Chapter 42
Analyzing Virtualization Vulnerabilities and Design a Secure Cloud Environment to Prevent From XSS Attack

Nitin Nagar
Devi Ahiliya University, India

Ugrasen Suman
Devi Ahiliya University, India

ABSTRACT

Cloud virtualization has created an enormous impact on IT and networking worlds. A cloud environment is built on virtualization technology. Virtualization and its exclusive architecture have numerous features and advantages over non-conventional virtual machines. However, these new uniqueness create new vulnerabilities and attacks on a virtualization based cloud system. Cross Site Scripting (XSS) is among the top cloud vulnerabilities, according to recent studies. This exposure occurs when a user uses the input from a cloud environment application without properly looking into them. This allows an attacker to execute malicious scripts in cloud. The scripts execute harmful actions when a user visits the exploited cloud. Current approaches to mitigate this problem, especially on effective detection of XSS vulnerabilities in the application or prevention of real-time XSS attacks. To address this problem, the survey of different vulnerability attacks on cloud virtualization performed and also presents a concept for the removal of XSS vulnerabilities to secure the cloud environment.

1. INTRODUCTION

Cloud virtualization technology offers a direction to use IT resources among Virtual Machines (VMs) using hardware and software partitioning, emulation, time-sharing, resource sharing and so on. Traditionally, the OS manages the hardware resources, but virtualization technology adds a new layer between the operating system and hardware. A virtualization layer provides infrastructural support to an operating

DOI: 10.4018/978-1-5225-8176-5.ch042

system; therefore, multiple VMs can be created and managed independently. Virtualization layer is often called the hypervisor or Virtual Machine Monitor (VMM). A computer on which a hypervisor installed to control various virtual machines is defined as a host machine and each VM is called a guest machine. Various approaches are used to provide virtualization, such as para-virtualization (PV), full virtualization (FV), and hardware-assisted virtualization (HVM). PV requires changes to the client operating system when PV access to protect the resources and knowledge of the operating system on which the hypervisor is situated (Venkatesha, 2009). This mechanism simplifies the hardware abstraction layer, but provides difficulty between version control of the hypervisor and the PV operating system. FV supports unmodified guest passes through binary translation. VMware hypervisor uses the binary translation direct execution techniques for creating VMs on proprietary base operating system such as Windows (Buyya, 2011).

Several tools and techniques are used to implement cloud based virtualization. There exist commercial and open source solutions such as OpenNebula, Eucalyptus, Nimbus, OpenStack and so on (Nagar, 2012). The commercial solutions are Hyper-V, VMware, ESX, etc. It is observed that the open source solution such as OpenStack provides more flexibility than the other commercial solutions. Nevertheless, open source solutions suffer from a lack of documentation and are more difficult to enforce. The hypervisors, such as Hyper-V, KVM, Xen and VMware vSphere are used with this open source solution (Nagar, 2012). Hypervisor uses different architectures, although it is limited to hardware-assisted virtualization mode. The Windows-based Hyper-V delivers a significantly different architecture than the Linux based hypervisors. Xen and KVM are based on open-source modification of the Linux kernel, whereas VMware uses custom build functions (Nagar, 2012) (Hwang, 2013) (Clark, 2005). Xen hypervisor uses PV of separate management domain; controls the VMs, access to user defined block and network drivers. KVM considered as a core module that employs most of the Linux features. For example, instead of providing the CPU scheduler to VMs, each VM KVM treated as a process and uses the standard Linux scheduler to in order to allocate resources (Cherkasova, 2005). VMs services and cloud service providers offer more powerful and anchor ecosystem of cloud services. User provides their VMs and cloud provider leads them often without the knowledge of the guest operating system. Cloud providers, security-as-a-service based on VM introspection and ensures the best security (Christodorescu, 2009) (Kong, 2010).

Cloud virtualization threats and vulnerabilities are a foremost challenge in the field of research. The rest of the paper is organized as follows. Section 2 includes a virtualization security challenges and the associated issues in a cloud environment. The section 3 states literature reviews with virtualization threats and vulnerabilities. In section 4, we discuss the top most vulnerabilities of cloud virtualization named as XSS (Cross Site Scripting) attack or CSRF (Cross Site Request Forgery). We also discuss the seriousness of XSS attacks, their types and problems in XSS. In Section 5, we proposed work on XSS detection and recovery in the DOM. We also discuss the implementation work to solve the problems, HTML parsing, analyzing modification with Jsoup and performance evaluation of different aspects. In section 6, we state the conclusion and final, references of the paper.

2. VIRTUALIZATION SECURITY CHALLENGES AND ISSUES

The transmission of computing resources in a virtualized environment has unaffected on the majority of the resources through vulnerabilities and threats. For example, if service inherent vulnerabilities and service is moving from a non-virtualized server to a virtualized server, the revision is still as vulnerable