

Made in IBM Labs: IBM Drives 'Fort Knox'-Like Security Into Virtualized Data Centers

February 6 2007

IBM today revealed a new software technology from its Research labs designed to greatly enhance security and management capabilities in virtualized data centers.

The new advancement is the industry's first effort to embed trusted computing technologies directly into the virtualization and management software tools already used inside data centers. This new technology allows for stronger data integrity guarantees and offers a higher degree of confidence that workloads and data are secure.

Virtualized data centers are becoming increasingly common in business, where multiple workloads, consisting of operating systems, middleware and applications, reside on a single physical computer system. The IBM secure hypervisor architecture, or "sHype," is a Research technology designed to run in conjunction with commercial and open source hypervisors that control servers and data in a shared environment. sHype aims to provide a security "wrapper" around distributed workloads in the data center, extending mainframe-like security to pooled data and resources across multiple IBM and non-IBM systems.

sHype is designed to bring stronger security guarantees to popular x86 and blade servers. As is increasingly common, IBM Research developed the sHype technology not just in its own labs, but implementing early versions of sHype with customers to test and evaluate the code.

Additionally, portions of sHype have been contributed to the Open Source community and are being used, for example, as part of the open source Xen hypervisor kernel.

"IBM is a major contributor to the Xen Project, and the adoption of their sHype mandatory access control (MAC) technology allows Xen to offer a unified security framework for Windows and Linux virtualization without compromising performance," said Dr. Ian Pratt, Xen project leader and XenSource founder.

Hoping to extend sHype beyond x86 hardware, IBM plans to introduce several other technologies with sHype as part of a comprehensive strategy to give customers the simplest, most secure and most efficient data centers possible.

"Thanks to the simplification benefits of the technology, virtualization adoption is on the rise but concerns about securing the virtualized data center persist," said Rich Lechner, Vice President, IBM Virtualization. "By putting security directly into the hypervisor virtualization layer, IBM Research has created a unique capability in sHype, providing clients with additional assurance that their virtualized data is protected."

Traditional IT security is based on built-in security for one or more user-chosen operating systems, and additional security from applications running on these operating systems. However, the steady stream of patches and updates required to protect the bulky code of an operating system and application stack is causing a heavy burden on customers.

Designing security into the much smaller, much easier to protect hypervisor architecture code creates a very tight wall of protection around physical resources in the data center, including the hardware, operating systems, applications, software hypervisors, workloads and virtual resources running in the now-secured environment. It also creates

secure data pipes inside of a virtualized environment, essentially locking and monitoring data from outside threats or internal errors, by protecting the data from other workloads and applications running across the same virtualized data center.

sHype works in conjunction with hypervisors by establishing a virtual machine to act as a data center "security foreman." The foreman uses preset configurations, business policies and exceptions set by the customer to lock down all content of the data center. It then automatically sets policies that evaluate, rank and code workloads as well as the physical and virtual resources needed to run each workload. Once workloads and resources are locked together, the integrity of the data and resources is assured and can be better managed by hypervisors accordingly.

IBM Research has successfully implemented significant elements of their sHype architecture with multiple hypervisors as part of the company's effort to demonstrate the architecture's flexibility and security capabilities. IBM is also working with industry groups to help standardize the aspects of sHype in order to achieve strong guarantees in and to simplify management of security in heterogeneous virtualized environments.

Source: IBM

Citation: Made in IBM Labs: IBM Drives 'Fort Knox'-Like Security Into Virtualized Data Centers (2007, February 6) retrieved 3 May 2024 from <https://phys.org/news/2007-02-ibm-labs-fort-knox-like-virtualized.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.
