Volume-11| Issue-3| 2023 **Research Article**

ORGANIZATION OF INFORMATION SECURITY MECHANISM FOR VIRTUALIZATION ENVIRONMENT

https://doi.org/10.5281/zenodo.7699431

Mamajonov U.O
Cybersecurity Center" DUK, leading specialist of the Development Department, Uzbekistan
Abdunazarov B.A
Master's degree, Faculty of Cyber-Security, Tashkent University of Information Technologies
named after Muhammad al-Khwarizmi, Uzbekistan

Abstract: For cloud service providers, lightweight virtualization is a more economical way of virtualization. While the user is worried about the safety of applications and data of the container, due to the container sharing the underlying interface and the kernel, therefore the security and trusted degree of lightweight virtualization container isolation mechanism is critical for the promotion of lightweight virtualization service. Because the user cannot directly participate in the process of the construction and management of container isolation mechanism, it is difficult for them to establish confidence in the security and trusted degree of container isolation mechanism. In this paper, different aspects of Cloud virtualization security have been explored. Specifically, we have identified: i) security requirements for virtualization in Cloud computing which can be used as a step towards securing virtual infrastructure of Cloud, ii) attacks that can be launched on Cloud virtual infrastructure, and iii) security solutions to secure the virtualization environment by overcoming the possible threats and attacks. Based on the research and analysis of system credible and virtualization isolation mechanism, this paper puts forward a set of lightweight virtualization security isolation strategy mechanism, divides lightweight virtualization container storage address space into several parts, puts forward the definition of lightweight virtualization security isolation, gives the formal description and proof of container security isolation strategy, and combines with related technology to verify the feasibility of lightweight virtualization security isolation strategy mechanism. The mechanism has important guiding significance for cloud services providers to deploy container security isolation.

Keywords: Virtualization, Security, Cloud.

Received: 03-03-2023
Accepted: 04-03-2023
Published: 22-03-2023

Introduction. The recent and widespread adoption of virtualization technologies has changed the traditional view of ICT. Virtualization refers to the set of activities aimed at creating a virtual version of real components, including computer-hardware platforms, operating systems, storage, and networking. In the general understanding, virtualization encompasses all those technologies needed to set up virtual machines that provide virtual resources or devices. Virtualized resources or devices have the same functionalities and external APIs as physical ones, but with different characteristics (e.g., performance, costs). The virtualization concept is related to the concepts of emulation and simulation, which, while similar to virtualization, implement different approaches or paradigms. Emulation is an approach through which a system is executed as if it were another system. OSs, APIs, and operations are executed (emulated) on a machine for which they were not developed. The emulator replicates the exact behaviour of a piece of physical hardware, executing a copy of software by emulating the hardware for which the software was developed. Simulation, on the other hand, simulates the behaviour of a given system. It aims to achieve the same result as an emulator, but requires

rewriting part of the program to be simulated. Virtualization provides techniques for using resources and devices without considering their position and physical layout. It supports an encapsulated environment, guaranteeing machines isolation, hardware independence and hardware partitioning. Generally speaking, emulation and virtualization represent a target system accurately, but at high costs, whereas simulation is cheaper and more flexible, but less accurate. Virtualized security, or security virtualization, refers to security solutions that are software-based and designed to work within a virtualized IT environment. This differs from traditional, hardware-based network security, which is static and runs on devices such as traditional firewalls, routers, and switches. In contrast to hardware-based security, virtualized security is flexible and dynamic. Instead of being tied to a device, it can be deployed anywhere in the network and is often cloud-based. This is key for virtualized networks, in which operators spin up workloads and applications dynamically; virtualized security allows security services and functions to move around with those dynamically created workloads. Cloud security considerations (such as isolating multitenant environments in public cloud environments) are also important to virtualized security. The flexibility of virtualized security is helpful for securing hybrid and multi-cloud environments, where data and workloads migrate around a complicated ecosystem involving multiple vendors.

To secure the virtualization hardware, (Cloud) service provider must limit access of hardware resources to authorized person. Similarly, proper access controlshould be implemented in the management layer, so that each administrator hasaccess only to its concerned data and software. The service provider also needto provide strong authentication mechanisms to users. Furthermore, securityprinciples for the development of trusted computing system such as economy ofmechanism, complete mediation, open design, principle of least privilege, psy-chological acceptability must also be followed by the service. These Cloud computing generally adopt virtualization technology to support themselves, the traditional virtualization technologies include Xen hypervisor, VMWare, and Linux kernel Virtual Machine (KVM) and so on, these virtualization technology can achieve extension, control computing resources, and can securely isolate Virtual Machine (VM), while the resources they consume is large, and the performance and economic benefits they bring are relatively low. With the increased number of cloud users, the demand for physical resources is growing at an order of magnitude, so from the perspective of reducing the hardware cost, people hope for the appearance of a more economical virtualization solutions. In recent years, operating system-level virtualization which based on the Linux Containers (LXC) technology is becoming more and more popular, such lightweight virtualization has many advantages compared to the traditional way of virtualization. First of all,

container can start in the second level, it is much faster compared to the traditional way of virtualization. Second, container run on a shared operating system kernel, this allows multiple virtual environment to share the underlying operating system interface and a public host kernel, therefore the system resource utilization is very high, and virtual machine density that single server can support is big, so as cloud service providers can have better profit space.

Materials. The problem lightweight virtualization bringing is users worrying about whether the strength of container isolation mechanism is safe enough, and whether or not they can ensure the security of user's application and data. So the method of lightweight virtualization technology attracting more users is to prove the effectiveness of their isolation, enabling users to establish enough confidence level for the services it provides.

Methods. At present domestic research, the lightweight virtualization field focus on implementation method, lacking of basic research such as container isolation mechanism security policies. This paper proposes a safety isolation strategy mechanism under lightweight virtualization environment with the help of lightweight virtualization containers technology and virtualization isolation mechanism, aims to solve the problem of container security isolation.

Results. Innovation point of this article is: 1) based on the characteristics of lightweight virtualization, putting forward the address space division of lightweight virtualization storage resources and the definition of isolation; 2) adopting the trusted computing technology, turning it into the formal security isolation strategy, providing guidelines for developing container, and improving the user's confidence in lightweight virtualization technology. In this paper, the first chapter introduces the research status of the related technology, including the current research status of the system trust and virtualization isolation mechanism; The second chapter embarks from dividing the address space of lightweight virtualization storage resources, researches lightweight virtualization security isolation strategy mechanism, proposes lightweight virtualization security isolation definition, formally describe container security isolation strategy; The third chapter certificates the strength of these container security isolation strategy; The forth chapter analyzes in detail the technical feasibility of above-mentioned lightweight virtualization security isolation strategy mechanism. the publisher. Trusted computing group described credible as "an entity’ behavior is always carried out in accordance with the expected targets and the way", whether the system is trusted or not, it can guaranteed from two aspects: one is the system to act in accordance with the code of conduct, only within the scope of the code of conduct, the behavior of the system is considered credible. Second, conduct itself needs to meet the requirements of people's confidence level. For the first assurance requirements,

through the trust root and trust chain mentioned in the basic consider of the trusted compute to ensure that the system runs in accordance with the code of conduct, Trusted Computing Group (TCG)put forward the Trusted Computing platform technical specification. Cybercrime continues to emerge, with new threats surfacing every year. Every business, regardless of its size, is a potential target of cyber-attack. Cybersecurity in today's connected world is a key component of any establishment. Amidst known security threats in a virtualization environment, side-channel attacks (SCA) target most impressionable data and computations. SCA is flattering major security interests that need to be inspected from a new point of view. As a part of cybersecurity aspects, secured implementation of virtualization infrastructure is very much essential to ensure the overall security of the cloud computing environment. We require the most effective tools for threat detection, response, and reporting to safeguard business and customers from cyber-attacks. The objective of this chapter is to explore virtualization aspects of cybersecurity threats and solutions in the cloud computing environment. The authors also discuss the design of their novel 'Flush+Flush' cache attack detection approach in a virtualized environment. Each component of virtualization layer can act as an attack vector to launchmultiple attacks on the system. Attacks that target different components ofvirtualization environment may result in security issues such as compromise ofcomplete Cloud infrastructure, stealing of customer data and system hacking.

In a container-based scenario, an application's operating environment is virtualized. The result is an isolated container in which the application can run.40 Examples of this scenario include application virtualization, Linux containers, FreeBSD-style jails, and sandboxing. Containers are different from guest OS and virtual machines in general, but they share some security vulnerabilities, such as access control, privilege permissions, and coding weaknesses. Specifically, container vulnerabilities mainly aim to escape from container isolation, similar to VM escape, or to escalate privileges in the container software layer (e.g., symbolic link traversal on container respawn). Privilege escalation in containers is considered very risky, since it allows gaining the same privilege level on the host OS (e.g., container breakouts) mainly because not all resources at container level are namespaced (a namespace uniquely identifies a set of names so that there is no ambiguity when objects having different origins but the same names are mixed together). For instance, in a kernel keyring for handling cryptographic keys, keys are generally separated by a UID not normally namespaced at the container level, so users with the same UID may gain access to the keys. Other vulnerabilities related to weak permissions or improper authorization permit local users to obtain sensitive information, to perform protocol downgrade attacks via a crafted image

or to edit their profiles. As with a VM, image management and protection is crucial i) for preventing attackers from running maliciously poisoned images, putting that host and data at risk, and ii) for keeping the image updated to avoid known vulnerability exploits. Proper management of credentials is critical in all virtualization components (i.e., compromised secrets). It is even more vital with containerization applied to micro-service architectures, where containers are continuously started and stopped. Specifically related to containerization, every kernel-related vulnerability (called kernel exploit) is magnified by the fact that, unlike in case of a VM, the kernel is shared among all containers and the host. Thus, any kernel issue raised at the container level has great potential impact, even leading to DoS when exhausting certain specific kernel-level resources

Conclusion. Malicious programs in different virtual machines can achieve required accesspermissions to log keystrokes and screen updates across virtual terminals that can be exploited by attackers to gain sensitive information. If isolation isnot properly implemented covert channels can be used for unauthorized com-munication with other VMs in the system. Attackers can use Trojans, malwaresand botnets for traffic monitoring, stealing critical data, and tampering thefunctionality of guest OS. Conficker, Zeus botnet, command and control botnetcommunication activity are the examples of such attacks that result in data de-struction, information gathering and creation of backdoors for attackers. Attacksthrough buggy software, viruses and worms can exploit the guest OS in VMs.Furthermore, unpatched VM operating systems can be exploited by zero dayattacks. According to the characteristics of the lightweight virtualization, security isolation strategy mechanism proposed in this paper can be realized by Namespace and Copy-On-Wirte(COW) technology. Namespace is an operating system level environmental isolation method provided by Linux, in order to realize the lightweight virtualization services. COW is only in the process of paragraphs in the space content will change, will be a copy of the contents of the parent for the child process technology. Of which PID is used to isolate the process of different containers; NET makes the container has an independent Network Devices, IP Addresses, IP Routing Tables, /proc/net directory, that each container network can be isolated; MNT makes the process of different Namespace see file system is different, so that the file system saw by process in different Namespace is isolated from each other. The biggest difference between COW file system and other systems is that: COW never overwrite the existing content of the file system. COW makes container to read or write its own address space rather than to read-only storage address space of a host computer, can be used to separate the container storage address space and the hosting read-only storage address space. COW will merge two address space (the hosting read-only storage address space and the

container storage address space) into one, therefore the angle of view on the container is all content of combined address space. If the container needs to update its perspective /etc/hosts file, the file happens to be contents of the hosting read-only storage address space, COW will firstly not overwrite /etc/hosts file on the read-only storage address space in the host machine, secondly it will copy the file to the container storage address space, namely copy to/etc/hosts file on the container storage address space , and then conduct update operation on the latter .In this way, even if the host machine read-only storage address space and the container storage address space both have /etc/hosts file ,and COW can ensure that container only read or write contents of /etc/hosts file on the container storage address space , namely the updated content.

REFERENCES:

1. Perez R, Sailer R, van Doorn L. vTPM: virtualizing the trusted platform module[C]. Proc 15th Conf on USENIX Security Symposium; 2017; 2017. p. 305-20.

2. England P, Loeser J. Para-virtualized TPM sharing[C]. Trusted Computing-Challenges and Applications: Springer; 2018: 119-32.

3. Stumpf F, Eckert C. Enhancing trusted platform modules with hardware-based virtualization techniques[C]. Emerging Security Information, Systems and Technologies, 2018 SECURWARE'08 Second International Conference on; 2008: IEEE; 2018. p. 1-9.

4. Greve D, Wilding M, Vanfleet WM. A separation kernel formal security policy[C]. Proc Fourth International Workshop on the ACL2 Theorem Prover and Its Applications; 2020: Citeseer; 2020.

5. Pauley WA. Cloud provider transparency: an empirical evaluation [J]. Security & Privacy, IEEE 2090; 8(6): 32-9.

6. Whaiduzzaman M, Gani A. Measuring security for cloud service provider: A Third Party approach[C]. Electrical Information and Communication Technology (EICT), 2019 International Conference on; 2019: IEEE; 2019. p. 1-6.

7. Wüllenweber K, Weitzel T. An empirical exploration of how process standardization reduces outsourcing risks[C]. System Sciences, 2017 HICSS 2017 40th Annual Hawaii International Conference on; 2017: IEEE; 2017. p. 240c-c.

8. Chakraborty S, Roy K. An SLA-based framework for estimating trustworthiness of a cloud[C]. Trust, Security and Privacy in Computing and Communications (TrustCom), 2018 IEEE 11th International Conference on; 2018: IEEE; 2018. p. 937-42.

9. Zadeh LA. Probability measures of fuzzy events [J]. Journal of mathematical analysis and applications 2018; 23(2): 421-7.

10. Shapley LS. A value for n-person games[R]: DTIC Document, 2020.