World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:9, No:11, 2015

Modelling Insider Attacks in Public Cloud

Authors : Roman Kulikov, Svetlana Kolesnikova

Abstract : Last decade Cloud Computing technologies have been rapidly becoming ubiquitous. Each year more and more organizations, corporations, internet services and social networks trust their business sensitive information to Public Cloud. The data storage in Public Cloud is protected by security mechanisms such as firewalls, cryptography algorithms, backups, etc.. In this way, however, only outsider attacks can be prevented, whereas virtualization tools can be easily compromised by insider. The protection of Public Cloud's critical elements from internal intruder remains extremely challenging. A hypervisor, also called a virtual machine manager, is a program that allows multiple operating systems (OS) to share a single hardware processor in Cloud Computing. One of the hypervisor's functions is to enforce access control policies. Furthermore, it prevents guest OS from disrupting each other and from accessing each other's memory or disk space. Hypervisor is the one of the most critical and vulnerable elements in Cloud Computing infrastructure. Nevertheless, it has been poorly protected from being compromised by insider. By exploiting certain vulnerabilities, privilege escalation can be easily achieved in insider attacks on hypervisor. In this way, an internal intruder, who has compromised one process, is able to gain control of the entire virtual machine. Thereafter, the consequences of insider attacks in Public Cloud might be more catastrophic and significant to virtual tools and sensitive data than of outsider attacks. So far, almost no preventive security countermeasures have been developed. There has been little attention paid for developing models to assist risks mitigation strategies. In this paper formal model of insider attacks on hypervisor is designed. Our analysis identifies critical hypervisor`s vulnerabilities that can be easily compromised by internal intruder. Consequently, possible conditions for successful attacks implementation are uncovered. Hence, development of preventive security countermeasures can be improved on the basis of the proposed model.

Keywords : insider attack, public cloud, cloud computing, hypervisor
Conference Title : ICCCNS 2015 : International Conference on Computer Communications and Networks Security
Conference Location : Kyoto, Japan
Conference Dates : November 12-13, 2015