*Journal of Innovative Engineering and Research (JIER)*
*Vol.- 5, Issue -1, April 2022, pp. 5- 10 (6 pages)*

# A Security-focused Review on Virtual Machines

MAYANK YADAV

*Department of Software Engineering, Delhi Technological University, New Delhi, India*
*Correspond Author Email: mayankyadav_2k21swe13@dtu.ac.in*

***Abstract*—Within the cloud context, virtualization is crucial. The article discusses a range of virtual machine security techniques which will be utilized in a cloud environment where we'll access virtual hard discs and virtual servers. It examines kernel attacks, critical concerns, and the way designs are accustomed to solve virtualization problems. During this article, we'll examine the protection issues that include hardware virtualization. We explore recent attacks on a range of virtualization technologies.**

***Index Terms*— Hardware virtualization, operating systems, virtual machine security, kernel attacks**

## I. INTRODUCTION

Virtualization is a potentially new technology that increases the performance of computer servicesprovided to consumers. Because virtualization abstracts physical resources, the identical services can care for many physical hardware platforms. Virtualization may additionally be made to run services in parallel on the identical physical hardware by controlling access to physical resources. It permits the simultaneous execution of several operating systems on the identical physical host. This permits for more efficient use of resources.

To utilize the cloud, you want to have a browser with limited capability. During this project, we hope to convey a summary of security concepts, structures, and approaches.

We have an interest in current virtualization platform exploits. Material Amazon [1] could be a cloud service provider that has SAAS, PAAS, and IAAS services. Applications (Software as a Service—SaaS), platforms (Platform as a Service—PaaS), and virtual machines with storage capabilities (Infrastructure as a Service—IaaS) are often ordered on a pay-per-use basis from the cloud operator using these.

Virtual machine monitors (VMMs) are hypervisors that allow several operating systems to control on the identical host. Hypervisors are classified into two types.

The foremost common type of hypervisor operates directly on the hardware. On this, we may run a range of virtual computers [1]. VMware and Microsoft's Hyper-V hypervisor are samples of type 1 hypervisors. Running above the package is permitted within the second kind of hypervisor. VMware workstation, virtual box, and other type 2 hypervisors are examples.

## II. SECURITY ARCHITECTURES

In virtualization, five primary security designs are frequently used; they are HIMA (two), KVMSEC (two), LARE (two), XENaccess (two), and Vmscope (two).

### A.HIMA

The idea for HIMA is that the integrity of Virtual Machines (VMs) running on top of the hypervisor. HIMA [2] is accountable for two functions:

(1) keeping track of guest events
(2) Guest memory security.

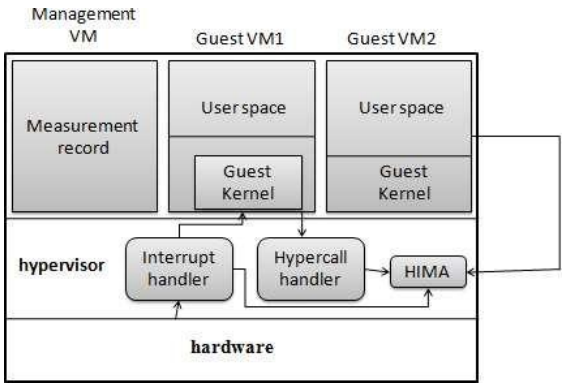



**Figure 1**: HIMA structure

HIMA is isolated from the targets being measured during this figure. It saves kernel component code segment hashes. The user programs are run within the guest virtual machines.

**Advantage:**

•A dedicated administration VM is present to trace the occurrences.

Disadvantage:

•It's not excellent with writable memory pages.

To handle privileged events on guest VMs, HIMA adds hooks into the hypervisor's code. The HIMA intercepts hypervisor service requests (for example, hypercalls and VMExits), system calls, and hardware interrupts. The created measurement lists are retained within the management VM for validation purposes.

### B. KVMSEC: SECURITY EXTENSION FOR LINUX KERNEL VIRTUAL MACHINES

The ultimate purpose of this architecture (KvmSec) [2] is to make safer guest virtual machines. KvmSec includes the subsequent features as standard: It's a transparent guest machine architecture; it's difficult to access from a compromised virtual machine; and it should collect data, assess it, and act on guest machines as a consequence.
The most widely used open-source virtualization designs, Xen and KVM [1], employ Full-virt technology, which takes advantage of CPU virtualization capability (AMD-V and Intel-VT).

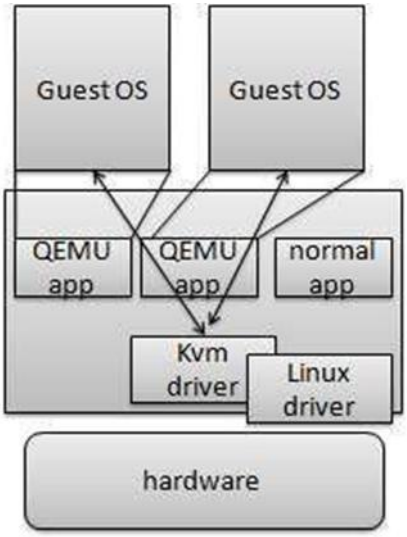



**Figure 2:** Architecture of KVMSEC

**Advantage:**
•It can collect data and reply on guest machines, but its heart is on the protected host PC.
Disadvantage:
•The system's overall performance is poor.

### C. LARE

LARE [3] architecture takes a hybrid approach, giving security tools the pliability to undertake to try to do all active monitoring while still benefiting from the increased security of an isolated virtual machine.

**Advantage:**
• The hook may be a host-based intrusion detection system that's accustomed to detect and stop attacks in real-time.
Disadvantage:
• Active monitoring isn't possible with these designs.

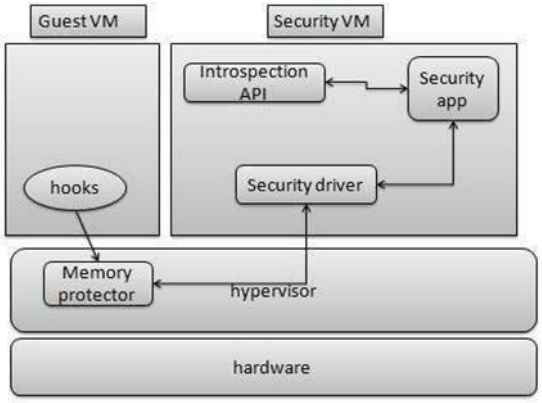



**Figure 3**: LARE Architecture

### D. XENACCESS

This architecture is concentrated on the event of XenAccess[3], a monitoring library for Xen-based operating systems.

**Advantage:**
• Monitoring of virtual machines
Disadvantage:
• Because it's para-virtualized, it's at risk of kernel assaults.

### E. VM SCOPE

This architecture consists of some virtualization-based monitoring systems referred to as VMscope[3], which offer us with the identical deep inspection capability as current internal monitoring tools (e.g. Sebek) while being as transparent and tamper-resistant as existing external monitoring tools (e.g. a network sniffer).

**Advantage:**
• Virtual machines are constantly monitored.
Disadvantage:
•Through a trust computing foundation, attackers can gain access to VMscope.

## III. VIRTUALIZATION CONCEPTS

A virtual machine (VM) could be a computer resource abstraction that permits many services to manage the identical actual hardware infrastructure at the identical time. Process virtual machines and system virtual machines are the 2 forms of virtual machines. Because it executes only 1 process, a process VM has the identical lifespan because the corresponding process. This kind of virtual machine might also be found in well-known programming platforms like Microsoft.NET [4]. System virtualization could be a kind of virtual computer that has a full OS and several other processes. The processing system that runs a virtual machine is named guest, whereas the host is platform that allows the VM to run.

Hypervisors enable hardware virtualization by allowing them to share hardware resources. Hypervisors are software components that intercept all hardware access requests from VMs and arbitrate these requests to physical devices.

### A. GUEST ENVIRONMENTS

A guest environment is defined by each virtual machine, which consists of a package and its programs. All of the guests are segregated from each another while sharing the hypervisor's virtual platform.

A hosting package usually includes a more privileged role than guest VMs to watch and control hardware resources directly or through the hypervisor. The hosting package might potentially be native software, like VMware WS, or a privileged virtual machine, like Microsoft Hyper-V [Microsoft 2008] or Xen [5].

### B. MONITOR FOR HYPERVISORS AND VIRTUAL MACHINES

The hypervisor, as previously stated, are a software component that intercepts all hardware access requests from VMs and mediates these requests to physical devices. The VMM's responsibilities include selective hardware resource control, the supply of duplicated platforms, and therefore the sharing of hardware resources amongst guest operating systems. Furthermore, VMMs may administer and maintain the programs on the visitors' computers [1].

Vendors provide management interfaces for his or her solutions to configure and manage guest VMs. Privileged users can create, demolish, and alter virtual computers and virtual infrastructures. Management interfaces are situated at various levels of the software stack that wishes to use virtualization technologies. One method of classifying them is to work out whether management interfaces (and maybe virtualization technologies) are associated with a group of software packages.

### C. NETWORK

Virtual networks allow users to attach VMs within the same manner as physical networks do; networking is additionally possible within one virtual server host moreover between several hosts. To place it in a different way, network virtualization encases traditional networking components like switches and routers for virtual appliances to link VMs.
VLANs in virtual networks are frequently inbuilt within the identical manner as they're in physical networks. Furthermore, virtual computers can have one or more virtual Ethernet adapters, each with its IP and MAC address, with increased flexibility, scalability, and redundancy.

Storage virtualization isolates physical storage components and offers one device which will be used directly or over a network. However, this conceptual simplicity comes with the value of enhanced data management and distributed access requirements [2]. VMware, for instance, enables datastores, which enable the transparent allocation of board space for VMs to access an intensive choice of physical storage options.

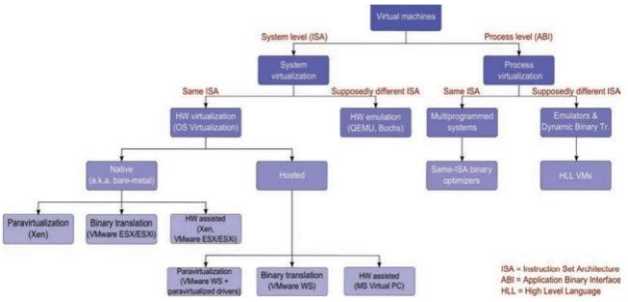



**Figure 4**: Concepts of virtualization

## IV. VIRTUAL MACHINES DETECTION

To begin, transparency is critical for interoperability and ensuring that old software continues to work effectively in a heavily virtualized environment. A second, more important reason for our talk is that anti-virus developers rely significantly on virtualization to discover new vulnerabilities and rootkit strategies. Several VMM-based malware detectors [Sidiroglou et al. 2005; Dagon et al. 2004] and malware analyzer environments [iSecLab 2007; Song et al. 2008; Offensive Computing 2003; Dinaburg et al. 2008] make use of transparency to identify and evaluate malware [5]. As a result, establishing whether or not a virtualized execution environment exists is critical.
Because virtualization is now so widely utilized, it's not just in malware developers' interests to avoid virtualized systems. As a result, malicious software in virtual environments tries to mimic normal behavior to propagate extensively and cause large-scale infestations [6]. As a result, anti-virus providers, like McAfee DeepSAFE [McAfee 2011], still continue to move their products into hypervisor address space, allowing them to operate at greater privilege levels (ring -1) than infected VMs while remaining transparent.

## V. EXPLANATIONS FOR SYSTEM VIRTUOSITY

System virtualization is used for several objectives, including the consolidation of guest operating system and software debugging should be separated.
A modern software program, such as Linux, is exceedingly sophisticated, resulting in increased vulnerability.

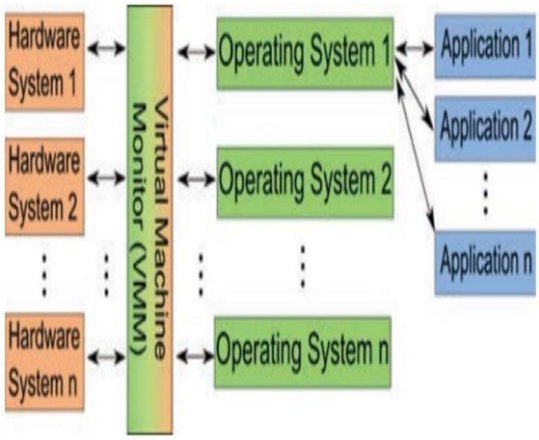



**Figure 5**: The additional layer of abstractions

System virtualization enables many operating systems to be installed on a single VMM by reducing the reliance of operating systems on a system's physical state [3]. Allowing many VMs to run on the same hardware has numerous benefits. Because of the abstraction from the hardware state, many operating systems may coexist on the same hardware, and a single VMM can function on multiple physical systems at the same time [6]. Virtualization converts the one-to-one mapping of operating systems to hardware to a many-to-many mapping by employing a VMM to mediate between the OS and then the hardware.

1.Storage virtualization:

gives a logical representation of physical storage This is frequently a single volume that spans many physical devices.

2.Application virtualization:

This is a method of virtualizing the underlying operating environment of an application. As a result, the software may run in a separate container.

3.Desktop virtualization:

Remote desktop access is similar to program streaming, except that it is directed towards the user.

## VI. FACTORS INCENTIVISING THE USE OF VIRTUALIZATION IN SECURITY

By enclosing operating systems within virtual machines, strong isolation may be achieved between applications running on the same hardware, as well as between guest operating systems and the hardware itself.

A VMM's resource control attribute ensures that nothing happens within the VM in which the VMM cannot intervene. VMM has a thorough knowledge of the operation. VM actions are watched independently of the guest OS state, and the state may be readily preserved and recovered. [3].


**Figure 6**: The initial steps in the threat modeling approach

- define the system's security requirements;
- communicate Aspects of the virtual machine's security architecture;
- analyze components to look for potential security issues;
- discover fears that VM infrastructures will be jeopardized;
- manage security-related mitigations

## VII. THE SOURCE AND TARGET OF THE ATTACK WERE SUPPORTED BY ATTACK CLASSIFICATION

• Attacks against the VMM can be carried out by an attacker with the speed of a guest VM. Because the VMM isolates the surroundings, this is frequently a massive attack.

• On some hypervisors, a privileged guest VM is available. During this form of attack, a guest VM escapes the hypervisor and executes code on the host OS.

• To capture control of the VMM, an assault on the host is often used.

• An attack can breach the VMM's isolation and impact the behavior of another guest VM maintained by the same VMM.

The attacker wants to run arbitrary code. To imitate the functioning of guest virtual machines, a hypervisor intercepts specific command from them.

Assembly instructions in Parallels Desktop [5] induce a VMM abort, which may be leveraged to launch DoS attacks. When a guest VM with a GPU in pass-through mode is launched [1].

## VIII. THE INFLUENCE OF VIRTUALIZATION TECHNOLOGIES ON HOST SECURITY

A conventional computer's gadgets are configured to run in privileged mode. Because devices may be set by an entity not trusted by the entire system, including the guest VMs, virtualization modifies this idea [4]. Virtualization of devices is required in some form. While virtualizing I/O operations increases utilization, the isolation required between the host and the guest, VMs, adds a new degree of complexity.
As a solution, CPU makers provide hardware support for I/O Virtualization [5]. For example, Intel Virtualization Technology for Directed I/O has an Input/Output Memory Management Unit that links the I/O bus.

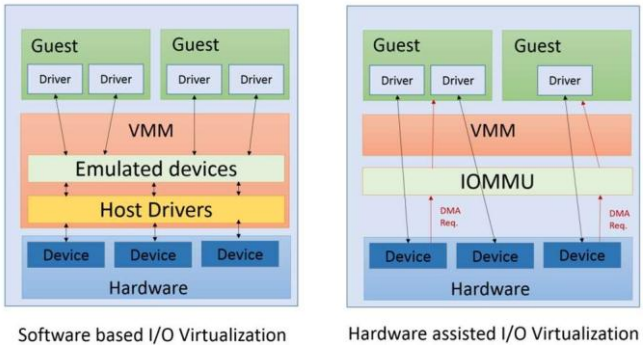
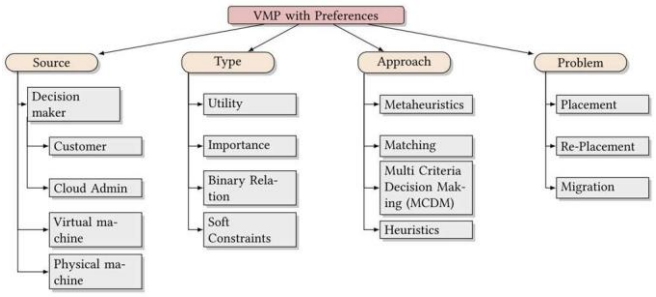



**Figure 7**: The engine processes DMA requests from devices anddirects them to the specified domain alone

The IOMMU may be a hardware safeguard that cannot work on its own: it requires assistance from the Firmware and hence the Software System. Project Thunderclap [2] developed an open-source platform capable of developing a software model for a wide range of DMA-enabled peripherals, allowing it to test everything from simple DMA requests to sophisticated interactions.
The Trusted Computing Group [1] may propose a set of specifications as Trusted Computing. These standards' solutions aim to safeguard computer systems through the collaboration of software and hardware. The use of a VMM as a trustworthy platform component is demonstrated in Project Terra. This Reliable VMM improves on the classic.




To save money, security technology assistance is being implemented at centres. The VMP is crucial for cloud design to remain viable. The usage of virtualization technologies has resulted in a reduction in resource utilization. These advantages have come at the expense of increased security complexity. When developing innovative virtualization technologies, security should not be overlooked. [1].

| | objective | Virtualization Type | Advantages | Disadvantages |
|---|---|---|---|---|
| **HIMA** | guest memory safety | Full virtualization | Kernel assaults should be avoided. | App writable memory pages are not supported. |
| **Xen access** | Xen Access contains information about virtual memory. | Paravirtualization | Monitoring of virtual machines | It is vulnerable to kernel assaults since it is para-virtualized. |
| **Lare** | A hybrid architecture that allows security products to do active monitoring. | Full virtualization | Detection and prevention ofattacks in real-time | Security mechanism The impact on system performance is of concern |
| **VMscope** | is capable of externally evaluating internal system events | Full virtualization | Active monitoring | An assault on the kernel occurs when attackers get access to the interrupttable. |
| **Kvm Sec** | It protects guest virtual machines from dangerous threats like viruses. | Full virtualization | It can collect data and respond on visitor machines. | The system's performance is inadequate. |

## IX. CONCLUSION

We investigated the benefits and drawbacks of several hypervisors and virtual machine designs. As a result of this investigation, a comparative evaluation of the various hypervisors assures the security mechanism of the cloud environment. We focused on probable flaws and active attacks in hardware virtualization systems. We built the presentation around their intended audience, which may include the visitor, the host operating system, and the many networks that make up a virtual infrastructure.

While virtualization is not a new concept, recent hardware and software advancements have given it fresh life. The VMM's validity is crucial for secure virtualization. Cloning VMs may be dangerous if done wrong since a cloned VM is difficult to identify from an original.

Cloud data has become of such high quality as a result of virtualization technologies that hardware- level virtualization solutions will benefit. One of the study's key findings is that the number of reported vulnerabilities and attacks on various virtualization platforms is now rather high, and it is expected to rise significantly in the future as the platforms' complexity and new services increase. Given the expanding popularity of virtualization technologies, particularly the proliferation of cloud computing services, it's vital to be aware of and address these security problems.

Preferences can be used as a guideline to improve the performance of a system. Such preferences are frequently inspired by issue meta-analysis and acknowledged as preferred machine settings or configurations. In a physical system, the operating system places a high level of faith in the hardware. Similarly, the operating system on a virtual machine trusts the virtual hardware, and hence the VMM. Because it is a single point of failure, a hostile, hacked, or otherwise, defective VMM may interfere with the VM.

## REFERENCES

[1] Pearce, M., Zeadally, S., and Hunt, R. 2013. Virtualization: Issues, security threats, and solutions. ACM Comput. Surv. 45, 2, Article 17, Pages 39, February 2013.

[2] Abdulaziz Alashaikh, Eisa Alanazi, and Ala Al Fuqaha. 2021. A Survey on the Use of Preferences for Virtual Machine Placement in Cloud Data Centers. ACM Comput. Surv. 54, 5, Article 96 , 39 pages, May 2021.

[3] Federico Sierra-Arriaga, Rodrigo Branco, and Ben Lee. 2020. Security Issues and Challenges for Virtualization Technologies. ACM Comput. Surv. 53, 2, Article 45, 37 pages, May 2020.

[4] Steve Harrington, Linette Williams, and Mike Murphy. Solving the HA Challenge: Placement Groups for Virtual Servers.

[5] Gorka Irazoqui Apecechea, Mehmet Sinan Inci, Thomas Eisenbarth, and Berk Sunar. Fine-grain cross-VM attacks on Xen and VMware are possible!IACR Cryptology ePrint Archive, 2014.