Security Threats & Attacks on Virtualization for Cloud Computing

by
Kushan Sharma (108287X)

A thesis submitted to University of Moratuwa in partial fulfilment of the requirements for the
Master of Computer Science, *Specialized in Computer & Network Security*

Department of Computer Science & Engineering
University of Moratuwa, Sri Lanka

December 2012

Security Threats & Attacks on Virtualization for Cloud Computing

by
Kushan Sharma (108287X)

A thesis submitted to University of Moratuwa in partial fulfilment of the requirements for the
Master of Computer Science, *Specialized in Computer & Network Security*

Department of Computer Science & Engineering
University of Moratuwa, Sri Lanka

December 2012

Declaration

I declare that this is my own work and this thesis/dissertation does not incorporate without acknowledgment any material previously submitted for a Degree or Diploma in any University or other institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgment is made in the text.

_____ _____

Kushan Sharma: Date

Approved by:

_____ _____

LtCol Dr Chandana D. Gamage Date
Department of Computer Science and Engineering
University of Moratuwa

Copyright Statement

Abstract

Enterprises continuously seek innovative approaches to reduce operational computing costs while getting the most from their resources. Cloud Computing infrastructures are the latest technological advancement with the potential to maximize resource utilization while reducing costs.

The new paradigm of Cloud Computing possesses severe security risks to its adopters due to the distributed nature of Cloud Computing environments which make them a rich target for malicious individuals. Cloud infrastructure commonly relies on virtualization. The virtualization techniques used in Cloud possess numerous security threats and attacks. In order to cope with these risks, appropriate taxonomies and classification criteria for attacks on Cloud Computing are required. On the other hand Cloud Consumers runs numerous applications/scripts in order to complete their computing tasks. Most of them are too complex and complicated to trust. Even with access to the source code, it is difficult to reason about the security of these applications. They might harbor malicious code such as computer viruses, worms, bots, Trojan horses and spyware or contain bugs that are exploitable by carefully crafted input. It is essential that instead of just relying on conventional defense techniques, the next generation of system software must be designed from the ground-up to provide stronger isolation of services running on computer systems.

To address the above described security threats to Cloud Instances, we propose an architecture for confined execution environment to test untrusted applications/scripts inside Cloud Instances. Modern day security researchers consider malware sandbox analysis is as one of the promising approaches for exploring malware. But most of the previous proposed solutions have various security vulnerabilities due to the way of they have been implemented and the technologies that have been used in the implementation. The proposed architecture and proof-of-concept implementation address all the discovered drawbacks of previously presented sandbox solutions. We monitor all the system calls that are executed by the adversary to confine the adversary and limit the damage an attacker can cause to the Cloud Instance.

The research work related to the proposed sandbox architecture has been tested through LangshaJail, which is the proof-of-concept, built for the Cloud

Instances, using latest open source technologies that includes Linux as the Operating System Environment, Linux Resource Containers (LXC) as the virtualization environment and Seccomp as the system call filtering technology. The LangshaJail system was tested for compliance to Cloud Computing security objectives and adherence to performance criteria in order to validate the design approaches and implementation mechanisms used in the research.

Further as a part of the this thesis we present a taxonomy based on the notion of attack surfaces of virtualization for Infrastructure-as-a-Service-based Cloud offerings, thus making them more concrete and improving their analysis. The presented taxonomy specially addresses attacks based on residues of Cloud Instances. These residue based attacks are new venues for attackers that have previously not been addressed.

Acknowledgements

First of all I would like to thank my supervisor Dr. Chandana Gamage whose encouragement, guidance, support, and criticism from start to the very end, allowed me to understand the objectives and challenges of a master degree thesis. I would also like to thank Dr. Shehan Perera (Project Cordinator) for extensive advice, helpful feedback, and constant support.

Furthermore, my special thanks go to Prof. Gihan Dias, Dr. Shantha Fernando and Mr. Dileepa Lathsara from TechCERT who provided an excellent, supporting, innovative, and inspiring environment in which it was a pleasure to create this thesis. Last but not its a pleasure to thank all my TechCERT colleagues those who helped to make my thesis in a motion. I would also like to express my sincere gratitude to Mr Ben Grass from Vrije Universiteit Amsterdam for the technical expertise provided.

Finally, words alone cannot express the thanks I owe Mr. Dayananda Liyanage my father, Mrs. Kusuma Gamage my mother, Mr. Roshan Maduranga my brother, Mr. Hashan Dananjaya my brother and Ms. Umangee Chandrakumara my loving girl friend for all the encouragement extended.

Abbreviations

ABI - Application Binary Interface
ACL - Access Control List
API - Application Programming Interface
CC - Cloud Computing
CI - Cloud Instance
CISC - Complex Instruction Set Computing
COW - Copy-on-Write
CPU - Central Processing Unit
DLL - Dynamic Link Library
DNS - Domain Name System
FTP - File Transfer Protocol
GDT - Global Descriptor Table
HTTP - Hypertext Transfer Protocol
ICSPS - International Conference on Signal Processing Systems
IDT - Interrupt Descriptor Table
IDTR - Interrupt Descriptor Table Register
IPC - Inter Process Communication
IRC - Internet Relay Chat
ISA - Instruction Set Architecture
LDT - Local Descriptor Table
LXC - Linux Resource Containers
MMU - Memory Management Unit
MAC - Mandatory Access Control
MMU - Memory Management Unit
NIC - Network Interface Card
OS - Operating System
P2P - Peer-to-Peer
RISC - Reduced Instruction Set Computing
RM - Resource Monitor
SCSI - Small Computer System Interface
SIDT - Store Interrupt Descriptor Table
SDT - Software Dynamic Translation
SFI - Software-based Fault Isolation
SMTP - Simple Mail Transfer Protocol
SNMP - Simple Network Management Protocol

TCG - Trusted Computing Group
TCP - Trusted Computing Platform
TOCTOU - Time of Check to Time of Use
TPM - Trusted Platform Module
VM - Virtual Machine
VME - Virual Machine Environment
VMM - Virtual Machine Monitor

Table of Contents

List of Tables

List of Figures