Trust Technology Assessment Program

Validation Report

U.S. Department of Defense Traffic Filter Firewall Protection Profile for Medium Robustness Environments version 1.4

TTAP Report Number: TTAP-VR-0009
May, 2000

Mutual Recognition Arrangement
of
Common Criteria Certificates in the Field of
Information Technology Security

The Trust Technology Assessment Program (TTAP) Oversight Board is a member of the above Arrangement. As such, it confirms that a Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements contained in the evaluation and this Validation Report are those of the Oversight Board which issues it and of the evaluation facility which carried out the evaluation. There is no implication of acceptance by Members of the Arrangement of liability with respect to judgements or losses sustained as a result of reliance placed upon information contained herein.

Executive Summary

Production and evaluation of the U.S.Department of Defense Traffic Filter Firewall Protection Profile for Medium Robustness Environments, version 1.4 was sponsored by the National Security Agency.

This profile has been designed for use under a Common Criteria Scheme party to the Mutual Recognition Arrangement. It completed evaluation in May, 2000 by Computer Sciences Corporation (an accredited Trust Technology Assessment Program evaluation facility in the United States) and has been shown to be conformant with Part 3 of the Common Criteria for Information Technology Security Evaluation, version 2.1 (CCv2.1) requirements for Protection Profiles.

Products found to be compliant with this protection profile meet the minimum security requirements for firewalls used by the U.S. Department of Defense handling mission critical information in a medium robustness environment. Such devices are capable of screening network traffic at the network and transport protocol levels (i.e., TCP/IP), authenticating authorized administrators for actions taken on the firewall, and auditing security-relevant events that occur through and on the firewall.

1.0 Introduction

This report states the outcome of the IT security evaluation of the U.S. Department of Defense Traffic Filter Protection Profile-Medium Robustness, Version 1.4 dated May, 2000 (TFPP-M). It is intended to characterize the nature of the profile and its evaluation to assist potential users when judging the suitability of the PP in the context of their specific requirements. Prospective users are advised to read this report in conjunction with the TFPP-M which specifies the functional, environmental and assurance requirements for TFPP-M conformant firewalls.

2.0 Protection Profile Overview

The TFPP-M comprises functional and assurances requirements. The functional behavior of TFPP-M compliant products as well as the assurance activities of an evaluation of those products are described, explicitly identifying CCv2.1 functional and assurance requirements.

2.1 TFPP-M Functional Characteristics

TFPP-M compliant products selectively route information flows among internal and external networks according to a site's security policy rules (defined by the firewall authorized administrator). Only an authorized administrator has the authority to change the security policy rules. Traffic filtering decisions are based on source address, destination address, transport layer source port, transport layer destination port and the network from which packets arrive. Administration of a firewall may be provided locally or remotely. If performed locally, the authorized administrators must identify and authenticate before accessing the TOE (e.g., name and password). If the firewall provides the capability for remote administration, then authorized administrators must identify and authenticate themselves using a single use authentication mechanism (e.g., name and one time password). Upon authentication via a remote means, administrative traffic is protected via an encrypted link using U.S. nationally approved encryption (i.e., FIPS PUB 140-1 compliant) algorithms and modules. TFPP-M compliant firewalls provide auditing functions to record firewall security relevant events and audit trail data is stamped with a dependable date and time of action. Auditable events include modifications to the group of users associated with the authorized administrator role, all use of the identification/authentication mechanism, and all information flow control decisions made by the firewall according to the security policy.

Common Criteria Requirements. The TFPP-M comprises functional and assurance requirements. Functional requirements drawn from Part 2 of CCv2.1 included in this PP are:

Cryptography for Remote Administration	FCS_COP.1
Routing Information Flow Control	FDP_IFC, FDP_IFF.1
Authorized Administrator (I/A and administrative functions	FIA_UAU.1, FIA_UAU.4, FIA_UID.1, FIA_ATD.1, FMT_SMR., FIA_AFL.1

Object Reuse Prevention	FDP_RIP.1
Non-Bypassability, Domain Separation	FPT_RVM, FPT_SEP.1
Protection by Default	FMT_MSA.3

2.2 TFPP-M Assurance Characteristics

The TFPP-M assurance requirements comprise developer and evaluator activities that contribute to confidence that compliant firewalls perform as specified. The activities include specifying the functional behavior and design of the product to facilitate testing, performing evaluator analysis on the product, functionally testing the product against its specification and various delivery and configuration management documentation. It also includes ad hoc penetration testing by a third party evaluation laboratory as well a more concentrated effort staffed by the U.S. Government.

Assurance requirements drawn from Part 3 of the CCv2.1 included in this PP are the requirements which comprise the Evaluation Assurance Level 2 (EAL2) augmented with specific additional penetration activities. They are:

Configuration Manage-ment	ACM_CAP.2
Delivery	ADO_DEL.1
Installation	ADO_IGS.1
Functional Specification	ADV_FSP.1
High Level Design	ADV_HLD.2
Implementation Represen-tation	ADV_IMP.1
Low Level Design	ADV_LLD.1
Design Representative Correspondence	ADV_RCR.1
Administrative Security Guidance	AGD_ADM.1
User Security Guidance	AGD_USR.1
Tools and Techniques	ALC_TAT.1
Functional Testing	ATE_COV.1, ATE_FUN.1, ATE_IND.2

Search for Obvious Vulnerabilities	AVA_VLA.3
Probabilistic Security Feature Strength of Function	AVA_SOF.1

3.0 Evaluation Results

The TFPP-M evaluation was performed by Computer Sciences Corporation in the United States. It was completed and certified by the TTAP Oversight Board in May, 2000. The evaluation was carried out in accordance with requirements drawn from CCv2.1, Part 3, Class APE: Protection Profile Evaluation. The assurance activities in this CC class offer confidence that the TFPP-M contains requirements that are:

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

A CCv2.1 PP evaluation using these requirements comprises the following evaluator activities:

Evaluation of the TOE Description	APE_DES.1
Evaluation of the Security Environment	APE_ENV.1
Evaluation of the PP Introduction	APE_INT.1
Evaluation of the Security Objectives	APE_OBJ.1
Evaluation of the IT Security Requirements	APE_REQ.1
Evaluation of Explicitly (i.e., non-CC) stated requirements	APE_SRE.1

References

1. Common Criteria, v2.1, Part 1
   Common Criteria Implementation Board
   August, 1999.

2. Common Criteria, v2.1, Part 2,
   Common Criteria Implementation Board,
   August, 1999.

3. Common Criteria, v2.1, Part 3,
   Common Criteria Implementation Board,
   August, 1999.

4. [DRAFT] Common Evaluation Methodology, v 0.6
   Common Evaluation Methodology Editorial Board,
   January 1999.

5. Federal Information Processing Standard Publication 140-1,
   Security Requirements for Cryptographic Modules,
   National Institute of Standards and Technology,
   January 1994.

6. U.S. Government Traffic Filter Firewall Protection Profile for Low-Risk Environments, v1.0
   National Security Agency/National Institute of Standards and Technology
   April 1999.