OpenFlow Virtual Appliance:
An Efficient Security Interface For Cloud Forensic Spyware Robot

Ifeyinwa Eucharia Achumba, Federal University of Technology, Owerri, Nigeria

Kennedy Chinedu Okafor, Federal University of Technology, Owerri, Nigeria

Gloria N. Ezeh, Federal University of Technology, Owerri, Nigeria

Uchenna Hermes Diala, Federal University of Technology, Owerri, Nigeria

ABSTRACT

Network forensics vis-a-vis cloud computing offerings can be leveraged to address the needs of enterprise-grade spyware solutions online. A modular, extensible cloud architecture with intrinsic support for efficient security monitoring is proposed and an implementation architecture which facilitates dynamic interface with OpenFlow hardware to create infinite flexibility in managing security decisions is presented. A forensic DataCenter model that integrates remote security monitoring using an intelligent Virtual Security Gateway in a cloud domain was developed as part of the work. An OpenFlow Virtual Appliance is proposed as a security hardware interface for thin clients connected to the Cloud Sypware Robot (CSR) server. The cloud ontology-Software as a Service (SaaS) model was used for the CSR application conveying several security benefits. The goal is to facilitate an open, service-based, online network forensics application that is transparently provisioned for users. The paper proposes a security foundation for next-generation enterprise-grade cloud computing.

Keywords: *Cloud Computing, DataCenter, Network Forensics, OFVA, Openflow Hardware, Security, VSG*

1. INTRODUCTION

1.1. Background of Study

In many real world applications such as the earlier proposed Smart Green Energy Management System (SGEMS) which uses the DCCN (Okafor, Ugwoke, & Oparaku, 2015) to house the Enterprise Energy Analytic Tracking Cloud Portal EEATCP and Cloud Sypware Robot (CSR), sensitive data are kept in physical server machines. When a hacker exploits the server vulnerabilities, little or no damage can be done to the log files because the OFVA is shielding the log files. It is possible to forensically monitor the entire network and still deliver the required Quality of Service (QoS). The network forensics presented in this paper offers a computationally cost effective approach for generating audit or log trails prior to the logging into the network server that runs the CSR. This makes it difficult for an attacker to launch a read, modify or destroy attack on the DCCN. This paper establishes an OFVA as a

DOI: 10.4018/IJDCF.2015040103

special type of network forensics module that monitors the network users and their activities with little overhead on the network performance.

According to (Palmer, 2001), network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. There are numerous areas of digital forensics, but a distinguishing feature of network investigations is that it deals with volatile and dynamic information. The two broad application areas of network forensics are: security monitoring which involves monitoring a network for anomalous traffic and detecting intrusions. An attacker might be able to erase all log files on a compromised host; network-based evidence might therefore be the only evidence available for forensic analysis (Hjelmvik, 2012). The second form of network forensics relates to law enforcement. In this context, analysis of captured network traffic is the major consideration.

With cloud computing virtualization, computing as a network-centric pool could facilitate outside disk-based digital evidence. Two approaches that are commonly used to collect network data: a brute force "catch it as you can" and a more intelligent "stop look listen" method. Both approaches were applied in the Cloud forensic robot design. For the CSR, this could either be deployed in a Virtual Local Area Network (VLAN) based switch (Tariq, Mansy, Feamster, & Ammar, 2009) or an OpenFlow based switch (Bianco, Birke, Giraudo, & Palacin, 2010) (Heller, 2014). The security framework of CSR leverages and extends the advantages of OFVA and cloud virtualization. It also embeds autonomous management capabilities into the OpenFlow hardware infrastructure. Furthermore, the advent of Software Defined Networking (SDN) (Bianco, Birke, Giraudo, & Palacin, 2010) as a scheme that separates the data and control functions of networking devices with a well-defined Application Programming Interface (API) allows background processes for security monitoring (see figure 1). This makes the security framework more robust than in traditional large enterprise networks in which the security devices such as switches and routers encompass both data and control functions.

1.2. Network Platform Considerations for Cloud Sypware Robot (CSR) Server

For a forensic DCCN, the increasing use of server virtualization makes for efficient integration of OFVA which is the Pix-firewall in context. Server virtualization embeds server resources such as CPUs, Operating System (OS), memory, etc for end-users on the cloud Software as a Service (SaaS). This embedded automation (virtualization) facilitates server partitioning into multiple, independent servers, conserving hardware resources. It also makes it possible to migrate a server quickly from one machine to another for load balancing (Heller, 2014) or for dynamic switchover in the case of machine failure. However, there must be a port assignment on the server for every Virtual Machine (VM). The challenges of dynamically adding, dropping, and changing network resources and profiles in conventional networks running SaaS are alleviated with OFVA. Server virtualization makes traffic flows substantially different from the traditional client-server model. Typically, there is a considerable amount of traffic among virtual servers, for such purposes as maintaining consistent images of the database and invoking security functions such as access control. These server-to-server traffic flows change in location and intensity over time, demanding a flexible approach to managing network resources.

Another factor highlighting the need for rapid response in allocating network resources for cloud based applications (virtualization) is the ability to respond to rapidly changing resource, QoS, and security requirements. In most large scale computer platforms, a variety of operating systems (Windows, Linux, or Mac OS) run on top of the hardware via virtualization (Okezie, Okafor, & Udeze, 2013). In this case, the OS provides Application Program Interface (APIs) that enables interoperability among hardware vendors. However, in conventional

Related Content