International Journal of Software Engineering and Knowledge Engineering

Knowledge-driven User Behavior Pattern Discovery for System Security Enhancement

Weina Ma

Department of Electrical, Computer, and Software Engineering
University of Ontario Institute of Technology
Oshawa, Ontario L1H 7K4,Canada Weina.Ma@uoit.ca

Kamran Saritpi

Department of Electrical, Computer, and Software Engineering
University of Ontario Institute of Technology
Oshawa, Ontario L1H 7K4,Canada
Kamran.Sartipi@uoit.ca

Duane Bender

Department of Electrical and Computer Engineering Technology
Mohawk College
Hamilton, Ontario L8N 3T2, Canada
Duane.Bender@mohawkcollege.ca

Insider threats posed by authorized users have caused significant security and privacy risks to IT systems. The behavior of authorized users in using system services must be monitored and controlled. However, the administrators in large distributed systems are overwhelmed by the number of system users, the complexity and changing nature of user activities. This paper presents a new generation of intelligent decision support systems that effectively assist the system administrators to get deep insight into the system users' dynamic behavior patterns. With these patterns, the system administrators are capable of constructing dynamic refinement to the existing security policies. We explore the method of interactively and incrementally extracting user's behavior patterns by combining data mining techniques with domain and system knowledge, and applying such knowledge to provide recommendations throughout the whole process. A prototype tool has been developed to analyze the audit logs from distributed medical imaging systems to validate the proposed approach.

Keywords: Behavior pattern discovery; association mining; sequential pattern mining; pattern query language; security enhancement.

1. Introduction

Despite the availability of common security mechanisms such as authentication, authorization and secure communication in most systems, authorized users intentionally or carelessly demonstrate risky behaviors that may cause data leakage or damage to the protected resources. Behavioral activities of authorized users must be monitored and controlled to protect user's private data and identify malicious