Research on Data Security and Protection Technology under Cloud Environment

Qi Xu[1,a], Yuangen Xu[1,b], Yong Li[1,c]

[1] China Tobacco Zhejiang Industrial Co., LTD, Hangzhou, 310009, China

[a] xuq@zjtobacco.com; [b] xuyg@zjtobacco.com; [c] liy@zjtobacco.com

Keywords: Cloud Computing, Data Security, Protection Technique

Abstract. With the rapid and bursting development of computational science and data engineering related techniques, the transmission and protection of data is crucial in the computer science community. Cloud computing is becoming increasingly important for provision of services and storage of data in the Internet. However there are several significant challenges in securing cloud infrastructures from different types of attacks. The focus of this article is to cloud providers can provide security services infrastructure, its customers (tenant) to offset these attacks. Our main contribution is the security architecture which provides a flexible security as a service model, cloud providers can provide the tenant, tenant's customers. Our security as a service model while offering a baseline security to the provider to protect its own cloud infrastructure also provides flexibility to tenants to have additional security functionalities that suit their security requirements. In this paper, we generally describe the design and implementation of the security architecture. The experimental analysis illustrates the effectiveness of our proposed technique.

Introduction

As the operating systems and applications of the tenants can be potentially large and complex, they may contain security vulnerabilities. Furthermore, there can be several tenants on the same physical platform sharing re-sources in a cloud infrastructure. The vulnerabilities in operating systems and applications can be potentially exploited by an attacker to generate different types of at-tacks. These attacks can target cloud infrastructure as well as with other virtual ma-chine belongs to other tenants. So need to design the security architecture and development of technology, you can use the cloud service provider of virtual machine security infrastructure and the tenant [1-2].

Our main contribution in this paper is a security architecture that provides a flexible security as a service model that a cloud provider can offer to its tenants and customers of its tenants. Our security as a service model while offering a baseline security to the provider to protect its own cloud infrastructure also provides flexibility to tenants to determine how much control they wish to have over their own virtual machines [3]. Baseline provider required security is to ensure that the malicious tenants don't attack the cloud infrastructure even hosting malware. Each tenant security functions, form part of the safety baseline, the default mode of operation to provide basic security. But there will be other tenants who will require additional security services (baseline) cloud provider, to meet their needs, and protect them from other malicious tenants [4-5]. So our security as a service model provides the choice of additional security features, meet the demand of the safety of the residents. Our approach offers a choice to the tenant to managing this tension between the privacy concerns and the security con-trols offered by the cloud provider. An important feature of our model is that it makes this trade-off between security and privacy explicit. Furthermore, the choice by a tenant to opt in for additional security services can provide the cloud provider to develop a framework for charging the tenants for these additional security services.

Threat Model

Our system model involves cloud service provider which includes cloud system administrators, tenant administrators (or operators) who manage the tenant virtual machines, and tenant users (or

tenant's customers) who use the applications and services running in the tenant virtual machines. Cloud providers are entities such as Amazon EC2 and Microsoft Azure who have a vested interest in protecting their reputations. The cloud system administrators are individuals from these corporations entrusted with system tasks and maintaining cloud infrastructures, who will have access to privileged domains. Consider a typical configuration of our system architecture shown in Figure 1. In determining the threat model, we need to see different types of attacks, may be in such a configuration. Circle in the figure shows the source of the attack and the arrow shows the target. We identify three areas related to architecture model of the threat. A tenant user domain includes the tenant administrators and the tenant. Each tenant has its own tenant domain. This is the cloud of cloud system domain by the system administrator and VMM platform. Then there is the cloud cluster domain comprising cloud system domains that constitute the cloud infrastructure. There can be attacks from tenant administrators on the tenant virtual machines [6]. That is, the tenant administrators can exploit the vulnerabilities in the tenant virtual machine for malicious purposes. Such attacks can target both the cloud infrastructure as well as co-located tenants.

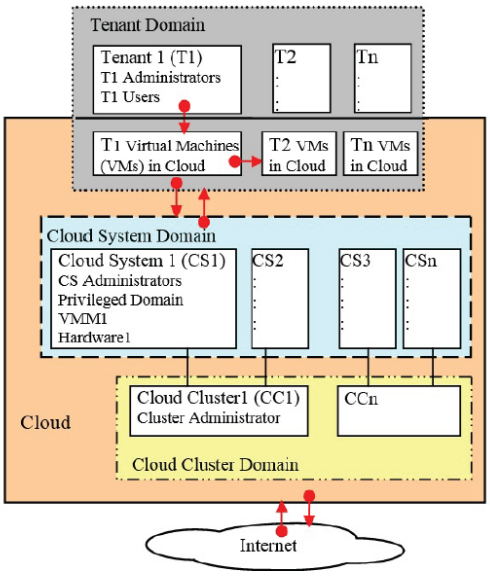

Figure 1. The Threat Model

Then there can be attacks from tenant users (customers).Consider, for instance, a tenant which is a software development company making use of cloud resources. Although the tenant administrators have provided host based security tools in their tenant virtual machines, a malicious tenant user (tenant employee) may be able to circumvent such security tools. Consider Figure 2 where the virtual machines which belong to a single tenant are hosted on multiple physical servers. In general, a malicious user or tenant more important is a malicious tenant administrator can generate attack virtual machine belongs to another tenant. The cloud service provider needs to provide secure isolation between the tenant virtual machines. However the cloud service provider may not be aware of the operating systems and applications running in a tenant virtual machine. Hence it is not an easy task for the cloud service provider to enforce security policies on the tenant virtual machines. Furthermore since the elastic nature of cloud allows the ability to dynamically increase the resources allocated to tenant virtual machines, the attacker can use this capability in compromised tenant virtual machines to generate sophisticated attacks. Finally our security architecture provides the ability to charge a tenant depending on the security services that are required by the tenant. For example, a tenant virtual machine that is running financial services may need more security measures than a tenant that is running basic web hosting.

The Proposed Security Model

Cloud Architecture Overview. Let us consider a generic cloud service provider architecture as shown in Figure 2. Tenants (T1, T2, T3) are hosting one or more virtual machines on the cloud service provider infrastructure and remotely managing their virtual machines. The Cloud Controller

(CLC) is the main interface for the cloud tenants and it is the top level management for the IaaS cloud. It can query other controllers such as the Cluster Controllers (CC) and Node Controllers (NC), Storage Controller (SC) to make high level decision on the implementation of the tenant virtual machines and storage of the data. CLC has policies required in the IaaS infrastructure. It also handles the authentication service for the users. Storage Controller provides storage for the VM images, and user data. Node Controller is implemented on each physical server. Node Controller is responsible for managing the tenant virtual machines hosted on each VMM.A group of Node Controllers report to the Cluster Controller. The security architecture proposed in this paper focus mainly on the infrastructure-as-a-service (IaaS) platform. There are also other delivery models for cloud such as software as a service (SaaS) and platform as a service (PaaS). In the case of SaaS or PaaS, the tenants have very limited access tithe cloud resources compared to the IaaS. Hence the attacks that can be generated in SaaS or PaaS are limited to the specific application software or platforms to which they have access. For example, if an attacker can exploit the vulnerability in Gmail, the attacks are limited to the Gmail application. The SaaS and PaaS providers can use security features available in the operating system and traditional security tools to protect from such malicious tenants. Hence the proposed techniques can be used as an additional layer of defense in SaaS and PaaS deployments.

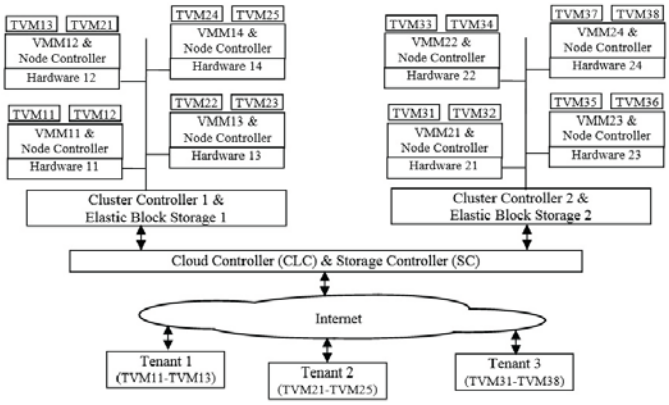

Figure 2. The Cloud Scenario

Basic Assumptions. Let us now consider the assumptions made in our architecture. We assume that tenant virtual machines accept a security baseline (mentioned earlier) functionalities specified by the cloud service provider. If there are any special requirements for the tenant which do not comply with the baseline security requirements of the cloud service provider, then these need to be resolved at the time of the registration. The security baseline is enforced by our architecture in the node controller. With respect to the applications running in the tenants, we assume that the tenants are aware of the applications that are running in their own machines. We also assume that the tenant may have their own host-based security tools (HBST) running on their virtual machines. In addition, the default security baseline provides the best choice for those who are worried about the tenant's privacy applications and services running on a virtual machine. That is to say, in this case, the tenant does not reveal any additional information in their application and cloud service providers.

Security Architecture Overview. Consider the basic security architecture diagram shown in Figure 3. As mentioned above, the tenants may wish to have their own host based security tools (HBST) to run on the virtual machines that they are obtaining from the cloud provider. Since host based security tools have good visibility into the system being monitored, this acts as a primary layer of defense in our security architecture.

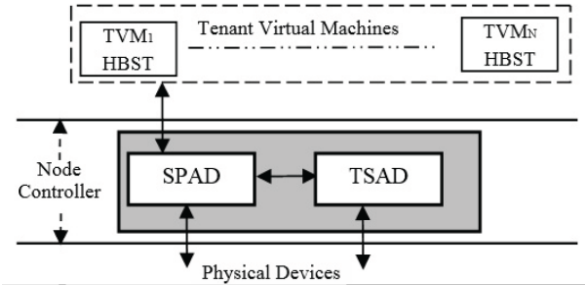

Figure 3. The Basic Security Architecture

Component Description. Service Provider Attack Detection (SPAD): SPAD is designed to enforce security policies in the baseline that is offered by the cloud provider. Note SPAD policies are enforced on all the tenant virtual machines. Pro_Val first checks if the host based security tool related processes (see Figure 4) are running in the tenant virtual machine. If the tenant virtual machine is compromised, then the processes related to the security tool in the tenant virtual machine will not be detected in the Pro_Val report. In such cases, the tenant virtual machine is considered to be compromised with malware. Hence attacks such as conficker and torpig which disable security tools in the tenant virtual machine are detected by Pro_Val. The figure 4 illustrates this.

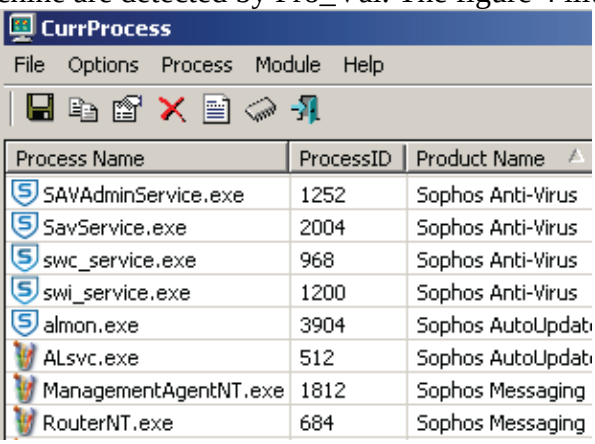

Figure 4. The Security Processes of Sophos Security Tool

Using the Template Experimental Analysis

In this section, we discuss the implementation and analysis of our security architecture. We have used the open source based system Xen hypervisor to implement our architecture. However it is to be noted that our security architecture can be implemented using other VMM based systems such as VMWare or HyperV. Fig. 5 shows the basic implementation of our security architecture at a single VMM platform level using Xen hypervisor.

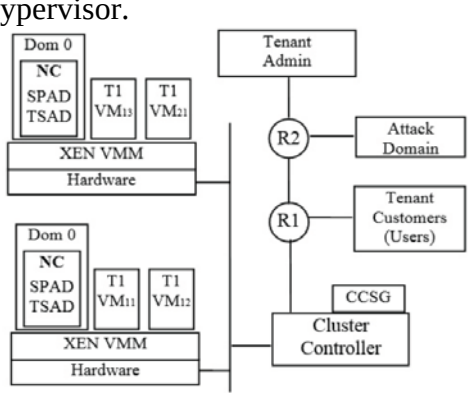

Figure 5. The Implementation Setup

Figure 6 shows different cases of process validation by Pro_Val. First run shows the result for a legitimate scenario, where no hidden processes are detected in the tenant virtual machine with Linux OS. Second run shows the result where

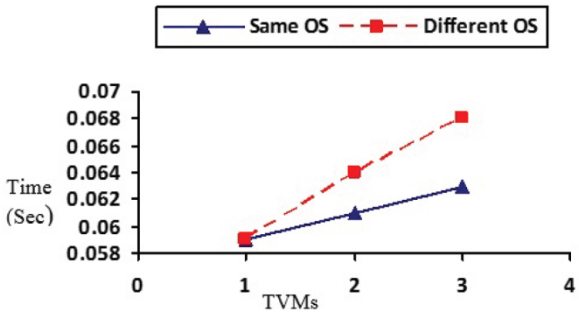

Figure 6. The Process Validation Time

Conclusions and Summary

In this paper we have proposed a security architecture that provides a security as a service model that a cloud provider can offer to its multiple tenants and customers of its tenants. Our security acts as a service model, at the same time provide a baseline security providers to protect their own cloud infrastructure also provides flexibility, the tenant has additional security functions, meet the safety requirements. This article describes the design of the security architecture and discusses the different types of attacks are offset by the proposed architecture. We have described the implementation of the security architecture and gave a detailed analysis of the security mechanisms and performance evaluation results. In the future, we plan to use more related methodologies to achieve the related approaches.

References

[1] Chen D, Zhao H. Data security and privacy protection issues in cloud computing[C]//Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on. IEEE, 2012, 1: 647-651.

[2] Wang C, Ren K, Lou W, et al. Toward publicly auditable secure cloud data storage services[J]. Network, IEEE, 2010, 24(4): 19-24.

[3] Chow R, Golle P, Jakobsson M, et al. Controlling data in the cloud: outsourcing computation without outsourcing control[C]//Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009: 85-90.

[4] Song D, Shi E, Fischer I, et al. Cloud data protection for the masses[J]. Computer, 2012 (1): 39-45.

[5] Takabi H, Joshi J B D, Ahn G J. Security and privacy challenges in cloud computing environments[J]. IEEE Security & Privacy, 2010 (6): 24-31.

[6] Jansen W. Cloud hooks: Security and privacy issues in cloud computing[C]//System Sciences (HICSS), 2011 44th Hawaii International Conference on. IEEE, 2011: 1-10.