**Analysis of Virtual Machine Rootkit Detection**

**Michael Malkowski, Rachel Pekarek, and Prashanta Gyawali**

**Terms:**

**Hypervisor:**  A hardware virtualization that enables multiple guest operating systems to run on a single host system at the same time. The guest operating system shares the hardware of the host computer such that each operating system appears to have its own processor, memory and other hardware resources. Type 2 Hypervisors, also known as hosted hypervisors, run within a formal operating system environment. In this type, the hypervisor runs as a distinct second layer while the operating system runs as a third layer above the hardware.

**Rootkit:** A rootkit is a type of malicious [software](http://www.webopedia.com/TERM/S/software.html) that is activated each time your system [boots](http://www.webopedia.com/TERM/B/boot.html) up. Rootkits are difficult to detect because they are activated before the system's [Operating System](http://www.webopedia.com/TERM/O/operating_system.html) has completely booted up. A rootkit may allow the installation of hidden files, processes, hidden user accounts, and more in the systems OS. Rootkits are able to intercept data from terminals, [network](http://www.webopedia.com/TERM/N/network.html) connections, and the [keyboard](http://www.webopedia.com/TERM/K/keyboard.html). (1) A Virtual machine rootkit can drop a VMM (virtual machine monitor) underneath a Windows or Linux installation. Once the target operating system is hoisted into a virtual machine, the rootkit may become impossible to detect because its state cannot be accessed by security software running in the target system.

**Introduction:**

Virtual Machines simulate a machine (abstract or real) that is typically different from the target machine it is being simulated on. Virtual machines can emulate the [computer architecture](http://en.wikipedia.org/wiki/Computer_architecture) and functions of a real world computer without extra hardware. This power and convenience has caused virtual machine applications to become increasingly more popular. This virtualization, however, may bring some new security risks to the table. “Rootkits have been created as Type 2 [Hypervisors](http://en.wikipedia.org/wiki/Hypervisor) in academia as proofs of concept. By exploiting hardware virtualization features such as [Intel VT](http://en.wikipedia.org/wiki/X86_virtualization#Intel_Virtualization_Technology_for_x86_.28Intel_VT-x.29) or [AMD-V](http://en.wikipedia.org/wiki/X86_virtualization#AMD_virtualization_.28AMD-V.29), this type of rootkit runs in Ring -1 and hosts the target operating system as a [virtual machine](http://en.wikipedia.org/wiki/Virtual_machine). Unlike normal hypervisors, they do not have to load before the operating system, but can load into an operating system before promoting it into a virtual machine. A hypervisor rootkit does not have to make any modifications to the kernel of the target to subvert it; however, that does not mean that it cannot be detected by the guest operating system.” (2) A proof-of-concept virtual machine rootkit called “SubVirt” was created by Microsoft in 2006 and proved existing virtual machines to be an easy target. In 2009 a hypervisor-layer anti-rootkit called “Hooksafe” was introduced by Microsoft and NCSU to protect against such rootkits. Hooksafe, along with other detection methods, will be analyzed in this project.

**Objectives:**

1. Identify strengths, weaknesses, and vulnerabilities of hypervisor security services.
2. Identify current measures being taken to prevent the exploitation of these vulnerabilities by virtual machine rootkits.
3. Provide new insight on potential methods of prevention and detection of virtual machine rootkits.

**Sources:**

1. <http://www.webopedia.com/TERM/R/rootkit.html>
2. <http://en.wikipedia.org/wiki/Rootkit#Hypervisor_level>
3. <http://www.virtuatopia.com/index.php/An_Overview_of_Virtualization_Techniques>
4. <http://www.eweek.com/c/a/Security/VM-Rootkits-The-Next-Big-Threat/1/>
5. <http://it.slashdot.org/story/07/10/02/0323237/vm-based-rootkits-proved-easily-detectable>