Journal of Network and Computer Applications 36 (2013) 781–790

Contents lists available at SciVerse ScienceDirect

Journal of Network and Computer Applications

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

Quantitative survivability evaluation of three virtual machine-based server architectures

Yan Yang [a], Yulong Zhang [a], Alex Hai Wang [d], Meng Yu [a,*,1], Wanyu Zang [a], Peng Liu [b,2], Sushil Jajodia [c,3]

[a] Department of Computer Science, Virginia Commonwealth University, United States
[b] Pennsylvania State University, United States
[c] George Mason University, United States
[d] Verisign Labs, United States

ARTICLE INFO

Article history:
Received 10 November 2010
Received in revised form
23 September 2012
Accepted 12 December 2012
Available online 11 January 2013

Keywords:
Server architecture
Survivability
Continuous time Markov chain
Virtual machine
Cost analysis

ABSTRACT

Virtual machine-based services have become very popular in data centers and cloud computing in recent years. Efficient redundancy technology of virtual machine provides good availability for services; thus, it has become possible to provide continuous services even if the system suffers intrusions. So far, many intrusion tolerant server architectures have been developed based on virtual machine technology in academia and industry. Unfortunately, to the best of our knowledge, there is very little work done on evaluating the survivability of virtual machine-based server architectures in the literature.

In this paper, we focus on analyzing and evaluating the survivability of three virtual machine-based architectures, which are load balance server architecture (LBSA), isolated component server architecture (ICSA), and Byzantine fault tolerant server architecture (BFTSA). As a reference, a traditional server cluster without virtual machines is also analyzed and compared. We model different architectures with Continuous Time Markov Chain (CTMC). We analyze the transient behaviors and steady states of different virtual machine-based architectures. Furthermore, the costs of the traditional server cluster and the virtual machine-based architectures are compared in terms of processing costs, memory costs, communication costs, and fail-safe fault tolerance. The results show that BFTSA has better survivability than LBSA and ICSA, but with longer time to reach the steady states and higher communication costs.

1. Introduction

Due to resource and service consolidation, data centers are becoming the "backbone" of the infrastructure for IT operations in companies, governments, and military. Accordingly, two top requirements for modern data centers are *business continuity* and *information security*. Although these two requirements clearly show the importance of data center protection, from the security viewpoint, consolidating services and resources do not automatically consolidate the corresponding security mechanisms. Without security consolidation, the cost of protection can be much higher than it should be. Unfortunately, current security consolidation has been lagging behind service/resource consolidation in the data center industry.

As a major solution to the above problem, in recent years, virtual machine (VM) technology has been widely applied in various computing environments. The virtual machine-based server architecture has become a very popular technology to make users share the same hardware resources in data centers or cloud computing. According to a report from the research firm Gartner (Gartner, 2007), millions of virtual machines have been or are being deployed in data centers around the world, and virtualization is becoming a dominant indispensable technology for IT departments.

Survivability, as one of the most important evaluation metrics of server architectures is the ability to remain alive or continue to provide services in a hostile environment. With the increase of new attack technologies, it is very important to evaluate survivability of server architectures before putting them into practice to save time and money. When designing survivable architecture, we usually consider two types of failures which are fail-stop failures and Byzantine failures (Lamport et al., 1982) (or arbitrary failures). Once a fail-stop failure occurs, a system will stop working. For instance, a system may stop working because of component aging. If a system experiences arbitrary failures, the system may exhibit arbitrary behaviors. The consequence of the arbitrary failure is the same as that a system has been compromised. In this paper, we mainly focus on the failures caused by attacks.

Byzantine fault tolerance, or intrusion tolerance, can be achieved through replication (Castro and Liskov, 2002). While

* Corresponding author. Tel.: +1 804 827 3986.
E-mail address: myu@vcu.edu (M. Yu).
[1] Partially supported by NSF CNS-1100221.
[2] Partially supported by AFOSR FA9550-07-1-0527 (MURI), ARO W911NF-09-1-0525 (MURI), NSF CNS-0905131, and AFOSR W911NF1210055.
[3] Partially supported by NSF CNS-0905189.

1084-8045/$ - see front matter © 2013 Published by Elsevier Ltd.
http://dx.doi.org/10.1016/j.jnca.2012.12.006

the performance was a concern of these approaches, recent advance of research has led to more practical performance, e.g., in Zyzzyva (Kotla et al., 2007). The peak throughput achieved by Zyzzyva is within 35% of that of an unreplicated server that simply replies to client requests over an authenticated channel. With replications, compromised nodes can be removed through a voting mechanism. Therefore, the attackers have to compromise replicas more than a threshold number, usually more than $\lfloor(n-1)/3\rfloor$ replicas, of a replicated system with n replicas to disable the system (Castro and Liskov, 2002). However, replication itself cannot defeat attacks that can be applied to all replicas. Diversification (Cox et al., 2006; Nguyen et al., 2007; Pucella and Schneider, 2006) is a solution to protect replicas with different variations when one or more replicas are compromised.

To combine all aforementioned technologies, a basic idea of diversified replication using virtual machines has been described in Chun et al. (2008). The combination of diversification and replication is capable of defeating unknown attacks with practical costs. Properly configured diversified replication will be immune to attacks based on single vulnerability and can remove compromised node even if less than $\lfloor(n-1)/3\rfloor$ nodes are compromised. However, this method has not been implemented or evaluated with respect to the effectiveness or performance.

Current evaluation techniques for attacks or defense, such as attack graphs (Noel et al., 2003; Sawilla and Ou, 2008; Noel and Jajodia, 2009), attack tree (Mauw and Oostdijk, 2005), queuing networks and CTMC (Sahner et al., 1996a; Tijms, 1994), etc., have been used to evaluate some server architectures. Some models that can be used to evaluate dependability and security have been summarized in Nicol et al. (2004). However, to the best of our knowledge, evaluating the survivability of virtual machine-based architectures has not been investigated as yet.

In this paper, we focus on evaluating the survivability of three typical virtual machine-based server architectures and compare them with a traditional server cluster architecture. The three architectures are *Load Balanced Server Architecture* (LBSA), *Isolated Component-based Server Architecture* (ICSA), and *Byzantine Fault Tolerant* (Castro and Liskov, 2002) *Server Architecture* (BFTSA). Also, the survivability of traditional server cluster is analyzed as a reference. The probabilistic analysis, cost analysis and simulation results provide a significant reference for server architecture designers.

The paper is organized as follow. Section 2 covers the related work. One traditional architecture and three VM-based architectures are introduced in Section 3. We discuss the assumptions and definitions in Section 4.1. Section 4 analyzes the survivability of all architectures from the probabilistic viewpoint. Furthermore, the cost of each architecture is analyzed in Section 5. Finally, we conclude our paper in Section 6.

2. Related work

There are a significant number of models that can be used to evaluate the security state of information systems. Examples include the attack graphs (Noel et al., 2003; Sawilla and Ou, 2008; Noel and Jajodia, 2009), attack tree (Mauw and Oostdijk, 2005), stochastic activity network (Sanders et al., 2001), reliability block diagram (RBD) (Sahner et al., 1996b), and Continuous Time Markov Chain (CTMC) (Sahner et al., 1996b), to name a few. Trivedi even introduced a useful tool kit called SHARPE (Trivedi, 2002), which included eight interchangeable types of evaluation models. All the above models have been widely used to obtain estimate of security level in many different applications, such as web server architectures (Gokhale et al., 2006), data flow software architecture (Padilla et al., 2008), etc.

Among the above models, the attack graph-based methods (for example Noel and Jajodia, 2009) can reveal paths of vulnerability allowing attackers to penetrate through a network. It identifies critical vulnerabilities and provides strategies for protection of critical network assets, allowing us to harden networks before attacks occur, and handle intrusion detection more effectively and appropriately. Although the attack graph-based methods can better expose the vulnerabilities. they do not quantify the survivability of target systems. In the situations where the defence methods are expensive, the system maintainers need to know the survivability of each design and judge if a defence mechanism is worthwhile.

The attack tree model has also been used to analyze the vulnerability of information assets of a business enterprise. In Moore et al. (2001), the authors described and illustrated an approach for documenting attack information in a structured and reusable form based on attack tree modeling, thus security analysts can use the approach to document and identify commonly occurring attack patterns and information system designers and analysts can use these patterns to develop more survivable information systems. However, this kind of analysis methods is more strategy-based than time-domain-based. Sometimes it is quite difficult to predict the attackers' strategies statically. In our work, we do not simply consider the attack steps as strategic increments; we take the attacks as a stochastic process with uncertainty. Namely we concern the state transitions of the target system more than the attackers' strategies.

Except the above two models, the stochastic activity networks are used in security evaluation as well, which are probabilistic extensions of "activity networks" . In Nicol et al. (2007), the authors adopt the stochastic activity networks to model a random scanning worm with preferential scanning. They mainly consider the problem of deciding whether to allocate resources to remove an infected host (and thereby reduce the threat), or remove a susceptible but as-yet uninfected host, to directly save it from attack. They find out that whether preference should be given to infected hosts or susceptible hosts depend on the relative speeds at which they are removed. Nevertheless, this approach is only specified to model the attackers' behaviors. Only a certain attacking scheme could be addressed during each analysis. Our work aims at providing a more general heuristic for the defenders by evaluating the survivability of the systems.

Moreover, the reliability block diagrams (RBD) (Sahner et al., 1996b) are commonly used for evaluating the system's reliability. The diagrams are drawn as a series of blocks connected in parallel or series configuration, of which each block represents a component of the system with a failure rate. In RBDs, parallel paths means that the network would not fail unless all the paths fail; on the contrary, the network would fail if any failure happens on a block of a series path. The RBDs can measure the system reliability in regard to failures, but is incapable to evaluate the survivability under attacks.

In this paper, we analyze the survivability of the virtual machine-based architecture using CTMC, which is a powerful and popular state-based stochastic method to evaluate security and survivability of system. An example of application of CTMC is Yu et al. (2004), where a practical solution for on-line attack recovery of work-flows is proposed and then the behaviors of the attack recovery system is analyzed based on CTMC. In our earlier work (Yu et al., 2010), we specifically evaluated the survivability of virtual machine-based architecture with the help of CTMC. However, we had a strong assumption that each server has only one processor. Such assumption is not realistic since multi-core processors are predominant in server systems. The state transition of the whole system will be different if multi-processors present in a system. This paper considered more complex and