Common Criteria Evaluation and Validation Scheme

National Information Assurance Partnership (NIAP)

Title: General-Purpose Computing Platform Protection Profile

Maintained by: NIAP

Unique Identifier: 42

Version: 0.2

Status: draft

Date of issue: 15 September 2020

Approved by:

Supersedes:

Background and Purpose

This document describes the high-level security requirements to be met by general-purpose computing platforms. The resulting Protection Profile will define baseline security functionality with additional security options.

A platform is a collection of hardware devices and firmware that provide the functional capabilities and services needed by tenant software. Such devices typically include embedded controllers, trusted platform modules, management controllers, host processors, network interface controllers, graphics processing units, flash memory, storage controllers, storage devices, boot firmware, runtime firmware, human interface devices, and a power supply.

Use Cases

A general-purpose computing platform is a hardware device that it capable of hosting more than one different operating system, virtualization system, or bare-metal application. Typical platform implementations include--but are not limited to--servers, PC clients, laptops, and tablets.

Resources to be protected

The platform has three major security responsibilities:

- ensuring the integrity of its own firmware
- ensuring that it is resilient
- providing security services to tenant workloads

These responsibilities manifest as protecting:

- Platform firmware
- Platform firmware updates
- Tenant initialization (boot)

Attacker access

The attackers are assumed to have compromised the tenant software such that malicious code can run remotely or automatically to attack the platform. The attackers are assumed to have network access to the platform such that they can launch remote attacks.

Essential Security Requirements

The following are the essential security requirements that are expected to be enforced by any GPCP TOE:

1. Platform Integrity—Roots of Trust

   Roots of trust are security primitives that provide a set of trusted, security-critical functions. They must always behave in an expected manner because their misbehavior cannot be detected.

   A platform must implement the following roots of trust:

   1. Root of Trust for Storage (RTS) – provides protected repository and protected interface for storing keying material.
   2. Root of Trust for Verification (RTV) – provides protected engine and interface to verify digital signatures associated with firmware and to create assertions based on the results.
   3. Root of Trust for Integrity (RTI) – provides protected storage, integrity protection, and a protected interface to store and manage assertions.
   4. Root of Trust for Reporting (RTR) – provides a protected environment and interface to manage identities and sign assertions.
   5. Root of Trust for Measurement (RTM) – provides measurement used by assertions protected via the RTI and attested to with the RTR.
2. Platform Resilience—Protect, Detect, Recover

   The platform must support the following security capabilities to ensure its own integrity:

   1. Protection of Platform Integrity:
      1. Protect Platform Firmware – The platform firmware can be modified only through an authorized mechanism.
      2. Authenticated Update – The platform firmware updates must be authenticated via a root of trust before they are applied.
   2. Detection of Platform Integrity
      1. Hardware Integrity – The platform must be able to detect changes in its hardware configuration.
      2. Firmware Integrity. – The platform must be able to detect changes to its firmware made outside of an authenticated update mechanism.
   3. Platform Recovery
      1. The platform must be capable of restoring platform firmware and critical data that has been corrupted or changed from its authorized state.
3. Security Services for Tenant Software

   The platform must provide the following security services to tenant software:

   1. Protected Storage – The platform must support a mechanism for protecting the confidentiality and integrity of sensitive data while at rest.
   2. Assured Erase – The platform must provide a mechanism for assured erasure of unencrypted sensitive data at rest.
   3. Isolation – The platform must provide a mechanism that can be leveraged by tenant software to support the isolation of different computing contexts. This could be something as simple as processor support for process isolation, processor support for virtualization, or platform support for application isolation.
   4. Platform Identity – The platform must have a unique identity for purposes of platform authentication.
   5. Cryptographic Services – The hardware platform may implement cryptographic services in hardware. This could include RNGs, entropy sources, and cryptographic functions implemented in hardware.
   6. Management Services – Baseboard Management Controller (BMC)/Management Engine (ME) – The platform may provide out-of-band management services for tenant software.

Assumptions

It is assumed that an attacker has no access to the physical device, but has access to the tenant workload and to tenant workload networks.

Outside the TOE's Scope

This section has been intentionally left blank.