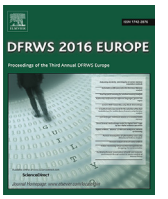
Digital Investigation 16 (2016) S1–S10

Contents lists available at ScienceDirect

Digital Investigation

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



DFRWS 2016 Europe — Proceedings of the Third Annual DFRWS Europe

Evaluating atomicity, and integrity of correct memory acquisition methods

Michael Gruhn*, Felix C. Freiling**

Department of Computer Science, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Martensstr. 3, 91058 Erlangen, Germany

Keywords:
Memory acquisition
Atomicity
Memory forensics
Integrity
Forensic tool testing

A B S T R A C T

With increased use of forensic memory analysis, the soundness of memory acquisition becomes more important. We therefore present a black box analysis technique in which memory contents are constantly changed via our payload application with a traceable access pattern. This way, given the correctness of a memory acquisition procedure, we can evaluate its atomicity and one aspect of integrity as defined by Vömel and Freiling (2012). We evaluated our approach on several memory acquisition techniques represented by 12 memory acquisition tools using a Windows 7 64-bit operating system running on a i5-2400 with 2 GiB RAM. We found user-mode memory acquisition software (ProcDump, Windows Task Manager), which suspend the process during memory acquisition, to provide perfect atomicity and integrity for snapshots of process memory. Cold-boot attacks (memimage, msramdump), virtualization (VirtualBox) and emulation (QEMU) all deliver perfect atomicity and integrity of full physical system memory snapshots. Kernel level software acquisition tools (FTK Imager, DumpIt, win64dd, WinPmem) exhibit memory smear from concurrent system activity reducing their atomicity. There integrity is reduced by running within the imaged memory space, hence overwriting part of the memory contents to be acquired. The least amount of atomicity is exhibited by a DMA attack (inception using IEEE 1394). Further, even if DMA is performed completely in hardware, integrity violations with respect to the point in time of the acquisition let this method appear inferior to all other methods. Our evaluation methodology is generalizable to examine further memory acquisition procedures on other operating systems and platforms.

Introduction

Volatile memory (RAM) is an increasingly valuable source of digital evidence during a forensic investigation. Not only are cryptographic keys for full disk encryption kept in RAM, but also many other pieces of information like the list of running processes and the details of active network connections are kept in RAM and are lost, if the computer would be simply turned off during evidence collection.

There are many ways to acquire volatile memory on standard desktop and server systems today (Vömel and Freiling, 2011). The possibilities range from software-based methods with tools like mdd[1] or WinPMEM,[2] over DMA attacks (Becher et al.) up to cold boot attacks (Halderman et al., 2009). All these methods have their advantages and disadvantages. On the one hand, while software-based methods are very convenient to use, they can be subverted

* Corresponding author.
** Corresponding author.
E-mail addresses: michael.gruhn@cs.fau.de (M. Gruhn), felix.freiling@cs.fau.de (F.C. Freiling).

[1] http://sourceforge.net/projects/mdd/.
[2] http://www.rekall-forensic.com/.

http://dx.doi.org/10.1016/j.diin.2016.01.003

by malware (Stüttgen and Cohen, 2013). On the other hand, DMA and cold boot attacks are often defeated by unfavorable system configurations (BIOS passwords or inactive DMA ports) or technology-immanent problems (Gruhn and Müller, 2013). Overall, these hindrances might produce memory images that are not forensically sound. To what extent this happens, is still rather unclear.

To address this point, Vömel and Freiling (2012) integrated the many different notions of forensic soundness in the literature into three criteria for snapshots of volatile memory: (1) correctness, (2) atomicity and (3) integrity. All three criteria focus on concrete requirements that are motivated from practice:

- A memory snapshot is *correct* if the image contains exactly those values that were stored in memory at the time the snapshot was taken. The degree of correctness is the percentage of memory cells that have been acquired correctly
- The criterion of *atomicity* stipulates that the memory image should not be affected by signs of concurrent activity. It is well known that unatomic snapshots become "fuzzy" (Libster and Kornblum, 2008). The degree of atomicity is the percentage of memory regions that satisfy consistency in this respect.
- A snapshot satisfies a high degree of *integrity* if the impact of a given acquisition approach on a computer's RAM is low. For instance, by loading a software-based imaging utility into memory, specific parts of memory are affected and the degree of system contamination increases (and consequently, integrity decreases).

All three criteria were formally defined and shown to be independent of each other.

With these criteria it was now possible to measure and not only estimate the forensic soundness of snapshot acquisition techniques. This was then done by Vömel and Stüttgen (2013) for three popular memory acquisition utilities: win32dd (Suiche, 2009), WinPMEM (Cohen, 2012), and mdd (ManTech CSI Inc., 2009). Their study exhibited some correctness flaws in these tools (which were later fixed), but also showed that their level of integrity and atomicity was all quite similar.

The reason why Vömel and Stüttgen (2013) only evaluated three software-based acquisition methods lies in their measurement approach: They used the open-source Intel IA-32 emulator Bochs running a Windows XP SP3 on which the acquisition utilities ran. The utilities were instrumented such that every relevant event was recorded using a hypercall into the emulator, thus enabling the measurement. Naturally, this white-box measurement approach was only possible for tools that were available to the authors in source code, thus severely restricting the scope of their measurement. It is clear that approaches such as DMA and cold boot attacks can only be measured using a black-box approach. Furthermore, these measurements were performed in a situation where the Windows system was basically idle, thus giving a lower-bound measurement. The impact of system load on the quality of memory acquisition is not yet precisely known.

Related work

Vömel and Freiling (2012) defined correctness, atomicity and integrity as criteria for forensically-sound memory acquisition and provided a comparison matrix (Vömel and Freiling, 2011, Fig. 5) with regard to the different acquisition methods. However, they also indicate that "the exact positioning of the methods within the fields of the matrix may certainly be subject to discussion" (Vömel and Freiling, 2011, p. 7). The first to evaluate these memory acquisition criteria were Vömel and Stüttgen (2013). As already stated they relied on a white box methodology restricting them to open source tools. In 2015 Gruhn (2015) introduced a gray-box methodology with which memory address translation could be inferred. Gruhn notes the methodology can also be used to evaluate the memory snapshot correctness criteria. We build up on the results of Gruhn (2015) and extend the methodology to enable the evaluation of atomicity and integrity in addition to correctness.

Other work using the notion of atomicity are BodySnatcher (Schatz, 2007), HyperSleuth (Martignoni et al., 2010) and Vis (Yu et al., 2012), all of which try to increase atomicity of forensic memory acquisition by suspending execution of the operating system, hence reducing concurrency.

Contribution

In this paper, we present the first black-box methodology for measuring the quality of memory acquisition techniques. Extending the insights of Vömel and Stüttgen (2013), we take correctness for granted and focus on integrity and atomicity. Our approach allows to compare not only different software utilities with each other but also to compare them with totally different approaches like DMA and cold-boot attacks.

The idea of our approach is to apply the memory acquisition method to memory content that changes in a predictable way: Briefly spoken, we use a program that writes logical timestamps into memory in such a way that investigating the memory snapshot yields the precise time when a certain memory region was imaged. This allows to infer an *upper bound* in integrity and atomicity meaning that these criteria will be at most as bad for the respective procedures.

More precisely, our contributions are as follows:

- We provide a framework to evaluate memory forensic tools using a black-box approach.
- We evaluate 12 memory forensic acquisition tools and methods.

We make our tools, programs and scripts used in our evaluation available to the forensic community. This material is available at https://www1.cs.fau.de/projects/rammangler.

Outline

This paper is structured as follows: First in Section Background: criteria for forensically sound memory