Published on *CPS-VO* (https://cps-vo.org)

Catching Falling Dominoes: Cloud Management-Level Provenance Analysis with Application to OpenStack

Submitted by grigby1 on Wed, 05/05/2021 - 12:23pm

Title	Catching Falling Dominoes: Cloud Management-Level Provenance Analysis with Application to OpenStack
Publication Type	Conference Paper
Year of Publication	2020
Authors	Tabiban, Azadeh, Jarraya, Yosr, Zhang, Mengyuan, Pourzandi, Makan, Wang, Lingyu, Debbabi, Mourad
Conference Name	2020 IEEE Conference on Communications and Network Security (CNS)
Date Published	July 2020
Publisher	IEEE
ISBN Number	978-1-7281-4760-4
Keywords	cloud computing, Communication networks, Complexity theory, Conferences, Forensics, metadata, pubcrawl, Scalability, Scalable Security, security

Abstract

The dynamicity and complexity of clouds highlight the importance of automated root cause analysis solutions for explaining what might have caused a security incident. Most existing works focus on either locating malfunctioning clouds components, e.g., switches, or tracing changes at lower abstraction levels, e.g., system calls. On the other hand, a management-level solution can provide a big picture about the root cause in a more scalable manner. In this paper, we propose DOMINOCATCHER, a novel provenance-based solution for explaining the root cause of security incidents in terms of management operations in clouds. Specifically, we first define our provenance model to capture the interdependencies between cloud management operations, virtual resources and inputs. Based on this model, we design a framework to intercept cloud management operations and to extract and prune provenance metadata. We implement DOMINOCATCHER on OpenStack platform as an attached middleware and validate its effectiveness using security incidents based on real-world attacks. We also evaluate the performance through experiments on our testbed, and the results demonstrate that DOMINOCATCHER incurs insignificant overhead and is scalable for clouds.

URL https://ieeexplore.ieee.org/document/9162251
DOI 10.1109/CNS48642.2020.9162251
Citation Key tabiban_catching_2020

Cloud Computing Communication networks Complexity theory Conferences Forensics metadata pubcrawl Scalability Scalable Security security