Journal of Network and Computer Applications ■ (■■■■) ■■■–■■■

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Counteracting security attacks in virtual machines in the cloud using property based attestation

Vijay Varadharajan *, Udaya Tupakula

Advanced Cyber Security Research Centre, Faculty of Science, Macquarie University, Sydney, Australia

ARTICLE INFO

Article history:
Received 7 January 2013
Received in revised form
11 July 2013
Accepted 5 August 2013

Keywords:
Trusted computing
TPM attestation
Cloud
Virtual machine monitors
Rootkits
Zero day attacks
Malware

ABSTRACT

Cloud computing technologies are receiving a great deal of attention. Furthermore most of the hardware devices such as the PCs and mobile phones are increasingly having a trusted component called Trusted Platform Module embedded in them, which helps to measure the state of the platform and hence reason about its trust. Recently attestation techniques such as binary attestation and property based attestation techniques have been proposed based on the TPM. In this paper, we propose a novel trust enhanced security model for cloud services that helps to detect and prevent security attacks in cloud infrastructures using trusted attestation techniques. We consider a cloud architecture where different services are hosted on virtualized systems on the cloud by multiple cloud customers (multi-tenants). We consider attacker model and various attack scenarios for such hosted services in the cloud. Our trust enhanced security model enables the cloud service provider to certify certain security properties of the tenant virtual machines and services running on them. These properties are then used to detect and minimise attacks between the cloud tenants running virtual machines on the infrastructure and its customers as well as increase the assurance of the tenant virtual machine transactions. If there is a variation in the behaviour of the tenant virtual machine from the certified properties, the model allows us to dynamically isolate the tenant virtual machine or even terminate the malicious services on a fine granular basis. The paper describes the design and implementation of the proposed model and discusses how it deals with the different attack scenarios. We also show that our model is beneficial for the cloud service providers, cloud customers running tenant virtual machines as well as the customers using the services provided by these tenant virtual machines.

1. Introduction

Distributed systems have fundamentally changed the way individuals and enterprises share, process and store information today. Security issues play a vital role in distributed systems, as greater availability and access to information in turn imply that there is a greater need to protect them. To address these issues, several security techniques, mechanisms and systems have been proposed over the years (Ferraiolo and Kuhn, 1992; Jajodia et al., 1997; DeTreville, 2002; Li and Mitchell, 2003; Herzberg et al., 2000; Blaze et al., 1996, 1999). Many of these systems have addressed the authentication and authorisation requirements that relate to human users. They make some basic assumptions about the state of the platform that is hosting and running the systems software and applications. There is an inherent trust that is placed on the underlying platform when a higher level application or user is authenticated or authorised.

In the current networked world with heterogeneous platforms and numerous software applications and system software running on these platforms, it is important that such underlying trust assumption about the system state be properly examined. There are several reasons for this. First, computing platforms have become very powerful and can run many applications simultaneously. In particular, as the number of software applications increases, greater is the potential for security vulnerabilities to arise. These vulnerabilities in turn make the platform more vulnerable to attacks. Second, attacks themselves are becoming more and more sophisticated. Furthermore, attackers also have easier access to ready-made tools that enable exploitation of platform vulnerabilities more effective. Third, platforms are being shared by multiple users and applications (belonging to different users) both simultaneously as well as at different times. Therefore there is a great chance of the platform being left in a vulnerable state as different users and applications run. Finally, because platforms have become much more complex today, users themselves are unaware of their platform vulnerabilities. Let us assume, for example, a user is authorised to download and execute a confidential file on his/her platform. A typical authentication and

* Corresponding author. Tel.: +61 2 98509534.
E-mail addresses: vijay.varadharajan@mq.edu.au (V. Varadharajan).

1084-8045/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jnca.2013.08.002

authorisation system only verifies if the user is authenticated and has the necessary rights to perform the action. As soon as the file is downloaded and executed, if there is malicious software in the platform (which the user is not aware of), it can make copies of the file and distribute it to others without the user's knowledge. Such vulnerability renders the entire authorisation process useless. The challenge is then, given the dynamic nature of attacks, the complexity of software and hence the increased vulnerable nature of these platforms (hosting possibly malicious software), how can one reason about the identity, integrity and security of a platform in a distributed system environment. Such issues get even further aggravated in cloud infrastructures (Subashini and Kavitha, 2011; Takabi et al., 2010), as in the cloud, the platforms are shared between different customers of the cloud service provider; furthermore the cloud service provider itself may not even be aware of the services that are being hosted by their customers.

A detailed discussion on the security and privacy challenges in cloud computing is outlined in Takabi et al. (2010). For example, Takabi et al. (2010) emphasise that security in Infrastructure-as-a-Service (IaaS) cloud is a shared responsibility of the tenant and the cloud service provider. Also it identifies trusting the tenant virtual machines and securing tenant communications as critical requirements for an IaaS cloud. In this paper, we propose techniques to address these requirements of establishing trust on the tenant virtual machines as well as securing tenant communications.

This paper aims to take advantage of the features of trusted computing technology to enhance the design and enforcement of security policies and mechanisms in a cloud environment. The main rationale behind trusted computing technology is to enhance the reasoning about the identity and state of a platform to determine whether it is in a suitable state. Two features are being used to achieve this. A trusted platform has special processes that dynamically collect evidence of behaviour of different applications installed on a platform. This is then used to reason about the platform's overall state by comparing it to known or acceptable reference states to decide whether or not a platform can be trusted. Our approach is to use this reasoning to enhance the quality of the security decisions by taking into account the state of the platform. For instance, authorisation decisions in trusted platforms can be made not only by taking into account the identities and privileges of users and applications but also the state of the platform in terms of what types of applications and software components are running on that platform. Then one can design policies such as restricting the types of communication or types of activity involved in the interaction based on the platform state. This approach is referred to as “trust enhanced security”, as we make use of the notion of trust derived from the state of the platform before performing the transactions; furthermore, we enhance the trust of cloud service provider platform (using Trusted Platform Module (TPM)) (TCG, 2007) to certify and enforce some of the security policies on the tenant virtual machines.

A fundamental concept when it comes to determine the state of a platform is that of attestation. Section 2 considers generic cloud architecture, the attacker model and the aims of our model. In Section 3 we propose our security model which makes use of property based attestation and cloud service provider as Certification Authority to deal with the attacks. Our attestation technique overcomes the limitations of previously proposed attestation techniques. We also present a detailed discussion on how our model is able to efficiently deal with the attacks between the tenants and their customers. Section 4 presents a detailed analysis on how the security model deals with the attacks during and after transactions. Section 5 presents a brief overview of Xen virtualization platform and describes the model implementation using Xen. We also demonstrate how the model deals with the different attack scenarios. Section 6 presents a general discussion and provides a comparison of our model with other relevant related works. Finally, Section 7 concludes.

2. Security challenges and aims

In this section, we will first consider a generic architecture for cloud. Then we consider an attacker model that is specific to the cloud and present the requirements for our model.

2.1. Architecture overview

Since cloud customers can use their machines to provide different services to their customers, we use the term tenant to refer to the cloud customers. Customers in this paper refer to the customers of the tenants. So in our model, we have cloud service providers, cloud customers (tenants of cloud providers running virtual machines (VM) on cloud provider platform) and customers (customers of tenants). For example, the Tenant Virtual Machine (TVM) can be used for selling music files online, the customers are the ones who purchase the music files from the tenant.

Let us consider generic cloud service provider architecture as shown in Fig. 1. The Cloud Controller (CLC) is the main interface for the cloud customers 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) and make high level decision on the implementation of the tenant virtual machines and storage of the data. CLC has the security policies for the IaaS infrastructure and also handles the authentication of the tenants. Storage Controller provides storage for the virtual machine images and user data. Node Controller is implemented on each physical server and is responsible for managing the tenant virtual machines and a group of Node Controllers report to the Cluster Controller. The Elastic Block Storage (EBS) runs on the same machine as the cluster controller.

Let us first consider some of the assumptions before examining the operation of our model. We consider that each physical server which is used for hosting the tenant virtual machines is equipped with a TPM (TCG, 2007) chip. Most of the server, desktop, laptops that are being shipped today have the TPM chip embedded in them. Hence this is a reasonable assumption with the current state of the art systems. Basically TPM allows us to measure the state of the system. It uses the attestation mechanism to disclose the

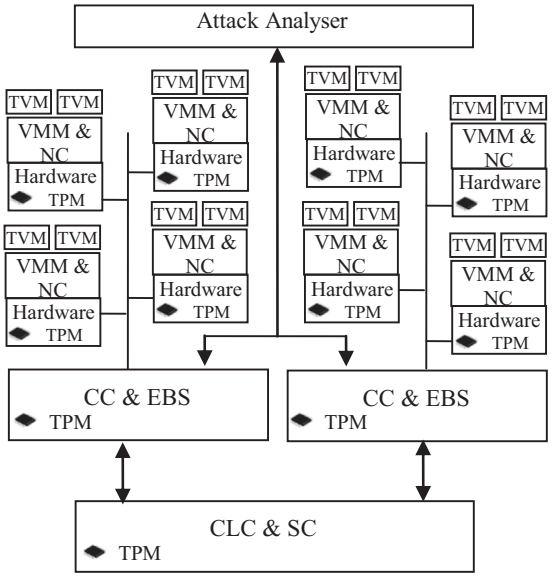

Fig. 1. Trust enhanced cloud architecture.

Please cite this article as: Varadharajan V, Tupakula U. Counteracting security attacks in virtual machines in the cloud using property based attestation. Journal of Network and Computer Applications (2013), http://dx.doi.org/10.1016/j.jnca.2013.08.002