Hypervisor Security Analyses Based on Ishikawa Methodology

Svetlana Kolesnikova*, Danil Melnik , Roman Kulikov, Yuriy Gatchin
ITMO University, St. Petersburg, Russia.

* Corresponding author. Tel.: +7 (963) 303-17-01; email: s_kolesnikova@yahoo.com
Manuscript submitted May 5, 2017; accepted July 25, 2017.
doi: 10.17706/jcp.13.5.511-518

Abstract: Nowadays Virtualization is an underlying technology in cloud computing that simplifies data center management improves corporate resource utilization, minimizes IT hardware costs. However, cloud environment faces new security challenges as the architecture of virtualized environments differs dramatically from non-virtualized. The traditional security methods cannot be applied any more to secure system in effective way as it used to be in the past. New approaches should be applied in order to be able to meet new security challenges of technology. In this research, we apply Ishikawa approach, method from Quality Management System in order to identify many possible causes and factors for hypervisor security risks. In addition to that, to better structure the risks we based Ishikawa method on traditional security model, STRIDE Model, proposed by Microsoft. Hence, this paper firstly analyses malicious environment of virtualization technology. Secondly, it applies quality-based methodology for security analyses. As a result, we see that such approach helps to identify preventive security countermeasures that have to be considered at the earlier stage before real attacks occur.

Key words: Secure cloud computing, hypervisor security, virtualization, threat modeling, Ishikawa, fishbone diagram, cause and effect analysis.

1. Introduction

In recent years use of virtualization technology has increased significantly, thanks to explosive growth of cloud computing, not only for private but also mostly for corporate users. Virtualization is the key underlying technology enabling cloud providers to host services for a large number of customers. In this way, there is a tendency to use virtualization, minimizing costs on IT infrastructure and services. Furthermore, hypervisor and virtualization tools are large complex software products with a number of different vulnerabilities enabling various types of attack surface.

On the one hand, benefits for big corporations and small companies from cutting-edge cloud computing technologies are undeniable. There have been different cloud types introduced (IaaS, SaaS, PaaS) to optimize collaboration and improve IT business-processes within the company. On the other hand, these technologies revealed not only strategic and competitive opportunities, but new vulnerabilities, threats and possibilities for the systems to be compromised. Therefore, the question of protecting cloud, in particular virtualization technology, from cyber-crime should constitute the highest priority for researches and business executive.

2. Attack Surface in Virtualization Environment

Virtualization is seen as an efficient solution for optimum use of hardware. NIST defines virtualization as the simulation of the software and/or hardware upon which other software runs [1]. Server consolidation that refers to ability for multiple systems to be multiplexed over the same hardware, is a major benefit driving virtualization in corporate environments [2]. Notably, virtualization technology has enabled new attack surface. On the one hand, Intruder can use the same tools to violate security for a virtual machine (VM) as for a physical one. The addition of a virtualization layer, on the other hand, provides Intruder with new possibilities of reaching its target. Indeed, as shown in Fig. 1 vulnerabilities in the virtualization layer may allow attacks to be performed from a VM against another VM, hypervisor or the host OS. Every VM possess virtual CPU, network interfaces, storage and operating system that can be violated.

Furthermore, security is the greatest challenge in virtual environment as virtualization architecture has enabled new attack surface where classical security mechanisms are incapacitated. The security of a virtualization is heavily dependent on the hypervisor.

Hypervisor or virtual machine monitor (VMM) is a main target for an attack. Indeed, if this key element is compromised, all virtualization tools in the system are potentially at risk.

VMM is a complex privileged software program that allows multiple operating systems (OS) to share a single hardware processor. Thereafter, Hypervisor controls guest OS from disrupting each other and from accessing each other's memory or disk space. On the other hand, Hypervisor is one of the most critical and vulnerable elements in Cloud Computing infrastructure due to the fact that with the increase of Cloud Computing, cases in which co-hosted VMs on the same hypervisor can be malicious towards each other have brought security concerns. As a result, resources can be shared and mediated by a Hypervisor, which is compromised by a rogue VM.

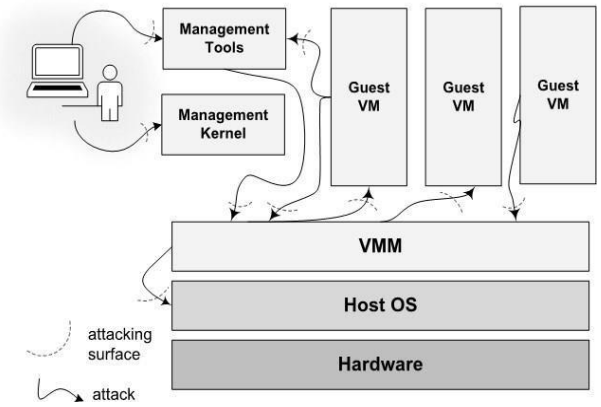

Fig. 1. (After Fig. 1 from [3]) Attack surface in virtualization environment.

Hypervisor is a main risk factor unique to virtual environments. In case hypervisor is compromised, security of all guest VMs hosted on that hypervisor can be easily violated. Due to providing a potential entry point to the guest VMs, the hypervisor itself creates a new attack surface that does not exist in the physical environment. Weaknesses in hypervisor isolation technology, access controls, security hardening, and patching could be identified and exploited, allowing Intruder to gain access to individual VMs [4].

3. Stride Model

The STRIDE model is an alternative approach to threat modeling that was proposed by Microsoft in 2002. In this model, we categorized threats by the goals and purposes of the attacks on hypervisor. By using these categories of threats, one has the ability to create a security strategy for a particular system in order to have

planned responses and mitigations to threats or attacks. The name STRIDE is based on of the initial letter of possible threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege [5].

S. Spoofing Identity

Identity spoofing is illegally accessing and then using another user's authentication information, such as username and password.

VM Cloning. In order to add an additional entity to physical environment real equipment is needed, in virtual environment, however, VM can be added just by coping a file. Hence, it is complicated to distinguish a cloned entity from an original one. VM are identified by certain parameters such as OS Security Identifiers, MAC address, virtual network adapter, Hard Drive IDs. Cloning methods in this way generate new identifiers in the VM [6]. Spoofed VM is a major security concern of virtualization technology. Firstly, spoofed VM inherits permissions that are granted to original VM, so that it is automatically trustable by hypervisor. Secondly, address and name collisions on network can occur. Cloned VM problem can be referred not only to Spoofing issue, additionally, it can be referred to some following sections (Tampering, Information Disclosure, Availability) as it causes problems of confidentiality, integrity and availability of data and components in virtualization environment [2].

Man-in-the-Middle Attack. Malicious VM is placed in the path of communication of VMs, so that Intruder intercepts network traffic between two VMs. Thereafter, network traffic among the dual computers goes over malicious system that enables Intruder to revise the data. Intruder uses ARP spoofing/ ARP poisoning to send faked messages to a receiver VM. By attacking one single VM, Intruder might be able to get access to other guest VMs and host VM. Thereafter, Intrusion Detection System (IDS) has to be integrated to prevent from this type of attacks [7].

T. Tampering with Data

Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a data storage, and the alteration of data as it flows between two VMs. In virtualization technology, a new security concern introduced such as Tampering with OS or virtualization and cloud architecture.

Incorrect Configuration of VMs and Hypervisors. The integrity of data within complex cloud hosting environments such as SaaS configured to share computing resource amongst customers could provide a threat against data integrity if system resources are effectively segregated [8].

Inserted VMM (Hyper-Jacking). By using these methods Intruder coverts insertion of a VMM under an OS. Hence, the OS can be moved from physical to virtual almost undetectably, either on boot or while the system is running. Two methods used include the use of raw disk reads to alter device drivers that are paged out to disk, and the modification of system startup files [6].

Man-in-the-Middle Attack mentioned in previous section has to be also associated with data tampering as it is serious concern for data integrity.

R. Repudiation

Repudiation involves activities that cannot be traced, thereafter; Intruder can claim to have not performed a specific action.

Data Stealing. Stolen data is one of the major security concerns in virtualization environment due to the fact that data can be stolen by authorized administrator without leaving any trace of such malicious actions. By administrator login in hypervisor, data replication schemes have to be created that apply policies like RAID and mount the disk image onto the hypervisor and delete the original copy and lost [9].

I. Information Disclosure

Information disclosure threats involve the exposure of information to individuals who are not supposed

to have access to it—for example, the ability of an intruder to read data in transit between two computers.

Faulty Implementation of Memory Management Unit (MMU). Hypervisor runs a software-based MMU in the form of a shadow page table for VM. Guest VMs cannot be granted direct access to the hardware-based MMU. Otherwise, guest VMs could have had direct access to memory belonging to the hypervisor and other cohosted VMs. However faulty implementation of software-based MMU could lead to disclosure of data in arbitrary address spaces such as memory segments belonging to hypervisor and co-located VMs [10].

VM Cloning. This issue has been already mentioned in Section, concerning Spoofing. However, VM Cloning deserves to be mentioned in Information Disclosure as well. Sensitive data such as personal details or encryption keys becomes vulnerable for Information Disclosure. Among other places, data can reside in deleted files or memory snapshots, on virtual hard drives, or be retained in previous snapshots. It can also be part of logging data external to the VM that the VMM undertakes [11]. Methods to reduce these risks include encryption of VM data with keys unknown to the VM, and externalizing encryption from the VM, for example, by storing encryption keys in the VMM or hardware TPM [11]. This approach can cause problems for VM migration if measures are not taken to migrate or regenerate keys [6].

D. Denial-of-Service (DoS)

DoS threats affect system availability and reliability.

Distributed Denial of Service (DDOS). DoS attack surface differs dramatically in virtual environment from physical one due its distributed and virtual architecture such kind of DoS occur as attack that disrupt service by consuming resources.

Resource Exhaustion Attacks affect CPU, RAM, thread execution time, memory, storage requests and network interfaces, etc. A DoS attack that ramps up CPU or memory consumption on a virtual machine, compromises Hypervisor, so that resources from other VMs can be exhausted as well. Hence, DoS attack in virtualization environment addresses not only targeted entity [12]. This type of attack is also called Shared resource consumption attack.

Hypervisor Exploitation is an attack that exploits vulnerabilities in the underlying hypervisor, or operating system hosting a virtual machine instance, so that Intruder is able to cause targeted outages or instability. Attacks using these methods are designed to circumvent traditionally well-defined cloud architecture that has concentrated on securing against external network-based DoS attacks [8]. In addition to that, according to [10] one of the Hypervisor key functions is Execution Isolation for VMs. Scheduling of individual VM's tasks by handling register states appropriately. In other words, VMM manages vCPU tasks by allocating guest VM a set of virtual CPUs (vCPUs). To enable saving and loading of the state of each vCPU, the hypervisor uses a data structure called Virtual Machine Control Structure (VMCS). Faulty implementation of this data structure has been known to cause hypervisor memory leaks. Furthermore, Hypervisor emulates interrupt and timer mechanisms that the motherboard normally provides to a physical machine. Faulty implementation of interrupt and timer related data structure has been known to cause denial of service attacks [10].

E. Elevation of Privilege

In this type of threat, an unprivileged entity is granted privileged permissions. Hence, Intruder might be able to compromise the entire system.

Rogue VM. According to [10] the first threat to any hypervisor is from rogue VMs. The rogue VMs are the ones that manage to subvert the access control function provided by Hypervisor to hardware resources such as memory and storage. Potential downstream consequence of a rogue VM taking control of the hypervisor is:

(a) installing rootkits and

(b) attack on another VM on the same virtualized host

Privileged Interfaces. Hypervisors provide privileged interfaces (generally called by the name Introspection API) to virtual security appliances (such as IPS/IDS). These interfaces could also become another target for exploitation by rogue/misconfigured *VMs.* [10]

In [13] proof–of–concept of such attack was developed. Virtual-Machine-Based Rootkits (VMBRs) is injected underneath the targeting *VMs*. In case Intruder obtains administrative privileges on a VM. Once the rootkit is successfully installed and configured, it functions as a modified hypervisor on the infected physical server and loads all *VMs.* Consequently, Intruder seizes control of every VM on the hypervisor.

In addition to written above threats, concerning STRIDE Model, at the end we will concentrate more in the detail on formal model of getting escalated privileges on hypervisor. In [6] such kind of attack was proposed, where Intruder by the means of rough VM targets hypervisor in order to get escalated privileges. Furthermore, hypervisor is represented as a set of finite state machines, emulation devices. Attack is the sequence of events, being generated by virtual machine (VM). Hypervisor is defined as a set of emulators $\{u\}$, that process events from set V. Set of events V consists of 2 non-overlapping subsets: V_g is a set whose members are events generated by VM, V_h is a set whose members are events generated by hypervisor components. Device emulators are located in components of hypervisor. These components $c = (\{uc\},Adc,Lvlc)$ of hypervisor share common address space Ad_c and have the same privilege level Lvl_c. Each emulator is described as finite state machine with specific level and with defined acceptance state function:

$u=(V_u,S_u,s_0,Tr_u,Sq_u,Lvl_u)$, where

$V_u \in V$ – input alphabet (set of events),

S_u – set of emulator states,

S_0 – initial emulator state under start of virtual machine,

Tr_u: $S_u \times V_u \to S_u$ – transition function between emulator states,

Sq_u: $S_u \to \{true, false\}$ – acceptance state function that is logical conjunction of predicates that characterize emulator states as acceptable and non-acceptable,

Lvl_u – level of emulator privileges.

In the model three emulator privilege levels are considered that are granted to: (1) non-privileged components in hypervisor; (2) system administrator; (3) kernel level OS. Attack on virtualization tools is set as the sequence of m events v_i, $i = 1,...,m$. In an attack at least one emulator in a hypervisor is transited into non-acceptable state. As a result, intruder gets escalated privileges till the level Lvl':

$$Attack = (\{v_i\}_{i=1}^{m}), v_i \in V_g,$$
$$\exists u \in H : Sq(Tr(s_{t+m}, v_m)) = false, Lvl' = Lvl_u \quad (1)$$

That model indicate that hypervisor stability towards attacks on virtualization tools is defined by: Cardinality of set V_g , permissions granted to emulators that process events from set V_g, vulnerabilities of software code design, written to automatizes emulators' processes. In this model artifact is defined as the block of code that makes state transition of at least one emulator possible. After that, each attack on virtualization tools is based on the vulnerability in artifact. It is evidently that not every artifact is, in fact, vulnerable. Consequently, the set of artifacts is reflected subjectively on the set of hypervisor vulnerabilities that can be used to make attacks on the VM's internal infrastructure.

Therefore, the emulator artifacts that are located in one component increase this component's amenability to possible attacks. As we see, the primary concern to mitigate security risks of hypervisor is

questions of software code design and development.

4. Ishikawa Model

Research in security of virtualization technology concentrates mostly on particular vulnerabilities exploiting. Consequently, there is often excessive emphasis of effort on vulnerabilities, or a vulnerability-driven approach in cloud computing services, whereas little effort has been done to identify general root problems of security issues. System vulnerabilities and incidents are paid attention at a micro level rather than addressing larger scale threat scenarios and patterns and further risk mitigation strategies development.

Thus, in this research we apply Fishbone or Ishikawa diagram to determine Security characteristic using a structured approach. Our motivation came from its main advantage to outline the root causes of a problem, security issue, in our case.

The Fishbone diagram has been originally used to identify and group the causes of quality problem on the production line. Thereafter, it has been widely adopted in Quality Management. This methodology was named after Kaoru Ishikawa, a Japanese quality control statistician, the man who pioneered the use of this chart in the 1960's [14]. The Fishbone diagram is an analysis tool that provides a systematic way of looking at effects and the causes that create or contribute to those effects. Because of the function of the Fishbone diagram, it may be referred to as a cause-and-effect diagram [15].

Hence, we apply Ishikawa diagram for hypervisor security risks analysis. This methodology outlines in diagrammatic form the causes that may generate a given outcome. We stated the outcome as a compromised hypervisor. Furthermore, each main cause we corresponded to a threat, defined by STRIDE Model: Spoofing, Tampering, Repudiation, Information Disclosure, Denial-of-Service, and Elevation of Privileges. The diagram identifies hypervisor security concerns as those uncertain events that could result in occurrence of the impact.

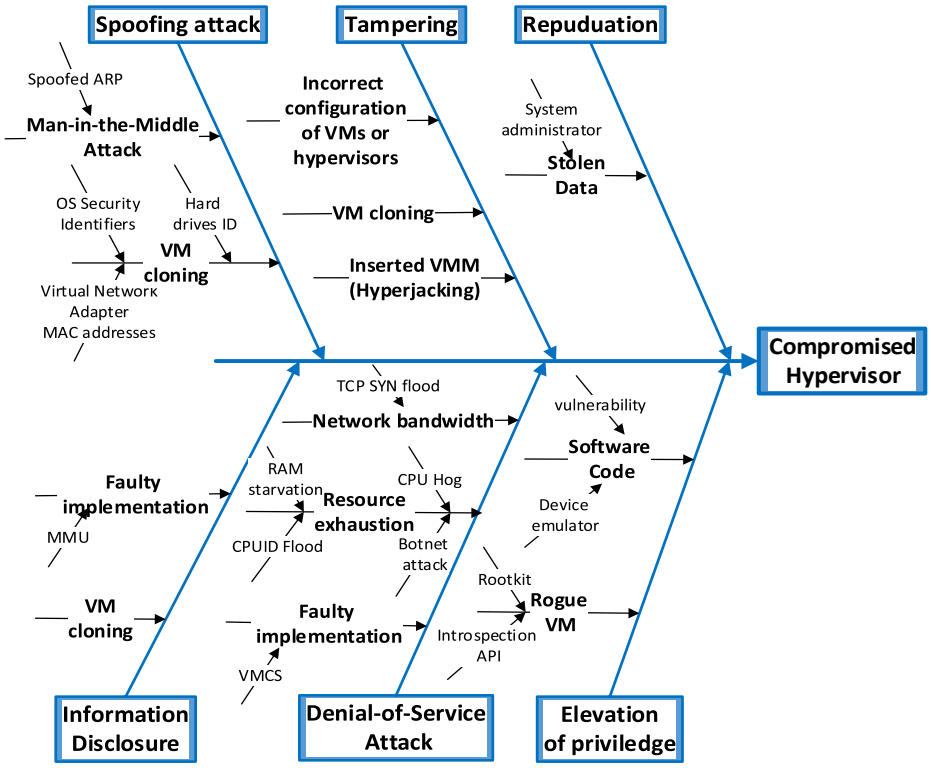

Fig. 2. Hypervisor security cause effect analysis based on Ishikawa diagram.

5. Conclusion and Future Research

Hypervisor is a key underlying technology of virtualization that enables several operating systems to consume the same hardware resources. In fact, hypervisor could be considered the heart of cloud computing, that is based on virtualization platform. As the corporations are moving infrastructure and services to the "Cloud", the security issues of protecting corporate data and privacy should be under the highest priority for data centers suppliers, for corporate CIOs, for technology vendors. Multiple stakeholders have to be involved in security risk mitigation process and cross-functional process has to be considered for successful cloud security enhancing. However, so far security issues are tried to be solved in isolated way. Moreover, there has been little research done to analyze the whole picture of threats and formal attack modeling, whereas much attention paid to exploiting certain vulnerabilities and particular attacks. We implemented double threat model design to outline where the potential risks come from. Firstly, we applied STRIDE methodology, proposed by Microsoft, to categorize threats. Secondly, we applied cause and effect analyses, developed by Professor Ishikawa to outline the causes that adverse hypervisor.

From diagram, we see that most of the cases come from vulnerable software code design and product architecture. Thus, the preventive security countermeasures have to be considered at the earlier stages before going to production. Our threat model can be used for developing security risk mitigation strategies in virtualization environment. We see two possible directions for further research. The first topic could address design of proper cross-functional stakeholders' collaboration for enhancing protection of different types of cyber security attacks, additionally, applying Ishikawa diagram not only for hypervisor, but also for cloud computing security analyses. The second topic could address applying quantitative risk analyses together with Ishikawa diagram to calculate and decrease the probability and impact of events that adverse hypervisor.

References

[1] National, N. (2001). *Institute of Standards and Technology, Guide to Security for Full Virtualization Technologies.*

[2] Rosenblum, M., & Garfinkel, T. (2005). Virtual machine monitors: Current technology and future trends. *Computer, 38(5),* 39–47.

[3] Zhang, F., Chen, J., Chen, H., & Zang, B. (2011). Cloudvisor: Retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization. *Proceedings of the 23rd ACM Symposium on Operating Systems Principles* (pp. 203–216).

[4] (2011). *Virtualization Special Interest Group PCI Security Standards Council, Standard: PCI Data Security Standard* (2nd ed.).

[5] Swiderski, F., & Snyder, W. (2004). *Threat Modeling.* Microsoft Press.

[6] Pearce, M., Zeadally, S., & Hunt, R. (2013). Virtualization: Issues, security threats, and solutions. *ACM Comput. Surv, 4(2)*, 39.

[7] Kaur, A., & Sharma, V. (2015). Hypervisor security framework. *Proceedings of International Conference on Networking and Computer Application.*

[8] Jaydip, S. Security and Privacy Issues in Cloud Computing Innovation Labs, Tata Consultancy Services Ltd. Kolkata, INDIA. Sheet. Retrieved from https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf

[9] Joshi, M., Kumar, L., & Bharti, R. (2015). Understanding threats in hypervisor, its forensics mechanism and its research challenges. *International Journal of Computer Applications, 119(1).*

[10] Chandramouli, R. (2014). *Draft Nist Special Publication 800-125-A Security Recommendations for Hypervisor Deployment.*

[11] Wimmer, M. (2008). Virtual security. *Proceedings of the 1st Conference on Computer Security Incident Handling: Vol. 20.*

[12] (2015). *Management Association, Information Resources, Standards and Standardization: Concepts, Methodologies, Tools, and Applications* (1st ed.). IGI Global.

[13] Samual, T. K. *et al.* (2006). SubVirt: Implementing malware with virtual machines. *Proceedings of the 2006 IEEE Symposium on Security and Privacy* (pp. 327-341).

[14] Juran, J. M. (1999). *Juran's Quality Handbook* (5th ed.). McGraw-Hill.

[15] Watson, G. (2004). The legacy of ishikawa. *Quality Progress 37(4).*

Svetlana Kolesnikova was born in St.-Petersburg, Russian Federation. She received the B.S. degree in mathematics from National Research University of Information Technology, Mechanics and Optics (ITMO Univ ersity), St.-Petersburg, Russian Federation. Afterwards, she received M.S. degree in information technology from Technical University Hamburg-Harburg, Germany and MBA (Master of Business Administration) in technology management from NIT (Northern Institute of Technology), Hamburg, Germany. Svetlana was awarded SIEMENS scholarship "youth and knowledge" to complete her education abroad. She used to work for Siemens, Germany, and for Carlsberg Group, Russia. She is currently pursuing the Ph.D. degree with the Department of Computer Systems Design and Security, ITMO University. Her research interests include cloud computing, virtualization, corporate security, information security and quality management. S. Kolesnikova has over 10 scientific works.

Danil Melnik was born in Krivoy Rog, Ukrain. He received the B.S. degree in computer science and the M.S. degree in information security from National Research University of Information Technology, Mechanics and Optics (ITMO University), St.-Petersburg, Russian Federation. He is currently pursuing the Ph.D. degree with the Department of Computer Systems Design and Security, ITMO University. His research interests include cloud computing, virtualization and information security.

Roman Kulikov was born in St.-Petersburg, Russian Federation. He received the B.S. degree in Computer Science and the M.S. degree in Information Security from National Research University of Information Technology, Mechanics and Optics (ITMO University), St.-Petersburg, Russian Federation. He is currently pursuing the Ph.D. degree with the Department of Computer Systems Design and Security, ITMO University. His research interests include cloud computing, virtualization and information security. R. Kulikov has 5 scientific works

Yurii Gatchin was born in Priiskovii, Russian Federation. Yuri Gatchin is a Ph.D, senior researcher, associate professor, doctor of science, professor. Gatchin graduated from Leningrad Institute of Fine Mechanics and Optics in 1975. He is the head of the Department of Computer System Design and Security, dean of the Faculty of advanced training of teachers. Y. Gatchin has over 80 scientific works and 4 inventor's certificates. He is a recipient of numerous awards and honors.