Singapore Standards Council

TR 30 : 2012
(ICS 35.040)

TECHNICAL REFERENCE

Virtualisation security for servers

Published by

Enterprise Singapore

TR 30 : 2012
(ICS 35.040)

TECHNICAL REFERENCE

Virtualisation security for servers

ISBN 978-981-4353-24-3

First published, 2012

NOTE

1. *Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions.*

2. *An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR.*

3. *Compliance with a SS or TR does not exempt users from any legal obligations.*

Contents

Foreword

This Technical Reference was prepared by the Virtualisation Security Best Practices Working Group of the Cloud Computing Standards Coordinating Task Force (CCSCTF) under the direction of the Information Technology Standards Committee (ITSC). The ITSC endorsed the Technical Reference on 1 March 2012.

This Technical Reference aims to address and mitigate the concerns potentially posed by the compute hypervisors that are used on server hardware, through the identification of key security risks and best practices input received from key compute hypervisor vendors and other stakeholders. This Technical Reference provides common guidelines to help local enterprise users implement a set of recommended security controls for their virtualised IT environment.

This Technical Reference is not to be regarded as a Singapore Standard. This Technical Reference is made available for provisional application over a period of two years, but does not have the status of a Singapore Standard. The aim is to use the experience gained to modify the Technical Reference so that it can be adopted as a Singapore Standard. Users of the Technical Reference are invited to comment on its technical content, ease of use and any ambiguities or anomalies. These comments can be submitted using the feedback form provided at the end of the Technical Reference and will be taken into account in the review of the publication. At the end of the two years, the Technical Reference will be reviewed by the WG to discuss the comments received and to determine its suitability as a Singapore Standard. Submission for approval by the Standards Council as a Singapore Standard will be carried out only upon agreement after review.

Attention is drawn to the possibility that some of the elements of this Singapore Standard may be the subject of patent rights. Enterprise Singapore shall not be held responsible for identifying any or all of such patent rights.

Technical Reference for virtualisation security for servers

0 Introduction

Cloud computing offers a means to provide computing as a service, with an efficient pooling of an on-demand virtual infrastructure and the underlying IT complexity hidden from users. In order to take full advantages of economies of scale by sharing infrastructure resources, virtualisation technologies (especially server virtualisation) are widely used for the deployment of cloud computing services.

This Technical Reference (TR) aims to provide users a set of best practices to address security risks posed by virtualisation based on compute hypervisors.

The best practices specified in this TR are not exhaustive and do not cover other aspects such as required skill competency of the data centre personnel to manage a virtualised environment.

Figure 1 is an overview of the landscape of server virtualisation technologies. The scope of this TR focuses on soft partitioning, as compared to hard partitioning, although some of the described mitigation controls can well apply to all. (Hard and soft partitioning refers to the isolation of execution environments using electrical components and software respectively.)

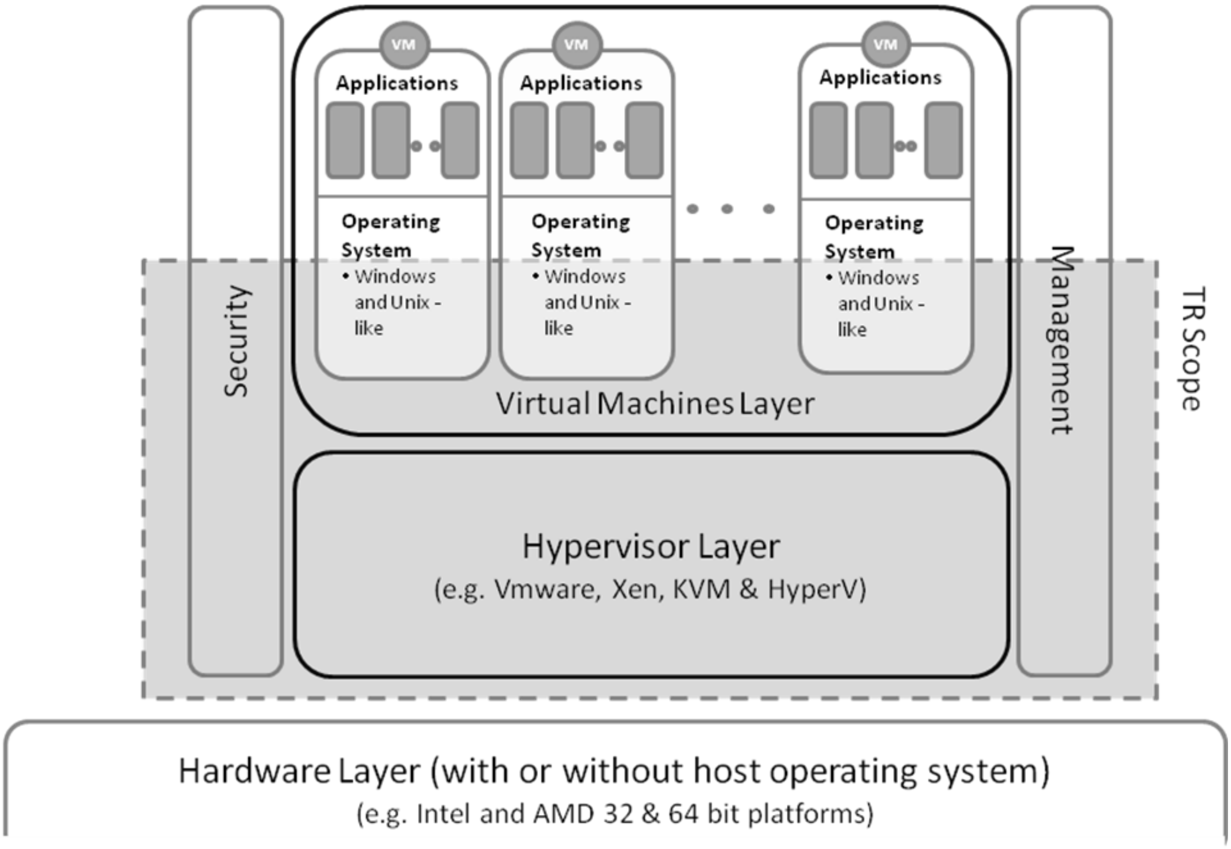
VM
Applications
Operating System
• Windows and Unix - like
VM
Applications
Operating System
• Windows and Unix - like
VM
Applications
Operating System
• Windows and Unix - like
Security
Management
TR Scope
Virtual Machines Layer
Hypervisor Layer
(e.g. Vmware, Xen, KVM & HyperV)
Hardware Layer (with or without host operating system)
(e.g. Intel and AMD 32 & 64 bit platforms)

Figure 1 – Server virtualisation and scope of TR

1 Scope

This Technical Reference intends to provide guidance on the identification and management of security risks specific to virtualisation technologies that run on a server hardware (as opposed to, as examples, desktop or network or storage virtualisation). It focuses on virtualisation security with respect to the server virtualisation technologies applied to server platforms illustrated in Figure 1. The users include enterprise infocomm personnel and service providers, although the main focus is targeted on the former.

2 Normative references

No normative references are cited.