Chapter 10
DBMS Log Analytics for Detecting Insider Threats in Contemporary Organizations

Muhammad Imran Khan
Insight Centre for Data Analytics, Ireland

Simon N. Foley
IMT Atlantique, France

Barry O'Sullivan
University College Cork, Ireland

ABSTRACT

Insiders are legitimate users of a system; however, they pose a threat because of their granted access privileges. Anomaly-based intrusion detection approaches have been shown to be effective in the detection of insiders' malicious behavior. Database management systems (DBMS) are the core of any contemporary organization enabling them to store and manage their data. Yet insiders may misuse their privileges to access stored data via a DBMS with malicious intentions. In this chapter, a taxonomy of anomalous DBMS access detection systems is presented. Secondly, an anomaly-based mechanism that detects insider attacks within a DBMS framework is proposed whereby a model of normative behavior of insiders n-grams are used to capture normal query patterns in a log of SQL queries generated from a synthetic banking application system. It is demonstrated that n-grams do capture the short-term correlations inherent in the application. This chapter also outlines challenges pertaining to the design of more effective anomaly-based intrusion detection systems to detect insider attacks.

DOI: 10.4018/978-1-5225-5984-9.ch010

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

Database Management Systems (DBMS) are at the heart of contemporary organizations. Contemporary organizations deploy DBMS to store and manage access to their application data. There exist traditional security controls including role-based access and authentication that control privileges to stored data. However, there is still the concern of insider threats within the DBMS framework whereby legitimate users of the system misuse their access privileges to access stored data with malicious intentions. For example, there are number of reported incidents (Carr, 2008; Report, 2007) where hospital staff, without cause, looked up the medical records of celebrity patients. It has been reported in a recent survey that 89% of respondent organizations are vulnerable to insider attacks (Insider Threat Report, Insider Threat Security Statistics, Vormetric, 2015). Another survey reports that malicious insiders are the cause of the costliest cybercrimes (2015 Cost of Cyber Crime: Global, 2015).

In order to detect insider attacks, intrusion detection systems can be deployed. An intrusion detection system can be further classified into either anomaly detection systems or misuse detection systems (Kemmerer & Vigna, 2002). Misuse detection systems look for well-known attack patterns that are a priori defined. Thus, misuse detection systems can detect previously known or existing attacks. In contrast to misuse detection systems, anomaly detection systems (Forrest, Hofmeyr, & Somayaji, 2008; Forrest, Hofmeyr, Somayaji, & Longstaff, 1996; Laszka, Abbas, Sastry, Vorobeychik, & Koutsoukos, 2016; Pieczul & Foley, 2013) look for deviations from normal behavior. Anomaly detection systems have the potential to detect previously unknown, or *zero-day*, attacks (Jamrozik, von Styp-Rekowsky, & Zeller, 2016; Pieczul & Foley, 2016). We are interested in considering the challenge of detecting anomalous DBMS queries made by insiders; while the insider may hold the correct access permission to make the query. This article provides two contributions on this challenge. Firstly, a taxonomy for understanding DBMS anomaly detection systems is proposed. Secondly, an n-gram model for DBMS anomaly detection, that extends (Khan & Foley, 2016), is developed and evaluated.

Anomaly-based intrusion detection techniques have been shown to be effective in detecting insider attacks (Sallam et al., 2015). The basic building block of an anomaly detection technique is how it models normative behavior. Existing anomaly-based intrusion-detection technique considers a query in isolation in order to construct a model of normative behavior. We consider sequences of SQL queries made to a DBMS (Khan & Foley, 2016) whereby n-grams are used to capture normal query patterns.

The book chapter is organized as follows. Section 2 provides an introduction to the problem of insider threat. A taxonomy for anomalous DBMS-access detection

26 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/dbms-log-analytics-for-detecting-insider-threats-in-contemporary-organizations/210945

Related Content

Service Platform Development: Comparison of Two E-Services Platforms
Tugrul Daim, Marius Brandand Linda Lin (2013). *Implementation and Integration of Information Systems in the Service Sector (pp. 297-316).*
www.irma-international.org/chapter/service-platform-development/72556

On the Use of Similarity or Query Languages in Cloud Discovery Based on Ontology
Rawand Guerfel, Zohra Sbaïand Rahma Ben Ayed (2017). *International Journal of Service Science, Management, Engineering, and Technology (pp. 60-78).*
www.irma-international.org/article/on-the-use-of-similarity-or-query-languages-in-cloud-discovery-based-on-ontology/182515

Student Learning and Information Technology Nexus
Neeta Baporikar (2016). *International Journal of Service Science, Management, Engineering, and Technology (pp. 34-45).*
www.irma-international.org/article/student-learning-and-information-technology-nexus/149897

Organization Communiqué Effect on Job Satisfaction and Commitment in Namibia
Neeta Baporikar (2017). *International Journal of Service Science, Management, Engineering, and Technology (pp. 19-41).*
www.irma-international.org/article/organization-communiqu-effect-on-job-satisfaction-and-commitment-in-namibia/188874

The Trusted Hierarchical Access Structure-Based Encryption Scheme for Cloud Computing
Tabassum N. Mujawarand Lokesh B. Bhajantri (2022). *International Journal of Cloud Applications and Computing (pp. 1-17).*
www.irma-international.org/article/the-trusted-hierarchical-access-structure-based-encryption-scheme-for-cloud-computing/308273