Digital Investigation 9 (2012) S90–S98

Contents lists available at SciVerse ScienceDirect

Digital Investigation

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

Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques

Josiah Dykstra*, Alan T. Sherman

Cyber Defense Lab, Department of CSEE, University of Maryland, Baltimore County (UMBC), 1000 Hilltop Circle, Baltimore, MD 21250, USA

Keywords:
Computer security
Cloud computing
Digital forensics
Cloud forensics
EnCase
FTK
Amazon EC2

ABSTRACT

We expose and explore technical and trust issues that arise in acquiring forensic evidence from infrastructure-as-a-service cloud computing and analyze some strategies for addressing these challenges. First, we create a model to show the layers of trust required in the cloud. Second, we present the overarching context for a cloud forensic exam and analyze choices available to an examiner. Third, we provide for the first time an evaluation of popular forensic acquisition tools including Guidance EnCase and AccesData Forensic Toolkit, and show that they can successfully return volatile and non-volatile data from the cloud. We explain, however, that with those techniques judge and jury must accept a great deal of trust in the authenticity and integrity of the data from many layers of the cloud model. In addition, we explore four other solutions for acquisition—Trusted Platform Modules, the management plane, forensics-as-a-service, and legal solutions, which assume less trust but require more cooperation from the cloud service provider. Our work lays a foundation for future development of new acquisition methods for the cloud that will be trustworthy and forensically sound. Our work also helps forensic examiners, law enforcement, and the court evaluate confidence in evidence from the cloud.

1. Introduction

Discovery and acquisition of evidence in remote, elastic, provider-controlled cloud computing platforms differ from that in traditional digital forensics, and examiners lack appropriate tools for these tasks. While there are many important issues in this new field, we focus explicitly on data acquisition. Crimes that target or use cloud computing will undoubtedly emerge in this landscape, and investigators will rely on their existing expertise in tools like Guidance EnCase or AccessData Forensic Toolkit (FTK) unless alternative tools and techniques are provided.

Digital forensics for cloud computing brings new technical and legal challenges. Cloud computing makes forensics different, particularly given the remote nature of the evidence, lack of physical access, and trust required in the integrity and authenticity. While the goals of the forensic examiner are the same as before, the non-conventional difficult problems include forensically sound acquisition of remote data, large data volumes, distributed and elastic data, chain of custody, and data ownership.

Seizure and acquisition of digital artifacts are the initial steps in the forensic process (Casey, 2004). Two possible scenarios exist: remote investigators could collect forensic evidence themselves from the source, or providers could deliver it. Each scenario requires a different degree of trust in the data returned. Further, each scenario uses different technical implementations to recover the data. Given years of development, acceptance by the judicial system, and expertise in the field, market leaders in the commercial forensic tool space including EnCase and FTK are ideally prepositioned for the cloud forensic challenge (SCMagazine, 2011). One question that remained until now, however,

* Corresponding author.
E-mail addresses: dykstra@umbc.edu (J. Dykstra), sherman@umbc.edu (A.T. Sherman).

1742-2876/$ – see front matter © 2012 Dykstra & Sherman. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2012.05.001

was an evaluation of the ability of such tools to acquire and analyze cloud-based evidence.

Cloud computing is a broad, generic term with many meanings and definitions. It has infiltrated the vernacular, bastardized in marketing and media. Cloud computing is an evolution and combination of decades of technology, resulting in a model of convenient, on-demand, elastic, location-independent computing resources. Though some definitions of cloud computing include popular web-based services such as email and social networking, we limit the scope of this paper to computing resources that are billed as utilities. More specifically, we use the *Infrastructure-as-a-Service* (IaaS) model (National Institute of Standards and Technology, 2011). In this model, the consumer has complete control over a guest operating system running in a *virtual machine* (VM). The provider retains control and responsibility for the hypervisor (HV) down to the physical hardware in the datacenter. Since the Platform-as-a-Service and Software-as-a-Service models are built on IaaS, beginning with IaaS provides a fundamental basis from which to build future work.

In this paper, we assume that the target system of the forensic investigation still exists in the cloud. The elastic nature of cloud computing makes it possible for a criminal to commit a crime and then immediately destroy the evidence, but that situation is not considered here. While some cases will involve the cloud as the instrument of the crime, others will involve the cloud-hosted service as the target of the crime. The later is the scope of this paper.

In draft guidance (Federal CIO Council, 2011, p. 21) on the secure use of cloud computing, the Federal Chief Information Officers Council states that "incident response and computer forensics in a cloud environment require fundamentally different tools, techniques, and training." In this paper, we evaluate the validity of that statement with respect to data acquisition. Contributions of our work include:

- Results from three experiments that exercise existing tools for persistent and non-persistent data collection in a public cloud, Amazon's *Elastic Compute Cloud* (EC2).
- Analysis of alternatives for forensic acquisition at lower levels of the infrastructure stack, for cases when there is insufficient trust in data acquisition using the guest operating system.
- A demonstration of how virtual machine introspection can be used to inject a remote forensic agent for remote acquisition.
- Exploration of four strategies for forensic data acquisition with an untrusted hypervisor.

The rest of the paper is organized as follows. Section 2 reviews previous and related work. Section 3.1 presents a model of cloud trust. Section 3.2 presents the context for a cloud examination. Section 4 presents our experiments in using the native capabilities of EnCase, FTK, Fastdump, and Memoryze for data acquisition in EC2. Section 5 suggests alternative approaches. Section 6 discusses considerations and Section 7 concludes the work.

2. Previous and related work

The US federal government evaluates some of the most widely used forensic tools to ensure reliability. The National Institute of Standards and Technology's (NIST) Computer Forensic Tool Testing (CFTT) project is charged with testing digital forensic tools, measuring their effectiveness, and certifying them (National Institute of Standards and Technology, 2003). They evaluated EnCase 6.5 in September 2009, and FTK Imager 2.5.3.14 in June 2008 (National Institute of Standards and Technology, 2009, 2008). They have never tested nor certified the enterprise versions of these products that include remote forensic capabilities. NIST also publishes a Digital Data Acquisition Tool Specification, which "defines requirements for digital media acquisition tools in computer forensic investigations" (National Institute of Standards and Technology, 2004). The most recent version of the specification was written in 2004, before cloud computing as we know it existed.

Several researchers have pointed out that evidence acquisition is a forefront issue with cloud forensics (Dykstra and Sherman, 2011a; Ruan et al., 2011; Taylor et al., 2011). Dykstra and Sherman's analysis of two hypothetical case studies illustrated the non-trivial issues with collecting evidence from a cloud crime (Dykstra and Sherman, 2011a,b). Ruan *et al.* (Ruan et al., 2011) suggested that evidence collection should obey "clearly-defined segregation of duties between client and provider," though it was unclear who should collect volatile and non-volatile cloud data and how. Taylor *et al.* (Taylor et al., 2011) also lamented about the lack of appropriate tools for data from the cloud, noting that "Many of these tools are standardised for today's computing environment, such as EnCase or the Forensics Tool Kit [sic]."

Virtual machine introspection (VMI) is a technique whereby an observer can interact with a virtual machine client from the outside through the hypervisor. In 2003, Garfinkel and Rosenblum (Garfinkel and Rosenblum, 2003) first demonstrated a technique for intrusion detection inside a virtual guest using VMI. In 2009 using VMware's VMSafe, Symantec demonstrated injecting anti-virus code into a virtual machine from the VMware hypervisor (Conover and Chiueh, 2008). From that year, researchers have proposed various applications of VMI to forensic memory analysis (Nance et al., 2009; Dolan-Gabitt et al., 2011). Santana (Santana, 2009) reports that Terremark uses introspection for monitoring, management and security for their vSphere cloud computing offering. So far no attempt has been made to inject a forensic tool, such as an EnCase servlet, into a virtual machine from the hypervisor.

In 2009, Gartner (Heiser, 2009) published an overview of remote forensic tools and guidance for their use, targeted at enterprise environments. They cited EnCase and FTK as the most widely used products, with the greatest international support. These tools, however, have their faults: in 2007, a vulnerability was found in the authentication between the remote EnCase agent and the server (Giobbi and McCormick, 2007). From a legal perspective, Guidance Software's own "EnCase Legal Journal" for 2011, a comprehensive examination of legal issues and decisions