Digital Investigation 9 (2012) 125–137

Contents lists available at SciVerse ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Correctness, atomicity, and integrity: Defining criteria for forensically-sound memory acquisition

Stefan Vömel*, Felix C. Freiling

Department of Computer Science, Friedrich-Alexander University of Erlangen-Nuremberg, Am Wolfsmantel 46, 91058 Erlangen, Germany

ARTICLE INFO

Article history:
Received 22 November 2011
Received in revised form 25 March 2012
Accepted 9 April 2012

Keywords:
Memory forensics
Memory acquisition
Live forensics
Correctness
Atomicity
Integrity of a memory snapshot
Forensic soundness

ABSTRACT

While procedures for forensic memory *analysis* have been well described in the literature, the actual data *acquisition* process has been researched to a lesser degree. In particular, even though forensic analysts commonly agree that a memory snapshot should be "correct", "sound", and "reliable", the meaning of these terms still remains informal and vague. In this paper, we formalize three fundamental criteria, *correctness*, *atomicity*, and *integrity*, that determine the quality of a forensic memory image. We illustrate the criteria with the help of a number of intuitive examples, discuss the meaning of *forensic soundness* as well as outline implications and challenges for memory acquisition solutions available on the market to date.

1. Introduction

The forensic acquisition and analysis of volatile information in system RAM has moved more gradually into the focus of security professionals over the last years and is increasingly regarded as an integral part of an investigation. This shift in practices has been driven by several limitations and challenges traditional, persistent data-oriented approaches in computer forensics are confronted with. These include, for instance, examining ever-growing hard drives in time (Roussev and Richard, 2004; Shipley and Reeve, 2006; Mrdovic et al., 2009), coping with encrypted files, folders, and system partitions (Getgen, 2009) as well as detecting malicious software applications that are resident in memory only and do not leave any traces on the hard disk of the user any more (Moore et al., 2003; Sparks and Butler, 2005).

To a great degree, research in the area of memory forensics has concentrated on RAM *analysis* to date. For this purpose, a forensic image of a computer's memory is created and typically examined offline on a trusted workstation (Walters and Petroni, 2007). Relevant pieces of information that may be contained in a memory dump comprise, for example, the list of (currently as well as priorly) running processes on the target machine (Burdach, 2005; Schuster, 2006b; Dolan-Gavitt et al., 2009; Zhang et al., 2009, 2010), the list of open network connections (Schuster, 2006a; Ligh et al., 2010; Okolica and Peterson, 2010), open files (Dolan-Gavitt, 2007; van Baar et al., 2008), cryptographic keys (Kaplan, 2007; Hargreaves and Chivers, 2008; Maartmann-Moe et al., 2009; Halderman et al., 2009), remnants of the system registry (Dolan-Gavitt, 2008), and a myriad of system state- and application-related data, e.g., timestamps, IP addresses, and authentication credentials such as usernames and passwords (Stover and Dickerson, 2005; Beebe and Clark, 2007; Beebe and Dietrich, 2007; Zhao and Cao, 2009). The forensic *acquisition* of memory, on the other hand, has been described more marginally.

* Corresponding author.
E-mail addresses: stefan.voemel@cs.fau.de (S. Vömel), felix.freiling@cs.fau.de (F.C. Freiling).

1742-2876/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2012.04.005

1.1. Related work

Existing literature on forensic memory acquisition frequently either illustrates specific technical aspects that are important to the imaging operation, e.g., the layout of the address space, the virtual-to-physical address translation process, or the paging mechanism (Maclean, 2006; Kornblum, 2007), or merely distinguishes *hardware-based* from *software-based* solutions (e.g., see Vidas, 2006, 2010; Garcia, 2007). In the latter case, the acquisition process depends on functions that are provided by the operating system. In contrast, hardware-based approaches are capable of accessing physical memory directly and, thus, do not rely on the integrity of the operating system. As we have argued in a previous paper, this terminology is impractical and outdated though, because a number of *hybrid* methods that have been developed more recently cannot be clearly categorized any longer (Schatz, 2007a; Libster and Kornblum, 2008; Halderman et al., 2009). We therefore suggested evaluating the different technologies upon the requirements that are needed for obtaining a sound image of a host's volatile storage. Schatz (2007a) was first in identifying three major criteria for this task, namely the *fidelity* and *reliability* of the created snapshot as well as the *availability* of the respective acquisition method.

The principle of *fidelity* dictates that the generated memory image is "a precise copy [of] the original host's memory" (Schatz, 2007a, p. S128). Reliability stipulates that an acquisition technique is not vulnerable to subversion and either produces "a trustworthy result or none at all". Last but not least, *availability* refers to the applicability of a method "on arbitrary computers (or devices)".

In a later work, Schatz (2007b) adapted these criteria and outlined a preliminary evaluation framework for memory acquisition techniques based on the two dimensions *atomicity* – which serves as a metric for fidelity – and *availability*. However, both dimensions were only vaguely described. In particular, the definition of atomicity remained unclear. Neither was it explicitly pointed out that the availability of a certain solution strongly depends on the prevailing execution environment. For instance, within a controlled area such as a large organization, it is possible to prepare for an incident more carefully and take specific preparatory measures, e.g., deploying special hardware cards that are capable of creating memory snapshots on demand and may greatly facilitate a subsequent investigation. On the other hand, the same technology may not be available or applicable in a "smoking gun" situation, i.e., when raiding the home of a suspect or when examining a computer shortly after a break-in has occurred.

In a recent study, Inoue et al. (2011) describe four metrics for estimating the quality of a physical memory snapshot, namely *correctness*, *completeness*, *speed*, and the *amount of interference*. This publication is closest to our work. As we will see, however, the presented metrics may be broken down and mapped to the three evaluation criteria we introduce in this paper.

For reasons of completeness, we regard the work of Afek et al. (1993) as also relevant to this topic. Within an abstract distributed system model, the authors outline a solution for producing atomic snapshots of shared memory. The proposed algorithms require additional registers though to keep track of read and write operations to the individual memory regions. Due to the large overhead that is caused by these registers, the approach, although quite elegant, therefore remains mainly theoretic.

1.2. Motivation for this paper and results

In order to assess the performance and quality of forensic memory acquisition solutions, it is first necessary to precisely define the different evaluation criteria and, in the next step, derive suitable metrics based on these definitions. In our previous paper, we have already attempted to describe the dimensions introduced by Schatz more accurately. As such, we depicted a memory snapshot as *atomic* if it is "obtained within an 'uninterrupted' *atomic action* in the sense of a *critical section*" as used in operating system theory and concurrent programming (Vömel and Freiling, 2011, p. 8). In particular, an atomically-generated snapshot is free of the signs of concurrent system activity.

In this paper, we will further elaborate the characteristics of an atomic memory image. We will show that satisfying atomicity does not also automatically imply the *correctness* of the respective acquisition method, a second major factor that must be kept in mind when creating a copy of a computer's RAM. We will describe the fundamental differences between these two criteria with the help of terms originally used in distributed system theory and a number of intuitive examples. We will also define the *integrity of a memory snapshot* and discuss different perceptions in the literature concerning the meaning of *forensic soundness*. Last but not least, we will outline how the terminology coined by Schatz and Inoue et al. can be mapped and integrated into our model.

We hope that with the evaluation criteria and metrics presented in this paper, we can define a starting point for *measuring*, instead of estimating, the atomicity, correctness, and integrity of an acquisition technique. Please note that, even though we briefly discuss various limitations of selected memory imaging solutions used in practice to date in a later section of this article, a detailed analysis of these products would be out of scope. Therefore, we rather illustrate the theoretic background of our work. A more extensive evaluation of existing technologies is left for future work.

1.3. Outline of the paper

The remainder of this paper is outlined as follows: In Section 2, we give a short overview of distributed system theory. Our explanations are mainly derived from the work of Lamport (1978) as well as Mattern (1989) and need to be thoroughly understood because they form the foundation for the definition of a forensic memory snapshot and three fundamental evaluation criteria, *correctness*, *atomicity*, and *integrity*. These criteria are explained with the help of a number of intuitive examples in Section 3. Challenges that memory acquisition solutions must frequently cope with in practice are subject of Section 4. We conclude with a short summary of our findings and illustrate various topics for future research in Section 5.