Trust Technology Assessment Program

Validation Report

U.S. Government Traffic Filter Firewall Protection Profile for Low-Risk Environments version 1.1

TTAP Report Number: TTAP-VR-0007
June, 1999

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. Government Traffic Filter Firewall Protection Profile for Low-Risk Environments, version 1.1 was sponsored by the National Institute of Standards and Technology and 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, 1999 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 2.0 (CCv2.0) 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. Government handling unclassified information in a low-risk 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.

Introduction

This report states the outcome of the IT security evaluation of the U.S. Government Traffic Filter Protection Profile for Low-Risk Environments, Version 1.1 dated April, 1999 (TFPP). 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 which specifies the functional, environmental and assurance requirements for TFPP conformant firewalls.

Protection Profile Overview

The TFPP comprises functional and assurances requirements. This section of the report characterizes the functional behavior of TFPP compliant products and explicitly identifies the CCv2.0 functional and assurance requirements that have been included.

TFPP Functional Characteristics

The TFPP defines the minimum security requirements for firewalls used by U.S. Government organizations handling unclassified information in a low-risk environment. 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 a trusted channel using U.S. Nationally approved encryption (i.e., FIPS PUB 140-1 compliant) algorithms and modules.

TFPP Compliant firewalls provide auditing functions to record firewall security relevant events. 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 comprises functional and assurance requirements. Functional requirements drawn from Part 2 of CCv2.0 included in this PP are:

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

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

Assurance requirements drawn from Part 3 of the CCv2.0 included in this PP are the requirements which comprise the Evaluation Assurance Level 2 (EAL2). They are:

Configuration Management	ACM_CAP.2
Delivery	ADO_DEL.1
Installation	ADO_IGS.1
Functional Specification	ADV_FSP.1
High Level Design	ADV_HLD.1
Design Representation Correspondence	ADV_RCR.1
Administrative Security Guidance	AGD_ADM.1
User Security Guidance	AGD_USR.1
Functional Testing	ATE_COV.1, ATE_FUN.1, ATE_IND.2
Search for Obvious Vulnerabilities	AVA_VLA.1
Probabilistic Security Feature Strength of Function	AVA_SOF

Evaluation Results

The TFPP evaluation was performed by Computer Sciences Corporation in the United States. It was completed and certified by the TTAP Oversight Board in April, 1999. The evaluation was carried out in accordance with requirements drawn from CCv2.0, Part 3, Class APE: Protection Profile Evaluation.[1] A CCv2.0 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.

Application of these requirements in the context of a CCv2.0 PP evaluation offers assurance that the TFPP contains requirements that are:

a) justifiably included to counter stated threats and meet realistic security objectives,
b) internally consistent and coherent and
c) technically sound.

1. A draft version of the Common Evaluation Methodology (version 0.6) was used as input into the evaluation. Because of its draft nature, strict compliance to this draft version was not required.

References

1. Common Criteria Part 1,
   Common Criteria Implementation Board
   CCIB-98-026, Version 2.0, May 1998.

2. Common Criteria Part 2,
   Common Criteria Implementation Board,
   CCIB-98-027, Version 2.0, May 1998.

3. Common Criteria Part 3,
   Common Criteria Implementation Board,
   CCIB-98-028, Version 2.0, May 1998.

4. [DRAFT] Common Evaluation Methodology,
   Common Evaluation Methodology Editorial Board,
   CEMEB-99/08, Version 0.6, January 1999.

5. Security Requirements for Cryptographic Modules
   National Institute of Standards and Technology,
   FIP PUB 140-1, January 1994.

6. U.S. Government Traffic Filter Firewall Protection Profile for Low-Risk Environments
   National Security Agency/National Institute of Standards and Technology
   Version 1.0, April 1999.