Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 147 (2019) 140–144

Procedia Computer Science

www.elsevier.com/locate/procedia

2018 International Conference on Identification, Information and Knowledge in the Internet of Things, IIKI 2018

Security Strategy for Virtual Machine Allocation in Cloud Computing

Hefei Jia[a,b], Xu Liu[a,b], Xiaoqiang Di[a,b,c,*], Hui Qi[a,b], Ligang Cong[a,b], Jinqing Li[a,b], Huamin Yang[a,b]

[a] *School of Computer Science and Technology, Changchun University of Science and Technology, Changchun 130022, China*
[b] *Jilin Province Key Laboratory of Network and Information Security, Changchun 130022, China*
[c] *Information Center, Changchun University of Science and Technology, Changchun 130022, China*

Abstract

In the cloud infrastructure, the co-resident attack is a critical security threat. Through virtualization technology provided by Cloud Service Provider, tenants' virtual machines (VMs) are possible to be allocated on the same host. Multi-tenant environment provides malicious tenants an opportunity to launch the co-resident attack and steal other tenants' information by side channels. To prevent this type of attack, previous works mostly pay attention to eliminating side channels and few of them study VM deployment strategy. Hence, we focus on deploying VMs with a secure and effective allocation strategy to reduce the probability of VM co-residence. A novel VM allocation strategy is proposed with three optimization objectives including security, load balancing and energy consumption. Finally, we implement our VM allocation strategy and prove its effectiveness on the simulation platform CloudSim.

Keywords: virtual machine allocation, co-resident attack, security strategy, cloud security;

1. Introduction

Cloud Service Providers (CSPs) such as Google, Amazon and Alibaba are developing their cloud platforms. Tenants have a chance to reduce their IT cost through this technology because they can pay only for the resources used at any time and any place.

In the IaaS layer, CSPs usually create multiple virtual machines (VMs) on a single host for different tenants. In this way, they can maximize the resources utilization and increase revenue. Yet, this also brings a new security threat.

* Corresponding author. Tel.: +86-431-85583330 ;
E-mail address: dixiaoqiang@cust.edu.cn

10.1016/j.procs.2019.01.204

In 2009, Thomas et al. [1] first proposed the concept of VM co-resident attack, which also brings a series of security problems: reducing the resources availability [2], making victim VMs free up resources [3], and stealing private information [4].

To defend the co-resident attack, many attempts have been taken in previous studies where VM allocation strategy is proved to be effective by reducing the co-resident probability [5, 6, 7, 8], it can be seen as a process of mapping virtual machines to physical machines [9]. Yi et al. [7] proposed a VM allocation strategy called the previous-selected-server-first policy (PSSF) that not only focused on the problem of security, but also paid more attentions on workload balancing and power consumption of hosts. They control the quantity of running hosts to reduce power consumption. However, CPU utilization of hosts also has a great impact on power consumption [3]. Consequently, we focus on both the number and CPU utilization of running hosts to reduce energy consumption. Then we propose a novel VM allocation strategy named select least number VMs based on PSSF (SC-PSSF) which reduces the power consumption of PSSF. Finally, we implement SC-PSSF on CloudSim and validate its effectiveness by the evaluation metrics of attack efficiency and attack coverage.

2. Related Work

2.1. Eliminating the side channel attack

For the side channel attack, there are lots of solutions such as addressing from the perspective of hardware [10, 13], system [11, 12] and so on.

At the hardware layer, Kong et al. [13] suggest using two caches to efficiently resist this attack, but the cost is so high along with the quantity of caches that this method is not widespread used. There is no doubt that the scheme of adding caches can increase hardware resource costs. To avoid potential resource waste, B. Lee et al. [10] present a random permutation cache scheme (RPcache). Through randomizing the memory-to-cache mapping, attackers cant extract useful information because they don't know the correct cache line. These methods have a good effect on L1 cache without performance degradation but have not been investigated on much larger Last Level Cache (LLC).

The solutions based on hardware are inconvenient to apply due to some changes on VM Monitor such as hypervisor. Scholars turn to study strategy in the system layer. Zhang et al. [14] propose a system called Dppel from the perspective of tenants, here a tenant VM could add noise to its caches frequently and confuse attackers. Consequently, attackers cannot extract effective message. Moreover, their system requires no changes to hypervisor. Besides, the study [11] puts forward a STEALTHMEM system from the point of system to ensure every tenant not be interfered by others. It designs the STEALTHMEM system that provides tenants a private memory to access and then help tenants free from the other tenants. They are both effective [11, 14] on LLC, yet they require a large number of additional computing resources.

2.2. VM allocation strategy

Besides eliminating the side channels, raising the difficulty for attackers to locate with other tenants on the same host also offers an alternative that is suitable for immediate deployment. Generally, hypervisor is in charge of two types of VM allocation: one is initial allocation (It refers to that a VM firstly allocated to a certain allocation policy) and the other is reallocation.

In previous research about VM initial allocation policies, scholars have considered security, together with other objectives including: resource utilization [15, 16, 17], load balancing [8], power saving [6, 18]. For example, Qiu et al. [8] design a VM allocation strategy according to security and load balancing. Ding et al. [6] establish a VM allocation model based on security and performance of the system. Except security, they just take account into one optimized objective, which may not be the best global solution. Thus, Yi et al [7] propose an effective allocation s-trategy (Previous-Selected-Server-First, PSSF) that covers security, work-load balancing and energy saving to weaken the VM co-resident attack, and the energy saving is achieved via reducing the number of running hosts. Nevertheless, there are still some other elements effecting energy consumption, such as CPU. Therefore, we improve the VM allo-cation strategy which not only considers security, but also load-balancing and energy consumption that is defined as the running number and CPU utilization of hosts.

Algorithm 1 A new VM Allocation Strategy for Resisting Co-residence

Input:
N^* : the number of VMs started by a tenant in a server
Output:
Chosen_Server: the server where VMs are placed

```
for i=1 to Num_Group do do
  if (s_i has enough remaining resources & has u's VMs & numbers(u's VMs) less N* ) then
    PList.add(s_i)
    s_ i is placed in Chosen_ Server
    else
    NPList.add(s_i)
  end if
end for
if (PList.isEmpty()) then
  Sort (NPList, group index)
  Mark NPList.get(min(NumOfVMs(Server)) as selected for u, and place in Chosen_ Server)
end if
```

3. Analysis and metrics of VM allocation strategy

3.1. Load balancing

Over-utilized hosts influence greatly running of tenants' VMs. And for CSPs, the improper distribution of VMs may cause waste of resources. Therefore, we consider the load balancing as spreading VMs among hosts with an average distribution. The following Equation (1) shows our ideas about it. U indicates a set of tenants U=$\{ u_1, u_2, ..., u_k \}$. $|VM_s(u)|$ is the subset of VMs launched by U. N is the total number of hosts. What's more, to show the effect of load balancing of hosts, we calculate the standard deviation of VMs number (include legal and malicious tenant) in hosts.

$$W = \frac{\sum\limits_{u \in U} |VM_s(u)|}{N} \tag{1}$$

3.2. Energy consumption

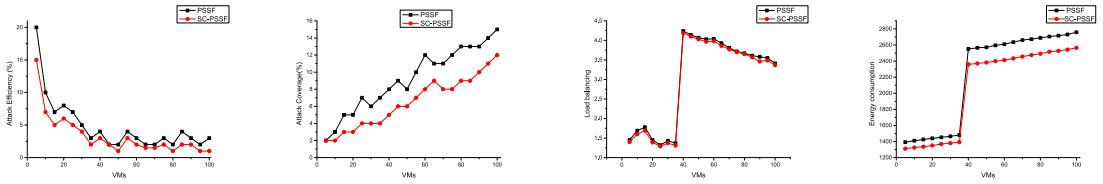
From CSPs' opinion, an important issue is to reduce energy consumption. Yi et al [10] propose to reduce the amounts of running hosts. It is rather remarkable that energy consumption by CPU occupied 90% of the total energy consumption in a cloud center. So, we take the CPU consumption as the total consumption. In the work of Clark et al [15], they suggest that if a host is idle, its power consumption is about 70% of full workload. The definition of energy consumption is shown in Equation (2):

$$P = 70\% \times P_{max} + (1 - 70\%) \times P_{max} \times R \tag{2}$$

P_{max} represents energy consumption when the CPU proportion of the host is 100%. According to Gao et al [9], a Dell host consumes between 162 and 215 Watt with full load. So, we take the value is 200 Watt in order to calculate conveniently. R indicates actual CPU proportion of the host.

3.3. The new secure VM allocation strategy

Through optimized objectives previously proposed, our SC-PSSF strategy takes effect as follows while a tenant named u creates a VM.



(a) Attack Efficiency (b) Attack Coverage (c) Load Balancing (d) Energy Consumption

Fig. 1. The experiment results on CloudSim

As Algorithm 1, when NPList is null, we select a host with least number of VMs rather than randomly select one of the hosts with same remaining resources. If remaining resources of all hosts are not same, PSSF is just a VM random policy. In this case, the possibility of VM co-residence may increase.

4. Experiment and evaluation

To prove the effectiveness of the SC-PSSF, we perform the experiment on CloudSim. It is an open source software for cloud computing simulation, which was developed by Grid Laboratory from the university of Melbourne in 2009. CloudSim offers several features such as: (1) modeling and simulation of large cloud infrastructure, (2) supporting data centers, service brokers, scheduling and distribution strategies [19].

4.1. Experiment setting

As can be seen in Table 1, a data center with 150 hosts and more than 1500 VMs is set in the simulation. It should be noted that there are three sets of VMs. And the difference of each type of VM is CPU capacity or RAM capacity. When CSPs receive VM request, they randomly select the type of VM and allocate to hosts. In the experiments, a legal tenant can start 20 VMs. The malicious tenant respectively starts 5,10,15 $\cdots$ 100 VMs under our VM allocation policy.

Table 1. Configurations of hosts and VMs.

	Quantity	MIPS	CPU cores	RAM
Hosts	150	2600	12	49152
VMs	random	500	1	613
	random	1000	1	870
	random	2500	1	1740

4.2. Results analysis

We compare our strategy with PSSF in Fig. 1 from the perspective of attack Efficiency, attack Coverage, Load Balancing and power consumption. The value of ttack Efficiency and attack Coverage is calculated by the Equation in Yi et al.[8]. It can be seen that our strategy (SC- PSSF) is better than PSSF. In Fig. 1(a) and 1(b), the Efficiency of SC- on average. As for Efficiency and Coverage, the value is lower and VMs is more secure. That is to say, SC-PSSF has a high success rate to defend VM co-resident attack. Hence, SC-PSSF is greatly improved the level of VMs security. In order to show the effect of load balancing, we calculate the number of VMs on each host through Equation (1). As illustrated in Fig. 1(c), load balancing's value of SC-PSSF is slightly lower than PSSF with the growth of VMs number, and it is worth being expected. Additionally, in Fig. 1(d), SC-PSSF's value of power consumption is lower than PSSF's. It is proved that SC-PSSF is more energy-saving.

5. Conclusion

In this paper, to solve the security problems about VM co-residency, we propose a novel VM allocation strategy (SC-PSSF) with the optimization objectives of load balancing and energy saving. The energy saving is realized via

reducing the numbers and CPU of the host. The simulation experiments on CloudSim prove that SC-PSSF has a good effect on resisting VM co-resident attack. Moreover, it also can reduce the total energy consumption of hosts while load balancing of hosts deserves better.

In the future, we will do some works to improve our VM allocation policy. (1) We will test and verify how it performs in the OpenStack. (2) We will go on to analyze the influencing factors of security, load balancing and energy consumption, and make the process of placing VM better. (3) Live VM migration is also an important stage at lifecycle of VM, and studied less in the VM co-resident attack. There is the probability that the malicious tenant can achieve the co-residence with target VMs.

Acknowledgements

This work has been partially supported by Science and Technology Development Project (20150204081GX) and the projects in the Education Department of Jilin Province (JJKH20170628KJ and JJKH20170630KJ).

References

[1] T. Ristenpart, E. Tromer, H. Shacham and S. Savage. (2009) "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds." *ACM Conference on Computer and Communications Security (CCS)*: 199–221.

[2] HS. Bedi, S. Shiva. (2012) "Securing cloud infrastructure against co-resident DoS attacks using game theoretic defense mechanisms." *International Conference on Advances in Computing, Communications and Informatics(ICACCI)* : 463–469.

[3] V. Varadarajan, T. Kooburat, B. Farley, T. Ristenpart, and MM. Swift. (2012) "Resource-freeing attacks: improve your cloud performance (at your neighbors expense)." *ACM Conference on Computer and Communications Security(CCS)* : 281–292.

[4] M. Wei, B. Heinz, and F. Stumpf. (2012) "A cache timing attack on AES in virtualization environments." *International Conference on Financial Cryptography and Data Security(Fc)* : 314–328.

[5] J. Kong, O. Aciicmez, JP. Seifert, and H. Zhou. (2008) "Deconstructing new cache designs for thwarting software cache-based side channel attacks." *ACM Workshop on Computer Security Architecture(Csaw)* : 25–34.

[6] Y. Azar, S. Kamara, I. Menache, M. Raykova, and B. Shepard. (2014) "Co-location-resistant clouds." *ACM Cloud Computing Security Workshop(Ccsw)* : 9–20.

[7] W. Ding, C. Gu, F. Luo, U. Rugwiro, X. Li, and G. Wen. (2018) "DFA-VMP: an efficient and secure virtual machine placement strategy under cloud environment." *Peer-to-Peer Networking and Applications* **11** (2): 318–333.

[8] Y. Han, J. Chan, T. Alpcan, and C. Leckie. (2017) "Using virtual machine allocation policies to defend against Co-resident attacks in cloud computing." *IEEE Transactions on Dependable & Secure Computing* **14** (1): 95–108.

[9] Y. Qiu, Q. Shen, Y. Luo, C. Li, and Z. Wu. (2017) "A secure virtual machine deployment strategy to reduce co-residency in Cloud." *IEEE Trustcom\BigDataSE\ICESS* : 347–354.

[10] Y. Gao, H. Guan, Z. Qi. (2013) "A multi-objective ant colony system algorithm for virtual machine placement in cloud computing." *Journal of Computer & System Sciences* **79** (8): 1230–1242.

[11] Z. Zhou, MK. Reiter, Y. Zhang. (2016) "A software approach to defeating side channels in last-level caches." *ACM Sigsac Conference on Computer and Communications Security(CCS)*: 871–882.

[12] T. Kim, M. Peinado, G. Mainar-Ruiz. (2012) "STEALTHMEM: system-level protection against cache-based side channel attacks in the cloud." *Usenix Conference on Security Symposium*: 11–11.

[13] X. Liang, X. Gui, H. Dai, and C. Zhang. (2016) "Cross-VM cache side channel attacks in cloud." *Chinese Journal of Computers***40** (2): 317–336.

[14] Y. Zhang, MK. Reiter. (2013) "Dppel: retrofitting commodity operating systems to mitigate cache side channels in the cloud." *ACM Sigsac Conference on Computer & Communications Security(CCS)* : 827–838.

[15] A. Beloglazov, R. Buyya. (2010) "Energy efficient resource management in virtualized cloud data centers." *International Conference on Cluster, Cloud and Grid Computing(CCGRID)* : 826–831.

[16] A. Hameed, A. Khoshkbarforoushha, R. Ranjan, PP. Jayaraman, and J. Kolodziej. (2016) "A survey and taxonomy on energy efficient resource allocation techniques for cloud computing systems." *Computing***98** (7) : 751–774.

[17] C. Hyser, B. Mckee, R. Gardner, and BJ. Watson. (2009) "Autonomic virtual machine placement in the data center." *IEEE 33rd International Conference on Distributed Computing Systems Workshops(ICDCSW)* : 220–225.

[18] P. Graubner, M. Schmidt, B. Freisleben. (2011) "Energy-efficient management of virtual machines in eucalyptus." *IEEE International Conference on Cloud Computing* : 243–250.

[19] K. Mills, J. Filliben, and C. Dabrowski. (2012) "Comparing VM-placement algorithms for on-demand clouds." *Cloud Computing Technology and Science* : 91–98.