

ViMaSS (Virtual Machines for Seamless Security)

ViMaSS (Virtual Machines for Seamless Security) - Traditional computer security techniques find it difficult to protect user data. Cyber security technology has concentrated on guaranteeing the confidentiality, integrity, reliability and availability of computer system functions. While this paradigm shows promise in protecting computer systems, networks, and applications, it has not been able to protect data. Unlike systems and applications, a fence of protection cannot surround data. By its nature, data is required to be freely accessible to users; if data were locked away from the users, it would cease to be useful data. This raises the possibility of exploitation of data by user-level processes that inveigle themselves into the system. Malware entering a user environment is commonplace. Microsoft Word macros, email worms, and Trojan horses are a few types of malicious programs that need only be processed to run on a target system. Once invoked, these programs can wreak havoc on the target system, collecting, exfiltrating, corrupting, and deleting valuable user data. Computer security specialists know that segregating sensitive data onto machines protected from the network or using trusted multi-level systems is more secure than using standard machines, but the inconvenience of multi-level systems and the inconvenience of maintaining and using multiple machines tends to outweigh any security gains. Users don't like them and won't use them. Data ceases to be useful if it is segregated from the normal working environment. Virtual machines, however, promise to grant some of the isolation required by good data security practices without sacrificing the usability that makes data useful.

In this research project, multiple virtual machines are integrated into a production environment by creating a seamless desktop in which multiple virtual machines populate the screen real estate without interacting with each other. Security separation is achieved by creating a segregated machine to run the vulnerable Internet functions in an isolated environment. The email client and web browser, for example, will run on the "Internet" machine. If the user wants data to cross from the Internet machine into the processing core of the machine (where the important, sensitive data is held), the action will be virtually transparent to the user.¹ When the user clicks "Save As", for example, the Internet computer will transfer the data to a separate virtual machine for scanning. The separate virtual machine contains scanning software and nothing else. Once the data has been scanned for malicious content, it can be transferred to its destination machine. The destination machine puts up the "Save As" dialog that gives the user access to the sensitive file system. The "Save As" dialog (indeed, the entire secured environment) is not visible to the Internet machine. Similarly, URLs requested by the user physically sitting at the terminal can be passed out to the internet machine for network processing when necessary. There is a possibility that despite scanning, malware will be imported into the interior environment. By isolating the interior environment from the network, the VM manager can minimize the possibility that the illicit code will exfiltrate critical data from the interior environment. By integrating the visual output from multiple machines seamlessly on the desktop, the system can provide a familiar environment to the user while maintaining a strong separation between sensitive data and publishable data.

POC: Michael Neegaard, MS; Erik Ferragut, PhD
Cyber Security & Information Infrastructure Research Group
Oak Ridge National Laboratory P.O. Box 2008, Oak Ridge, TN 37831-6418
www.ioc.ornl.gov