Applied Mathematics and Computation 307 (2017) 299–310

Contents lists available at ScienceDirect

Applied Mathematics and Computation

journal homepage: www.elsevier.com/locate/amc

Non-zero-sum cooperative access control game model with user trust and permission risk

Nurmamat Helil[a,b,*], Azhar Halik[a], Kaysar Rahman[a]

[a] College of Mathematics and System Science, Xinjiang University, China
[b] Department of Computer Science and Engineering, University of Minnesota, USA

ARTICLE INFO

Keywords:
Access control
Trust
Risk
Multi-stage game
Nash equilibrium

ABSTRACT

In access control, there exists a game between an application system and its user, in which both the system and the user try to maximize their own utility. Establishing a reasonable, general purpose access control game model of cost-benefit analysis is a non-trivial research issue. Considering the practical existence and involvement of user trust and permission risk, we construct a non-zero-sum game model for access control, choosing trust, and risk or cost as metrics in players' payoff functions. We analyze the optimal strategies for the application system, the user, and also the Pareto efficient strategy from the viewpoint of both the application system and the user. A Nash equilibrium emerges that improves the rationality of access control decision-making under uncertain situations. In addition, we propose a proper risk estimation method. We also solve the risky permission set problem originated from access control constraints by utilizing optimal strategy in a finite multi-stage game.

1. Introduction

In a dynamic, uncertain environment, an application system requires a reasonable access control policy or mechanism, in which the trade-off between information sharing and protection results in a socially beneficial outcome for both the application system and its user. Although the traditional access control models and practices such as Discretionary Access Control (DAC) [1,2], Mandatory Access Control (MAC) [3–5], and Role-Based Access Control (RBAC) [6,7] and their variants meet the access control needs of most application systems, there are still some needs they cannot meet. Static, pre-defined access control policies fail to capture the user's "good" or "bad" access behavior and poorly define the inherent value or risk in a permission, especially as, a user's access to a permission may cause risks at different amounts.

As users exhibit dynamic behavior, practical access control systems have utilized trust [8–12]. To better quantify the value or risk of a permission, researchers have empirically discussed risk into access control [13–17]. Additionally, user trust and permission risk have been correlated in works [18–24].

Many information security related research areas, including network security [25–28], intrusion detection [29,30] and access control [18,31–33], have made use of game theory [34,35] to drive advancements. Game theory provides mathematical rigor to interactive situations among entities, taking into consideration entities' predictions about others' actions and the outcomes of such actions to derive an optimal strategy.

[*] Corresponding author at: College of Mathematics and System Science, Xinjiang University, China.
E-mail addresses: nur924@sina.com, nurmamat@xju.edu.cn (N. Helil).

http://dx.doi.org/10.1016/j.amc.2017.03.006

In most dynamic access control models and practices, both the application system and the user take actions to maximize their own utility, that means there exists a game between the application system and its user. According to the collected information about the user, the application system predicts the benefit or risk a user's access to its permission will bring, and also evaluates the benefit or loss after a user's successful access to its permission. Although the user understands using granted permission normally will lead to more future permissions, and also understands that permission abuse will lead to punishment from the system, such as losing chances for accessing more permissions. However, a user can achieve extra benefit from abusing his permission, and this extra benefit can not be achieved via normally using this permission.

Conventional access control models and practices do not account for the characteristics of this access control game. In fact, application systems and users play many different kinds of access control game of varying complexity, requiring further detailed analysis from both the access control and game theory disciplines.

There exist some permissions combination thereof is sensitive or risky if they are successively accessed by a user or group of similar users [20,36]. These situations can also be solved in the access control game model.

Much similarity exists between the access control process of the permission and the game. The scenario of access control can be regarded as a game. This paper proposes applying game theory analysis to the access control process. In this paper, we construct a reasonable, general purpose access control game model, properly define its components, and solve the utility maximizing optimal strategy for the application system and its user, both individually and collectively. We also examine challenges the access control game model might confront. Game theory based access control using user trust and risk of permission can capture the dynamic and complex characteristics of users and improves the rationality of access control decision making. We also solve the risky permission set problem, originated from access control constraints, using finite multi-stage game model.

The remainder of this paper is divided into the following sections. Section 2 constructs a general access control game model, in which user trust is not involved, and discusses the optimal strategies of the application system and its user. Section 3 constructs a trust and risk-aware access control game model and derives the optimal strategies. Section 4 discusses a game model for a risky permission set. Section 5 goes through a case study to explain how the system and the user play the access control game. In Section 6, we survey related works. Section 7 summarizes our work.

2. Access control game model without user trust

When a user accesses a permission, he might bring to the application system benefit or loss. For example, Alice is a university student authorized to use a free version of a software program with a 30-day free student user license. By using the software to further her studies and by recommending the software to fellow students, both the software company and Alice can economically or socially benefit from the permission of free use of this software. However, Alice might also share the software permission with some friends who are not university students and therefore are supposed to use the paid version of the software. Perhaps her non-university friends pay Alice to use the free version of the software for some commercial purpose. In this situation, Alice benefitted from abusing her permission and brought damages to the software company. Of course, the company will seek recourse. In summary, the choice of permission abuse or normal use leads to potential costs or benefits and gives rise to the need for a game model of this access control scenario.

So, when a user accesses a permission, he might have the temptation of abusing the permission because there are some extra benefits after abuse, but if he abuses, then the application system might punish him, denying his further access requests. From this example, we can see that there is a need to construct a game model for access control scenario and then solve the access control decision-making problem via solving for the optimal strategy for the players in the game. First, we establish a mapping between access control and the game model, define the components of the access control game model, and also define the type of the game the application system (hereafter we call the system) and its user play.

Define the basic components of the access control game model as follows:

Suppose $\mathcal{G} =< s, u, A_s, A_u, U_{s,u} >$ is an access control game model where:

- s is the system;
- u is the user;
- $A_s = \{G, D\}$ is the action set of the system (G denotes grant access, D denotes deny access);
- $A_u = \{A, N\}$ is the action set of the user (A denotes abuse, N denotes normal use);
- $U_{s,u}$ is the payoff function of the system and the user in one access process.

To analyze the characteristics of the access control game for one access process, we assume:

1. Two player game: in an access process of a permission, players are the system and the user,
2. Finite strategy game: the strategy of the system and the user are finite,
3. Non-zero-sum cooperative game: both the system and the user can win, only if the user normally uses his permission,
4. Static game: the system and the user choose actions simultaneously, or they do not know each other's chosen action before the game starts.

If a user accesses permissions more than once, additionally assume:

5. Perfect information game: the system and the user know what they have chosen in their earlier access processes,