A Secure Access Control Architecture for Multi-Tenancy Cloud Environments

Ronald Beaubrun
Department of Computer Science and Software Engineering
Laval University
Quebec, Canada
e-mail: ronald.beaubrun@ift.ulaval.ca

Alejandro Quintero
Department of Computer and Software Engineering
Polytechnique Montreal
Montreal, Canada
e-mail: alejandro.quintero@polymtl.ca
Outline

INTRODUCTION
CONTEXT AND BACKGROUND
EXISTING METHODS AND MODELS
THE PROPOSED ARCHITECTURE
A USE CASE SCENARIO
CONCLUSION
INTRODUCTION

**Multi-tenancy**

- Customers share computing resources, including CPU time, network bandwidth, data storage space, with other users.

**Access control**

- Security feature that controls how users and systems communicate and interact with other systems and resources.

- 3 types: physical access control, technical access control, and administrative access control.
• Model for a multi-tenant cloud service provider
• 3 main components
  • Cloud manager
  • Hypervisor or Virtual Machine Manager
  • Virtual Machines
• Types of possible attacks
  • Virtual Machine (VM) Hopping
  • Denial of Service (DoS)
EXISTING METHODS AND MODELS

• Distributed Access Control (DAC)
  • 3 main components: Cloud Service Provider (CSP), Cloud Service Consumer (CSC) and Identity Provider (IdP)

• Adaptive access algorithm
  • Combination of trust management and Role-Based Access Control (RBAC)
  • Based on loyalty

• Multi-Tenancy Access Control Model (MTACM)
  • Based on limiting the management privilege of Cloud Service Provider and letting the customers manage the security of their own business.
EXISTING METHODS AND MODELS (cont’d)

• Role-Based Multi-Tenancy Access Control (RB-MTAC)
  • Combination of identity management and role-based access control.

• CloudPolice
  • Hypervisor-based access control mechanism
  • Effective to prevent denial of service (DoS) attacks
THE PROPOSED ARCHITECTURE

Main assumptions
- The virtual machines and physical servers are co-located at the same cloud provider.
- Each physical server has only one hypervisor.
- Each physical server is hosting at least one tenant, and each tenant has at least one virtual machine.
- All access control lists are defined and stored in the hypervisor.
- In its startup process, a hypervisor sends an update message to the other hypervisors that are located at the same Cloud.
• Principles
  • Source VM
  • Destination VM
  • Control packet
  • Incoming/outgoing traffic filter
  • Access control list
THE PROPOSED ARCHITECTURE (cont’d)

Flowchart
THE PROPOSED ARCHITECTURE (cont’d)

Destination hypervisor’s tasks upon control packet reception
A USE CASE SCENARIO

• 3 physical servers
  • Server 1: Tenant 1 (VM1, VM2) and Tenant 2 (VM3)
  • Server 2: Tenant 1 (VM4, VM5) and Tenant 3 (VM6, VM7)
  • Server 3: Tenant 4 (VM8) and Tenant 3 (VM9, VM10)
A USE CASE
SCENARIO
(cont’d)

Illustration of phase one
A USE CASE SCENARIO (cont’d)

Illustration of phase 2
CONCLUSION

• Advantages of the proposed architecture
  • Scalability
  • Security

• Future works
  • Implementing a prototype of the proposed architecture
Questions?