International Journal of Grid Distribution Computing
Vol. 8, No.4, (2015), pp.27-36
http://dx.doi.org/10.14257/ijgdc.2015.8.4.03

The Dynamic Access Control Model for Cloud Web Based on Repeated-game Theory

Yixuan Zhang, Jingsha He and Bin Zhao
School of Software Engineering, Beijing University of Technology, Beijing 100124, China
s201125006@emails.bjut.edu.cn, jhe@bjut.edu.cn, zhaobin@email.bjut.edu.cn

Abstract

Access control, what is a core technology in information security, has been widely used cloud web. It is used to distribute objects' resources to subjects according to some principles. But until now, most traditional access control models are focused on the distributional principles; the security of systems is always ignored. Protecting data and resources in computers from threats and attacks is also an important aspect in access control, especially in cloud web where there are a great deal of threats and attacks. In this paper, we introduce the present situation and related work of access control. Then we analyze the security problems in computer systems with traditional access control model, and get the prisoner's dilemma in it through Nash equilibrium. To solve this dilemma, we applied repeated-game theory to access control and build a new model RTAC. The ultimate goal of RTAC is to encourage subjects' honest accesses and discourage subjects' malicious accesses through Nash equilibrium. At last, we perform some experiments and show the advantages of RTAC over the traditional access control model.

Keywords: *Access Control, Repeated-game Theory, Cloud Web, Prisoner's Dilemma, Nash Equilibrium*

1. Introduction

Access control, as the basic of computer systems, was first proposed by Lampson in early 1970 [1]. It refers to the whole suite of models and mechanisms used to govern user access to information, resources, services, etc. and to counter malicious attacks. At first, there are three basic elements in access control model: subjects who propose access requests; objects who get subjects' requests and determine whether authorize or not; and permission matrix in which the row represents subject, the column represents object, and the element represents whether the corresponding subject could access the corresponding object or not. Based on these elements, access control has three functions mainly: allow legitimate subjects to make accesses to the protected network resources, prevent illegal subjects from making accesses to the protected network resources, and prevent legitimate users from making unauthorized accesses to the protected network resources.

The rest of this paper is organized as follows. In section 2, we review some related work. In section 3, we apply game theory to analyze an original single game playing between subject and object, and get the prisoner's dilemma through Nash equilibrium. In section 4, to solve the prisoner's dilemma, we use repeated-game theory to build a new dynamic access control model for cloud web. In section 5, we perform a simulation to show the benefit of the infinite repeated-game-based access control model in cloud web. Finally, in section 6, we conclude this paper and discuss our future work.

ISSN: 2005-4262 IJGDC

2. Related Work

We have introduced the three basic elements in access control in section 1: subject, object and permission matrix. Permission matrix is the first method to determine permissions distribution in access control. With the in-depth study, there have been many new distribution methods, like discretionary access control (DAC) [2], mandatory access control (MAC) [3] and role-based access control (RBAC) [4, 5]. In DAC, the distribution method determines which subject can access the object [6], and the object can give the access to some subjects that he trusts. In MAC, mandatory access control policy is enforced throughout a system without the discretion of any owners to confine the flow of information resulting from access to objects to one direction in a lattice of security labels. But in DAC, most risks are from the fact that the objects may trust some subjects who are malicious, and objects can't entirely control their access rights because the subject whom he give access rights to may give access rights to others who may give the access rights to others... and at last, the access rights are given to malicious subject. In MAC, the access control policy is enforced; even an object can't decide the allocation of their access rights. To solve the problems in DAC and MAC, RBAC is proposed. In RBAC, a set of roles are defined in addition to subjects and objects and access rights or permissions are assigned to roles rather than to subjects directly. RBAC uses the notion of role to embody a collection of permissions within an organizational setup. Permissions are associated with roles through a permission-to-role assignment and subjects are granted access to resources through a subject-to-role mapping.

As the development of computer science, the network environment is more and more open, especially the appearance of cloud web, in which there are a great deal of users and the real identities of subjects is unknown so that there are more and more threats and attacks like intrusion [7], phishing [8], viruses [9], cybercrimes [10]. To solve this problem, experts have done many researches and proposed some access control models such as context-based access control (CBAC) [11] and attribute-based access control (ABAC) [12]. Each model has its advantages and disadvantages, but actually most researches focused on the new distribution methods, and not solves the security problem completely. So we introduce repeated-game theory to the access control model to solve the security problem in cloud web, and make subjects to be more honest in access control.

In game theory, a repeated game is an extensive form game which consists in some number of repetitions of some single game [13]. It captures the idea that a player will have to take into account the impact of his current action on the future actions of other players; this is sometimes called his reputation. The presence of different equilibrium properties is because the threat of retaliation is real, since one will play the game again with the same person. It can be proved that every strategy that has a payoff greater than the max payoff can be a Nash Equilibrium, which is a very large set of strategies. And in the game theory, Nash equilibrium describes the conditions for a stable state of a game in which no player would unilaterally change its strategy as doing so would lower its own payoffs provided that all other players would adhere to the prescribed strategy [14].

3. The Prisoner's Dilemma in Traditional Access Control

Prisoner's dilemma is a representative example of game theory. And there are two participants (the arrested prisoner) and a dealer in it. In prisoner's dilemma, although the prisoners know that if they cooperate with each other and not spit real fact, they can bring the best interests for all, but in the case that the information is unknown to all, the selling partner can bring benefits to it, and his accomplice who

moves out of him can bring benefits to his accomplice. Therefore, most prisoners choose move out of another to protect them.

From the introduction above, we have known that most traditional access control models are essentially identity-based, and they are more suitable to closed environments such as organizations that have a known set of principals or subjects who can access the information and services provided within the organizations. And in cloud web, subjects and objects will get into prisoner's dilemma. Using game theory to analyze the traditional access control, we should seek for the basic elements of a single game to be considered in access control.

The game between subject and object is shown in Table 1.

Table 1. The Game between Subject and Object

Subject / Object	Honest	malicious
Permit	$O_{permit}^{honest}, S_{permit}^{honest}$	$O_{permit}^{malicious}, S_{permit}^{malicious}$
Deny	$O_{deny}^{honest}, S_{deny}^{honest}$	$O_{deny}^{malicious}, S_{deny}^{malicious}$

In fact, if subject chooses honest strategy, object will get more payoffs when he chooses permit strategy than that when he chooses deny strategy, because permit strategy can make object be fully utilized safely. On the contrary, if subject chooses malicious strategy, object will get more payoffs when he chooses deny strategy than that when he chooses permit strategy. So we can get the conclusion that: $O_{permit}^{honest} > O_{deny}^{honest}$, and $O_{permit}^{malicious} < O_{deny}^{malicious}$. And in the same reasons, if object chooses permit strategy, malicious strategy will bring subject more extra payoffs compared to honest strategy. If object chooses deny strategy, no matter which strategy subject chooses, he will get nothing. So we get the conclusion that $S_{permit}^{honest} < S_{permit}^{malicious}$, and $S_{deny}^{honest} = S_{deny}^{malicious}$. Then we get the equilibrium ($O_{deny}^{malicious}, S_{deny}^{malicious}$).

According to the two conclusions above, we could get the Nash equilibrium (malicious, deny). It means that if and only if subject chooses malicious strategy and object chooses deny strategy; the payoffs of the two players can get equilibrium. If subject chooses the other strategy or object chooses the other strategy, the equilibrium will be broken so that payoffs will change, and the constantly changing of payoffs will result in this Nash equilibrium (malicious, deny) again. So subject and object both know this result and they will insist on this Nash equilibrium to ensure the maximum benefit of mutual accommodation.

But in actual, in the access control, subject's real purpose is to get some permissions by legal way or illegal way, and object's purpose is to be more accessed and protect the security of his resources, service and information. Unfortunately, to get the Nash equilibrium, they both choose uncooperative action. This means that subject and object fall into the prisoner's dilemma which is deviated from their original purpose. And in the prisoner's dilemma, the subject and the object both know that cooperation would bring them more payoffs, but to keep Nash equilibrium, they choose uncooperation, which causes a result they do not really want. They waste their cost and resouces in networks like time, money and broadband.

4. The Dynamic Access Control Model Base on Repeated-Game Theory

To solve the prisoner's dilemma in traditional access control for cloud web, we apply repeated-game theory to build a new model RTAC. In this model, there is an access control mechanism to deal with the access process. If a subject makes an honest access, he will give a good impression on the mechanism, and his next access request will be more likely to be permitted by the object; on the opposite, if he makes a malicious access, he will give a bad impression on the mechanism, and his next access request will be more likely to be denied by the object. So with this mechanism, cooperative strategies are encouraged and uncooperative strategies are punished. Next, we will introduce the access control mechanism in detail. The game players in RTAC are subject and object, too. And the access control mechanism deals with access requests from subjects and post the final access result to subjects and objects. The specific process of RTAC is shown in Figure 1.

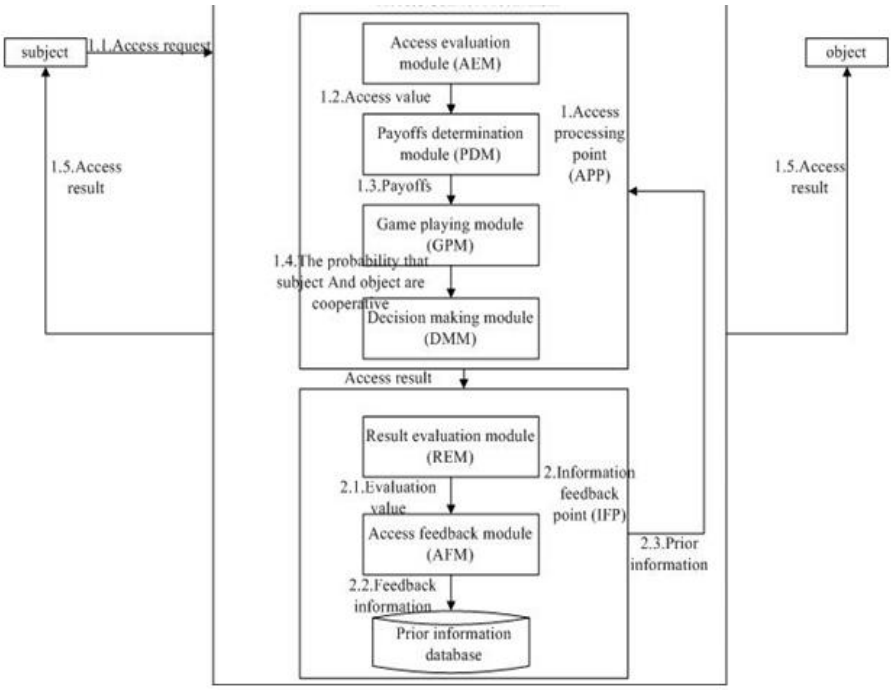

Figure 1. The Specific Process of RTAC

From Fig. 1, we see that in access control mechanism, there are two points: access processing point (APP) and information feedback point (IFP). APP includes four modules, they are access evaluation module (AEM), payoffs determination module (PDM), game playing module (GPM) and Decision making module (DMM). When a subject sends an access request, the access control mechanism will start APP first.

4.1. The workflow of APP

(1) AEM gets the request from subject and extracts the request parameters like IP address, access time, access network conditions and subject's prior information from prior information database in IFP to compute an access value. To compute the access value, we suppose that each parameter has four cases, and we divide access value interval into four disjoint subintervals corresponding to different cases. For example, the access value interval is A= [0, 1], the relations between the four parameters and access value is shown in Table 2.

Table 2. The Relations between Parameters and Access Value

IP address	very dangerous	dangerous	safe	very safe
Access time	never	occasional	normal	frequent
Network condition	very dangerous	dangerous	safe	very safe
History information	very dangerous	dangerous	safe	very safe
Access Value	[0, 0.25)	[0.25,0.5)	[0.5, 0.75)	[0.75, 1]

We denote t_1, t_2, t_3, t_4 to represent the values of IP address, access time, network condition and history information respectively, and V_i to represent the access value. Then V_i is computed by t_1, t_2, t_3, t_4. There are many methods to complete this calculation. In this paper, we first determine access value subinterval by the four parameters, then select an apposite access value in the corresponding intervals randomly. To reflect dynamicity of access value incloud web, we give weights a_1 , a_2 , a_3 and a_4 for corresponding parameters and compute V_i with Formula. 1 as follows:

$$V_i = a_1 t_1 + a_2 t_2 + a_3 t_3 + a_4 t_4, a_1 + a_2 + a_3 + a_4 = 1 \quad (1)$$

Then we send V_i to the next module PDM.

(2) PDM gets the access value V_i and computes the payoffs for subject and object when they choose different strategies based on V_i. And these payoffs will be sent to GPM to play a game.

(3) GPM is the module where the game is played. Then, this module will compute the probabilities that subject chooses honest strategy and that object chooses permit strategy. And send these probabilities to next module DMM. In this module, because the payoffs are related to the access value V_i, whose calculation process needs to consider prior information, countless times of accesses between subject and object could be regarded as repeated game. So if a subject takes malicious behavior, he will be punished by decreasing his V_i through prior information so that his payoffs will be influenced in later accesses. Therefore, subject tends to chooses to be honest to get more payoffs.

(4) DMM gets the probabilities that subject chooses honest strategy and that object chooses permit strategy from GPM. And based on these probabilities, DMM will get the final decision that whether authorize subject's access request or not. Then this decision will be sent to subject and object as an access result, which indicates that the access process is over.

4.2. The workflow of IFP

At the same time, this access result will also be sent to next point IFP of access control mechanism to start feedback process. There are two modules and a database in IFP: result evaluation module (REM), access feedback module (AFM) and Prior information database. Its workflow is as follows:

(1) REM gets the access result from access processing point (APP). And REM will evaluate this result and get an evaluation value E. The formula to compute E is as follows:

$$E = F(z) = 1 - a^{z}, 0 < a < 1 \quad (2)$$

In Formula 2, a is a parameter selected from (0, 1). According to what REM needs, it determines the value of a. When there are some other protective measures in cloud web, it has strong ability to withstand risks and threats. So REM will set the value of a bigger so that the E will not change too much to resist attacks in cloud web. On the opposite, when the system is vulnerable to outside attacks, the value of a should be smaller to make E have a wide range so that the mechanism is more effective to risks and threats in cloud web. z represents the value of damage or goodness subject brings to objects because its malicious behavior or honest behavior. If the permissions that subject requests is more that what he could get, z will be a negative number, it causes C to be a negative number from $[-\infty, 0)$. If the subject makes access normally, z will be a positive number, it causes C to be a positive number from [0, 1). Then AFM post E to next module AFM.

(2) AFM gets the evaluation value E from AFM and corrects this value according to the system requirements if necessary to get feedback information. Then it sends the feedback information to the prior information database.

(3) Prior information database is used to store past access results. When next access request from the same subject is received by the access control mechanism, prior information will be sent to AEM of APP to compute a new V_i for the subject.

Until now, a cycle of repeated game between subject and object is finished. When the subject makes access request to the object again, the cycle will start again. With this access control mechanism, especially AEM of APP and REM of IFP which we focused on, the application of repeated-game theory prompt subject tend to be more honest and object tend to be more willing to permit at the same time. So the threats and attacks become less and less because both subject and object select to cooperation. And we solve the prisoner's dilemma in section 3.

5. Simulation

To evaluate the effectiveness of RTAC in cloud web, we have performed some experiments to compare it with traditional access control. In these experiments, we suppose that there are 10 objects and 200 pads or phones as subjects. We divide the subjects into two sets S_1 and S_2 in average. S_1 make access requests to the objects under traditional access control model and S_2 make access requests to the objects under RTAC.

In scenario 1, the subjects in S_1 make accesses with a higher probability 0.8 and those in S_2 make accesses with a lower probability 0.2 as the original probability to choose honest strategy. The scenario is repeated 1000 times from which we randomly pick 30 continuous accesses starting from a randomized stage. And we repeated this experiment 100 times and compute the average value. The result of the scenario is shown in Figure 2.

In scenario 2, the subjects in S_1 and S_2 all make accesses with a middle probability 0.5 as the original probability to choose honest strategy. The scenario is repeated 1000 times from which we randomly pick 30 continuous accesses starting from a randomized stage. And we repeated this experiment 100 times and compute the average value. The result of the scenario is shown in Figure 3.

In scenario 3, the subjects in S_1 make accesses with a lower probability 0.2 and those in S_2 make accesses with a higher probability 0.8 as the original probability to choose honest

strategy. The scenario is repeated 1000 times from which we randomly pick 30 continuous accesses starting from a randomized stage. And we repeated this experiment 100 times and compute the average value. The result of the scenario is shown in Figure 4.

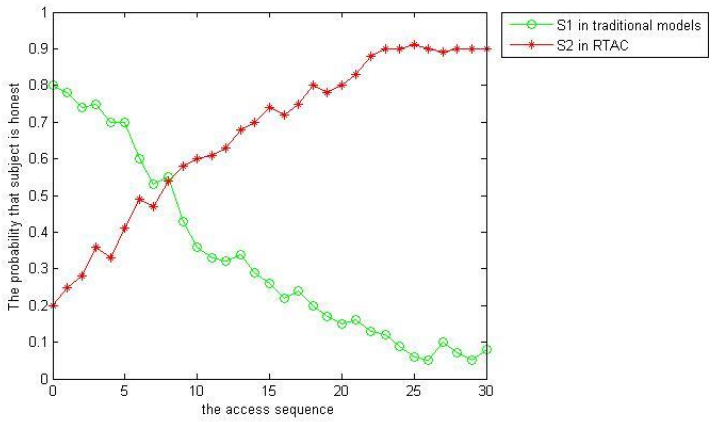

Figure 2. The Probabilities That Subject Is Honest In Scenario 1

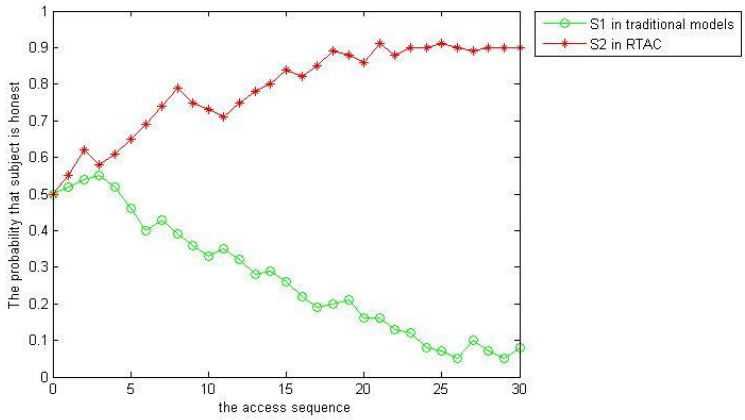

Figure 3. The Probabilities That Subject Is Honest In Scenario 2

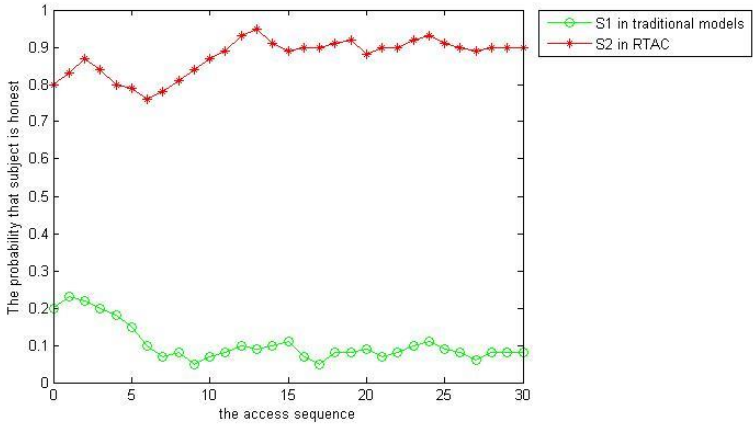

Figure 4. The Probabilities That Subject Is Honest In Scenario 3

From Figure 2, 3 and 4, we get a conclusion: no matter what the original probability is, subjects in S_1 tend to betray the cooperation because they don't need to worry about

the punishments from traditional access control model in these scenarios. So when they make actions, what they need to consider is only that which strategy would bring them more payoffs. Under this situation, objects would betray the cooperation to protect them, too. And they get into the prisoner's dilemma. But in the RTAC, no matter what the original probability is, subjects in S_2 tend to maintain the cooperation because they would be punished for their dishonest behavior in these scenarios. If they are dishonest this time, the permissions that they could get next time will be reduced. So when they make actions, what they need to consider is that which strategy would bring them more payoffs now and in future, so subjects in S_2 tend to be more honest. And under this situation, objects would also select cooperative strategies to get maximum benefit.

6. Conclusion

In this paper, we introduce the present situation and related work of access control. Then we analyze the security problems in computer systems with traditional access control model, and get conclusion that there is prisoner's dilemma in traditional access control through Nash equilibrium. To solve this dilemma, we applied repeated-game theory to access control and build a new model RTAC. The ultimate goal of RTAC is to encourage subjects' honest accesses and discourage subjects' malicious accesses through Nash equilibrium. At last, we give a simulation and show the advantages of RTAC over the traditional access control model. In the future, we will carry out in-depth study on how to make RTAC adapt to a large amount of disorder access requests from subjects.

Acknowledgements

The work in this research has been supported by National Natural Science Foundation of China (61272500), Beijing Natural Science Foundation (4142008), the Pre-launch of Beijing City Government Major Tasks and District Government Emergency Projects (Z131100005613030) and Shandong National Science Foundation (ZR2013FQ024).

References

[1] B. W. Lampson, "Protection, Proceedings of the 5th Princeton Symposium on Information Sciences and Systems", **(1971)**, pp. 437-443.
[2] S. Lawrence, "Formal Models of Capability-Based Protection Systems", IEEE Transactions on Computers, vol. C-30, no. 3, **(1981)** March, pp. 172-181.
[3] D. E. Bell and L. LaPadula, "Secure Computer Systems, A Mathematical Model", Mitre Corporation, Bedford, MA, **(1973)**.
[4] S. Ravi, C. J. Edward, F. L. Hal and Y. E. Charles, "Role-based Access Control Models, Computer", vol. 29, no. 2, **(1996)** February, pp. 38-47.
[5] D. Ferraiolo and D. Kuhn, "Role-based Access Control", Proceedings of the NIST-NSA National Computer Security Conference, **(1992)**, pp. 554-563.
[6] R. S. Sandhu and P. Samarati, "Authentication, Access Control, and Audit. ACM Computing Surveys", vol. 28, no. 1, **(1996)**.
[7] W. A. Wulf and A. K. Jones, "Reflections on Cybersecurity", JScience, vol. 326, **(2009)**, pp. 943-944.
[8] F. R. Chang, "Is Your Computer Secure", J.Science, vol. 325, **(2009)**, pp. 550-551.
[9] K. Gammon, "Four Ways to Reinvent the Internet", Nature, vol. 463, **(2010)**, pp. 602-604.
[10] A. Martin, "How Safe Are Your Data", Nature, vol. 464, **(2010)**, pp. 1260-1261.
[11] H. Yao, H. Hu, Z. Lu and R. Li, "Dynamic role and context-based access control for grid applications", IEEE Region 10 Annual International Conference, Proceedings/TENCON, vol. 2007, **(2007)**.
[12] B. Wang and L. Wang, "Design of attribute-based access control model for power information systems", Dianli Xitong Zidonghua/Automation of Electric Power Systems, vol. 31, no. 7, **(2007)** April 10, pp. 81-84, 98.
[13] R. J. Aumann and M. Maschle, "Repeated Games with Incomplete Information", Cambridge London, MIT Press **(1995)**.
[14] J. F. Nash, "Equilibrium Points in N-Person Games", Proc. National Academy of Science of the United States of America, **(1950)**, pp. 48-49.

Authors

Yi-xuan Zhang, is a Ph.D. candidate in the School of Software Engineering at Beijing University of Technology, Beijing, China. She received her B.S. degree in Beijing University of Technology in 2011. Her research interests include network security, access control, game theory and distributed network technology.

Jing-sha He, is a professor in the School of Software Engineering at Beijing University of Technology (BJUT) in Beijing, China. He received a Ph.D. degree from the University of Maryland at College Park in 1990. Prior to joining BJUT in 2003, he worked for IBM, MCI Communications and Fujitsu Laboratories engaging in R&D of advanced networking and computer security. His main research interests include information security, network measurement, and wireless ad hoc, mesh and sensor network security. He has published nearly 200 papers in the above areas.

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