WinWizard: Expanding Xen with a LibVMI Intrusion Detection Tool

Jereme Lamps Imani Palmer Read Sprabery

University of Illinois at Urbana-Champaign

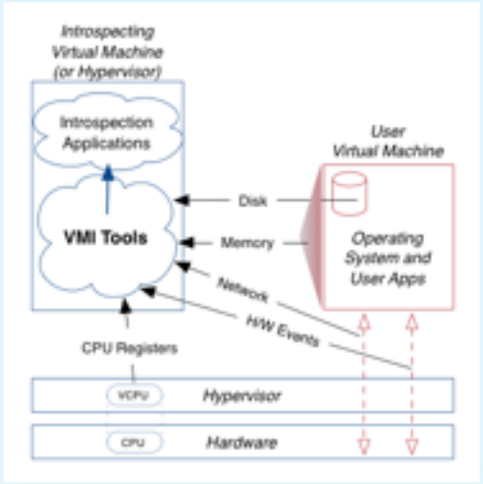
Anchorage, Alaska
June 27 - July 2, 2014

Overview

A need for virtualized based security is driven by the threat of malware at the kernel level. One way to attack this threat is to enhance the security outside the machine through the use of introspection of guest machines.

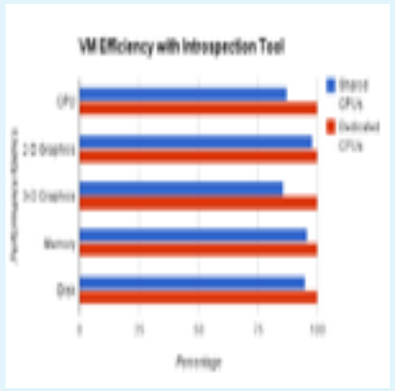
Xen/LibVMI

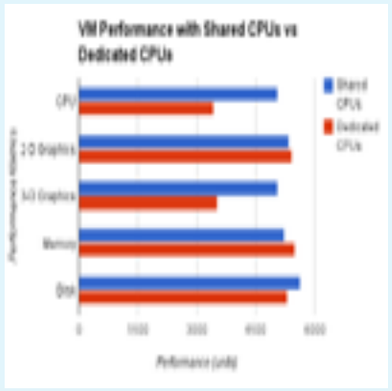
Xen is a class of virtual machines managers which have direct access to hardware. It allows operating systems to share conventional hardware in a safe and resource managed fashion. LibVMI is a project aimed to provide tools to enable virtual machine introspection.



Results

Our tool was successful in detecting both rootkits. To determine feasibility, we performed a number of performance tests. The tests consisted of running a VM without our introspection tool, sharing all 8 cores of the machine between the VM and dom0, and assigning the VM 4 virtual CPU's. The first figure shows a performance drop of 13%. Increasing the cores assigned to dom0 was that the introspection code was taking the majority of the execution time assigned to the dom0. We found that sampling the memory while letting Xen manage CPU cores and sharing cores between dom0 and Vm yielded the best performance. The final test, determined the impact on an additional guest not being scanned while a neighboring guest was having its memory scanned. The impact was a drop of about 10% on the neighboring VM.





WinWizard

WinWizard is a combination of two components. The first component gives an operating system level view of currently running processes. The second component utilizes LIBVMI to give an hypervisor perspective of what is going on. Through the comparison of both results we are able to determine whether or not something is wrong within the system.

Experiment

There were two separate experiments:

Hacker Defender: Used Hacker a Windows operating system rootkit that allows processes, files and registry keys to be hidden from systems administration tools.

Real World Simulation: One group was the hacker and our group were the defenders

ILLINOIS

We Would Like To Also Acknowledge: University of Illinois at Urbana-Champaign, Matt Caesar, Roy Campbell

This material is based upon work supported by the National Science Foundation Graduate Research Fellowship Program under Grant Number DGE-1144245. This material is also based upon work supported by the National Science Foundation under Grant Number FIA-1040391.