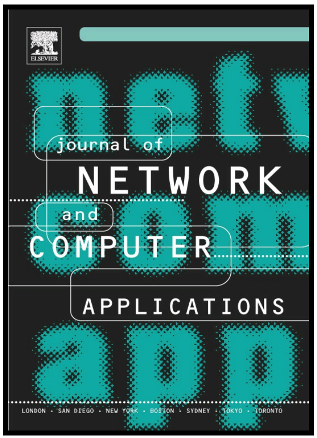
journal of
NETWORK
and
COMPUTER
APPLICATIONS
LONDON • SAN DIEGO • NEW YORK • BOSTON • SYDNEY • TOKYO • TORONTO

www.elsevier.com/locate/jnca

On Cloud Security Attacks: A Taxonomy and Intrusion Detection and Prevention as a Service

Salman Iqbal, Miss Laiha Mat Kiah, Babak Dhaghighi, Muzammil Hussain, Suleman khan, Muhammad Khurram Khan, Kim-Kwang Raymond Choo

PII: S1084-8045(16)30177-1
DOI: http://dx.doi.org/10.1016/j.jnca.2016.08.016
Reference: YJNCA1698

To appear in: *Journal of Network and Computer Applications*

Received date: 31 May 2016
Revised date: 19 July 2016
Accepted date: 15 August 2016

Cite this article as: Salman Iqbal, Miss Laiha Mat Kiah, Babak Dhaghighi Muzammil Hussain, Suleman khan, Muhammad Khurram Khan and Kim-Kwan Raymond Choo, On Cloud Security Attacks: A Taxonomy and Intrusion Detection and Prevention as a Service, *Journal of Network and Compute Applications,* http://dx.doi.org/10.1016/j.jnca.2016.08.016

On Cloud Security Attacks: A Taxonomy and Intrusion Detection and Prevention as a Service

Salman Iqbal[1*], Miss Laiha Mat Kiah[1*], Babak Dhaghighi[1], Muzammil Hussain[1], Suleman khan[1], Muhammad Khurram Khan[2], Kim-Kwang Raymond Choo[3]

[1]Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, 50603, Malaysia

[2]Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia

[3]Information Assurance Research Group, Advanced Computing Research Centre, University of South Australia

*Corresponding Authors: [Salman Iqbal, Miss Laiha Mat Kiah]

Abstract

Major provisioning of cloud computing is mainly delivered via Software as a Service, Platform as a Service and Infrastructure as a Service. However, these service delivery models are vulnerable to a range of security attacks, exploiting both cloud specific and existing web service vulnerabilities. Taxonomies are a useful tool for system designers as they provide a systematic way of understanding, identifying and addressing security risks. In this research work, Cloud based attacks and vulnerabilities are collected and classify with respect to their cloud models. We also present taxonomy of cloud security attacks and potential mitigation strategies with the aim of providing an in-depth understanding of security requirements in the cloud environment. We also highlight the importance of intrusion detection and prevention as a service.

Keywords—Cloud computing, Taxonomy, Security attacks, Intrusion detection

1. Introduction

While Cloud Computing (CC) is not entirely new, it is still gaining traction among organizations and individual users. For example, Garner predicted that cloud adoption will continue to rise at a compound increase rate of 41.7% in 2016. However, transition to the cloud environment is not straightforward and there are a number of operational and security challenges. Ensuring the security of data outsourced to the cloud is increasingly important due to the trend of storing more data in the cloud [1, 2].

The use of hypervisor and Virtual Machine (VM) technologies are also a security threat, as these hypervisor and VM technologies are vulnerable to VM level attacks. In reality, these systems consist of a number of on-site computer organizations which may have a large number of hardware and software systems. Vulnerabilities in VM infrastructure can be exploited by attackers to exfiltrate data or conduct attacks such as DDoS [3, 4]. This is due to the inherent weaknesses in the TCP/IP stack. Additionally, several new attacks have appeared in recent times that make use of polymorphism and metamorphisms to evade detection. In an IaaS cloud environment, for example, information about victim's machines can easily be acquired and exploited; thus, facilitating attacks on VMs [5-7].

Attackers can inject kernel scripts to the host operating system (OS), and as all guest OS run their OS on this kernel, attackers can control all VMs. Furthermore, by successfully exploiting known or zero-day vulnerabilities in the hosted VM, the attackers can then gain access to the server's VMs since the hypervisor shares the hardware and software in the shared virtual environment [8]. Some hypervisors provide APIs which render the VM facility completely visible to network traffic. However, these APIs provide additional avenues for attackers to monitor and exploit the network communication [9]. There are also other attacks such as data intrusion, data availability and data integrity targeting CC [10].