

Accepted Manuscript

Towards More Pro-active Access Control in Computer Systems and Networks

Yixuan Zhang, Jingsha He, Bin Zhao, Zhiqing Huang, Ruohong Liu

PII: S0167-4048(14)00181-3

DOI: [10.1016/j.cose.2014.12.001](https://doi.org/10.1016/j.cose.2014.12.001)

Reference: COSE 861

To appear in: *Computers & Security*

Received Date: 20 November 2013

Revised Date: 30 September 2014

Accepted Date: 19 December 2014

Please cite this article as: Zhang Y, He J, Zhao B, Huang Z, Liu R, Towards More Pro-active Access Control in Computer Systems and Networks, *Computers & Security* (2015), doi: 10.1016/j.cose.2014.12.001.

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.



Towards More Pro-active Access Control in Computer Systems and Networks^{*}

Yixuan Zhang^a, Jingsha He^{a,b†}, Bin Zhao^a, Zhiqing Huang^a, Ruohong Liu^b

^aSchool of Software Engineering

Beijing University of Technology, Beijing 100124, China

S201125006@emails.bjut.edu.cn, jhe@bjut.edu.cn, jnzhaobin@163.com, zqhuang@bjut.edu.cn

^bGeneral Administration Department

Beijing Development Area Co., Ltd., Beijing 100176, China

lrh450820@126.com

Abstract

Access control is a core security technology which has been widely used in computer systems and networks to protect sensitive information and critical resources and to counter malicious attacks. Although many access control models have been developed in the past, such as discretionary access control (DAC), mandatory access control (MAC) and role-based access control (RBAC), these models are designed primarily as a defensive measure in that they are used for examining access requests and making authorization decisions based on established access control policies. As the result, even after a malicious access is identified, the requester can still keep issuing more malicious access requests without much fear of punitive consequences from the access control system in subsequent accesses. Such access control may be acceptable in closed systems and networks but is not adequate in open systems and networks where the real identities and other critical information about requesters may not be known to the systems and networks. In this paper, we propose to design pro-active access control so that access control systems can respond to malicious access pro-actively to suit the needs of open systems and networks. We will first apply some established principles in the Game Theory to analyze current access control models to identify the limitations that make them inadequate in open systems and networks. To design pro-active access control (PAC), we incorporate a constraint mechanism that includes feedback and evaluation components and show based on the Game Theory how to make such access control respond to malicious access in a pro-active manner. We also present a framework design of PAC and demonstrate through the implementation of trust-based access control the feasibility of design, implementation and application of pro-active access control. Such kind of models and mechanisms can serve as the foundation for the design of access control systems that will be made more effective in deterring malicious attacks in open systems and networks.

Key Words: Security; Access Control; Game Theory; Evaluation; Payoffs; Trust.

1. Introduction

Access control in computer systems and networks refers to the whole suite of models and mechanisms that are used to govern user access to information, resources, services, etc. and to counter malicious attacks. Access control was first introduced by Lampson in early 1970s in the form of an

^{*}The work in this paper has been supported by National Natural Science Foundation of China (61272500), Beijing Natural Science Foundation (4142008), Pre-launch of Beijing City Government Key Tasks and District Government Emergency Projects (Z131100005613030) and the 12th Graduate Technology Fund of Beijing University of Technology (yjkj-2013-9929).

[†]The corresponding author, tel:+86-13501029035, email: jhe@bjut.edu.cn.

Download English Version:

<https://daneshyari.com/en/article/6884302>

Download Persian Version:

<https://daneshyari.com/article/6884302>

[Daneshyari.com](https://daneshyari.com)