Common Criteria Evaluation and Validation Scheme

National Information Assurance Partnership (NIAP)

Title: General Purpose Operating System

Maintained by: NIAP and CESG

Unique Identifier: 42

Version: 0.8

Status: draft

Date of issue: 19 March 2015

Approved by:

Supersedes:

Background and Purpose

An operating system is software that manages computer hardware and software resources, and provides common services for application programs. The hardware it manages may be physical or virtual.

This essential security requirements (ESR) document outlines the high-level security requirements for a general-purpose operating system (OS), which will be expressed in a Common Criteria Protection Profile (PP). These requirements address threats within a scope established by use cases and environment assumptions. In addition to stating what properties an OS must minimally exhibit, this document also identifies functionality that vendors should consider as extensions that go beyond the expected minimal baseline, and which may be appropriate in more-specific use cases.

The security functionality must be realistic and achievable by commercially available products. The resulting PP will also include objective and repeatable evaluation activities, so that evaluations can be executed in a manner that tracks with industry's release of operating system products.

With regard to evaluation scope, the operating system itself is composed of the software that is delivered to the end user in the operating system product. This typically includes a kernel and drivers that run with elevated privileges, common software libraries, and a great deal of application software which runs with varying levels of privileges. Many of these applications provide security services and are an essential part of the operating system product. However, applications that are covered by more-specific Protection Profiles should not be evaluated as part of the OS evaluation, even when it is necessary to evaluate some of their functionality as it relates to their role as part of the OS.

Use Cases

The OS is installed on a platform to allocate platform resources among applications. This includes several use cases in which the OS acts as a platform for applications:

- End user systems such as a desktop or laptop, which is optionally bound to a directory server or management server
- Server systems, which run on physical or virtual hardware, and can run highly specialized configurations
- Cloud systems, end user or server systems running on physical or virtual hardware hosted in a data center

Resources to be protected

- Physical and logical resources managed by the OS (e.g. network interfaces, microphones, and storage media).
- Sensitive user data (e.g. home directories).
- Sensitive system data (e.g. account information, audit files, configuration files).
- Resources that comprise the OS itself, upon which its integrity depends. This includes files such as the kernel and its drivers, privileged applications that provide services to other applications, and shared software libraries.

Attacker access

The following assumptions are made about attackers' ability to develop attacks:

- An attacker has an arbitrary amount of time to analyze the behavior of the OS, its interaction with its platform, and the data it transmits over the network.
- An attacker is able to acquire their own copy of the target OS and study its behavior on a platform that they control.

The attacker is expected to engage in the following general classes of attack:

- Network eavesdropping, in which an attacker may monitor and gain access to data exchanged between the OS and other endpoints.
- Network attack, in which an attacker may initiate malicious communications with the OS or alter communications between the OS and other endpoints.
- Local attack, in which an attacker has gained the ability to execute code on the system, which may be used to escalate privilege or access data without authorization.
- Limited physical access attack, in which an attacker may attempt to access data on the system by virtue of being physically present for a limited period of time. This limited physical access does not include attacks in which the attacker could disassemble the system to gain access to its storage media or manipulate the OS's underlying hardware and firmware. Systems used for working remotely, such as laptops and tablets, for which an attacker could gain longer physical access to, should apply additional protections that are provided by products evaluated against other Protection Profiles (e.g. FDE cPP).
- Persistence, in which an attacker has already exploited the system and wishes to maintain presence on the system.

Essential Security Requirements

The following are the essential security requirements expected to be implemented by an operating system within the established scope:

- Implement modern anti-exploitation features, these include, but are not limited to Address Space Layer Randomization (ASLR), Stack Canaries/Cookies, and Data Execution Protection (DEP) to protect itself and its applications.
- Provide the following cryptographic services:
  - Asymmetric and Symmetric key generation
  - Asymmetric and Symmetric encryption and decryption
  - Deterministic random bit generation (DRBG)
  - Cryptographic hashing
  - Cryptographic signing and validation
  - Keyed-hash message authentication
  - TLS support
  - Certificate path validation
- Provide a trusted update mechanism to update itself, applications, and, optionally, firmware for the platform it runs on.
- Provide strong authentication mechanisms.
- Leverage a trusted or secure boot process.
- Provide the ability to whitelist application execution.
- Provide the ability to control external interfaces (e.g. radios, ports).
- Audit security-relevant events and provide mechanism for secure transmission of audit data.
- Provide mechanisms for management by the user and enterprise, to include optionally binding to:
  - directory servers, which provide support for centralized authentication and sophisticated password policies
  - management servers, which provide support for applying enterprise security policies

Assumptions

The following assumptions are made for the operating system product and its operational environment:

- The underlying platform is physically protected, to a large extent. The hardware that the OS manages is secured by defensive measures that make physical attacks impractical for most attackers. At the same time, casual passersby might attempt to trivially access the system.
- The OS implements some security-relevant functionality that does not require evaluation (e.g., network time synchronization, process scheduling, and virtual memory management including process separation).
- Depending on configuration and capability, the OS may or may not be:
  - configuration-managed by the enterprise

    - bound to directory services to support multi-user login
- The OS runs application software developed by a third-party. The applications are not intentionally developed to be malicious, but can contain inadvertent coding errors. These errors introduce risk that control of an application may be seized by a malicious entity. The OS shall confine these applications within the originally designated operating environment.
- The platform is connected to a network. For purposes of sending/receiving data, to include software updates, the platform is connected to other entities. Other entities on the network are not inherently trustable.
- Administrators are not malicious in nature.
- Users are not malicious in nature, though they may inadvertently or intentionally engage in risky behavior.

Optional Extensions

Additional security functionality that may be appropriate for some use cases, and can be expressed in extensions to this document, includes:

- Multi-level Security (MLS) access controls
- Attestation of security measurements
- Data-at-rest protection - already covered in other PPs
- IPSec VPNs - already covered in other PPs

Outside the TOE's Scope

The following list contains items that are explicitly out-of-scope for any evaluation against the OS PP

- Malicious, Highly-Privileged Administrators - Highly-privileged administrators acting maliciously can disable most, if not all, security protections on the OS. Additionally procedural controls that are out of scope of this document should be considered to help highlight administrator accounts acting suspiciously.
- Zero Days - The disclosure of recently published vulnerabilities (Zero Days) should not be used as a reason to fail an OS undergoing evaluation.
- Unofficial Versions - Non-vendor supplied install images often contain added functionality and may weaken the normal operating functionality of the OS
- Platform - The OS PP shall not address the hardware or firmware of its underlying platform to include the boot sequence before control is handed off to the OS. That the platform itself is virtual or physical is irrelevant to any evaluations.
- Applications - The OS PP shall not address applications that are not delivered as part of the OS installation process.