데스크톱 가상화를 위한 데이터 보안 요구 사항 분석 및 고찰

오대명, 박종혁*
서울과학기술대학교 컴퓨터공학과
e-mail:{damingwu, jhpark1}@seoultech.ac.kr

Analyses and Considerations for Data base Security Requirements for Desktop Virtualization

Daming Wu, Jong Hyuk Park*
Dept. of Computer Science and Engineering, Seoul National University of Science and Technology, Korea

Abstract

As the expansion of enterprise scale and the increase of staff, the amount of terminal is increasing as well. It is very difficult to the system manager of traditional data protection scheme to manage and maintenance for the large number of terminals. This problem can be solved by desktop virtualization, which use traditional security problems still exist and new security problems occur at the same time. Using desktop virtualization, it needs a method of automatic security protection. In this paper, the desktop virtualization security requirements are discussed.

1. Introduction

As in the popular technological environment, virtualization technology has attracted the extensive attention of academic circle and industrial circle. Virtualization is a term in broad sense, towards which people with various knowledge backgrounds have different understandings, including server virtualization, storage virtualization and network virtualization etc. This paper discussed about server virtualization technology. As we know that servers can abstract physical resources into logical resources, which may transform a server into multi separated virtual servers without resource limitations of physical hosts. Such hardware like CPU, RAM, disk and I/O could be transformed into dynamic resources, in order to improve the resource utilization rate and realize server consolidation. In recent years, performance of hardware has been significantly improved. The advantage of virtualization technology have been applied in businesses, such as energy consumption, integrated management of infrastructures, flexible extensiveness and cheap high availability etc. This paper listed ten major advantages of server virtualization [1][2]. Desktop virtualization takes advantages of server virtualization technology and carried out virtualization in servers of the data center, so that it generate numerous independent desktop operation systems and send images to client device according to special virtual desktop protocol. Client can be connected to virtual machines through the network. After typing in user name, password and gateway of virtual desktop, people can access their own desktop system anytime anywhere.

Nevertheless, security can be considered as an important area for future development of server virtualization technology. As we discussed in introduction of virtualization technology, there are new security problems, such as VM(Virtual Machine) image sharing, VM isolation, VM migration etc. [3]. User data in virtualization environment cannot be totally controlled by users. Lack of control in user data increases the probability of data leakage. Classified data showed core value for uses. So now a days data security will be hot research topic which deserves further study.

2. Related Works

2.1 Desktop Virtualization Definition

Desktop virtualization is the personal computer desktop environment will separate calculation mode from the local physical machine, through a desktop display protocol, the generated virtual desktop is stored in the enterprise data center or the server of remote operator data center, replacing to store in local storage [4]. In

this way, when users connect the virtual desktop from a remote terminal, the corresponding operating systems, application program, user profiles and user data are centralized operation in storage of data center. Users can access their virtual desktops through a variety of equipment, such as thin client, a zero client, PC, PDA, etc., simultaneously.

2.2 The Existing Research

In current researches, a variety of file encryption methods have been proposed. Kawser Wazed Nafi et al. proposed an architecture to improve the security of file encryption system based on AES(Advanced Encryption Standard) and asynchronous key system on cloud computing platform [5]. M. Raja Kumar et al. proposed a system that has network-based disk encryption function and data leakage detection function [6]. Yushi Omote et al. proposed a hypervisor-based full disk encryption system [7].

3. Security Considerations

In this section, security considerations of file encryption system are discussed from three aspects.

Confidentiality: Confidentiality refers to prevent the third party excepted from the stipulated security policy illegally leaked files. In the internal environment, the data should be encrypted storage, and it will be decrypted only when used. When break away from the internal environment, the data should be encrypted to ensure data security. Traditional desktop environment stores data in local disk of the network dispersedly, and the virtualization environment is centralized storage data in the data center. So there are changes about the way of data storage and it moves to remote from local. Equipment turns to Shared storage device from independent utility local disk. Such changes are easier to create data leakage problems in some aspects [8].

Integrity: Integrity refers to the information keep unchanging if unauthorized, withstanding active attack, and ensuring the consistency of the data in the process of storage or transport, to prevent data modified and destroyed by illegal users. File and strategy should be accurate and complete in the file encryption system, and will not be changed by unauthorized [9].

Availability: Protect users access encrypted files timely and reliably. File encryption system should be able to recover from collapse or fault in a secure and quick way, reducing the negative effect to the producing activities. At the same time, necessary protective measures should be taken to eliminate internal or external attack, which will affect all the usability and efficiency of business processing components [10].

Auditing: Strict IT audit can prevent the loss or leak of confidential files. But it can also track the source of the leak and the leak time, providing favorable evidence to the court debate after it has happened.

4. Conclusion

In recent years, network security has become an increasingly serious problem, the leakage of confidential files have occurred repeatedly, while the traditional file encryption method requires user to manually encrypt or decrypt the files while protecting confidential files, it is not user-friendly, and it has low efficiency; because files are exist as plaintext after decryption. It may easily lead to disclosure of confidential files. Another important problem is to improve the level of information technology while minimizing IT costs. Currently, virtualization technology is one of the main technical means to reduce IT costs. Therefore, data security in the virtualization environment will be a research topic which deserves further study.

Acknowledgment

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 ICT융합고급인력과정지원사업의 연구결과로 수행되었음 (IITP-2015-H8601-15-1009)

References

[1] Murat ÇalÕúkan, Mustafa Özsiginan, Emin Kugu, "Benefits of the virtualization technologies with intrusion detection and prevention systems", AICT, pp.1-5, 2013.

[2] Narsimha Reddy CH, "Hardware Based I/O Virtualization Technologies for Hypervisors, Configurations and Advantages-A Study", Cloud Computing in Emerging Markets, pp.1-5, 2012.

[3] Mazhar Ali, Samee U. Khan, Athanasios V. Vasilakos, "Security in cloud computing: Opportunities and challenges", Information Sciences, pp-357 - 383, 2015

[4] Li Yan, "Development and application of desktop virtualization technology", Communication Software and Networks, pp. 326-329, 2011.

[5] Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, M. M. A. Hashem, "A Newer User

Authentication, File encryption and Distributed Server Based Cloud Computing security architecture", International Journal of Advanced Computer Science and Applications, pp.181-186, 2012.
[6] M. Raja Kumar, G.Samuel Vara Prasad Raju, Bathula Yedukondalu, "An Efficient Network disk Encryption and Data Leakage Detection ", IJAIR, pp. 224-226, 2012.
[7] Yushi Omote, Yosuke Chubachi, Takahiro Shinagawa, "Hypervisor-based Background Encryption", ACM, pp.1829-1836, 2012.
[8] Chung Hwan Kim, Sungjin Park, Junghwan Rhee, Jong-Jin Won, Taisook Han, Dongyan Xu, "CAFE: A Virtualization-Based Approach to Protecting Sensitive Cloud Application Logic Confidentiality", Computer and Communications Security, ACM, pp.651-656, 2015.
[9] Zhu Wang, Tao Huang, Sha Wen, "A file integrity monitoring system based on virtual machine", IMCCC, IEEE, pp.653-655, 2012.
[10] Federico Calzolari, Silvia Arezzini, Alberto Ciampa, Enrico Mazzoni, Andrea Domenici, Gigliola Vaglini, "High availability using virtualization", Journal of Physics: Conference Series. IOP Publishing, 2010.