Method for VM Monitoring Using Hardware Virtualization

A security system using hardware virtualization features

Georgia Tech researchers have developed a security system using hardware virtualization features to create a virtual machine having both standard and hidden virtual address spaces. This general-purpose approach provides a security monitor that can reside in the hidden address space, monitoring the kernel without being modifiable by the kernel. The monitoring system can thus provide efficient, secure in-VM active monitoring of untrusted processes in a computer system.

Summary Bullets

- **More efficient** — at least 10 times performance improvement between switching to a monitor inside SIM and switching to a monitor residing in another trusted VM
- **Expandable** — new security applications can be built

Solution Advantages

- **More efficient** — at least 10 times performance improvement between switching to a monitor inside SIM and switching to a monitor residing in another trusted VM
- **Expandable** — new security applications can be built

Potential Commercial Applications

- Computer host-based security software
- Operating system security

Background and More Information

Kernel-level attacks or malicious programs, such as rootkits, that compromise the kernel of an operating system are one of the most important concerns in systems security. These attacks can modify kernel-level code or sensitive data to hide various malicious activities, to change operating system behavior, or even to take complete control of the system. Kernel-level security tools can be crippled and made ineffective by these attacks, which can run, access, and modify these security tools. Current approaches use virtual machine (VM) monitor technology in an effort to mitigate such attacks. A higher privileged hypervisor outside of a virtual machine in

which the kernel runs can enforce memory protections and preemptively intercept events throughout the operating system environment. However, these methods are limited-passive monitoring identifies problems after the fact and active monitoring requires too many resources to effectively monitor all threats.

Inventors

- Dr. Wenke Lee
  John P. Imlay, Jr., Chair of Software - Professor - Georgia Tech College of Computing
- Monirul Sharif
  Graduate Research Assistant — Georgia Tech College of Computing

IP Status

: US9129106B2

Publications

, -

Images

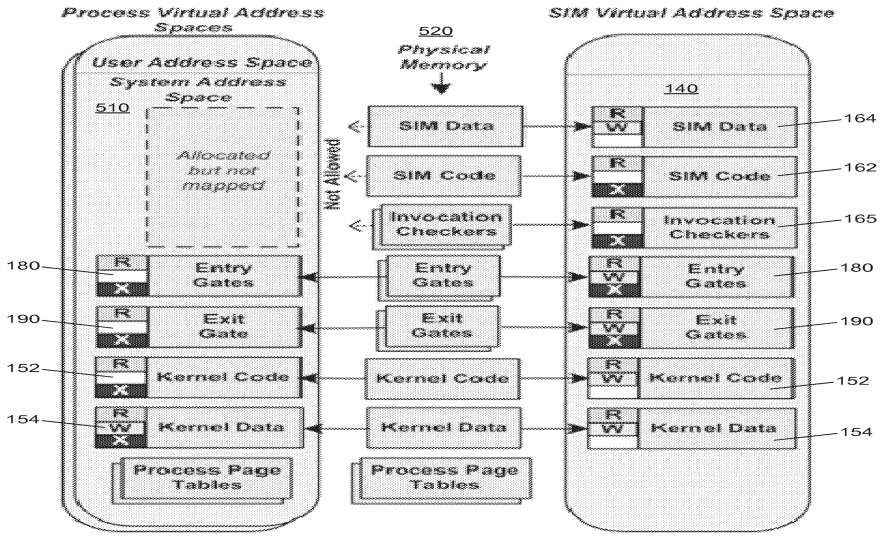

Fig. 5

Visit the Technology here:
[Method for VM Monitoring Using Hardware Virtualization]