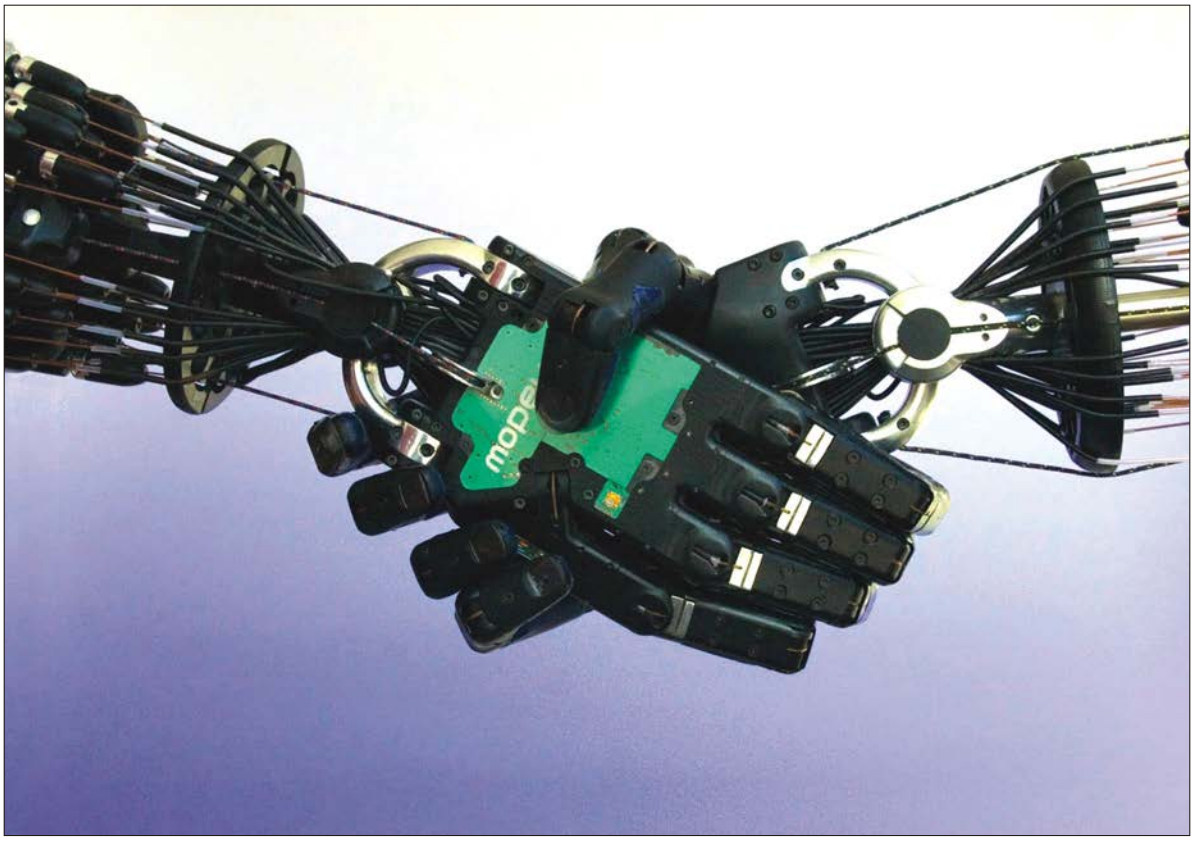

Journal of Artificial Intelligence

ISSN 1994-5450

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Artificial Intelligence 6 (1): 112-116, 2013
ISSN 1994-5450 / DOI: 10.3923/jai.2013.112.116

An Overview: Security in Virtualization Technology

V. Anitha and N. Keerthana
M. Tech Advanced Computing, SASTRA University, Thanjavur, India

Corresponding Author: V. Anitha, M. Tech Advanced Computing, SASTRA University, Thanjavur, India

ABSTRACT

In IT industries, securing the data plays a vital role. The aim of the study is to improve the security in virtualization technologies. Now-a-days IT industries prefer virtualization methods because it provides high security with low cost. The organizations enhance their security by providing different method through virtualization technology. This study explains the security in major virtualization technologies such as KVM, Xen, VMware and Microsoft.

Key words: Virtualization, security, hypervisor, VMware, KVM, Microsoft, Xen

INTRODUCTION

Virtualization was first developed by IBM Corporation in 1960's. At that time; virtualization technology has a capacity to run multiple operating systems on a host physical computer (Huang *et al*., 2012). The optimal server resources is used for improving the space and energy efficiency of data centers. Data center are the building blocks of IT business enterprises and it providing the capabilities of centralized repository for storage, management and networking (Uddin *et al*., 2012). Cloud computing typically begins with virtualization. It utilizes virtualization technologies to encapsulate collaborative manufacturing as service (Ding *et al*., 2012).

The vital goals are availability, confidentiality, data integrity, control and audit to achieve acceptable security. Availability means user can use the resource at any time, at any place. Confidentiality means keeping user data in secret manner and encrypted storage is another approach to improve the confidentiality. Data integrity means it is not lost or modify by any other unauthorized users. Audit means it look what happened in that environment. It can handle additional layer above the virtualized operation system hosted on VM to provide facilities to look what happened in the system (Zhou *et al*., 2010). Advantage of virtualization is flexibility, availability, scalability and security, cost, load balancing, resource allocation and isolation (Sahoo *et al*., 2010).

KVM can protect against the some attacks such as malicious (Root-kits), viruses and Trojans. XenServer has virtual network switching which provides data security in IT industries and delivering improved security for the business. VMware provide software based security and it secures the applications in the virtual data center and Microsoft also provides some security consolidation in virtualization (Zhang *et al*., 2011).

VIRTUALIZATION VENDORS

The major virtualization vendors provide different approaches to improve security for their platforms.

Security in KVM: KVM (Kernel-based Virtual Machine) is the best choice for virtualization technology and also gives trusted solution for implementing virtualized environment. KVM hypervisor is a full virtualization based on Linux operating system. Hypervisor equips with the security platforms and it has security tools. The KVM original source code is freely available. KVM hypervisor has Intrusion Detection System (IDS) and Accounting system. KVM is the best class performance for the enterprise workloads. It will manage more memory, processes and X86 Servers. KVM is the more efficient techniques in virtualization.

System security: KVM can protect against the many attacks such as Rootkit attack and Trojans. Some of the methods available in Rootkit Detection for securing the system are Detection recovery method and modifying the kernel code.

Root kit detection method: One of the kernel root kit is used to modify the parts of the kernel. It is more complicated because some of the security package is rely on kernel. By using the Root kit detection method, the difficulties are to be overcome:

- Prevent the root kit attacks
- Improve the isolation capacity
- Reduce overhead of the system

Detection recovery method: This method detects the data statically or periodically in manner, which is only happened in Root kit attack. It is also detect dynamically allocated data or code based on memory protection mechanism and this method is more efficient than modifying the kernel code method (Zhang *et al*., 2011).

Security management in KVM: KVM-security management will protect against attacks and secure kernel based virtual machine environment by extending the feature of KVM security such as securing remote management and storage devices, it is also protect against the timing attacks in the cryptosystem which is also used to execute the cryptographic algorithm. Intrusion Detection System is used to prevent the Malware attacks such as Root-kit. The KVM security management is used to detect the unauthorized modification in the virtual machine. To disable the presence of a Root kit, it can follow some hiding techniques such as Modify Interrupt Handler, Modify Interrupt Descriptor Table and Modify Syscall Handler (Lombardi and di Pietro, 2010).

XenServer: XenServer has virtual network switching which provides data security in IT industries. XenServer contains Memory Access API, which permits the integration of third-party security services into the virtualized environments (Garber, 2012).

Client virtualization security: In client virtualization security, it based on virtual desktop technology and that organization enables to extend the security. They also maintain security and data access in the applications. Industry have some rules, policy and also have the license to protect all the data from theft and prevent data from the users, apply and implement data protection policies and protect the data from organizations and also enable self-service recovery for every users and also for the workers.

Centralize management and control policy: In XenClient, it provides a single, centralized management to manage multiple client machines and have control policies. Client virtualization security based on the virtual desktops and it run on the top. IT provides security policies on virtual desktops. IT industries can selectively reject the access such as USB storage devices, CD, DVD to prevent loss of data in secure environment. Centralized laptop management increases security and IT efficiency.

Protect enterprise data: The multiple virtual desktops that run on XenClient that are completely isolated and Malware spreading among virtual desktops is almost nonexistent risks. Remotely they use some policy to prevent the enterprise data. They protect the confidential information and value properties are not compromised in this process (Citrix Systems Inc., 2011).

Server virtualization security: Server virtualization security in XenServer environment is more efficient and having some profiles to improve security. Three types of profiles are used in Citrix presentation server/terminal server environment (Wang *et al*., 2011):

- Roaming profiles
- Mandatory profiles
- Hybrid profiles

Roaming profiles: It is easy to setup, concept is simple and all user changes are observed and hold in this profile.

Mandatory profiles: This profile is simple to manage, loading is fast without corruptions.

Hybrid profiles: User changes can be observed as required and loading is fast with a greatly reduced chance of corruptions in this profile.

VMware: The largest virtualization vendor is VMware. It provides a software-based security, hypervisor-based firewall and also provides VM-traffic monitoring, security policy management, logging and auditing services.

The software-based security architecture called VShield and it provides several components. VShield App secures the applications in the virtual data center against network-based threats. VShield Edge protects the virtual data center's areas. VShield Endpoint off-loads some antivirus and anti-Malware functions to a security VM and removes the use of agents and thereby avoiding antivirus storms. A security management framework gives VShield products and VShield Manager communicates with management consoles that determines when and how to apply applications such as firewalls and antivirus scanners. VShield zones provides basic firewalling of traffic between VMs and traffic are analysed based on some constraints such as source and destination IP address and protocols. Third-party security vendors can support VShield and works only with VMware's virtual infrastructures (Garber, 2012).

Security advantages of VMware:

- After the attack recovery is faster
- Tracking is easy and safety

- Memory protection
- Kernel module protection such as digital signing
- High availability (Boesel, 2005)

Microsoft: Microsoft doesn't have a wide virtualization security framework. It has build architectural features that promote security. The features include isolation between virtual partitions. VM runs in its own processes and it also has own hypervisor resources. VMs can't communicate with one another except traditional networking and can't affect the contents of the host system, the hypervisor, or other VMs.

In Microsoft virtualization, centralized management is there around that it has server virtualization, presentation virtualization, Application virtualization and Desktop virtualization.

Server virtualization: In this virtualization want to focus on two areas ,one is securing the host area and other is securing the guest area, for that first want to understand the attack surface and secure virtual hard disk files. Other administration roles are Host, Network and Virtual machine ownership. For securing the guest we want to follow these things-Don't allocate over resources, Dispose unwanted storage devices, Give support for host time synchronization, Place the virtual machines of a same trust level on the same physical computer, Delete compromised high-security virtual hard disk files, manage the guest like any other physical server.

Presentation virtualization: In this virtualization the security considerations are to implement a single sign-on solution, Separate user to state the data, Testing the applications before present to end users, encrypt/sign the remote connection, set standardize settings across multiple servers in the environment, Manage the device redirection and Implement printer driver redirection.

Application virtualization: Some of the security considerations in the application virtualization are stream applications using encryption protocols such as RTSPS or HTTPS, secure package storage location, manage the application configuration if it physically installed.

Desktop virtualization: Security considerations in the virtualization are implementing a managed solution for non technical users and manage the guest like any other physical desktop.

CONCLUSION

Thus, the most of the organization enhance their security by providing different method through virtualization technology. Virtualization is the essential technology for cloud computing. So the virtualization vendors are securing the resources in effective manner by using different methods.

ACKNOWLEDGMENT

We thank the anonymous reviewers for comments that helped to improve the study. We also thank Dr. N. Sairam, Professor, School of Computing, SASTRA University, Thanjavur for giving support to do this study.

REFERENCES

Boesel, S., 2005. VMware security briefing. http://nvd.nist.gov/scap/docs/2008-conf-presentations/day2/VMware_Security_NIST.pdf

Citrix Systems Inc., 2011. Protect sensitive data on laptop-even for disconnected users. A White Paper by Citrix Systems. http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/citrix-xenclient-virtualization-security-paper.pdf

Ding, B., X.Y. Yu and L.J. Sun, 2012. A cloud-based collaborative manufacturing resource sharing services. Inform. Technol. J., 11: 1258-1264.

Garber, L., 2012. The challenges of securing the virtualized environment. Computer, 45: 17-20.

Huang, J.H., J. Huang, R. Li and X.M. Li, 2012. Virtualization-based recovery approach for intrusion tolerance. Inform. Technol. J., (In Press).

Lombardi, F. and R. di Pietro, 2010. A security management architecture for the protection of kernel virtual machines. Proceedings of the IEEE 10th International Conference on Computer and Information Technology, June 29-July 1, 2010, Bradford, UK., pp: 948-953.

Sahoo, J., S. Mohapatra and R. Lath, 2010. Virtualization: A survey on concepts, taxonomy and associated security issues. Proceedings of the 2nd International Conference on Computer and Network Technology, April 23-25, 2010, Bangkok, Thailand, pp: 222-226.

Uddin, M., A.A. Rahman, A. Shah and J. Memon, 2012. Virtualization implementation strategy for data centers to maximize performance and efficiency. Asian J. Sci. Res., 5: 45-57.

Wang, J., L. Yang, M. Yu and S. Wang, 2011. Application of server virtualization technology based on Citrix XenServer in the information center of the public security bureau and fire service department. Proceedings of the IEEE International Symposium on Computer Science and Society, July 16-17, 2011, Kota Kinabalu, Malaysia, pp: 200-202.

Zhang, X., E. Wang, L. Xin, Z. Wu, W. Dong and X. Dong, 2011. KVM-based detection of rootkit attacks. Proceedings of the 3D International Conference on Intelligent Networking and Collaborative Systems, November 30-December 2, 2011, Fukuoka, Japan, pp: 703-708.

Zhou, M., R. Zhang, W. Xie, W. Qian and A. Zhou, 2010. Security and privacy in cloud computing: A survey. Proceedings of the 6th International Conference on Semantics Knowledge and Grid, November 1-3, 2010, Beijing, pp: 105-112.