National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Protection Profile for General Purpose Operating Systems, Version 4.0, August 14, 2015

Report Number: CCEVS-VR-PP-0024
Dated: 17 December 2015
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Protection Profile Evaluation
Booz Allen Hamilton.
Linthicum, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Protection Profile for General Purpose Operating Systems, Version 4.0 (GPOSPP40). It presents a summary of the GPOSPP40 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the GPOSPP40 was performed against the APE class Security Assurance Requirements (SARs) defined in CC Part 3 [3] and the Common Evaluation Methodology (CEM) [4]. The evaluation was performed by the Booz Allen Hamilton. Common Criteria Testing Laboratory (CCTL) in Linthicum, Maryland, United States of America, and was completed in December 2015.

The evaluation determined that the GPOSPP40 is both Common Criteria Part 2 Extended and Part 3 Extended. The PP identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4).

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team found that the PP failed to meet several of the requirements of the APE components in its initial version. These findings were delivered to NIAP, which issued updated materials that resolved the failures, resulting in a fully conformant PP.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of PPs are typically performed concurrent with the first product evaluation against the PP. In this case, no evaluations have been conducted under this version of the PP, so the GPOSPP40 was evaluated as a standalone document.

The GPOSPP40 contains a set of “base” requirements that all conformant STs must include as well as “additional” requirements that are either conditional or strictly optional, depending on the requirement in question. The vendor may choose to include such requirements in the ST and still claim conformance to this PP. If the vendor’s TOE performs capabilities that are governed by any additional requirements, that vendor is expected to claim all of the additional requirements that relate to these capabilities.

Because no product has been evaluated against this specific PP, it is possible that the evaluation of a Security Target (ST) against this PP may necessitate updates to the PP. If this occurs, any appropriate updates to this validation report will be made.

The following identifies the PP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP, as well as subsequent evaluations that address additional optional requirements in the GPOSPP40.

Protection Profile	*Protection Profile for General Purpose Operating Systems, version 4.0, August 14, 2015*
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 extended
CCTL	Booz Allen Hamilton, Linthicum, MD USA

3 GPOSPP Description

This Protection Profile focuses on the security functionality of operating systems. 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.

The operating system boundary encompasses the OS kernel and its drivers, shared software libraries, and some application software embedded within the OS. The applications considered within the Target of Evaluation (TOE) are those that provide essential security services, many of which run with elevated privileges. The operating system boundary does not include applications that are covered by more specific Protection Profiles, even when it is necessary to evaluate some of their functionality as it relates to their role as part of the OS.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: TOE Assumptions

Assumption Name	Assumption Definition
A.PLATFORM	The OS relies upon a trustworthy computing platform for its execution. This underlying platform is out of scope of this PP.
A.PROPER_USER	The user of the OS is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy. At the same time, malicious software could act as the user, so requirements which confine malicious subjects are still in scope.
A.PROPER_ADMIN	The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy.

4.2 Threats

Table 2: Threats

Threat Name	Threat Definition
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with applications and services running on or part of the OS with the intent of compromise. Engagement may consist of altering existing legitimate communications.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between applications and services that are running on or part of the OS.
T.LOCAL_ATTACK	An attacker may compromise applications running on the OS. The compromised application may provide maliciously formatted input to the OS through a variety of channels including unprivileged system calls and messaging via the file system.
T.LIMITED_PHYSICAL_ACCESS	An attacker may attempt to access data on the OS while having a limited amount of time with the physical device.

4.3 Organizational Security Policies

There are no organizational security policies defined for this PP.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 3: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.ACCOUNTABILITY	Conformant OSs ensure that information exists that allows administrators to discover unintentional issues with the configuration and operation of the operating system and discover its cause. Gathering event information and immediately transmitting it to another system can also enable incident response in the event of system compromise.
O.INTEGRITY	Conformant OSs ensure the integrity of their update packages. OSs are seldom if ever shipped without errors, and the ability to deploy patches and updates with integrity is critical to enterprise network security. Conformant OSs provide execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems.
O.MANAGEMENT	To facilitate management by users and the enterprise, conformant OSes provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration and application execution control.

TOE Security Obj.	TOE Security Objective Definition
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of credentials in the event of loss of physical control of the storage medium, conformant OSs provide data-at-rest protection for credentials. Conformant OSes also provide access controls which allow users to keep their files private from other users of the same system.
O.PROTECTED_COMMS	To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant OSs provide mechanisms to create trusted channels for CSP and sensitive data. Both CSP and sensitive data should not be exposed outside of the platform.

The following table contains objectives for the Operational Environment.

Table 4: Security Objectives for the Operational Environment

TOE Security Obj.	TOE Security Objective Definition
OE.PLATFORM	The OS relies on being installed on trusted hardware.
OE.PROPER_USER	The user of the OS is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy. Standard user accounts are provisioned in accordance with the least privilege model. Users requiring higher levels of access should have a separate account dedicated for that use.
OE.PROPER_ADMIN	The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy.

5 Requirements

As indicated above, requirements in the GPOSPP40 are comprised of the "base" requirements and additional requirements that are conditionally optional. The following are table contains the "base" requirements that were validated as part of the APE class evaluation.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit Data Generation
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation
	FCS_CKM.2: Cryptographic Key Establishment
	FCS_CKM_EXT.3: Cryptographic Key Destruction
	FCS_COP.1(1): Cryptographic Operation – Encryption/Decryption
	FCS_COP.1(2): Cryptographic Operation – Hashing
	FCS_COP.1(3): Cryptographic Operation – Signing
	FCS_COP.1(4): Cryptographic Operation – Keyed-Hash Message Authentication
	FCS_RBG_EXT.1: Random Bit Generation
FDP: User Data Protection	FDP_ACF_EXT.1: Access Controls for Protecting User Data
	FDP_IFC_EXT.1: Information Flow Control
FIA: Identification and Authentication	FIA_AFL.1: Authentication Failure Handling
	FIA_UAU.5: Multiple Authentication Mechanisms
	FIA_X509_EXT.1: X.509 Certificate Validation

Requirement Class	Requirement Component
	FIA_X509_EXT.2: X.509 Certificate Authentication
FMT: Security Management	FMT_MOF_EXT.1: Management of Security Functions Behavior
FPT: Protection of the TSF	FPT_ACF_EXT.1: Access Controls
	FPT_ASLR_EXT.1: Address Space Layout Randomization
	FPT_SBOP_EXT.1: Stack Buffer Overflow Protection
	FPT_TST_EXT.1: Boot Integrity
	FPT_TUD_EXT.1: Integrity for Installation and Update
	FPT_TUD_EXT.2: Integrity for Installation and Update of Application Software
FTP: Trusted Path/Channels	FTP_ITC_EXT.1: Trusted Channel Communication
	FTP_TRP.1: Trusted Path

The following table contains the optional requirements contained in Appendices A through C, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_DTLS_EXT.1: DTLS Implementation	PP evaluation
	FCS_TLSC_EXT.2: TLS Client Protocol	PP evaluation
	FCS_TLSC_EXT.3: TLS Client Protocol	PP evaluation
	FCS_TLSC_EXT.4: TLS Client Protocol	PP evaluation
FPT: Protection of the TSF	FPT_SRP_EXT.1: Software Restriction Policies	PP evaluation
	FPT_W^X_EXT.1: Write XOR Execute Memory Pages	PP evaluation
FTA: TOE Access	FTA_TAB.1: Default TOE Access Banners	PP evaluation

6 Assurance Requirements

The following are the assurance requirements contained in the GPOSPP40:

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1 Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labeling of the TOE
	ALC_CMS.1: TOE CM Coverage
	ALC_TSU_EXT.1: Timely Security Updates
ATE: Tests	ATE_IND.1: Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey

7 Results of the Evaluation

The CCTL reviewed the GPOSPP40 to derive the following initial results.

APE Requirement	Evaluation Verdict

APE_CCL.1	Pass
APE_ECD.1	Fail
APE_INT.1	Pass
APE_OBJ.2	Pass
APE_REQ.1	Fail

The specific findings that caused the failures were the absence of an extended components definition and some incorrect use of operations in the FCS class SFRs. These were resolved in the following manner:

- An extended components definition, consistent with APE_ECD.1, did not previously exist. It was created as a separate document.
- Several SFRs required modifications as part of evaluating APE_REQ.1 because they did not have all operations performed. These SFRs were revised and issued as part of NIAP Technical Decision 0078 (https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=78). The following SFRs were affected:
  - FCS_CKM.1
  - FCS_CKM.2
  - FCS_COP.1(1)
  - FCS_COP.1(2)
  - FCS_COP.1(3)
  - FCS_COP.1(4)

As a result of these corrections, the failing verdicts were addressed and the PP was found to pass all applicable APE assurance requirements.

8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance in the ESMICMPP Assurance Activities to determine whether or not the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.

- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Protection Profile for General Purpose Operating Systems, version 4.0, August 14, 2015