Layered Assurance Enabling Virtualized Cross Domain Information Sharing

Charles Payne, Adventium Enterprises LLC

Objectives

Many military missions require cross domain information sharing using an approved transfer guard. Typically the guard software runs on dedicated hardware that provides the only link between the connected information security domain networks. As those networks grow more complex and as sharing increases, however, this guard deployment strategy does not scale effectively.

To address this problem, the information sharing community has investigated virtualization technology for guard deployment. Unfortunately, virtualization introduces shared hardware resources between the domain networks that could become direct information channels to bypass the guard. Demonstrating that the virtualization platform satisfies the guard's certification assumption of physically isolated domain networks remains a key challenge.

In this WIP, I will discuss that challenge and briefly describe our solution to address it. XEBHRA, or Xen-based, Host-Resident, Assurance, builds on the foundation of a trustworthy virtual machine monitor (VMM) that strictly isolates its virtual machines. XEBHRA layers on that foundation its own guarantees for controlled information flow through the guard. In addition, XEBHRA hosts an unmodified guard in order to avoid expensive recertification of that guard, and I will explain the impact of that decision on XEBHRA's architecture.

Accomplishments

Under a Phase II SBIR, we developed a prototype using Xen 4.0.1 as a placeholder for the trustworthy VMM, and we demonstrated operational relevance to our government customer by hosting on this prototype a fielded cross domain application and a certified guard. Recently we have successfully demonstrated key parts of the XEBHRA architecture on a candidate trustworthy VMM.

Future Plans

We intend to fully implement XEBHRA on a trustworthy VMM and then identify a sponsor to put XEBHRA through evaluation as a certified platform for operational use.

Contact

Charles Payne
Adventium Enterprises, LLC
111 Third Avenue South, Suite 100
Minneapolis, MN 55401 USA
Phone: 612.817.2525
Email: charles.payne@adventiumlabs.com