Cloud Forensics a Technical Approach to Virtual Machine Acquisition

Louis Antani Holt and Mohammad Hammoudeh
School of Computing, Mathematics & Digital Technology
Manchester Metropolitan University, Manchester, UK
Email@LouisAntani.com and M.Hammoudeh@mmu.ac.uk

Abstract — The cloud is radically changing the face of information technology. Traditional digital forensic procedures, software, and hardware are incapable of scaling to the cloud. This paper introduces a new system, leveraging cloud management SDK’s to enable highly scalable Virtual Machine (VM) acquisition from cloud infrastructures.

Keywords—Cloud Forensics; Virtualisation; VMware;

I. INTRODUCTION

Computer forensics has evolved around the practice of seizing and forensically imaging physical hardware. Forensic investigations rely upon acquiring forensically sound copies known as forensic images. Investigations are performed almost entirely on these images, ensuring the evidential integrity of the original hardware is maintained [1]. The cloud introduces a significant problem to this current forensic process.

One of the most substantial differences in cloud computing compared with traditional computing is the shift from physical to virtual. VMs delivered from the cloud are consumed remotely, unlinked from their physical implementations. The delivery, management, and migration technologies involved have the potential to entangle a single VM with numerous physical systems. This entanglement in a shared cloud environment renders seizure and imaging of physical hardware impractical; potentially averting forensic investigations.

II. IDENTIFYING AN ENTRY POINT

The cloud is the product of multiple layers of technology functioning coherently to provide network access to a shared pool of computing resources. Consumers of the cloud are typically abstracted from these layers, interacting at the highest possible level. From a forensic perspective interactions at this level are highly undesirable. Access to the target VM may be limited with a high risk of affecting evidence integrity.

Most cloud technology providers deploy cloud infrastructures from hypervisor platforms. Hypervisors are software managers responsible for managing a physical host’s hardware across multiple VM instances. In the VMware’s vSphere hypervisor platform, the hypervisor management layer presents the most suitable entry point for a forensic practitioner, providing near direct access to the target VM. Interfacing with the management layer is made possible through publically available management libraries. The VMware vSphere SDK and Citrix XenServer API provide functionality which can be adapted for forensic cloud acquisition systems. This paper will use VMware’s management SDK as the foundation for this concept.

III. IMAGING A VIRTUAL MACHINE

Unlike a physical system a VM is an encapsulated software implementation, operating almost identically to a physical system. Inadvertently, this is an advantage, effectively meaning the VM is already in a data state, eliminating the requirement for physical imaging. This creates numerous possibilities previously unseen in computer forensics, including automated acquisition, precision logging, and high levels of scalability. The following steps highlight the basic introduction to VM acquisition using VMware’s SDK.

A. Locating a Virtual Machine

The VMware vSphere management SDK employs an object oriented structure known as a management object model. This model defines the internal structure of the underlying management platform. Direct access to individual data stores and VM files is granted through the creation of a “Service Instance” object.

B. Isolating and Exporting a Virtual Machine

Once located, isolating the target VM is an essential initial step. This can be achieved by obtaining an export “HttpNFCLease” on the target VM. Whilst held, the lease blocks external operations from altering the state or integrity of the VM. Once in a “Ready” state the lease provides an array of corresponding HTTP URL’s enabling simple download and acquisition of the target VM.

IV. CONCLUSION & FUTURE WORK

This paper introduced a basic overview into the ongoing research into highly scalable VM acquisition from cloud infrastructures. The methods briefly introduced within this paper have been tested with promising results on small scale VMware cloud systems. Additional research into integrity validation and large scale deployment is planned.

V. REFERENCES