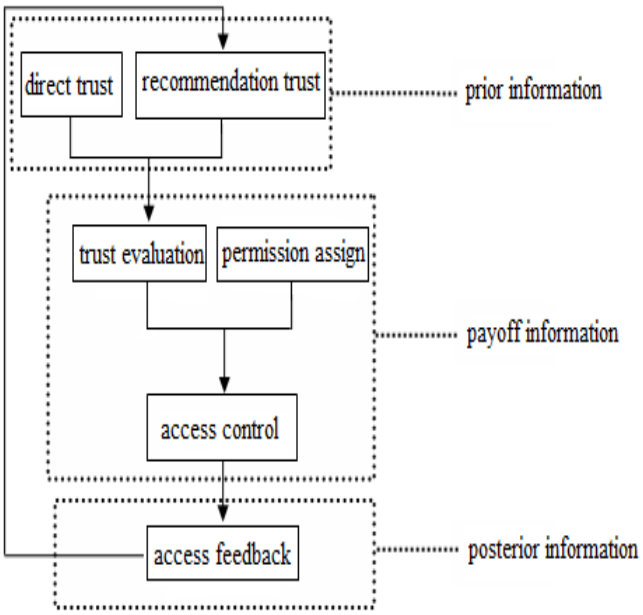

Figure 1. Game Information in Trust-Based Access Control Model

If $W > Q$, the subject believes that honest access in the future will get it more payoffs, so it will select the honest access strategy, namely,

$$\frac{S\_Income}{1-\sigma} > S_c\_Income - S\_Income \quad (5)$$

We can thus derive from Formula (5)

$$\sigma > \frac{(S_c\_Income - 2S\_Income)}{(S_c\_Income - S\_Income)} \quad (6)$$

From Formula (6), we can arrive at three cases:

(1) If $S_c\_Income \le S\_Income$, the subject should pursue the most payoffs. So, the subject would select the honest access strategy.

(2) If $S\_Income < S_c\_Income \le 2S\_Income$, $W > Q$ still holds because $\sigma \in (0,1]$ and $\frac{(S_c\_Income - 2S\_Income)}{(S_c\_Income - S\_Income)} \le 0$. The subject should still select the honest access strategy.

(3) If $2S\_Income < S_c\_Income$, we should set appropriate discount rate so that Formula (6) can hold in order to motivate the subject to select the honest access strategy.

5. Conclusion

In open and dynamic network environments, not every resource requestor can be known in advance by the resource owners because of the open and dynamic characteristics. Trust can thus be used as a tool to deal with the complexity of making access decisions, which can be accomplished by using trust to provide security. By considering several common network factors that affect trust, we can compute trust values on entities using these factors and develop trust-based access control.

At the same time, access control in open network environments can be viewed as a dynamic game issue between subjects and objects. From the perspective of game theory, we analyzed the game information in trust-based access control. Furthermore, In order to motivate a subject to make honest access to an object, we designed a constraint mechanism in access control to motivate subjects to continue behaving honestly in making access to objects.

In the future, we will analyze our trust-based access control in a more complicated and sophisticated scenario. We will also develop experiment to evaluate our trust-based access control as well as the game theory-based analysis to further improve the effectiveness of access control in open network environments.

Acknowledgements

The work in this paper has been supported by funding from National Natural Science Foundation of China (61272500) and from Beijing Education Commission Science and Technology Fund (KM201010005027).

References

[1] L. Alboaie and M. F. Vaida, "Trust and Reputation Model for Various Online Communities", Studies in Informatics and Control, vol. 20, no. 2, **(2011)**.
[2] L. Ma, Y.-M. Zhang and Q. Wei, "A Trust Evaluation Method for Dynamic Distribution Environment", Proceedings of the 9th International Conference on Machine Learning and Cybernetics, Qingdao, China, **(2010)** July 11-14.
[3] L. Snyder, "Formal Models of Capability-Based Protection Systems", IEEE Trans. Computers., vol. C-30, no. 3, **(1981)**.
[4] D. E. Bell and L. LaPadula, "Secure Computer Systems: A Mathematical Model", Mitre Corporation, Bedford, MA, **(1973)**.
[5] R. S. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Youman, "Role-based Access Control Models", Computers, vol. 29, no. 2, **(1996)**.
[6] A. Nagarajan, "Dynamic Trust Enhanced Security Model for Trusted Platform based Services", Future Generation Computer Systems, vol. 27, no. 5, **(2011)**.
[7] L. Alboaie and M. F. Vaida, "Trust and Reputation Model for Various Online Communities", Studies in Informatics and Control, vol. 20, no. 2, **(2011)**.
[8] M. Blaze, J. Feigenbaum and J. Lacy, "Decentralized Trust Management", Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA, USA, **(1996)** May 6-8
[9] S. S. Song, K. Hwan and M. Macwan, "Fuzzy Trust Integration for Security Enforcement in Grid Computing", Proceedings of IFIP International Conference on Network and Parallel Computing, Wuhan, China, **(2004)** October 18-22.
[10] T. Alessandra, "A Semantic Context-aware Access Control Framework for Secure Collaborations in Pervasive Computing Environments", Proceedings of the 5th International Semantic Web Conference, Athens, GA, USA, **(2006)** November 5-9.
[11] Y. Guo, H. Fan, Q. Zhang and R. Li, "An Access Control Model for Ubiquitous Computing Application", Proceedings of International Conference on Mobile Technology Applications and Systems, Guangzhou, China, **(2005)** November 15-17.

[12] S. Chakraborty and L. Ray, "TrustBAC: Integrating Trust Relationships into the RBAC Model for Access Control in Open Systems", Proceedings of the 11th ACM symposium on Access Control Models and Technologies, Lake Tahoe, CA, USA, **(2006)** July 7-9.
[13] A. Z. Lin, E. Vullings and J. Dalziel, "A Trust-based Access Control Model for Virtual Organizations", Proceedings of the 5th International Conference on Grid and Cooperative Computing, Hunan, China, **(2006)** October 21-23.
[14] F. Feng, C. Lin, D. Peng and J. Li, "A Trust and Context Based Access Control Model for Distributed Systems", Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, Dalian, China, **(2008)** September 25-27.
[15] D. Huang, "Means of Weights Allocation with Multi-Factors based on Impersonal Message Entropy", Systems Engineering-Theory Methodology Applications, vol. 12, no. 4, **(2003)**.
[16] R. Anderson and T. Moore, "The Economics of Information Security", Science, vol. 314, no. 5799, **(2006)**.
[17] S. Roy, "A Survey of Game Theory as Applied to Network Security", Proceedings of the 43rd Hawaii International Conference on System Sciences, Koloa, HI, USA, **(2010)** January 5-8.
[18] S. H. Chin, "On Application of Game Theory for Understanding Trust in Networks", Proceedings of International Symposium on Collaborative Technologies and Systems, Baltimore, MD, USA, (2009) May 18-22.
[19] D. Fudenberg and J. Tirole, Game Theory. MIT Press, **(1991)**.

Authors

Jingsha He received his B.S. degree from Xi'an Jiaotong University in Xi'an, China and his M.S. and Ph.D. degrees from the University of Maryland at College Park in USA. He is currently a professor in the School of Software Engineering at Beijing University of Technology in China. Professor He has published over 170 research papers in scholarly journals and international conferences and has received nearly 30 patents in the United States and in China. His main research interests include information security, network measurement, and wireless ad hoc, mesh and sensor network security.

Shunan Ma received her M.S. degree from Jiangnan University in Wuxi, China and her Ph.D. degree from Beijing University of Technology in Beijing, China. She is currently an assistant professor in the Institute of Information Engineering, Chinese Academy of Sciences in Beijing, China. Ms. Ma's research interests include network security and distributed network technologies.

Bin Zhao is currently a Ph.D. student in the School of Software Engineering at Beijing University of Technology in China. His research focuses on network security, cloud computing and information forensics and he has published several papers in scholarly journals and international conferences in the above research areas.