ITL BULLETIN FOR APRIL 2011

FULL VIRTUALIZATION TECHNOLOGIES: GUIDELINES FOR SECURE IMPLEMENTATION AND MANAGEMENT

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Virtualization is a technique for simulating the software and the hardware upon which other software runs. Organizations adopting virtualization technologies can operate their information systems more efficiently, reduce their energy, operations and maintenance costs, and spend less on hardware and space for hardware. Federal organizations, in particular, are alert to the need to reduce the costs of operating data centers and to manage their information systems costs effectively.

In a Presidential Memorandum on *Disposing of Unneeded Federal Real Estate*, issued in June 2010, executive departments and agencies were advised to “accelerate efforts to identify and eliminate excess properties” and “to make better use of remaining real property assets as measured by utilization and occupancy rates, annual operating cost, energy efficiency, and sustainability.” The Memorandum specifically addressed the issue of the growth of data centers across the federal government, and charged departments and agencies with adopting policies to avoid expanding data centers beyond current levels, and developing plans for consolidating and significantly reducing data centers within five years. The secure implementation and use of virtualization technologies can help federal agencies meet these goals.

Forms of Virtualization

Virtualization technology creates a simulated environment called a *virtual machine (VM)*. There are many forms of virtualization, and these various forms are distinguished primarily by the computing architecture layer where the technique is applied. In *full virtualization*, one or more operating systems (OSs) and the applications that they contain are run on top of virtual hardware. Each discrete operating system and its applications run in a separate VM called a *guest operating system*.

The guest OSs on a host are managed by the *hypervisor*, which controls the flow of instructions between the guest OSs and the physical hardware, such as the central processing unit (CPU), disk storage, memory, and network interface cards. The hypervisor can partition the system’s resources and isolate the guest OSs so that each has access to only its own resources, as well as access to shared resources such as files on the host OS, if needed. Also, each guest OS can be completely encapsulated, making it portable. Some hypervisors run on top of another OS, which is known as the *host operating system*.

In full virtualization, the hypervisor provides most of the same hardware interfaces as those provided by the hardware's physical platform. As a result, the OSs and applications running within full virtualization do not need to be modified for virtualization to work, if the OSs and applications are compatible with the underlying hardware. A technique known as *paravirtualization* provides a method for the hypervisor to make available interfaces that the guest OS can use instead of the normal hardware interfaces. These paravirtualized interfaces offer significantly faster access for resources such as hard drives and networks. Different types of paravirtualization are provided by different hypervisor systems.

There are two forms of full virtualization architectures. In *bare metal virtualization,* also known as *native virtualization,* the hypervisor runs directly on the underlying hardware, without a host operating system. The hypervisor can be built into the computer's firmware, and bare metal architectures can only run applications within virtualized systems. In the other form of full virtualization, known as *hosted virtualization*, the hypervisor runs on top of the host OS. Hosted virtualization architectures usually have an additional layer of software (the *virtualization application*) running in the guest operating system to provide utilities for controlling the virtualization while in the guest OS. Hosted virtualization architectures allow users to run applications such as file-sharing, Web browsers, and email clients along with the hosted virtualization application.

The two major applications for full virtualization are for **servers** and for **desktop computers**. Virtualization of servers provides some security benefits. Running a server within a hypervisor can limit the impact of a security breach, but server virtualization does not prevent attackers from compromising the server through vulnerabilities in the server application, the guest operating systems, or the host operating system. When many servers on the same host are virtualized, all can be affected by a single security compromise if the vulnerability is in the hypervisor. This results in a full breach of the host.

The virtualization of desktop computers results in a single computer running more than one operating system. Desktop virtualization can provide support for applications that run only on a particular OS. This allows changes to be made to an OS and subsequently for return to the original OS if needed. For example, changes that lessen security protections can be eliminated. Desktop virtualization also supports better control of OSs to ensure that they meet the organization's security requirements.

Virtualization and Operational Efficiency

Full virtualization is a technical approach that can provide flexibility and operational efficiency. The application of full virtualization products and services for servers allows organizations to use their existing and new hardware more efficiently by putting more work on each computer. Organizations applying full virtualization can achieve more efficient use of the processing and memory resources of their servers than is possible when each server is running a single OS and a single set of services.

Recent advances in CPU architectures have made full virtualization faster than it was just a few years ago, and similar advances are expected to continue to be made both by CPU vendors and virtualization software vendors. Also, CPU architecture changes have made full virtualization more secure by strengthening hypervisor restrictions on resources.

Operational efficiency of desktops results from the implementation of desktop virtualization enabling the use of applications that run only on an older version of an OS when the user's desktop is running a newer version. In such a situation, desktop virtualization is useful for continuity of applications as the OSs advance faster than the applications that run on them. As more applications become Web-based, desktop virtualization can become even more important to operational efficiency. A Web application that runs only on an older version of a particular browser can be run in a virtualized system with the older version of that browser, while the user's main environment is running the newer, and usually more secure, version of the browser.

Virtualization and Security Concerns

When adopting virtualization, organizations must address the increased risk and the security issues that may affect their systems. Virtualization adds layers of technology, which can increase security management concerns and require the implementation of additional security controls. Also, combining many systems onto a single physical computer can cause a larger impact on the organization if security is compromised. Some virtualization systems make it easy to share information between the systems; however, this feature can also increase risks to the security of information and systems, and must be carefully controlled. In some cases, virtualized environments are dynamic, making the creation and maintenance of the necessary security boundaries more complex.

Moving computing resources to a virtualized environment may not improve the security of the resources that are moved. A service with inherent vulnerabilities, which is moved from a non-virtualized server to a virtualized server, is still vulnerable to security risks. While the use of virtualization may help reduce the impact of any exploitation of systems, virtualization may also provide additional opportunities for attacks and may increase the likelihood of successful attacks.

NIST Special Publication (SP) 800-125, *Guide To Security for Full Virtualization Technologies: Recommendations of the National Institute of Standards and Technology*

New guidelines issued by the Information Technology Laboratory at the National Institute of Standards and Technology (NIST) help federal organizations to use full virtualization technology for their servers and desktop computers and to achieve cost savings in the management of their information systems. The guidelines address the security concerns associated with full virtualization technologies for server and desktop virtualization, and recommend steps for addressing these concerns.

NIST SP 800-125, *Guide To Security for Full Virtualization Technologies: Recommendations of the National Institute of Standards and Technology*, was written by Karen Scarfone of G2, Inc., Murugiah Souppaya of NIST, and Paul Hoffman of the VPN Consortium. The recommended practices discussed in this publication build on the practices described in other NIST publications, and adapt them to the virtual environment. See the **For More Information** section below for publications that support the recommendations included in NIST SP 800-125.

The guide starts with an overview of full virtualization technologies and explains the types of full virtualization. Virtualized networking, virtualized storage, and guest operating systems are discussed. Two types of full virtualization, server and desktop virtualization, are presented, along with the benefits and possible security impacts of virtualization. Other topics addressed include security recommendations for virtualization components, common threats against virtualization solutions, and recommendations for countering these threats.

Also discussed in the guide is the need to apply the steps in the system development life cycle to a virtualization application and to select and integrate appropriate security controls into each step of the life cycle. NIST SP 800-125 contains appendices with supporting material; Appendix A defines terms used and Appendix B lists acronyms and abbreviations used. The publication is available from the NIST Web page http://csrc.nist.gov/publications/PubsSPs.html.

NIST Recommendations for Security for Full Virtualization Technologies

Most existing recommended security practices that have been developed to protect information and information systems are applicable to virtual environments. The practices described in NIST SP 800-125 build on the implementation of security practices described in other NIST publications.

Virtualization can be used in many ways, and the appropriate security controls that should be selected and managed for each implementation vary. An important resource for organizations implementing virtualization is the risk management framework outlined in NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.* This publication assists organizations in assessing the risks associated with virtualization and selecting the appropriate methods for maintaining the security of information systems.

Organizations should implement the following recommendations to improve the security of server and desktop full virtualization technologies that they adopt for their systems:

• Secure all elements of a full virtualization solution and maintain their security.

The security of a full virtualization solution is heavily dependent on the individual security of each of its components, including the hypervisor, host OS, guest OSs, applications, networks, and storage. Organizations should secure all of these elements and maintain their security based on sound security practices: for example, keeping software up to date with security patches, using secure configuration baselines, and using host-based firewalls, antivirus software, or other appropriate mechanisms to detect and stop attacks. In general, organizations should have the same security controls in place for virtualized operating systems as they have for the same operating systems running directly on hardware. Organizations should apply the same security policies that they have adopted for the applications on operating systems that are running on hardware to the applications that are running on an operating system within a hypervisor.

- **Restrict and protect administrator access to the virtualization solution.**

The security of the entire virtual infrastructure depends on the security of the virtualization management system that controls the hypervisor and allows the operator to start guest OSs, create new guest OS images, and perform other administrative actions. Because of the security implications of these actions, access to the virtualization management system should be restricted to authorized administrators only. Since some virtualization products offer multiple ways to manage hypervisors, organizations should secure each management interface, whether locally or remotely accessible. For remote administration, the confidentiality of communications should be protected, such as through use of Federal Information Processing Standards (FIPS)-approved cryptographic algorithms and modules.

- **Ensure that the hypervisor is properly secured.**

Securing a hypervisor involves actions that are standard for any type of software, such as installing updates as they become available. Other recommended actions that are specific to hypervisors include disabling unused virtual hardware; disabling unneeded hypervisor services such as clipboard- or file-sharing; and considering the use of the hypervisor's capabilities to monitor the security of each guest OS running within it, as well as the security of activity occurring between guest OSs. The hypervisor itself should be carefully monitored for signs of compromise. It is also important to provide physical access controls for the hardware on which the hypervisor runs. For example, hosted hypervisors are typically controlled by management software that can be used by anyone with access to the keyboard and mouse. Even bare metal hypervisors require physical security protections. An individual who can reboot the host computer that the hypervisor is running on might be able to alter some of the security settings for the hypervisor.

- **Carefully plan the security for a full virtualization solution before installing, configuring, and deploying it.**

Planning helps ensure that the virtual environment is as secure as possible and is in compliance with all relevant organizational policies. Security should be considered from the initial planning stage at the beginning of the system development life cycle to maximize security and minimize costs. The five phases of the system life cycle -- initiation, planning and design, implementation, operations and maintenance, and disposition -- are discussed in NIST SP 800-64, *Security Considerations in the System*

Development Life Cycle. It is much more difficult and expensive to address security after deployment and implementation.

For More Information:

Presidential Memorandum, June 10, 2010, *Disposing of Unneeded Federal Real Estate*, is available on the following Web page: http://www.whitehouse.gov/the-press-office/presidential-memorandum-disposing-unneeded-federal-real-estate.

NIST publications that provide information and guidance on planning, implementing, and managing information system security and protecting information include:

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*
NIST Special Publication (SP) 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*
NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*
NIST SP 800-64 Revision 2, *Security Considerations in the System Development Life Cycle*
NIST SP 800-88, *Guidelines for Media Sanitization*
NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*
NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*

For information about these NIST standards and guidelines, as well as other security-related publications, see NIST's Web page http://csrc.nist.gov/publications/index.html.

For information about **FIPS-approved cryptographic algorithms and modules**, see NIST's Web page http://csrc.nist.gov/groups/STM/cmvp/index.html.

Information about NIST's information security programs is available from the Computer Security Resource Center at http://csrc.nist.gov/.

Virtualization technology facilitates the implementation of **cloud computing**, another approach to more efficient data center operation that was proposed by the Office of Management and Budget. For information about cloud computing, including the NIST definition of cloud computing, see the NIST Web page http://csrc.nist.gov/groups/SNS/cloud-computing/.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.