Securing Leased Systems with FlexVer™

Raptor Engineering, LLC
https://www.raptorengineering.com

Overview

In this document we explore the revolutionary FlexVer™ security technology first introduced on our Talos™ mainboards, and how this technology can be used to offer truly secure VPS and bare metal leased offerings.

What is FlexVer™?

FlexVer™ is a new type of auditable, owner-controlled hardware security module. For an overview of the FlexVer™ and LPC Guard™ technologies, please refer to the following two documents:

https://www.raptorengineering.com/TALOS/documentation/flexver_intro.pdf

https://www.raptorengineering.com/TALOS/security_features.php

Existing Technologies

Traditionally, Virtual Private Server (VPS) instances have been considered fundamentally insecure from the perspective of the lessee (client). This is largely due to the architecture of typical VPS hosting systems built on virtualization technology; by the standard definition of a virtual machine, there is theoretically no way to distinguish between a safe and unsafe hypervisor or method to detect tampering to or extraction of data from the VPS memory and/or execution state. When leasing a VPS from any current provider, even if the provider's production hypervisor denies access to VPS memory contents and execution state, the provider still has the technical ability to target any VPS under the provider's control with a custom hypervisor image; such tampering would be undetectable from the perspective of the client. There are instances in which the provider itself may be compelled to access VPS memory, such as after receipt of a National Security Letter (NSL), warrant or related document, or the provider's employees may be subject to coercion, e.g. for financial gain or under threat of harm.

In a nutshell, within the traditional VPS model, there is no way for the client to know if their VPS is being monitored or attacked by either the provider or its employees. This lack of verifiable trust has relegated VPS leases to relatively untrusted tasks, and has forced leasing of full bare-metal machines where sensitive data is involved, even in situations where the leased bare-metal machine is too powerful for the task at hand.

Using FlexVer™ To Guarantee Integrity of Leased VPS Instances

FlexVer™ turns the existing VPS security model completely around, taking control from the provider and its employees and placing it solely in the hands of trusted, auditable hardware and software. Unlike solutions based on an unauditable, silicon vendor controlled root of trust

such as Intel and AMD's encrypted virtual machines, FlexVer™ allows a hosting provider to establish public, traceable audit logs for their root of trust, and for independent certification entities to directly verify this root of trust. When FlexVer™-based security is properly implemented at the organizational level, the addition of secret backdoor(s) or other malware to a FlexVer™-secured datacenter would be essentially impossible; any attempt to do this would be detected in the public audit phase at some point, and the provider attempting to add the backdoor would be publicly discredited. This is in stark contrast to existing solutions that rely on a fully trustworthy silicon vendor and use a secret master vendor key that, if hacked, leaked, or forcibly seized would render all systems relying that vendor key permanently and undetectably insecure.

Securing the VPS Host

At its core, securing a VPS starts by securing the hypervisor and host system against all forms of access to VPS memory and execution state. There are multiple ways to do this, but we recommend usage of a minimal hypervisor kernel and userspace that contains no functions other than the bare minimum required to execute virtual machines and connect them to the network. The kernel in use should have all possible memory protection features enabled, and should lack the ability to access process memory state. Similarly, the userspace tools should lack any ability to save or restore the virtual machine state, and the root account should be permanently locked out. We call this the “Minimum Trusted Image”, or MTI, and provide full source and build tools required to build a reproducible copy of the MTI for comparison against the MTI running on the production VPS host(s).

There is still one attack vector not handled by the MTI, and that is the system firmware. Modern system firmware excecutes at a higher privilege level than the MTI and is fully capable of subverting all MTI security features. As a result, we exclusively use servers that can operate with fully open source firmware, no binary firmware (“blobs”) required. Similar to the MTI, we provide full source and build tools to allow reproducible firmware images to be built and compared against the firmware images running on the production VPS hosts(s).

Using FlexVer™ to Prevent Compromise of Secured VPS Hosts

At this point all VPS instances running on the host are secured against data exfiltration and tampering, provided that the firmware and MTI hashes being provided to the client actually correspond to the firmware and MTI images running on the VPS host. This is where FlexVer™ comes into the picture – FlexVer™ can guarantee that the hashes provided to the client are in fact correct, thus making any tampering with the system firmware or MTI immediately detectable to the client. This is an ability not present on any existing system; all existing solutions that attempt to implement this functionality force you to rely on blind trust of the silicon vendor and their proprietary firmware implementing these verification checks; effectively, trust has simply been moved from the VPS host to the silicon vendor. The general consensus in the security community is that the silicon vendor would be technically able to modify their verification firmware to report incorrect data, therefore these solutions only offer a level of indirection to a determined adversary, not any additional real security.

Given the above detailed secure VPS host implementation, the chain of trust has passed into the FlexVer™ system itself. As a result, it becomes vital that known trustworthy FlexVer™ images are used within the VPS provider's hosts. As with the firmware and MTI, reproducible

FlexVer™ build sources and image hashes are publicly posted, but there is no way for the client to directly verify that those images were in fact used to provision the FlexVer™-enabled VPS host without purchasing exclusive access to the host machine and either scheduling a visit to the datacenter or having the provisioned host shipped to the client for physical verification.

We begin to address these concerns with dedicated security officers that are responsible for provisioning FlexVer™ on the VPS hosts; these officers verify that the FlexVer™ images provided publicly are in fact used to provision the VPS host machines. Once FlexVer™ starts up for the first time and generates its public/private keypair, all security officers that oversaw the provisioning process attest that the public key was generated by the FlexVer™ image stated; this attestation takes place via table of the machine UUID, FlexVer™ image hash, the public key of that particular machine, and a written signature of the security officers overseeing the provisioning operation. This table entry is then cryptographically signed by the same officers, providing proof positive that the chain of trust is now resident in these security officers.

For some use cases, even higher standards of proof will be needed. FlexVer™ allows a readout of the programmed image without destruction of or revelation of its internal private key; as such, an independent certification authority can physically verify that the correct image has in fact been programmed by an on-site visit or by physical shipment of the machine to the certification authority. An alternative form of verification is available to clients that have leased exclusive access to the VPS host in question; for a fee, the client would be allowed to physically verify the hash of the FlexVer™ firmware installed and download the associated public key straight from the FlexVer™ system. Once verified through either method, the machine can be trusted as long as it is not tampered with; any tampering would reset the FlexVer™ private key as explained in the technical information pages on FlexVer™, causing an uncorrectable cryptographic key mismatch and client-visible verification failure.

VPS Client Responsibilities

It remains the responsibility of the client to implement proper security measures as they would normally on a physical machine. FlexVer™ only guarantees that the VPS cannot access data and state that would normally be rendered inaccessible by the nature of the CPU and memory components on a physical system; as such, full disk encryption of the VPS along with use of a hardened kernel is strongly recommended. If any FlexVer™ image hash or signature shows a mismatch with the master tables, the VPS host should be assumed to have been compromised and the encryption keys to unlock the disk must not be entered. Provided that the keys are not entered into such a compromised instance, there would be no way for an adversary to access the data originally stored on the VPS. We recommend providing open source client-side utilities to VPS clients in order to automatically check the signatures and hashes returned from the VPS. This is because there are several signatures and hashes that need to be verified to ensure integrity of the VPS before transmitting any sensitive data such as encryption keys, and fully manual verification would be labor intensive enough to encourage the client to bypass this critical step.

Related Technologies

For maximum security, VPS hosts should also utilize DRAM scrambling and/or memory encryption to prevent various forms of direct attack on physical memory. Minimum hypervisor features and userland utilities should be present within the MTI to reduce the potential attack surface as much as possible; this also minimizes the risk of zero-day exploits being used against the VPS host itself. Care must also be taken to secure the communication channel between the VPS host and the client; we have chosen to use end to end encryption between the VPS host and the client, then place the VPS host's private key into the FlexVer™ protected TPM, but other methods are also available.

It should be noted that the risk of zero-day exploits is not unique to the system described herein, and in fact the proposed system allows for patching of all affected hardware should an exploit be found, unlike competing systems based on proprietary, signed firmware or hardware. Additionally, by using well-audited software and firmware components with many eyes inspecting the source code, any potential zero-day exploits may be located faster, patched faster, and their presence made known to clients in order to allow for damage mitigation efforts to start as quickly as possible, instead of the quiet, insidious damage over many years that tends to occur with zero-day exploits in fully proprietary systems.

Conclusion

FlexVer™ enables the use of VPS instances in a secure environment for the first time, establishing a public audit trail that can be verified by any interested party. This in turn allows computing resources of powerful systems such as OpenPOWER to be better utilized, lowering cloud provider TCO and consuming less energy per unit work. If you would like additional information on FlexVer™, want to license it for use in your datacenter, or would like to integrate it onto your next-generation computing product, please feel free to contact us at sales@raptorengineering.com.