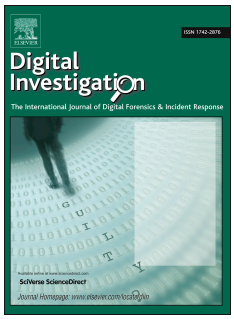
Accepted Manuscript



Graph clustering and anomaly detection of access control log for forensic purposes

Hudan Studiawan, Christian Payne, Ferdous Sohel

PII: S1742-2876(17)30143-3

DOI: 10.1016/j.diin.2017.05.001

Reference: DIIN 679

To appear in: *Digital Investigation*

Received Date: 15 July 2016

Revised Date: 21 March 2017

Accepted Date: 1 May 2017

Please cite this article as: Studiawan H, Payne C, Sohel F, Graph clustering and anomaly detection of access control log for forensic purposes, *Digital Investigation* (2017), doi: 10.1016/j.diin.2017.05.001.

Graph Clustering and Anomaly Detection of Access Control Log for Forensic Purposes

Hudan Studiawan[a,b,*], Christian Payne[a], Ferdous Sohel[a]

[a]*School of Engineering and Information Technology, Murdoch University, Australia*
[b]*Department of Informatics, Institut Teknologi Sepuluh Nopember, Indonesia*

Abstract

Attacks on operating system access control have become a significant and increasingly common problem. This type of security threat is recorded in a forensic artifact such as an authentication log. Forensic investigators will generally examine the log to analyze such incidents. An anomaly is highly correlated to an attacker's attempts to compromise the system. In this paper, we propose a novel method to automatically detect an anomaly in the access control log of an operating system. The logs will be first preprocessed and then clustered using an improved MajorClust algorithm to get a better cluster. This technique provides parameter-free clustering so that it automatically can produce an analysis report for the forensic investigators. The clustering results will be checked for anomalies based on a score that considers some factors such as the total members in a cluster, the frequency of the events in the log file, and the inter-arrival time of a specific activity. We also provide a graph-based visualization of logs to assist the investigators with easy analysis. Experimental results compiled on an open dataset of a Linux authentication log show that the proposed method achieved the accuracy of 83.14% in the authentication log dataset.

Keywords: authentication log, improved MajorClust, event log forensics, anomaly detection

*Corresponding author
Email addresses: hudan@if.its.ac.id (Hudan Studiawan), c.payne@murdoch.edu.au (Christian Payne), f.sohel@murdoch.edu.au (Ferdous Sohel)