Chapter 18
Forensic Implications of Virtualization Technologies

Cosimo Anglano
Universitá del Piemonte Orientale "A. Avogadro," Italy

ABSTRACT

In the recent past machine and application virtualization technologies have received a great attention from the IT community, and are being increasingly used both in the Data Center and by the end user. The proliferation of these technologies will result, in the near future, in an increasing number of illegal or inappropriate activities carried out by means of virtual machines, or targeting virtual machines, rather than physical ones. Therefore, appropriate forensic analysis techniques, specifically tailored to virtualization environments, must be developed. Furthermore, virtualization technologies provide very effective anti-forensics capabilities, so specific countermeasures have to be sought as well. In addition to the above problems, however, virtualization technologies provide also the opportunity of developing novel forensic analysis techniques for non-virtualized systems. This chapter discusses the implications on the forensic computing field of the issues, challenges, and opportunities presented by virtualization technologies, with a particular emphasis on the possible solutions to the problems arising during the forensic analysis of a virtualized system.

INTRODUCTION

The term "machine virtualization" refers to a set of technologies that enable the abstraction of computing resources, which is the ability of hiding the actual characteristics of the physical hardware to the operating system and to the user. In the recent past, the availability of mature software solutions, and the introduction of hardware support for virtualization in modern commodity microprocessors (like Intel's VT-X and AMD's AMD-V technologies), have stimulated a great interest and an increasing prolifera-

DOI: 10.4018/978-1-60566-836-9.ch018

tion of machine virtualization technologies. Machine virtualization is nowadays used both in the Data Center, where its main role is server consolidation, and by the individual user to simultaneously execute multiple operating systems on the same physical machine. This growing trend is expected to continue also in the future.

A first consequence of the growing popularity of machine virtualization technologies will be an increase in the number of illegal or inappropriate activities carried out by means of virtual machines, or will target virtual machines, rather than physical ones. Consequently, the probability that a compromised server will be running on a virtual machine, or that a given crime will be committed by using applications running on a virtualized system, will be significantly higher than now. In order to properly deal with these scenarios, forensic analysis methodologies able to properly deal with virtualized systems must be adopted. However, as discussed in this chapter, traditional forensic analysis methodologies and tools are not able to properly deal with all the peculiarities of virtualized systems. Therefore, methodologies and tools specifically tailored to virtualized systems must be developed.

As a second consequence of the spreading of virtualization technologies, we may expect an increasing use of virtual machines as anti-forensic tools. The traces generated by activities performed using a virtual machine (e.g., the Internet browsing history) are indeed stored into its virtual storage devices, and not directly on the file system of the physical machine on which it is running. Furthermore, some products allow the user to install the virtualization software on a removable storage device (such as a USB flash drive or hard disk) and to run his/her applications directly from that device, after attaching it to a physical computer, without ever "touching" the physical storage of that computer. In these cases, no traces of the activities performed by using the virtualized system will be left on the file system of the physical machine. To correctly deal with these scenarios, forensic computing methodologies and tools, able to understand whether such a virtualized system has been used on a physical machine, to recover traces stored on virtual storage devices, and to tie the usage of a "portable" virtual machine to a specific physical system and time frame, must be developed.

Besides the challenges mentioned above, however, machine virtualization technologies provide also several opportunities to the forensic analyst. First of all, they provide the technical substrate for the development of novel forensic analysis techniques for conventional (i.e., non-virtualized) systems. For instance, there are techniques that permit to build and run a virtual machine whose virtual disk is obtained from the forensic image of a suspect hard drive. In this way, the analyst is able to reproduce the behavior of the suspect machine in a forensically sound way, or to use techniques or tools that require to be directly executed on that machine. Furthermore, virtualization technologies can be used to ease the application of existing forensic analysis techniques. For instance, they greatly simplify the setup and deployment of computing test beds on which the behavior of operating systems and applications, as well as of malware, can be tested in a controlled and repeatable way.

In spite of the above considerations, however, the literature still lacks a comprehensive discussion of the problems and issues arising from the proliferation of machine virtualization technologies. This chapter aims at filling this gap by discussing these issues in a systematic way, by illustrating the forensic analysis techniques that are already available for dealing with virtualized systems, and by highlighting the challenges that are still open and waiting for a solution. Furthermore, several virtualization-based forensic analysis techniques will be discussed as well. Given the very large number of virtualization systems available today, we will neither focus on a single system, nor we will attempt to consider all of them, but we will keep our discussion as general and product-agnostic as possible, and will refer to specific virtualization system only when an example is necessary to clarify the matter.