Linux Memory Forensics: Methods and Techniques

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

in

Computer Science & Engineering

By

Trushna Parida
(Regn. No. NITD/PhD/CS/2018/01061)

Under the Supervision of

Dr. Suvrojit Das
Associate Professor
Department of Computer Science & Engineering, NIT Durgapur



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
NATIONAL INSTITUTE OF TECHNOLOGY DURGAPUR
WEST BENGAL – 713209
INDIA

September, 2022

Abstract

Recently, with the widespread use of digital devices for information processing and communication, there is a rapid rise of cyber-crimes. So, the need for digital forensic investigation has increased remarkably in past few years. Further, the increased use of systems and servers equipped with large memory and employment of sophisticated in-memory-only-malwares, drives the need to find better alternatives to the traditional forensics; thus, necessities the need for volatile memory forensics. Memory Forensics help analysts to reconstruct a meaningful picture of the system state, describing the cause and consequences of an incident through the analysis of the volatile memory contents. While the field of memory forensics have been studied for more than a decade, it still suffers from many open and unexplored problems. The research described in this dissertation proposes novel solutions for two such problems associated with the field of memory forensics.

The research community have focused on the development of various tools and techniques to retrieve and analyse the traces of malicious activities from memory snapshots. However, none of these have focused on retrieval of malware traces that utilize sophisticated run-time in-memory only data attack approaches to manipulate memory protection attributes, viz. the page table permission bits. This emerging data-only attack is known as the Page Table Manipulation (PTM) attack and has a high impact on system security, since it can bypass deployed defence mechanisms through the exploitation of existing memory corruption vulnerabilities.

Based on the insights we gain through our literature review; in our first contribution we design and implement a novel framework to collect and analyse the run-time memory-protection-attribute-manipulation based data attack (PTM attack) footprints from the volatile memory. The artifacts collected by the proposed utility helps investigators to identify such manipulation adopted to conceal malwares with the aim of subverting deployed prevention mechanisms and the memory analysis frameworks as well.

In our second research contribution, we present a novel mechanism to investigate the impacts of inconsistencies introduced by non-atomic memory snapshots on the page table data structures. The theory of operation and the subsequent implementation of the proposed mechanism are based on the extensive analysis of the memory management structures and the page table data structures. The resulting information helps the investigator to visualize the presence of inconsistencies within page tables and to perform a sound forensic analysis thereof.

Keywords: Memory Forensics, Kernel data attack, Page table manipulation, PageDumper, Smear-Aware Analysis, Page Table.