Information Sciences 423 (2018) 24–49

Contents lists available at ScienceDirect

Information Sciences

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

Multi-user permission strategy to access sensitive information

Dipankar Dasgupta[a], Arunava Roy[b,*], Debasis Ghosh[c]

[a] Center for Information Assurance, Department of Computer Science, The University of Memphis, Memphis, TN 38152, USA
[b] CorpLab, Information Systems Technology and Design Pillar (ISTD), Singapore University of Technology and Design, Singapore 487372, Singapore
[c] HCL America Inc., 11000 Regency Pkwy, Raleigh, NC, USA

ARTICLE INFO

Article history:
Received 9 October 2016
Revised 22 April 2017
Accepted 13 September 2017
Available online 18 September 2017

Keywords:
Insider threats
Access control
Access-approver
Classified data

ABSTRACT

Exfiltration of sensitive data and intellectual property theft have increased to a significant level affecting both government agencies as well as small to large businesses. One of the major reasons of data breaches is malicious insiders who have the access rights, knowledge of data values and technical know-how of escalating their privileges in launching such insider attacks. Traditional access control policies (to shared data and computing resources) were evolved around the trust on legitimate users' access rights (read, write and execute) based on their jobs and role hierarchy in an organization. However, such access privileges are increasingly being misused by hostile, oblivious, rouge and pseudo-insiders. This work introduces a multi-user permission strategy and formulates a methodology for shared-trustworthy access (to classified data and services) by considering organizational structure. Accordingly, based on the sensitivity of the information being requested by a user, approvers are selected dynamically to reflect the work environment such as mobility, use of the device, access policy, etc. For this purpose, the proposed methodology first generates an access control graph, based on inter-relationship among employees and their roles in an organization. Next, it generates a set of permission grantees who are allowed to approve the access request of a user at a given time. The proposed multi-user permission strategy is evaluated with two empirical datasets and reported results demonstrated its ability in selecting non-repetitive approvers for a user access under different organizational and environmental constraints.

1. Introduction

Traditionally, all devices and data were under the domain of an organization and the attacks were either from insiders or pure outsiders as the network perimeters were well-defined. With the advent of cloud computing, increased mobility, and the use of personal devices (Bring your own device, BYOD) and the vast amount of data are now distributed across customers, service providers, and other third-party storage, each with varying security capabilities and management policies. Thus, once a break-in becomes successful, an outsider sometimes behaves like an insider for finding more avenues to exploit. We define this scenario as a "pseudo-insider" attack, i.e., an outsider who gains access as a privileged insider and attacks the organization from the inside [1–13]. Also, there exist rogue insiders, whether employees or contractors, who use their access inappropriately and involve in data exfiltration [14].

* Corresponding author.
E-mail address: royism.arunava@gmail.com (A. Roy).

http://dx.doi.org/10.1016/j.ins.2017.09.039
0020-0255/

Nomenclature

The important symbols, used in the present work are described as follows:

Used Symbols	Related Descriptions
$O_{j\in\mathbb{Z}^+}$	jth object (mainly, classified files) in an organization.
$S_{m\in\mathbb{Z}^+}$	Sensitivities of the mth file O_m.
$P_{m\in\mathbb{Z}^+}$	Number of permissions required for the file with the degree of sensitivity S_m.
$R_{i\in\mathbb{Z}^+}$	ith role in an organization. The roles can be like manager, vice president, etc.
$A_i[j]; i, j \in \mathbb{Z}^+$	jth activity of the ith role ($R_{i\in\mathbb{Z}^+}$) in an organization.
E	Set of employees of an organization.
$E_{ij}; i, j \in \mathbb{Z}^+$	Employee working in $A_i[j]; i, j \in \mathbb{Z}^+$.
$\theta_{N_2\times N_2}$	Primary initiator.
$\theta_{N_1\times N_1}$	Optimum initiator.
$P\otimes Q$	Kronecker product of the two matrices P and Q.

Since 2005, Carnegie Mellon University's CyLab has been publishing different versions of "Common Sense Guide to Prevention and Detection of Insider Threats" [15]. These documents described different real-world cases on insider threats and profiled malicious user behavior patterns and current trends. According to a recent cybercrime survey [3], insider attacks make up 28% of all cyber crimes and more than 33% of organizations reported several incidents of insider attacks over the years, For example, trade secrets breach had occurred at Toyota North America [16] in 2012 and customer data were compromised at Vodafone Germany [17] in 2013, On 21st June 2013, reported a significant amount of data theft by Edward Snowden [18] who used his super user privilege to access sensitive data without anybody's notice. August 20, 2015, a former manager at a software company, which developed the online game "Game of War" was arrested by the FBI for stealing the corporate secret [19]. This theft was detected later by analyzing various access logs related to all his network activities. Another recent incident on the data breach was reported on September 21st, 2015, a Morgan Stanley employee has pleaded guilty of stealing 730,000 client accounts (name, address and other personal information along with investment values and earnings) over a period of several years [20]. This incident was also detected after the fact by analyzing his access logs. It appears that insider threats are more damaging to an organization than outsider/intruder attacks since there is a significant cost associated with the resolution of such insider attacks. It is estimated that insider attacks take on an average 20% more time than a cyber-attack, i.e., an attack from outside to contain. In recent Vormetric Report mentions a massive 93% respondents from U.S. organizations believe that they are vulnerable to insider threats, and plan to increase their spending on IT security and data protection [21]. Based on interviews conducted by Harris Poll of "more than 800 senior business managers and IT professionals in major global markets, roughly half from the USA and the rest from the UK, Germany, Japan, and ASIAN countries," 55% of respondents said their "privileged users", insiders pose the biggest threat to their corporate data, followed by contractors and other service providers (46%) [21]. However, current cyber defenses are hopelessly outmatched and are unsuitable to handle different insider threats since their purpose are to prevent/detect intrusions and attacks from outside. However, prevention of insider threats is a non-trivial task due to various factors, ranging from complexities of defining insider threats and in time detection of such threats (by matching current patterns with historical information stored in different logs).

In this work, we propose a permission granting strategy in order to prevent insider data breaches through shared responsibilities, in particular, a user activities with classified data in an organization (i.e., which sensitive data are being accessed, when and by whom) are to be regulated via an approval process so that a few others are aware of such an access. Such a permission strategy should take into account employee's role and hierarchy while determining the approvers.

Here "role" is a basis of access control policies or a specific task competency, such as that of a technologist or a physician or a pharmacist. It can represent the authority and responsibility of a Team or a member of a Team, say, a Manager, a supervisor, a Developer or an Analyst. Roles define specific individuals allowed to access specific resources for the specific purpose. For example, a system operator role might access to all computer resources but not change any access permissions; a system administrator might change any access permissions but not approve any access permissions. Hence, the goal is to develop a generalized model capable of supporting organizations of any size and can handle permissions and resources of varying degrees of sensitivity.

1.1. Background study

Since the 1970 s, computer systems have been featured as multi-user applications. It leads to a higher range of awareness of data security issues. Although, system administrators, and software developers focused on different kinds of access control to ensure the authorized users were given access to certain portion data or resources. One of such kind of access control came up with Role-Based Access Control (RBAC). In real-world organization structure, the core concept of this framework is that users and their access permissions are brought together indirectly by user roles. A user acquires access permission by virtue of being assigned to a role that has been assigned that access permission. The advantage of RBAC is that it enables the use of constraints to support policies, such as division of tasks [22].