National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

U.S. Government
Router Protection Profile
for
Medium Robustness Environments

Report Number: CCEVS-VR-VID10185-2007

Dated: 2007-01-05

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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Stephen C. Butterfield, Principal

MitreTek Systems, Inc.

Falls Church, VA

Common Criteria Testing Laboratory

James L. Arnold, Jr.

Jean Petty

Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300

Columbia, MD

Table of Contents

1. EXECUTIVE SUMMARY

This report is intended to assist the end-user of this Protection Profile (PP) with determining the suitability of the product type in their environment. End-users should review both the PP which is where specific security requirements are stated, and this Validation Report (VR) which describes how those security claims were evaluated.

This report documents the NIAP Validators' assessment of the evaluation of U.S. Government Router Protection Profile for Medium Robustness Environments. It presents the evaluation results, their justifications, and the conformance results. This Validation Report applies only to the specific version of the PP 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.

The information contained in this Validation Report is not an endorsement of the U. S. Government Router Protection Profile for Medium Robustness Environments, Version 1.0 by any agency of the US Government and no warranty of the PP is either expressed or implied

The technical information included in this report was obtained from the U. S. Government Router Protection Profile (PP) for Medium Robustness Environments, Version 1.0, produced by U.S Government and the U. S. Government Router Protection Profile for Medium Robustness Environments Evaluation Technical Report (ETR), dated December 31, 2006, produced by SAIC, a CCEVS approved Common Criteria Testing Laboratory (CCTL).

The U.S. Government Router PP for Medium Robustness Environments specifies a set of security functional and assurance requirements for Information Technology (IT) products. A router monitors, routes and manipulates network traffic to facilitate its delivery to the proper destination on a network or between networks. The Router PP was constructed to provide a target metric for the deployment of router devices. This protection profile identifies security functions and assurances that represent the lowest common set of requirements that must be addressed at a Medium Robustness level by a router.

The validation team agrees that the CCTL presented appropriate rationales to support the Results of Evaluation presented in Section 5, and the Conclusions presented in Section 6 of the ETR. The validation team therefore concludes that the evaluation and the Pass results for the U. S. Government Router Protection Profile (PP) for Medium Robustness Environments, Version 1.0 are complete and correct.

2. IDENTIFICATION

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	U. S. Government Router Protection Profile for Medium Robustness Environments, Version 1.0
Evaluation Technical Report	*Evaluation Technical Report for theU.S. Government Router Protection Profile for Medium Robustness, Version 1.0, 31 December 2006*
Conformance Result	CC V2.3, Part 2 extended, Part 3 conformant, Medium Robustness
Sponsor	NSA
Developer	NSA
Evaluators	SAIC
Validators	MitreTek Systems, Inc.

3. SECURITY POLICY

The PP requires the following Security functionality:

P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ADMIN_ACCESS	Administrators shall be able to administer the TOE both locally and remotely through protected communications channels.
P.CRYPTOGRAPHY	The TOE shall use NIST FIPS validated cryptography as a baseline with additional NSA-approved methods for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys), and for cryptographic operations (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).
P.VULNERABILITY_ANALYSIS_TEST	The TOE must undergo appropriate independent vulnerability analysis and penetration testing to demonstrate that the TOE

	is resistant to an attacker possessing a medium attack potential.
P.COMPATIBILITY	The TOE must meet Request for Comments (RFC) requirements for implemented protocols to facilitate interoperation with other routers and network equipment using the same protocols.

4. ASSUMPTIONS

The following Personnel and Physical Assumptions apply to the TOE usage and environment:

A.NO_GENERAL_PURPOSE	The administrator ensures there are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
A.PHYSICAL	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.
A.AVAILABILITY	Network resources shall be available to allow clients to satisfy mission requirements and to transmit information.

5. THREATS

The following threats apply to Medium Robustness TOEs:

T.ADMIN_ERROR	An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.
T.ADMIN_ROGUE	An administrator's intentions may become malicious resulting in user or TOE Security Functions (TSF) data being compromised.
T.AUDIT_COMPROMISE	A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.

T.CRYPTO_COMPROMISE	A malicious user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
T.FLAWED_DESIGN	Unintentional or intentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a malicious user or program.
T.FLAWED_IMPLEMENTATION	Unintentional or intentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a malicious user or program.
T.MALICIOUS_TSF_COMPROMISE	A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.MASQUERADE	A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain access to data or TOE resources.
T.POOR_TEST	Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered thereby causing potential security vulnerabilities.
T.REPLAY	A user may gain inappropriate access to the TOE by replaying authentication information, or may cause the TOE to be inappropriately configured by replaying TSF data or security attributes (e.g., captured as transmitted during the course of legitimate use).
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
T.RESOURCE_EXHAUSTION	A malicious process or user may block others from system resources (e.g., connection state tables, TCP connections) via a resource exhaustion denial of service attack.

T.SPOOFING	A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.
T.UNAUTHORIZED_ACCESS	A user may gain access to user data for which they are not authorized according to the TOE security policy.
T.UNIDENTIFIED_ACTIONS	The administrator may fail to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.
T.UNAUTHORIZED_PEER	An unauthorized IT entity may attempt to establish a security association with the TOE.
T.UNKNOWN_STATE	When the TOE is initially started or restarted after a failure, the security state of the TOE may be unknown.
T.EAVESDROP	A malicious user or process may observe or modify user or TSF data transmitted between physically separated parts of the TOE.

6. DOCUMENTATION

The TOE following documentation applies to the evaluation of this Protection Profile:

- U.S. Government Router Protection Profile for Medium Robustness Environments, Version 1.0

7. RESULTS OF THE EVALUATION

The Evaluation Team conducted the evaluation in accordance with the APE section of the CC and the CEM.

Section 5, *Results of Evaluation* states:

> "The evaluation determined the U.S. Government Router Protection Profile For Medium Robustness Environments to be Part 2 and Part 3 extended."

Section 5, *Conclusions* states:

"Each verdict for each CEM work unit in the APE ETR is a "PASS". Therefore, the U.S. Government Router Protection Profile For Medium Robustness Environments is a CC compliant PP."

8. VALIDATOR COMMENTS

The Validator determined that the evaluation and all of its activities were performed in accordance with the CC, the CEM and CCEVS practices. The Validator agrees that the CCTL presented appropriate rationales to support the Results of the Evaluation presented in Section 5 of the ETR. Therefore, the Validator concludes that the evaluation and the Pass results for the TOE identified below are complete and correct:

- U.S. Government Router Protection Profile For Medium Robustness Environments, Version 1.0

9. LIST OF ACRYONYMS

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

10. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 2.3.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 2.3.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 2.3.

[4] Common Evaluation Methodology for Information Technology Security – Version 2.3.