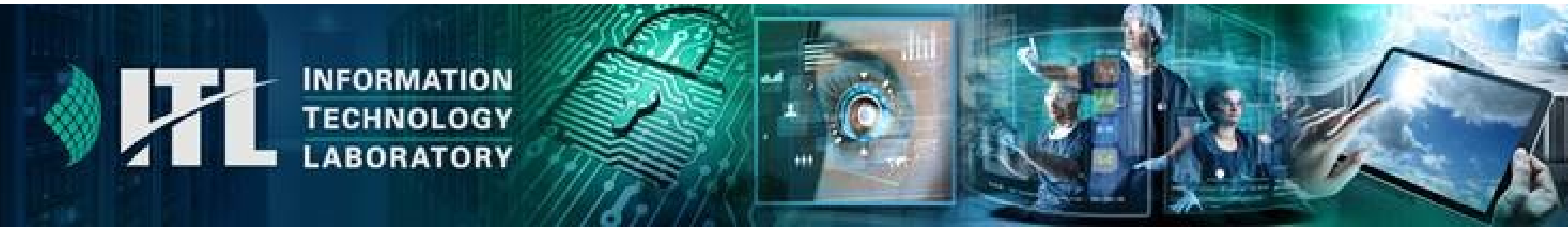

# ITL BULLETIN FOR MARCH 2018

# SAFEGUARDS FOR SECURING VIRTUALIZED SERVERS

Ramaswamy Chandramouli, Larry Feldman,[1] and Greg Witte,[1] Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

## Introduction

This bulletin outlines the security recommendations that NIST recently provided in Special Publication (SP) 800-125A, *Security Recommendations for Hypervisor Deployment on Servers*. The document provides technical guidelines about the secure execution of baseline functions of the hypervisor, regardless of the hypervisor architecture.

In the past, a user wishing to set up a computing server generally needed to use a dedicated host with dedicated resources, such as a central processing unit (CPU), memory, network, and storage. Modern systems have technology that lets one create virtual machines to emulate what used to be physical, dedicated resources. This practice is known as virtualization and supports more scalable and dynamic environments.

A critical component of this technology is the hypervisor, the collection of software modules that enables this virtualization and thus enables multiple computing stacks—each made of an operating system (OS) and application programs—to be run on a single physical host. Such a physical host is called a Virtualized Host and is also referred to as a Hypervisor Host. The individual computing stacks are encapsulated in an artifact called a Virtual Machine (VM).

To make a VM an independent executable entity, its definition should include resources, such as CPU and memory, allocated to it. The VMs are also called "Guests," and the OS running inside each of them is called "Guest OS." The resources associated with a VM are virtual resources, as opposed to physical resources associated with a physical host.

The hypervisor forms part of the virtualization layer in a virtualized host and plays many of the same roles that a conventional OS does on a non-virtualized host, or server. Just as a conventional OS provides

[1] Larry Feldman and Greg Witte are Guest Researchers from G2, Inc.

isolation between the various applications, or processes, running on a server, the hypervisor provides isolation between one or more VMs running on it.

Also, like an OS, the hypervisor mediates access to physical resources across multiple VMs. Therefore, all other functions needed to support virtualization—such as emulation of network and storage devices and the management of VMs and the hypervisor itself—can be accomplished using kernel-loadable modules, although some hypervisor architectures accomplish these tasks using dedicated VMs. The hypervisor can be installed either directly on the hardware, or bare metal (Type 1 Hypervisor), or on top of a full-fledged conventional OS, called Host OS (Type 2 Hypervisor).

Here, we discuss the baseline functions of a hypervisor, how these functions are distributed in a hypervisor, and how this information is used to develop security recommendations that provide assurance against potential threats to the secure execution of tasks involved in the hypervisor's baseline functions.

**Hypervisor Baseline Functions**

It might appear that all activities related to the secure management of a hypervisor and its hardware host—collectively called the hypervisor platform—should simply consist of established best practices for any server class software and its hosting environment. However, closer examination reveals that the unique functions provided by the Hypervisor Platform require a dedicated set of security considerations. These functions are called hypervisor baseline functions (HY-BF) and are labeled HY-BF1, HY-BF2, HY-BF3, HY-BF4, and HY-BF5. They are described below:

- **HY-BF1: VM Process Isolation –** Scheduling of VMs for execution, management of the application processes running in VMs (e.g., CPU and memory management), and context switching between various processor states during the running of applications in VMs;
- **HY-BF2: Devices Mediation & Access Control –** Mediates access to all devices (e.g., Network Interface Card [NIC], storage device such as IDE drive, etc.). One mediation approach is to emulate network and storage (block) devices that are expected by different native drivers in VMs by using emulation programs that run in the hypervisor kernel.
- **HY-BF3: Direct Execution of Commands from Guest VMs –** Certain commands from Guest OSs are executed directly by the hypervisor instead of being triggered through interrupts and context switching. This function applies to hypervisors that have implemented paravirtualization[2] instead of full virtualization;
- **HY-BF4: VM Lifecycle Management –** This baseline function involves all functions from creation and management of VM images, control of VM states (Start, Pause, Stop, etc.), VM migration, VM monitoring, and policy enforcement; and

[2] A paravirtualized hypervisor describes a condition where a specialized guest OS is aware of and works with the hypervisor to improve performance and efficiency.

- **HY-BF5: Management of Hypervisor –** This baseline function involves defining some artifacts and setting values for various configuration parameters in hypervisor software modules including those for configuration of a Virtual Network inside the hypervisor.

NIST SP 800-125A provides detailed security guidance based on an analysis of threats to the integrity of all the above functions. The only exceptions are the set of guidelines for configuration of virtual network (subset of HY-BF5), which are covered in a separate document (NIST SP 800-125B).

The above functions are carried out by different hypervisor components, or software modules. There are some minor differences among hypervisor products in the way that they distribute these functions. The mapping of these functions to hypervisor components and the location of these components within a hypervisor architecture are described in the table below:

| Baseline Function | Component (Software Module) | Location |
|---|---|---|
| VM Process Isolation (HY-BF1) | Hypervisor Kernel | Either an OS kernel (along with a kernel module) itself or a component installed on a full-fledged OS (Host OS) |
| Devices Mediation and Access Control (HY-BF2) | Device emulator or Device driver | Either in a dedicated VM (called Device-driver VM) or in the hypervisor kernel itself |
| Direct Execution of Commands from Guest VMs (HY-BF3) | Hypervisor Kernel | Pertain to only paravirtualized hypervisors and handled by hypercall interfaces in that type of hypervisor |
| VM Lifecycle Management (HY-BF4) | A management daemon | Installed on top of hypervisor kernel but runs in unprivileged mode |
| Management of Hypervisor (HY-BF5) | A set of tools with CLI (command line interface) or a GUI | A console or shell running on top of hypervisor kernel |

**Approach for Developing Security Recommendations**

Developing security recommendations for the deployment and use of a complex software such as the hypervisor requires knowledge of potential threats which, when exploited, would affect the three basic security properties—confidentiality, integrity, and availability—of hypervisor functions. The approach adopted for developing security recommendations for the deployment of hypervisors in NIST SP 800-125A is as follows:

- Ensure the integrity of all components of the hypervisor platform, starting from the host BIOS to all software modules of the hypervisor. This action is accomplished through a secure boot process, outlined as recommendation HY-SR1;
- Identify the threat sources in a typical hypervisor platform. The nature of threats from rogue or compromised VMs is briefly discussed in SP 800-125A; and
- For each of the five baseline functions HY-BF1 through HY-BF5 (except for HY-BF3, the direct execution of certain commands from guest VMs by the hypervisor), identify the different tasks under each function, and for each of the tasks, identify the potential threats to the secure execution of the task. The countermeasures that will provide assurance against exploitation of these threats form the basis of the security recommendations. The threat related to HY-BF3 emanates from a hypervisor design vulnerability that must be addressed through proper validation and testing of the relevant hypervisor code, not through configuration or deployment procedures, which is why this type of threat is not addressed through any security recommendation in SP 800-125A.

In the case of some large open source and commercial software environments (e.g., a database management system [DBMS] platform), the approach for secure deployment and usage is to study the reports published in public vulnerability databases for various product offerings, look for available patches from the software vendor, review online public resources, and seek out recommended security configuration settings. This approach was not adopted in NIST SP 800-125A because the intended purpose was to provide security recommendations for the entire product class based on its baseline functions instead of a specific open source or commercial hypervisor product offering.

**Summary of Security Recommendations**

The hypervisor is a complex server class software that virtualizes hardware resources to enable the execution of multiple computing stacks (VMs) with heterogeneous OSs and multiple applications hosted within them. Secure configuration of the hypervisor, together with its physical host (either hypervisor host or virtualized host)—collectively called the hypervisor platform—is needed to provide a safe platform for the execution of mission-critical applications.

Because the architecture of a hypervisor can be classified in many ways, the approach taken in NIST SP 800-125A is to identify the five baseline functions that a hypervisor performs, the tasks involved in each baseline function, the potential threats to the secure execution of any of these tasks, and the countermeasures that provide assurance against these threats in the form of security recommendations.

Overall, NIST SP 800-125A provides 20 security recommendations for the secure deployment of hypervisors. All but two (HY-SR-1 and HY-SR-2) relate to the configuration parameters of software modules in the hypervisor platform. These parameters include integrity metrics for software modules (e.g., device drivers and VM images), the setting of access controls (e.g., device access, VM image access, and VM administration), and the configuration of secure protocols (e.g., VM image server access and VM migration).

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov

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.