Review “Virtualization”

Name: Wenhui Zhang
Email: wuz49@ist.psu.edu

Paper Name：

Garfinkel, T., & Warfield, A. (2007). What virtualization can do for security. *The USENIX Magazine*, *32*(6), 28-34.

Contribution:

This paper reviews security benefits brought by introducing VMs. This paper then gives out a survey on security technologies supported by virtualization.

Motivation:

In data centers, different customers run their instances on the same physical machine, and insufficient isolation could lead to security issues. Thus people come up with the ideas of using system software to enable isolation instead of using system software to control sharing. One typical approach is VMs, which makes one physical resource appear as multiple logical resources, and in this way it enables isolation.

Related works:

VMs offer potential benefits over: (1) rule-based application-oriented access control schemes, such as domain and type enforcement (DTE); (2) system call interposition schemes such as Janus and Systrace; (3) mechanisms such as AppArmor and SELinux.

Methodology:

Isolation is achieved through virtualization, which makes an abstraction layer which decouples the physical hardware from the operating system to enlarge resource utilization and flexibility.
It allows multiple virtual machines, with heterogeneous operating systems to run in isolation, side-by-side on the same physical machine. Thus, each virtual machine has its own set of virtual hardware, each process executes on its own processor with its own (virtual) memory.
The host software which provides virtualization is often referred to as a virtual machine monitor (VMM) or hypervisor.

Results:

Using VMs, it achieves partitioning and isolation, and through partitioning and isolation, we achieve better security.
Partitioning: (1) multiple operating systems can be supported within a single physical system; (2) each Virtual Memory has its own memory space.
Isolation: (1) VMs are completely isolated from the host machine; (2) VMs are completely isolated from other virtual machines. If a virtual machine crashes, all others are unaffected; (3) there is no data leak across virtual machines.

Take away:

VM systems focus on isolation between VMs. As several VMs are sharing one real physical machine, this mechanism might introduce unstable performance. However, VMs introduce extra security to using one physical machine. At the meantime, security concern for VMs is rootkit is VMM rootkits.