Ain Shams University
Faculty of Engineering
Computer and Systems Engineering Department

Secure Virtual Machines Admission Control in Cloud Computing

by

Omnia Abdelrahem Mohamed
Bachelor of Electric Engineering
(Computer and Systems Engineering)
Ain Shams University, 2011

A THESIS
SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE DEGREE OF MASTER OF SCIENCE
(ELECTRIC ENGINEERING)
DEPARTMENT OF COMPUTER AND SYSTEM ENGINEERING

Supervised By

Dr. Ayman M. Bahaa-Eldin
Dr. Ayman Elsayed Taha

Cairo, Egypt
March, 2017

Faculty of Engineering
Computer and Systems
Eng. Dept.

Examiners Committee

Name : Omnia Abdelrahem Mohamed Mohamed Mahmoud

Thesis : Secure Virtual Machines Admission Control in Cloud Computing

Degree : Master of Science

Signature

Prof. Dr. Ihab A. Ali
Professor - Electronics, Communication and Computer Engineering - Helwan University

Prof. Dr. Hoda Korashy Mohamed
Emeritus Professor - Computer and Systems Engineering - Ain Shams University

Prof. Dr. Ayman M. Bahaa-Eldin (supervisor)
Professor - Computer and Systems Engineering - Ain Shams University

Date: 18/07/2017

Abstract

Omnia Abdelrahem Mohamed

Secure Virtual Machines Admission Control in Cloud Computing

MASTER OF SCIENCE dissertation

Ain Shams University, 2017

Cloud computing is a fast spreading model for service delivery, widely adapted in today's IT environment. It is a combination of other technologies working together, one of them is virtualization, which is the abstraction of computer resources, separating the physical resources from the final resources delivered to the user. Regardless of its wide spread, cloud computing still has security concerns, also there are the threats related to virtualization that are inherited by the cloud. In this paper; a framework is suggested to control the admission of new virtual machines into the cloud environment in an attempt to limit the number of malicious behaving machines that may contain a malware, risking its spread through the environment, or a machine user trying to attack another machine in the same environment. Also machines staying dormant for long periods of time are considered a new admission, for the risk of its disk may have been modified, or its patch level becoming too old.

Keywords:
Cloud Computing, virtualization, virtualization security, cloud admission, admission control

Acknowledgements

First of all I thank Allah for all his generosity and help.

Special thanks for Dr. Ayman Mohamed Bahaa El-Din and Dr. Ayman Elsayed Taha, for their valuable advises, and their enormous efforts in directing my work and revising the thesis.

I would like to thank all professors, and teachers, staff of Computer and Systems Engineering Department for all their help care and support that they give to me all the time of study and research.

I would like also to thank all my family and friends for their deep support, patience and encouragement they give to me during the thesis development.

Statement

This dissertation is submitted to Ain Shams University for the degree of Master of Science in Electrical Engineering, Computer and Systems

The work included in this thesis was out by the author at Computer and Systems Engineering Department, Ain Shams University.

No part of this thesis has been submitted for a degree or qualification at other university or institution.

Date : 21/03/2017

Signature :

Name : Omnia Abdelrahem Mohamed

Table of Contents

مستخلص

شـــكر

List of Tables

List of Figures and Illustrations

1: Introduction

1.1 Problem Definition

Cloud computing is a fast spreading model for service delivery, widely adapted in today's IT environment. It is a combination of other technologies working together, one of them is virtualization, which is the abstraction of computer resources, separating the physical resources from the final resources delivered to the user. Regardless of its wide spread, cloud computing still has security concerns, also there are the threats related to virtualization that are inherited by the cloud.

In the late 90s and the beginning of 2000 the dependence on computer systems increased more and more and it became a part of every industry, even an important part of our daily lives. But for starting and small businesses this dependence started to create a problem because this increased their costs as they are required to purchase computer systems and to hire skilled persona to handle them.

This is where the idea of time sharing started to seem like the solution. The idea of sharing resources in the IT industry is not new, it is as old as the start of the computer industry itself. The idea became known and started to spread with the UNIX operating system introduced in the 1960s. It allows different users to work together simultaneously on the same hardware, which helped in spreading of the computer technology by lowering the cost. Here again with the same idea companies can change from owning its hardware and software -which they must buy to use while they don't actually need all the features and capabilities of it or they may need to scale it in tight time frame- to service based per use model which is introduced by cloud computing where the company doesn't need

to buy all it needs but it can take it as a service from a cloud provide and pay per use. [1]

It wouldn't have spread this fast without the advancement shown in other technologies, like the advancement in network capacity and speed. Also the spread use of virtualization technology and service oriented architecture on which cloud computing is based on. In the early days as with the starting of any new technology companies where sceptical and struggled to understand what is cloud computing and how they could benefit from it, and how this doesn't affect their data confidentiality and consistency, but as they see more benefits and the technology becoming more mature and advanced, more and more companies today move to the cloud wither it is a private cloud, public or hybrid one. Even with owning their own cloud that may not lower the initial cost very much, but it makes the infrastructure easier to manage, new test and development environments take minutes instead of months to create that help in the quick advance of the business to meet up with the market needs. Different services serving different needs and businesses are developed and introduced with the advancements in cloud computing.

Virtualization is one of the reasons that made cloud computing possible. In virtualization the hardware resources are abstracted and pooled together forming logical resources first, and then these resources are delivered to the users each as per their needs from the pool. These resources include from example CPU, memory, network, storage or application. The motivation behind virtualization and its development is the advancement in computer hardware industry creating machines with capacity larger than most application workload can consume with lower cost, this is where virtualization is introduced to increase utilization. Although virtualization have developed form simply virtualizing physical resources like CPU and memory to virtualizing application, its remains

with the same concept of running multiple independent systems on the same environment at the same time. [2]

One of the problems that face virtualization is VM image management. As using images has the advantage of the customer working on the environment and with the configuration most suitable for him, it bears a risk from the cloud provider perspective that this image may contain malicious, illegal or unlicensed software. Or from an administrative perspective there is the concern of dormant VM images' security because security patches will not be applied on them. [3] [4]

Applying patch is a problem not only for images, but generally in large environment containing many virtual machines serving different customers, it becomes difficult to manage and keep track of the patch level and latest patches applied on each VM which is very important especially for security updates. The problem becomes more sever with ability to create snapshots and be able to rollback to it at any time, which will not be up to the latest patch level and needs applying of this patches again, other than snapshots some VMs may be dormant at the distribution of patches time, that makes it important to check every VM at start up to check for the needed patches if any. [3] [5]

1.2 Solution Methodology

A framework is suggested to control the admission of new virtual machines into the cloud environment in an attempt to limit the number of malicious behaving machines that may contain a malware, risking its spread through the environment. Also if a machine user trying to attack another machine in the same environment or the host machine the framework tries to detect that. Also machines staying dormant for long

periods of time are considered a new admission, for the risk of its disk may have been modified, or its patch level becoming too old.

1.3 Thesis Organization

In chapter two of this thesis we talk about virtualization technology focusing on virtual machines, its techniques showing how different instructions are handled by the CPU depending on the virtualization technique.

Then it surveys and illustrates virtualization threats, vulnerabilities and some of the countermeasures for each one of them where some are already adapted while others still under test and development. It includes VM escape, were VM can completely bypass the hypervisor. Proper configuration of the host and guest interaction rules can solve it, or using a safe hypervisor like HyperSafe, or a closed box execution environments like TCCP.

Denial of service is another threat that is similar to network DOS making computer resources unavailable can be prevented by enforcing policies to allocate limited resources to each VM.

Network attack on VM at migration shows that VMs with their data may be attacked while migrating from one physical machine to another. It needs Network security mechanism and policies should be taken into account, like communication channel security, encryption. Network attack on host machine emphasise on strictly protecting the host as it can control the VMs. Also sufficient isolation should be provided in order to not allow the host to be the gateways for attacks on the VMs.