CSE449: PARALLEL, DISTRIBUTED, AND HIGH-PERFORMANCE COMPUTING (HPC)

Submitted by:

Asibur Rahman Bhuiyan

ID: 23341095

Section: 01

Team: 26

Submitted to:

Annajiat Alim Rasel

Senior Lecturer,

Brac University

Submission No: 02

Task: Paper Review Presentation 2

Paper title: Identifying and Analyzing Security Threats to Virtualized Cloud Computing Infrastructures

Author: *Sarfraz Nawaz Brohi, Mervat Adib Bamiah, Muhammad Nawaz Brohi, Rukshanda Kamran*

TABLE OF CONTENTS

01 Introduction

02 Virtualizing Cloud Computing

03 Hypervisors

04 Attacks on VCCI

05 Vulnerabilities of VMM

06 Security tools and techniques

07 Implementation of security tools and techniques

08 Future Scopes

09 Conclusion

INTRODUCTION

- Aims for environmental benefits.
- Involves logically partitioning hardware or software resources for multiple users.
- Complexity and security concerns arise due to virtualization.
- Weak security standards in hypervisors create exploitable gaps.
- Confidentiality, integrity, and system security.
- Hinders widespread cloud computing adoption.

VIRTUALIZING CLOUD COMPUTING

- Cloud virtualization boosts efficiency.
- Hypervisor manages multiple user VMs.
- VCCI resembles an efficient OS.
- Type-I hypervisor enhances security and performance.
- Type-II hypervisor lacks some security features.

HYPERVISORS

Xen Hypervisor:

- Manages VMs with DomO (higher privileges) and DomU (lower privileges).
- DomO admin controls hypervisor interface for VM management.
- DomU VMs run modified Linux kernel with front-end drivers.

KVM Hypervisor:

- Developed as a Linux kernel module.
- Introduces guest mode with user and kernel modes.
- Guest processes execute in guest-user mode, handling exits to guest-kernel mode for I/O.
- Each VM is a Linux process running multiple applications concurrently, scheduled by the Linux scheduler.

ATTACKS ON VCCI

- Hypervisor security gaps
- Infrastructure attack vulnerabilities
- Interconnected VCCI components
- Isolate with security tools
- Major attacks, three vulnerabilities

VULNERABILITIES OF VMM

VM Hopping:

- Malicious attacker on one VM can exploit shared host environment.
- Access other VMs by knowing IP addresses.
- Risks of traffic manipulation, leading to Denial of Service.
- Modification of VM configuration files can disrupt communication.

VM Escape:

- Guest-level VM can attack the host.
- Untrusted user gains access to host OS and other VMs.
- Exploitation can lead to monitoring and control of resources.
- Potential to bring down resources, turn off hypervisor, affecting all VMs.

VM Mobility:

- VMs can move between physical hosts (VCCI).
- Risks of stolen VM files without physical theft.
- Moving over the network or copying through USB increases security threats.
- Compromises include modification of configuration files, offline attacks, and theft of credentials.
- Difficulty in tracing attackers due to copied VMs.
- Often caused by malicious cloud administrators.

SECURITY TOOLS AND TECHNIQUES

Encryption and Key Management:

- Data encryption at rest, in transit, and on backup media.
- Proper key management practices for secure access to encryption keys.

Intrusion Detection Tools (IDTs):

- Network-based IDTs (NIDTs) monitor network traffic.
- Host-based IDTs (HIOTs) monitor local activity on hosts.
- Both types employed in VCCI to detect and block intruders.

Virtual Firewall (VF):

- Firewall service in a virtualized environment.
- Packet filtering and monitoring services.
- Implemented in hypervisor-mode for VM and VMM protection.

Trusted Virtual Domains (TVDs):

- Group related VMs into a single network domain.
- Unified security policy for strong isolation among VMs.
- Prevents malicious VMs from affecting trusted users.

Access Control Mechanisms (ACMs):

- Limit, deny, or restrict access based on security policies.
- Includes Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Role-Based Access Control.

Virtual Trusted Platform Module:

- Virtualizes a physical TPM.
- Certificate chain linking for extending the chain of trust.
- Ensures secure access to TPM capabilities.

IMPLEMENTATION OF SECURITY TOOLS AND TECHNIQUES

- Secure tools for VCCI
- TVDc reduces security risks
- CloudVisor: Trusted VMM with encryption
- Monitor and enforce protection
- TVMM with TPM for isolation
- Page encryption using AES-128
- Ongoing research for VCCI security

FUTURE SCOPES

- Continuous effort required to establish and maintain security in cloud environments.
- Focus on identifying and addressing security issues in cloud computing from governance and operational perspectives.

CONCLUSION

- Multi-Tenancy in Cloud Computing.
- Share resources, multiple clients, virtualization.
- Vulnerable to insider and outsider attacks.
- VMM major target, ongoing challenge.
- Current Approaches to Secure VMM.
- Diverse techniques secure virtualized environments
- Security across layers, policy compliance.