An Insider Threat Detection Method Based on Business Process Mining

Taiming Zhu, Institute of Cyber Space Security, Information Engineering University, Zhengzhou, China
Yuanbo Guo, Institute of Cyber Space Security, Information Engineering University, Zhengzhou, China
Ankang Ju, Institute of Cyber Space Security, Information Engineering University, Zhengzhou, China
Jun Ma, Institute of Cyber Space Security, Information Engineering University, Zhengzhou, China
Xuan Wang, Department of Electronics Technology, Engineering University of the Armed Police Force, Xi’an, China

ABSTRACT

Current intrusion detection systems are mostly for detecting external attacks, but the “Prism Door” and other similar events indicate that internal staff may bring greater harm to organizations in information security. Traditional insider threat detection methods only consider the audit records of personal behavior and failed to combine it with business activities, which may miss the insider threat happened during a business process. The authors consider operators’ behavior and correctness and performance of the business activities, propose a business process mining based insider threat detection system. The system firstly establishes the normal profiles of business activities and the operators by mining the business log, and then detects specific anomalies by comparing the content of real-time log with the corresponding normal profile in order to find out the insiders and the threats they have brought. The relating anomalies are defined and the corresponding detection algorithms are presented. The authors have performed experimentation using the ProM framework and Java programming, with five synthetic business cases, and found that the system can effectively identify anomalies of both operators and business activities that may be indicative of potential insider threat.

KEYWORDS

Anomaly Detection, Insider Threat, Process Mining

1. INTRODUCTION

The insider threat is a long-term problem that faced by most organizations. It usually results in significant damage and could range from financial theft and intellectual property theft to the destruction of property and business process. Compared with attacks from external network incurred by hardware or software vulnerabilities, the insider threats are more harmful and more difficult to detect. The main causes of insider threats are as follows: First, part of employees may lack security awareness and violate the safety regulations by accident. Second, part of employees intentionally bypasses the security measures for their own convenience and efficiency in the works. Last but not least, some employees choose to leak the organization’s confidential information or sabotage the systems because of their resentment or other’s inducement. In general, insider threat a comprehensive problem, which

DOI: 10.4018/ijbdcn.2017070107

Copyright © 2017, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
consists of human factors and systemic factors. How to detect and prevent the insider threat has become a huge challenge for all organizations.

For organizations, various types of business activities are the main activities carried out during their daily operations, one of the main tasks is to ensure the successful completion of each business process. In order to improve the efficiency, more and more organizations begin to use various business systems to accomplish business activities. However, most business systems usually only consider how to ensure the achievement of normal business functions during the design phase and ignore the safety demands of business activities. This could make the business system vulnerable to insider threats and get caught in different kinds of anomalies, or even lead to the destruction and disclosure of critical business data in severe cases. Therefore, in this paper, we see this problem from the perspective of business activity and try to detect insider threat by a comprehensive analysis of operators’ abnormal behavior and anomalies emerged during business process execution.

Business processes are a series of activities completed by a group of people in organizations in order to achieve specific goals. The order between activities is strictly defined, so as to the content, modalities and responsibilities of each activity. In addition to the staff, the execution of a business process usually depends on specific business system and software program, which is a complex activity that involves human, machine, software and other multiple factors. Clearly, it can provide more comprehensive information support to insider threat detection by inspecting the daily work of organizations from the perspective of business process and establishing a normal business process model.

Since the actual business activity involves many factors, its process model must also be multidimensional, not only to reflect the sequence between business events, but also to reflect the behavior information of operators, the features of business cases and the time and frequency information of business events. There is no doubt that traditional pre-designed manual modeling methods are unable to meet this requirement. Manual modeling usually relies on limited expert knowledge and only provides an idealized view of part of factors in business activities, and cannot take complex realistic conditions into consideration, so it is often out of touch with reality and mostly useless. To solve this problem, most organizations turn to the log-based process mining method, which has many advantages. System log is easily available and has mostly no impact on the running system. Detailed information about the execution of a business system is recorded in the log and facilitates managers to understand what happened during the process. Finally, mining business process through the system log is more objective and efficient.

As far as we know, many of the current process mining methods establish a business process model from the perspective of control-flow [18-26], few of them can include human factor and performance factor into process mining in a multi-dimensional representation of business activities and the identification of human-oriented vulnerabilities and threats. In this paper, we present a business process mining based insider threat detection system, which includes the operators’ behavior into business process mining. The system mines normal business process models from the logs generated during the execution of business activities under a normal condition, and then detects anomalous behavior of operators, logical anomalies and performance anomalies in real-time logs by comparing them with the corresponding models, helping security managers to find out insider threats just in time. To test the performance of the approach, the system was implemented in ProM framework and Java Programming and the experimentation was conducted with synthetic data for evaluation. It was found that the system performed well for detecting the insider threats.

The remainder of this paper is organized as follows. The related works are introduced in Section 2. Section 3 briefly introduces the presented insider threat detection system and the details of each components are described in Section 4. Section 5 presents the process of conducting experimentation and discusses the results, and Section 6 concludes this paper.
Secure Resource Optimization in Distributed Service Computing
www.igi-global.com/chapter/secure-resource-optimization-distributed-service/21712?camid=4v1a

Fractional Reuse Partitioning Schemes for Overlay Cellular Architectures
www.igi-global.com/chapter/fractional-reuse-partitioning-schemes-overlay/62769?camid=4v1a