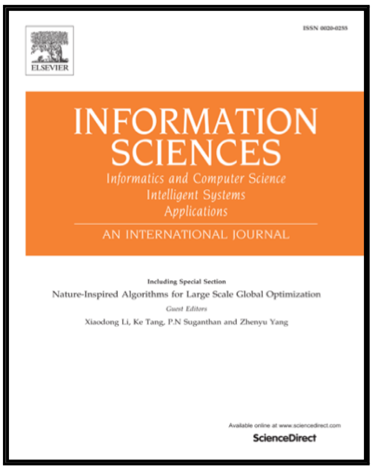

A Lightweight Live Memory Forensic Approach Based on Hardware Virtualization

Yingxin Cheng , Xiao Fu , Xiaojiang Du , Bin Luo ,
Mohsen Guizani

PII: S0020-0255(16)30501-1
DOI: 10.1016/j.ins.2016.07.019
Reference: INS 12345

To appear in: *Information Sciences*

Received date: 14 November 2015
Revised date: 29 June 2016
Accepted date: 6 July 2016

A Lightweight Live Memory Forensic Approach Based on Hardware Virtualization

Yingxin Cheng[a], Xiao Fu[a,*], Xiaojiang Du[b], Bin Luo[a], Mohsen Guizani[c]

[a] *State Key Laboratory for Novel Software Technology, Software Institute at Nanjing University, China.*

[b] *Dept. of Computer and Information Sciences, Temple University, USA.*

[c] *Dept. of Electrical and Computer Engineering, University of Idaho, USA.*

Abstract

The results of memory forensics can not only be used as evidence in court but are also beneficial for analyzing vulnerability and improving security. Thus, memory forensics has been widely used in many fields, including cloud security. Traditional memory forensics, usually an after-the-fact method, is time-consuming and often loses important transient information. Thus, live methods, which investigate memory directly, are presented. However, most of them are kernel based and easy to detect or confuse. Although virtualization technology can overcome these shortages, it must be preinstalled and has high cost. To solve these problems, we propose a lightweight live memory forensic framework based on hardware virtualization. It can build a virtualization environment on-the-fly. The operating system will be migrated to the virtual machine without termination or modifications. Then, the forensic methods can acquire and analyze evidence at the hypervisor level. Two novel forensic methods are proposed to verify the effectiveness of the framework. They focus on acquiring accurate data and system behavior, respectively. The main ideas are guaranteeing data accuracy in multi-view extraction and analyzing memory behavior in a para-synchronous style. Experiments have proved that these methods are able to obtain reliable and integrated evidence at an acceptable cost.

KeyWords: Hardware Virtualization, Live Forensics, Memory Forensics, Lightweight Forensic Framework

1. Introduction

MEMORY forensics investigates illegal behaviors by acquiring and analyzing volatile memory data. This is done

[*] Corresponding author at: State Key Laboratory for Novel Software Technology, Software Institute at Nanjing University, China. E-mail: fuxiao@nju.edu.cn.

E-mail addresses: yingxincheng@gmail.com (Yingxin Cheng), fuxiao@nju.edu.cn(Xiao Fu),xjdu@temple.edu(Xiaojiang Du),
luobin@nju.edu.cn (Bin Luo), mguizani@ieee.org (Mohsen Guizani).