RESEARCH AND EXPLAIN THE ROLE OF VIRTUALISATION AND EXPLAIN ITS BENEFITS FOR CYBERSECURITY

Mossé Cyber Security Institute

Aaron Amran Bin Amiruddin
nxCLnZGLgyOUMpnDw16rtDvYuTF2

Steps To Enable Windows Virtualisation

Enabling Windows virtualisation is done through the BIOS (Basic Input/Output System). The BIOS is a critical piece of software embedded in a computer's motherboard, acting as a bridge between the operating system and hardware. Enabling CPU virtualization may require accessing the BIOS settings.

Step 1: Access the BIOS or UEFI settings

Start by restarting your computer. As it begins to boot up, press the key that takes you into the BIOS setup. The most common keys are F1, F2, Del, Esc, or F10, but this can vary depending on your manufacturer. If you're unsure, check your manual or look for prompts during the boot process.

Step 2: Find the CPU settings section

Once inside the BIOS menu, look for categories such as "Advanced," "Processor," or "CPU Configuration." Since your mouse is usually disabled in BIOS, you'll need to use the keyboard to navigate through these sections.

Step 3: Locate the virtualization option

In the CPU-related settings, search for options like "Intel Virtualization Technology," "VT-x," "AMD-V," "SVM," or simply "Virtualization." These settings are typically found in the CPU section, and the exact names will depend on whether you're using an Intel or AMD processor.

Step 4: Enable virtualization

To enable virtualization, change the option from "Disabled" to "Enabled." If there are multiple virtualization options available (such as VT-d), refer to your processor's documentation to determine which ones best meet your needs.

Step 5: Save your changes and exit

After enabling virtualization, be sure to save your changes before exiting the BIOS. This is usually done by pressing the F10 key or selecting the "Exit" menu, where you will be prompted to confirm saving the changes.

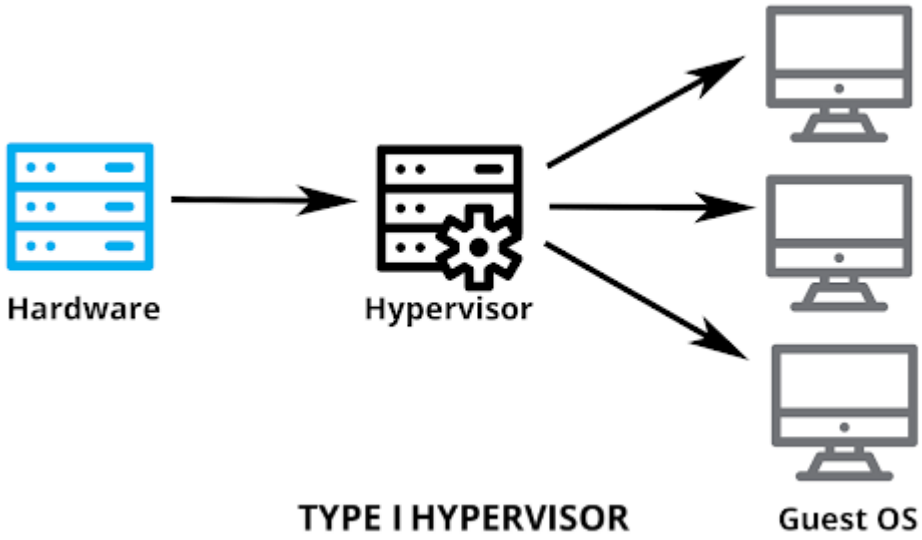
Step 6: Reboot your computer

Once you've saved and exited, allow your computer to reboot normally. With virtualization now enabled, your system is ready to support tasks like running virtual machines or hypervisors.

Hypervisors

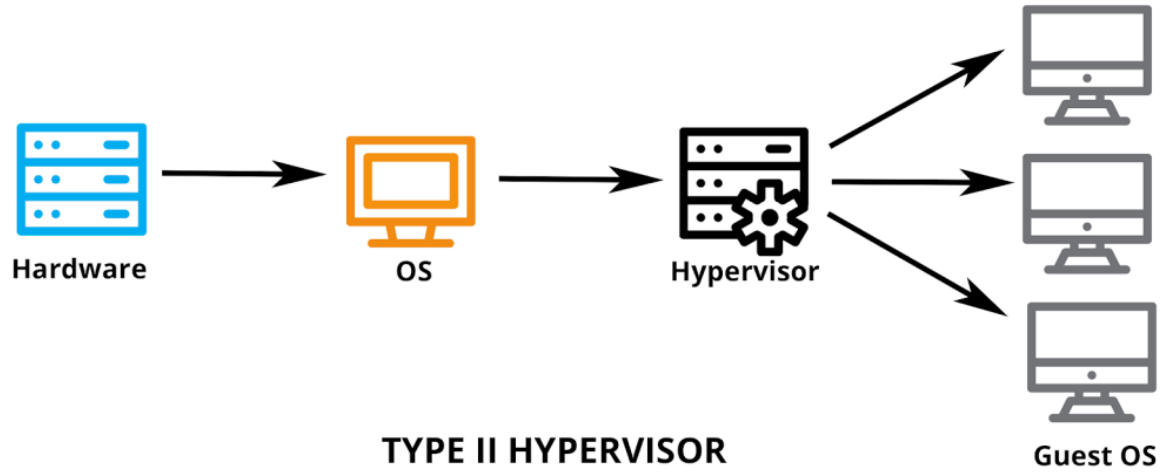
In this chapter, the different types of hypervisor, their usage, how they function, and the most common types of type-1 and type-2 hypervisors will be explained. There are two main types of hypervisors: Type 1 (bare-metal) and Type 2 (hosted). A Type 1 hypervisor runs directly on the host's hardware, functioning similarly to a lightweight operating system, while a Type 2 hypervisor operates as a software layer on top of an existing operating system, much like any other application.

Type 1 hypervisors are the most commonly deployed because they are installed directly on the hardware, where an operating system would typically reside. Since bare-metal hypervisors are isolated from the potentially vulnerable host operating system, they tend to offer superior security. Additionally, they generally perform better and more efficiently than hosted hypervisors. This is why most enterprises opt for bare-metal hypervisors for their data center operations.



The most common examples of type 1 hypervisors are VMware's ESXi and Microsoft's Hyper-V.

In contrast, Type 2 hypervisors run on top of an existing host operating system. While this setup allows for the installation of additional operating systems on the hypervisor, it introduces extra latency due to the added layer of the host OS. Hosted hypervisors, also known as client hypervisors, are often used for end-user environments and software testing, where the latency is less of an issue.



TYPE II HYPERVISOR

Examples of type-2 hypervisors include Oracle Solaris Zones, Oracle VM Server for x86, Oracle VM Virtual Box, VMware Workstation, VMware Fusion and more.

Both types of hypervisors benefit from hardware acceleration technology, which enhances processing speed. A specific type of hardware accelerator, called a virtual Dedicated Graphics Accelerator (vDGA), handles 3-D graphics processing, freeing up the main system and improving image display speed. This technology is particularly beneficial in industries like oil and gas exploration, where fast data visualization is crucial.

Both hypervisor types can run multiple virtual servers for different tenants on a single physical machine. In the case of public cloud services, providers lease virtual server space to various companies, with each virtual server potentially hosting workloads for multiple businesses. However, this shared environment can lead to a "noisy neighbor" effect, where the performance of one tenant's workload negatively impacts others. This shared resource model also introduces greater security risks compared to dedicated bare-metal servers.

A dedicated bare-metal server, which is under the exclusive control of a single company, will always outperform a virtual server that shares resources with others. Furthermore, bare-metal servers can be optimized for better performance, which is not possible with shared public cloud servers. Companies that must comply with regulations requiring the physical separation of resources will need to use their own dedicated bare-metal servers instead of shared virtual environments.

Differences Between Type-1 And Type-2 Hypervisors

Feature	Type-1 Hypervisor	Type-2 Hypervisor
Deployment	Installed directly on the hardware	Installed as an application on an operating system
Hardware Compatibility	Typically comes with a hardware compatibility list from various vendors	Hardware-agnostic, works with most systems
Setup	Requires some technical expertise to set up	Simple setup, similar to installing any other application on the host operating system
Management	Managed primarily via a web interface	Managed through a console application on the host operating system
Performance	Offers better performance since it has direct access to hardware resources	Performance may be slower due to the additional layer of the host operating system between the hardware and the hypervisor
Security	Hypervisor and virtual machines are fully isolated, reducing security risks	The guest operating system is isolated from the host operating system, but other applications running on the host may introduce additional vulnerabilities, increasing security risks
Stability	Only the hypervisor failure can impact guest virtual machines	Failures in the hypervisor, host operating system, or even applications can cause issues with the virtual machines
Multipurpose Usage of Hardware	Dedicated solely to virtualisation tasks	Other applications can run on the host operating system alongside the hypervisor
Additional Features	Often includes clustering, integrated software-defined storage, built-in disaster recovery, centralised management for multiple hypervisors, and role-based access credentials	Primarily focused on virtualisation, with no additional integrated features

Benefits of Virtualisation in Cybersecurity

Virtualization in cybersecurity offers several distinct benefits that can significantly enhance security measures, improve operational efficiency, and facilitate better management of IT resources. Here's a detailed explanation of these benefits:

1. Isolation of Systems and Applications

Virtualization allows for the creation of isolated environments, known as virtual machines (VMs), on a single physical server. Each VM operates independently, with its own operating system and applications. This isolation means that if a cyberattack or breach occurs within one virtual machine, it does not directly affect other VMs or the host machine. For example, if a malware infection compromises one VM, it cannot easily spread to other VMs or the underlying host, reducing the potential impact of a cyberattack.

2. Enhanced Security Testing and Sandboxing

Virtualization provides an ideal environment for conducting security testing, vulnerability assessments, and penetration testing. Cybersecurity professionals can create isolated virtual environments to safely test malicious software or run security tools without risking damage to the primary system. This process, often referred to as "sandboxing," ensures that potentially harmful activities are contained and do not affect critical infrastructure. Researchers can analyze malware samples, simulate attack scenarios, or test different security configurations in a controlled, virtual environment, all while avoiding risks to production systems.

3. Improved Disaster Recovery and Business Continuity

Virtualization plays a crucial role in enhancing disaster recovery (DR) and business continuity plans. With virtualization, entire virtual machines (VMs), including their operating systems, applications, and data, can be easily backed up and replicated across different physical locations. In the event of a disaster, such as a hardware failure or cyberattack, these VMs can be quickly restored to another physical machine or cloud infrastructure, minimizing downtime and ensuring that critical business functions continue uninterrupted. This ability to rapidly recover data and systems ensures resilience against various cybersecurity threats.

4. Faster Incident Response

When a security breach occurs, a rapid response is essential to minimize damage. Virtualization enables quicker incident detection and response by allowing security teams to quickly isolate compromised systems. For instance, if a virtual machine is detected as being compromised, it can be powered off or quarantined without impacting the rest of the environment. This isolation helps contain the threat more effectively and allows for faster remediation processes. Additionally, virtualization platforms often come with monitoring tools that provide visibility into system activity, making it easier for security teams to spot and address suspicious behavior.

5. Granular Control and Monitoring

With virtualization, organizations gain fine-grained control over their systems and networks. Administrators can configure specific security settings for individual virtual machines, networks, and storage environments, tailoring security policies for each virtualized resource. This level of control is especially beneficial for segmenting sensitive data or applications, which can be kept in isolated VMs

with stricter access controls. Additionally, virtualization platforms often come with advanced monitoring capabilities, allowing cybersecurity teams to track the behavior of virtual machines, identify potential vulnerabilities, and quickly spot signs of compromise.

6. Cost-Effective Security Infrastructure

Virtualization enables organizations to run multiple virtual machines on a single physical server, reducing hardware costs and increasing resource efficiency. From a cybersecurity standpoint, this consolidation of resources allows for more efficient use of security tools, such as firewalls, intrusion detection systems (IDS), and antivirus software. Rather than deploying these security measures on each physical server individually, they can be implemented at the virtual machine level, protecting multiple environments with a single set of tools. This reduces the overall cost of security infrastructure while maintaining strong protection.

7. Simplified Security Updates and Patches

Managing software patches and security updates can be a complex task, especially in large-scale environments. Virtualization simplifies this process by allowing administrators to quickly clone, update, and test virtual machines before applying changes to production systems. Patches can be applied in a non-production environment, tested for compatibility, and validated without disrupting the live environment. Once the updates are confirmed to be safe, they can be rolled out across all relevant VMs, ensuring a more consistent and timely patching process across the organization's infrastructure.

8. Increased Flexibility and Scalability

As cybersecurity threats continue to evolve, organizations must be able to scale their security measures quickly and efficiently. Virtualization makes it easier to deploy additional resources, such as VMs, firewalls, or intrusion prevention systems (IPS), as needed. Security teams can quickly spin up new virtual machines to handle increased workloads or to isolate systems for investigation, all while maintaining the flexibility to scale back when the threat has been mitigated. This adaptability is crucial in dynamic environments where new threats emerge frequently.

9. Seamless Integration with Cloud Environments

Cloud computing has become an integral part of modern cybersecurity strategies. Virtualization serves as the foundation for cloud-based services, allowing organizations to extend their security measures to both on-premises and cloud environments seamlessly. By leveraging virtualization technologies, businesses can maintain consistent security controls across hybrid infrastructures, monitor cloud-based resources, and implement unified security policies across both virtualized and physical systems. This integration simplifies security management and ensures that threats are detected and mitigated across all layers of an organization's infrastructure.

10. Access Control and User Privileges

With virtualization, security administrators can implement strict access control policies to regulate which users or systems have access to specific virtual environments. For example, virtual machines can be configured with different user privilege levels, ensuring that only authorized personnel can access sensitive information or perform high-risk actions. This level of control helps reduce the risk of insider threats and ensures that users operate within predefined security boundaries.

References

Broadcom, v. b. (n.d.). *What is a hypervisor?* Retrieved from vmware.com: https://www.vmware.com/topics/hypervisor

Buenning, M. (2024, October 16). *How to Enable CPU Virtualization in Your Computer BIOS*. Retrieved from ninjaone.com: https://www.ninjaone.com/blog/how-to-enable-cpu-virtualization-in-your-computer-bios/

Microsoft. (n.d.). *Enable virtualization on Windows*. Retrieved from support.microsoft.com: https://support.microsoft.com/en-us/windows/enable-virtualization-on-windows-c5578302-6e43-4b4b-a449-8ced115f58e1

Pankevych, O. (2023, July 20). *Hypervisors: Type 1 vs Type 2. [PART 1]*. Retrieved from starwindsoftware.com: https://www.starwindsoftware.com/blog/type-1-vs-type-2-hypervisor-what-is-the-difference/

Wright, C. (2019, June 8). *All You Need to Know About Hypervisors*. Retrieved from blog.resellerclub.com: https://blog.resellerclub.com/what-is-a-hypervisor-and-how-does-it-work/