Common Criteria Evaluation and Validation Scheme

National Information Assurance Partnership (NIAP)

Title: Client Virtualization Essential Security Requirements

Maintained by: National Information Assurance Partnership

Unique Identifier: 42

Version: 1.0

Status: final

Date of issue: 7 March 2016

Approved by:

Supersedes:

Status

This Essential Security Requirements (ESR) document specifies the essential requirements for client virtualization software. The creation of an ESR is a necessary prerequisite for the recognition of the Client Virtualization Protection Profile as a PP.

Background and Purpose

Client Virtualization, for the purposes of this PP, refers to a virtualization system (VS) that implements virtualized hardware components locally on an endpoint machine. Endpoints are typically client hardware such as desktop or laptop computers that a user interacts with directly, but may also include headless embedded systems without direct human interaction. It creates a virtualized hardware environment for each instance of a guest operating system (virtual machines or VMs) permitting these environments to execute concurrently while maintaining the appearance of isolation and exclusive control over assigned computing resources. Client virtualization is generally used on endpoint systems, making use of the local machine's resources (memory, CPU, etc.) to provide isolated user environments. This PP does not address virtualization on mobile devices (typically devices that use a baseband processor and/or connect to a cellular network). Nor does it address application virtualization or containers.

This document describes the high-level set of security requirements that client virtualization software must satisfy when evaluated against the PP under development.

Use Cases

- Locally Managed Client - A local administrator creates and runs one or more VMs locally. This client could be stand-alone or connected to a network.
- Enterprise Managed Client - An enterprise administrator for the VS centrally manages one or more client hypervisors, creating and configuring VMs which are then pushed to the clients. These VMs are then available for users on that client to run using the computing resources of that client. (Note that this is not Virtual Desktop Infrastructure where the hypervisors and the VMs run on remote servers. While both can be centrally managed and accessed from clients, for client virtualization, the VMs are local to the endpoint machine).
- Headless Client – A VM is used by a program without direct human interaction.

Resources to be protected

- The platform onto which the Virtualization System is installed including the hardware, firmware, and host operating system
- The Virtual Machine Manager (VMM) including the Hypervisor and Service VMs
- The Management Subsystem (if applicable)
- The VMs and their contents

Attacker access

An attacker has access to either:

- A VM or its network
- The Client machine hosting the VS or its network

Boundary of Device

- The Virtual Machine Manager (VMM)
  - The Hypervisor
  - Service VMs
  - VM containers/abstractions
- The Management Subsystem (if applicable)

Essential Security Requirements

The following are the essential security requirements that are expected to be implemented by any application that is compliant with the Client Virtualization PP. Note that these security requirements are conditional on that functionality being present. For example, a product that does not require an external network connection for any purpose is considered to satisfy any security requirements that pertain to the secure use of external network connections.

Any other conditional requirements that depend on whether or not the product implements a certain capability are listed in the “Optional Extensions” section below.

The Virtualization System shall:

- Maintain isolation between its VMs (and their resources)
- Maintain the integrity of the VMM
- Protect the platform from VMs and remote users of the VS
- Protect the Management Subsystem (if applicable) from unauthorized access
- Be capable of being updated/patched in a secure and timely manner
- Provide the VMs access to sufficient sources of entropy (or necessary platform resources)
- Provide audit capabilities for security-relevant events

Assumptions

- The VS relies on a trustworthy computing platform for its execution, and it is assumed that the platform has not been compromised prior to the installation of the VS.
- Physical security appropriate to the value of the VS and the data it contains is provided.
- The user of the VS is not willfully negligent or hostile, and uses the VS in compliance with the applied enterprise security policy and guidance.

Optional Extensions

The following requirements may already be realized in some products in this technology class, but the ESR is not mandating these capabilities exist in “baseline” level products:

- Access Banners

Objective Requirements

Requirements captured in this section specify security-relevant behavior that is not expected to be realized currently in products of this type, but they are capabilities that may be mandated in future versions of the ESR and resulting PPs.

- Support for Introspection
- Collection of Integrity Measurements
- Maintain the integrity of its communications channels according to system security policy

Outside the TOE's Scope

- The platform onto which the Virtualization System is installed including the hardware, firmware, and non-VS-essential portions of the host operating system
- Software installed inside VMs that is unrelated to the functioning of the Virtualization System
- Virtualization on mobile devices (typically devices that use a baseband processor and/or connect to a cellular network)
- Application virtualization
- Containers