"SVMM: A NESTED DUAL-MONITOR VIRTUALIZATION ARCHITECTURE FOR PRIVACY PROTECTION ON x86 CLOUD PLATFORMS" VCU #12-76

Applications

- Deployed in public cloud to reduce compromise of sensitive data
- Used in private clouds such as banks, military and governments

Advantages

- Removes unnecessary provider operations
- Enhanced user privacy
- Isolated users, preventing attacks from one to another
- Reduced vulnerability to cyber attacks
- Multiple levels of security
- Lower operating expenses
- Backwards compatible

Inventors

Youlong Zhang
Meng Yu, Ph.D.

Contact

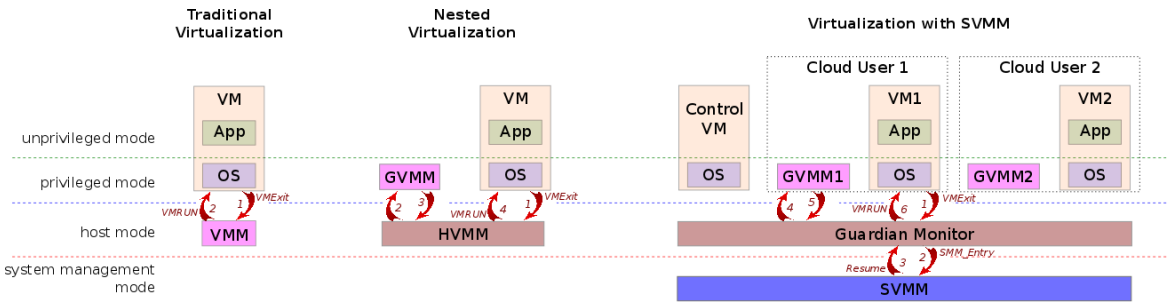
T. Allen Morris, Ph.D., MBA
Associate Director
amorris5@vcu.edu
Direct 804-827-2211

Market Need

Cloud computing and the elasticity it offers through virtualization has become very popular with corporations and private users alike. Currently available virtualization architectures commonly suffer from certain drawbacks. They are usually vulnerable to many known attacks at large software stacks. They are over complicated and large, making them difficult to test and to completely secure. The cloud providers have too much power, allowing access to information that they do not need for normal function. There is a lack of trusted isolation between virtual machines (VM). Inventors at VCU have developed a cloud architecture that addresses these issues.

Technology Summary

This invention addresses the major problem of cloud computing, **SECURITY,** through the use of both nested virtualization and dual-monitor architecture to provide content isolation between virtual machines (VM), with a thin, secured and attestable trusted computing base (TCB). At the same time, we introduce a set of corresponding protection mechanisms to repeatedly re-enforce privacy protection. This technology also features a lower operating cost, due to greater resource allocation, and is backwards compatible, an improvement from the competition that makes the system easier to integrate and update.



Technology Status

A prototype for the proposed novel architecture has been developed.
Patent pending: U.S. and foreign rights are available.
This technology is available for licensing to industry for further development and commercialization.