National Information Assurance Partnership

COMMON CRITERIA EVALUATION AND VALIDATION SCHEME

VALIDATION REPORT

Protection Profile for Multi-level Operating Systems in Environments Requiring Medium Robustness, Version 1.22, dated 23 May 2001

Report Number: CCEVS-VR-01-0003

Dated: JUNE 30, 2001

VERSION: 1.1

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 6740
FORT GEORGE G. MEADE, MD 20755-6740

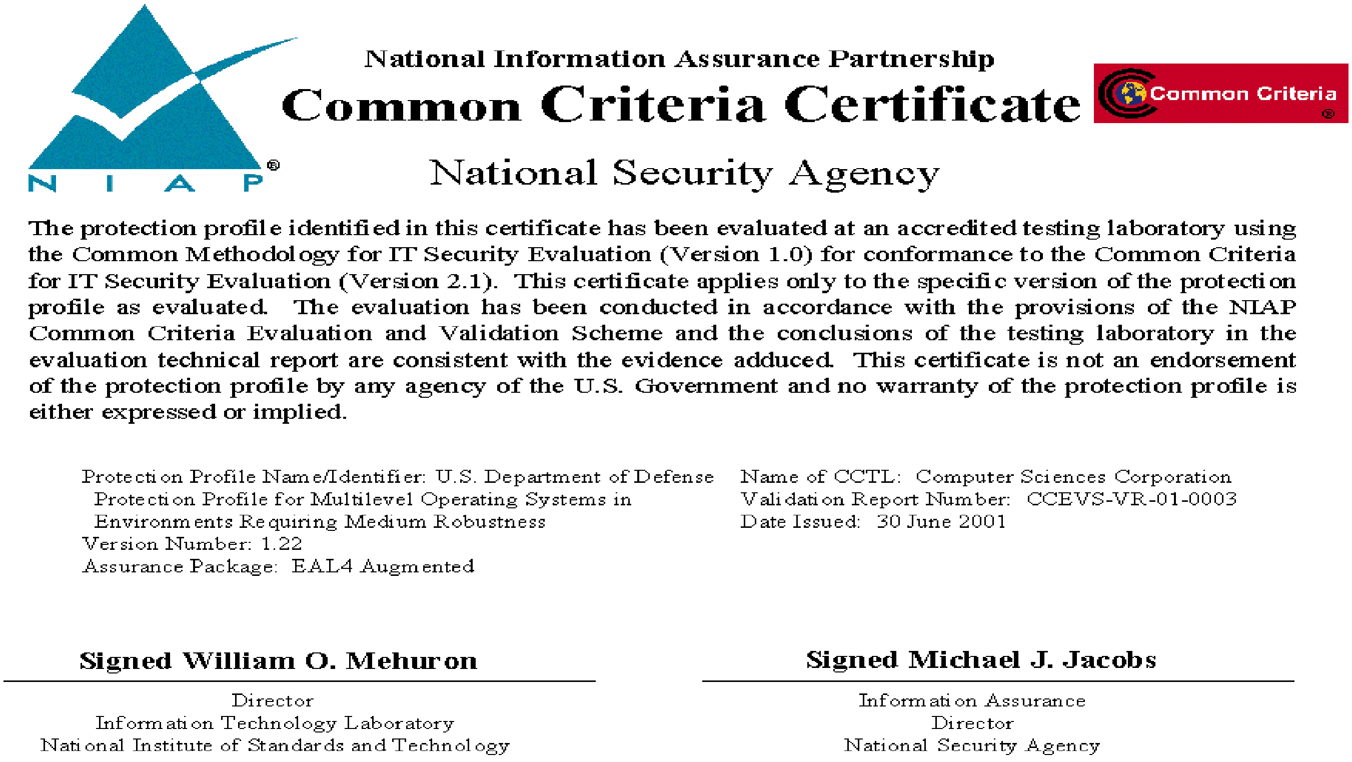
ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell
The Mitre Corporation
William R. Simpson
Institute for Defense Analyses

Common Criteria Testing Laboratory

Computer Science Corporation
Annapolis Junction, Maryland


N I A P ®
Common Criteria ®

National Information Assurance Partnership

Common Criteria Certificate

National Security Agency

The protection profile identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). This certificate applies only to the specific version of the protection profile as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the protection profile by any agency of the U.S. Government and no warranty of the protection profile is either expressed or implied.

Protection Profile Name/Identifier: U.S. Department of Defense Protection Profile for Multilevel Operating Systems in Environments Requiring Medium Robustness
Version Number: 1.22
Assurance Package: EAL4 Augmented

Name of CCTL: Computer Sciences Corporation
Validation Report Number: CCEVS-VR-01-0003
Date Issued: 30 June 2001

Signed William O. Mehuron
Director
Information Technology Laboratory
National Institute of Standards and Technology

Signed Michael J. Jacobs
Information Assurance
Director
National Security Agency

Executive Summary

An evaluation of the Protection Profile for Multilevel Operating Systems in Environments Requiring Medium Robustness [MLOS_PP] was begun 01 December 2000 and completed 30 June 2001. The [MLOS_PP] evaluation was performed by Computer Sciences Corporation in the United States. The evaluation was carried out in accordance with requirements drawn from the Common Criteria CCv2.1, Part 3, Class APE: Protection Profile Evaluation. The assurance activities in this CC class offer confidence that the [MLOS_PP] contains requirements that are:

- justifiably included to counter stated threats and meet realistic security objectives,
- internally consistent and coherent and
- technically sound.

Computer Sciences Corporation, the Common Criteria Testing Laboratory [CCTL], is certified by the NIAP validation body for laboratory accreditation. The CCTL has presented CEM work units and rationale that are consistent with the CC, the CEM and CCEVS publication number 4 Guidance to CCEVS Approved Common Criteria Testing Laboratories. The CCTL team concluded that the requirements of the APE class have been met. Therefore, a **pass** verdict has been issued, by the CCTL, for the protection profile assurance family.

The validation team followed the procedures outlined in the Common Criteria Evaluation Scheme [CCEVS] publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology [CEM], and CCEVS policy. The validation team concludes that the evaluation has completed and the evaluation team's results are valid. Therefore, the Common Criteria Evaluation and Validation Scheme grants a Common Criteria Certificate to the sponsor, acknowledging the successful completion of the evaluation and the validity of this Common Criteria Protection Profile.

Evaluation Specific Details
Dates of Evaluation: 1 December 2000 – 30 June 2001
Evaluated Product: Protection Profile for Multilevel Operating Systems in Environments Requiring Medium Robustness, version 1.22, dated 23 may 2001
Developer: Information Assurance Directorate, National Security Agency, 9800 Savage Road, Fort George G. Meade, MD 20755-6000.
CCTL: Computer Sciences Corporation
Evaluation Class: EAL4 Augmented
Validation Team: Paul Bicknell, The MITRE Corporation
William R. Simpson, Institute for Defense Analyses

Protection Profile Identification

Protection Profile for Multilevel Operating Systems in Environments Requiring Medium Robustness, version 1.22, dated 23 May 2001.

Protection Profile Summary

The [MLOS_PP] specifies functional and assurance security requirements for commercial-off-the-shelf (COTS) general-purpose multilevel operating systems in networked environments containing sensitive information. The functional behavior of [MLOS_PP] compliant products as well as the assurance activities of an evaluation of those products are described, explicitly identifying CCv2.1 functional and assurance requirements supplemented with explicitly stated functional and assurance requirements (SREs).

The [MLOS_PP] makes use of Department of Defense (DoD) Information Assurance (IA) guidance and policy as the basis to establish the requirements necessary to achieve the security objectives of the Target of Evaluation (TOE) and its environment.

Operating systems evaluated against the [MLOS_PP] will associate sensitivity labels with all objects and all its users will have an associated clearance level identifying the maximum security level of data that they may access. Operating systems evaluated against the [MLOS_PP] can operate in the following multilevel environments;

- Processing data up to the Secret level with uncleared authorized users,
- Processing data up to the Top Secret level with minimum user clearances of Secret, and
- Processing data up to the Top Secret/Sensitive Compartmental Information (TS/SCI) level with minimum user clearances of Top Secret.

Conformant products support Identification and Authentication, Discretionary Access Control (DAC), Mandatory Access Control (MAC), Mandatory Integrity Control (MIC), an audit capability, and cryptographic services. These systems provide adequate security services, mechanisms, and assurances to process sensitive information in medium robustness environments, as specified in the “Guidance and Policy for Department of Defense Information Assurance” (GiG). They can process mission supportive and mission administrative information.

PP conformant systems may be suitable for use in non-DoD environments. The mechanisms specified by this PP may be appropriate for the protection of administrative, private, and sensitive information.

Threats

Specific threats to IT security that should be countered by the operating system:

T.ADMIN_ERROR	Improper administration may result in defeat of specific security features.
T.ADMIN_ROGUE	Authorized administrator’s intentions may become malicious resulting in TSF data to be compromised.
T.AUDIT_CORRUPT	A malicious process or user may cause audit records to be lost or modified, or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker’s actions.
T.CONFIG_CORRUPT	A malicious process or user may cause configuration data or other trusted data to be lost or modified.
T.DATA_NOT_SEPARATED	Systems may not adequately separate data on the basis of its sensitivity or integrity label, thereby allowing users improper access to labeled data.
T.DOS	A malicious process or user may block others from system resources via a resource exhaustion denial of service attack.
T.EAVESDROP	A malicious process or user may intercept transmitted data inside or outside of the enclave.
T.IMPROPER_INSTALLATION	Operating system may be delivered, installed, or configured in a manner that undermines security.
T.INSECURE_START	Reboot may result in insecure state of the operating system.
T.MASQUERADE	A malicious process or user on one machine on the network may masquerade as an entity on another machine on the same network.
T.OBJECTS_NOT_CLEAN	Systems may not adequately remove the data from objects between usage by different users, thereby releasing information to a user unauthorized for the data.

T.POOR_DESIGN	Unintentional or intentional errors in requirement specification, design or development of the IT operating system may occur.
T.POOR_IMPLEMENTATION	Unintentional or intentional errors in implementing the design of the IT operating system may occur.
T.POOR_TEST	Incorrect system behavior may result from inability to demonstrate that all functions and interactions within the operating system operation are correct.
T.REPLAY	A malicious process or user may gain access by replaying authentication (or other) information.
T.SPOOFING	A hostile entity may masquerade itself as the IT operating system and communicate with authorized users who incorrectly believe they are communicating with the IT operating system.
T.SYSACC	A malicious process or user may gain unauthorized access to the administrator account, or that of other trusted personnel.
T.UNATTENDED_SESSION	A malicious process or user may gain unauthorized access to an unattended session.
T.UNAUTH_ACCESS	Unauthorized access to data by a user may occur.
T.UNAUTH_MODIFICATION	Unauthorized modification or use of IT operating system attributes and resources may occur.
T.UNDETECTED_ACTIONS	Failure of the IT operating system to detect and record unauthorized actions may occur.
T.UNIDENTIFIED_ACTIONS	Failure of the administrator to identify and act upon unauthorized actions may occur.
T.UNKNOWN_STATE	Upon failure of the IT operating system, the security of the IT operating system may be unknown.
T.USER_CORRUPT	User data may be lost or tampered with by other users.

Security Policy

Policy statements whose enforcement must be provided by the operating system’s security mechanisms:

P.ACCESS_BANNER The system shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

P.ACCOUNT The users of the system shall be held accountable for their actions within the system.

P.AUTHORIZATION The system must limit the extent of each user's abilities in accordance with the TSP.

P.AUTHORIZED_USERS Only those users who have been authorized to access the information within the system may access the system.

P.CLEARANCE The system must limit access to protected resources to authorized users whose security and integrity levels are appropriate for the labeled data.

P.CRYPTOGRAPHY The system shall use NIST FIPS validated cryptography (methods and implementations) for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).

P.I_AND_A All users must be identified and authenticated prior to accessing any controlled resources with the exception of public objects.

P.INDEPENDENT_TESTING The operating system must undergo independent testing as part of an independent vulnerability analysis.

P.LABELED_OUTPUT The beginning and end of all paged, hardcopy output must be marked with sensitivity labels that properly represent the sensitivity of the output.

P.NEED_TO_KNOW The system must limit the access to the information in protected resources to those authorized users who have a need to know that information.

P.REMOTE_ADMIN_ACCESS Authorized administrators may remotely manage the IT operating system.

P.RESOURCE_LABELS All resources must have associated labels identifying the security and integrity levels of data contained therein.

P.ROLES The authorized administrator and cryptographic administrator shall have separate and distinct roles associated with them.

P.SYSTEM_INTEGRITY The system must have the ability to periodically validate its correct operation and, with the help of administrators, it must be able to recover from any errors that are detected.

P.TRACE The operating system must have the ability to review the actions of individuals.

P.TRUSTED_RECOVERY Procedures and/or mechanisms shall be provided to assure that, after a system failure or other discontinuity, recovery without a protection compromise is obtained

P.USER_CLEARANCE All users must have a clearance level identifying the maximum security and integrity levels of data they may accessed.

P.VULNERABILITY_SEARCH The system must undergo an analysis for vulnerabilities beyond those that are obvious.

Usage Assumptions

This protection profile specifies DoD requirements for general-purpose multi-user COTS operating systems together with the underlying hardware that supports these systems. Such operating systems are typically employed in a networked office automation environment containing file systems, printing services, network services and data archival services and can host other applications (e.g., mail, databases). This profile does not specify any security characteristics of security hardened devices (e.g. guards, firewalls) that provide environment protection at network boundaries. When this TOE is used in composition with other systems to make up a larger system environment, the boundary protection must provide the appropriate security mechanisms, cryptographic strengths and assurances to ensure adequate protection for the security and integrity of this TOE.

Environmental Assumptions

Assumptions about the use of the IT operating system:

A.PHYSICAL It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the operating system and the value of the stored, processed, and transmitted information.

Clarification of Scope

Minimum requirements for medium robustness are specified in "GIG IA Implementation Guidance", Section 5.1.2 of the "DoD Chief Information Officer, Guidance and Policy Memorandum No. 6-8510" dated 16 June 2000 [GIG].

Security Content of PP

Conformant operating systems include the following security features:

- Identification and Authentication which mandates authorized users to be uniquely identified and authenticated before accessing information stored on the system;
- Discretionary Access Control (DAC) which restricts access to objects based on the identity of subjects and/or groups to which they belong, and allows authorized users to specify protection for objects that they control;
- Mandatory Access Control (MAC) which enforces the U.S. DoD data sensitivity classification model (i.e., Unclassified, Secret, Top Secret) on all authorized users and all TOE resources;
- Mandatory Integrity Control (MIC) which enforces an integrity policy on all authorized users and TOE resources to prevent malicious entities from corrupting data;
- Cryptographic services which provide mechanisms to protect TSF code and data and also provide support to allow authorized users and applications to encrypt and digitally sign data as it resides within the system and as it is transmitted to other systems; and
- Audit services which allow authorized administrators to detect and analyze potential security violations.

Other characteristics of complaint TOEs include:

- the ability to process multiple security levels of information in a multilevel environment,

The TOE does not provide:

- mechanisms or services to ensure availability of data residing on the TOE. [If availability requirements exist, the environment must provide the required mechanisms (e.g., mirrored/duplicated data)], and
- complete physical protection mechanisms, which must be provided by the environment.

Documentation

The evidence used in this evaluation is based solely upon:

[MLOS_PP] Protection Profile for Multilevel Operating Systems in Environments Requiring Medium Robustness, Version 1.22, 23 May 2001.

The evaluation and validation methodology was drawn from the following:

[CC_PART1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, version 2.1.

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, version 2.1.

[CC_PART2A] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, version 2.1.

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, version 2.1.

[CEM_PART1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[CCEVS_PUB 1] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0, May 1999.

[CCEVS_PUB 2] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures, Scheme Publication #2, Version 1.5, May 2000

.[CCEVS_PUB 3] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Technical Oversight and Validation Procedures, Scheme Publication #3, Version 0.5, February 2001

[CCEVS_PUB 4] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Scheme Publication #4, Version 1, March 20, 2001

[CCEVS_PUB 5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Sponsors of IT Security Evaluations, Scheme Publication #5, Version 1.0, 31 August 2000.

Additional data resides in:

[GIG] "GIG IA Implementation Guidance", of the "DoD Chief Information Officer, Guidance and Policy Memorandum No. 6-8510" dated 16 June 2000.

Results of the Evaluation

The Common Criteria Testing Laboratory [CCTL] team conducted the evaluation according to the CC and the CEM and concluded that the requirements of the APE class were met. Therefore, a **pass** verdict has been issued for the protection profile assurance family.