HyperPS: A VMM Monitoring Approach Based on Privilege Separation

***Abstract*—Privilege separation has long been considered as a fundamental principle in software design to mitigate the potential damage of a security attack. Much effort has been given to develop various privilege separation schemes where a monolithic OS or hypervisor is divided into two privilege domains where one domain is logically more privileged than the other even if both run at an identical processor privilege level.**

However, as malware and attacks increase against virtually every level of privileged software including an OS and a hypervisor, we have been motivated to develop a technique, named as HyperPS, to realize true privilege separation in hypervisor on x86. HyperPS does not rely on hardware or a higher privileged software. The key of HyperPS is that it decouples the functions of interaction between VM and the hypervisor. As a result, HyperPS monitors the interaction, controls memory mapping when a page is allocated, and resists system information leakage attack. We have implemented a prototype for KVM hypervisor on x86 platform with multiple VMs running Linux. KVM with HyperPS can be applied to current commercial cloud computing industry with portability. The security analysis shows that this approach can provide effective monitoring against compromised attack, and the performance evaluation confirms the efficiency of HyperPS.

***Index Terms*—Virtualization, VM Protection, VM Security**