2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC)

Towards a Security-Enhanced Cloud Platform

Junsik Seo
KAIST
Daejeon, Republic of Korea
js0780@kaist.ac.kr

Jaehyun Nam
KAIST
Daejeon, Republic of Korea
namjh@kaist.ac.kr

Seungwon Shin
KAIST
Daejeon, Republic of Korea
claude@kaist.ac.kr

***Abstract*—While cloud computing platform becomes popular and works as a platform for network function virtualization (NFV), the security of the cloud also becomes an important subject. However, although there are many works about security mechanisms, there has not been much research into what problems can occur when these conventional mechanisms are applied to the cloud system. Thus, we have given more attention to the robustness of communications resided in the cloud, not security mechanism itself, and found that security threats could arise from communication between cloud services and identification process. To cope with this problem, we propose three approaches: integrative identification system in a single cloud service, action-based token authorization, and partially encrypted communication between the identification system and cloud services. By implementing these approaches to open-source cloud computing platform, Openstack, we show that our approaches are feasible.**

I. Introduction

Recently, cloud computing platforms gain more and more popularity, and this expansion seems not to be over. In addition to their increasing number of users, scales of the cloud platforms are also increasing. In past years, the cloud platforms have provided not only software as a service (SaaS), but also platform and infrastructure as a service (PaaS and IaaS). These large-scale cloud platforms offer more flexible and agile resource allocation to network operators. Thus the cloud platforms can be effectively functioned as network function virtualization (NFV) platform, and many virtual network functions (VNFs) of NFV have run on them. This means that the cloud computing becomes a critical part of networking and will be more widely used in the future. Therefore, it naturally needs a high level of security management. As a response, cloud platforms implement authentication mechanisms to fulfill this need. There are already many techniques and schemes which have been proposed for the cloud, and several works have surveyed many of them [1], [3], [4].

While these security techniques have strengthened cloud platforms, they still have another critical issue - no unification with existing cloud services. It means that most implemented authentication approaches for cloud do not consider all related provided services, and we notice that this problem will cause unexpected security breaches degrading the robustness of cloud services. In this context, we first discover three critical vulnerabilities; (i) information leakage from identification service, (ii) excessive authorization to one token, and (iii) no encrypted communication between cloud services. In addition, we propose approaches to address these vulnerabilities and implement a prototype system of our approaches to the popular cloud computing service, Openstack [5].

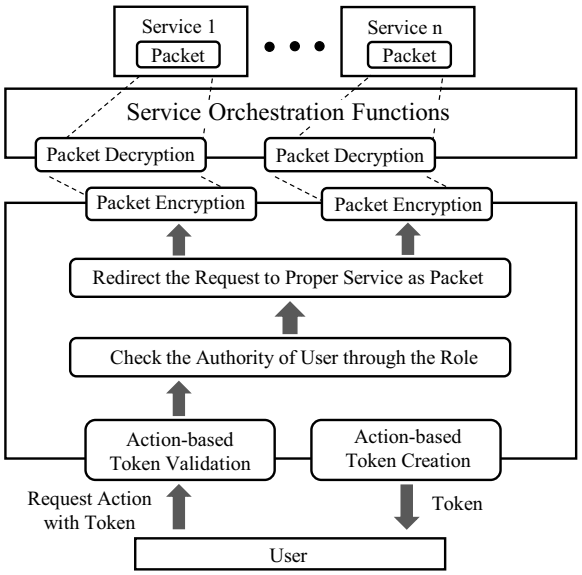

Fig. 1. The workflow of security-enhanced identification process of the cloud platform.

II. Our approaches

We make three approaches for the robustness and security of the cloud platform. These approaches are integrative identification system, action-based token identification, and the partially encrypted communication.

The workflow of our work is shown in figure 1. Tokens used for identification are created to authorize each action. When a user requests an action with the token, the validity of that token will be verified. In this process, an action contained in the token and action requested by the user must be the same. Then, the authority of the user and the authority required to execute requested action are compared. The former authority has to equal or greater than the latter one. After that, result is transmitted as a packet to proper service which will actually process that request. Just before the transmission, the content of the packet is partially encrypted only for sensitive user privacy, then the packet will be decrypted before it reaches the service.

2473-3105/18/$31.00 ©2018 IEEE
DOI 10.1109/PRDC.2018.00042

A. Integrative identification system

The first approach is integrative identification system. When a user requests a specific action in cloud system, user's authority and required authority to execute that action must be compared on authentication process. Nevertheless, if this authentication is processed on other services than identification service, the identification result has to be propagated to each service for the following authentication, and the chances of user privacy leakage also increase. Thus, integrative security service, which processes all of the identification, authorization, and authentication could be a fine approach for robustness of cloud platform. Therefore, through this integrative approach, security service in system verifies user's identity after a user requests specific action. If a user has a valid identity, it authenticates with policies and role of the user to determine whether this user has a right credential for the requested action. Finally, it returns a result of authentication with minimized user information. With this authentication system, we could achieve to minimize information flooding to other services from security service, and because all the security policies could be managed in one service, we also improve management effectiveness.

B. Action-based token identification

The second approach for the security-enhanced security service is deploying action-based token identification. Token is currently widely adopted as an identification mechanism in many domains [6], [7]. Although many cloud services also identify their users through tokens, if an attacker extorted the token of an administrative user, this attacker can disguise as an administrator and perform every action on the platform. This includes making new administrate account and deleting running VMs or containers. Thus, single token extortion could lead to a complete disaster of a single cloud system in current token authentication. To handle this problem, we make token be created for each specific action (e.g., getting the list of instance images, creating a new instance, or deleting a subnet) and only be used for authorization of initial action which it is created for. By doing this, if a single token were extorted by an attacker, the attacker can execute just single specific action authorized by that token and other action is prevented. As a result, the damage of token extortion would be minimized.

Alternatively, we could choose service-based token authentication, which authorizes users for each service, than each action. The reason we decided to design a more granular token is that the service-based token is still giving too much authority to a single token. For example, if a service token created for allowing access to computing service, which manages VMs or containers, was leaked, every instance can be deleted, thus the damage will be irreversible. Therefore, more fine-grained access control than service-based is needed.

C. Partially encrypted communication

The last one is partially encrypted communication between security service and other cloud services. Before the service executes a user's request, identification request has to be transmitted to security service and authentication with user information is processed by security service. Also, after the authentication, its result should be transmitted from security service to other services. Because this transmission could include the information related with user privacy, e.g., which action is requested with certain user id, transmitting those as plain text packets would be risky. However, in many cases, because it gives a considerable performance degradation and needs an additional effort for implementation, cloud systems do not commonly use encryption to communication at rest in their system [2]. Thus, we propose partial packet encryption, which is encrypting only sensitive user information, not all content of the packets. Because this information is typically short-length string values, the load of encryption is considerably small. Hence, this approach not only protects the user privacy but also minimize the degradation of communication performance caused by encryption.

III. Conclusions and Future works

As the scale of cloud platform continuously increases, the complexity of the cloud also increases steadily. In consequence, comprehensive vulnerability assessment for the cloud platform in consideration of the interaction between security service and others has become more and more difficult, and thus efforts to reinforce security service of the cloud grow in importance. In this work, we present the potential security risk factors of the cloud platform and address these weak points by implementing our feasible solutions to Openstack. However, we have a conviction that there are more undiscovered vulnerabilities. Our ultimate goal is finding these vulnerabilities and building a robust and secure cloud environment. To achieve this, we have kept on analyzing the security mechanisms and cloud platform to redeem its weaknesses.

Acknowledgement

This work KAIST was supported by Institute for Information & Communications Technology Promotion (IITP) grants funded by the Korean government (MSIT) (No. 2015-0-00575, Global SDN/NFV Open-Source Software Core Module/Function Development).

References

[1] Vaquero, Luis M., Luis Rodero-Merino, and Daniel Morn. "Locking the sky: a survey on IaaS cloud security." Computing 91.1 (2011): 93-118.

[2] Cameron Coles. "Only 9.4% of Cloud Providers Are Encrypting Data at Rest." https://www.skyhighnetworks.com/cloud-security-blog/verizon-data-breach-two-easy-steps-to-prevent-aws-s3-leaks (2015).

[3] Hashizume, Keiko, et al. "An analysis of security issues for cloud computing." Journal of internet services and applications 4.1 (2013): 5.

[4] Huang, Wei, et al. "The state of public infrastructure-as-a-service cloud security." ACM Computing Surveys (CSUR) 47.4 (2015): 68.

[5] Sefraoui, Omar, Mohammed Aissaoui, and Mohsine Eleuldj. "OpenStack: toward an open-source solution for cloud computing." International Journal of Computer Applications 55.3 (2012): 38-42.

[6] Zheng, Kai, and Weihua Jiang. "A token authentication solution for hadoop based on kerberos pre-authentication." Data Science and Advanced Analytics (DSAA), 2014 International Conference on. IEEE, 2014.

[7] Wang, Cong, et al. "Toward secure and dependable storage services in cloud computing." IEEE transactions on Services Computing 5.2 (2012): 220-232.