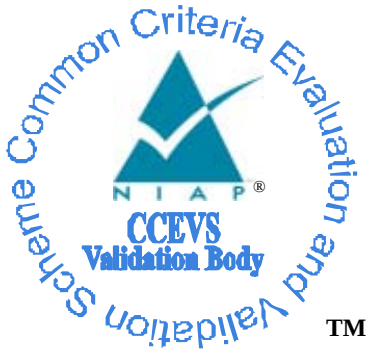
National Information Assurance Partnership



TM

Common Criteria Evaluation and Validation Scheme Validation Report

U.S. Government Protection Profile Intrusion Detection System – System For Medium Robustness Environments

Report Number: CCEVS-VR-07-0050
Dated: June 26, 2007
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

Scott Shorter
Orion Security Solutions
McLean, VA

Common Criteria Testing Laboratory

COACT, Inc., CAFÉ Lab
Rivers Ninety Five
9140 Guilford Road, Suite G
Columbia, MD 21046-2587

Table of Contents

1 Executive Summary

The evaluation of the U.S. Government Protection Profiles for Intrusion Detection System – System for Medium Robustness Environments was conducted by COACT, Inc., CAFÉ Lab CCTL in the United States and was completed on May 30, 2007. The Protection Profile (PP) identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Part 2 Version 2.2) for conformance to the APE requirements of the Common Criteria for IT Security Evaluation (Version 2.2).

This Validation Report applies only to the specific versions 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 Protection Profiles by any agency of the US Government and no warranty of the PP is either expressed or implied.

The COACT, Inc., CAFÉ Lab evaluation team concluded that the Common Criteria requirements for a PP Evaluation have been met.

The technical information included in this report was obtained from the Protection Profile produced by the U.S. Government, the Evaluation Technical Report produced by the COACT, Inc., CAFÉ Lab, and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.
The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List. Table 1 provides the details of the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme

Item	Identifier
Evaluated Protection Profile	Intrusion Detection System – System for Medium Robustness Environments, Version 1.0, April 2, 2006
Evaluation Technical Reports	U.S. Government Protection Profile Intrusion Detection System – System For Medium Robustness Environments Evaluation Technical Report, May 30, 2007, Document No. E4-0307-008
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.2
Common Criteria Testing Lab (CCTL)	COACT, Columbia, MD

3 Security Policy

The Security Functional Policies (SFPs) dictated by the PP are based upon the basic set of security policies including requiring collection, storage, and analysis of audit data collected by the scanning and sensing capabilities (the IDS audit data) as well as collection and storage of system audit data, cryptography, trusted path, identification and authentication, and administration.

3.1 Audit

3.1.1 Security Audit

"Security Audit" describes the TOE's generation of auditable events, audit records, alarms and audit management. The PP lists the minimum set of auditable system events and how the audit log must be protected. Each auditable event must generate an audit record. The TOE is also required to monitor the occurrence of auditable events and notify administrators if potential security violations occur.

3.1.2 IDS Audit

The TOE will generate an IDS audit log that contains events within the IT system being monitored. These events may include: static configuration information, misuse information, identification and authentication events, service requests, and events based on network traffic. The TOE will then perform analysis based on the information it has collected and generate alarms for potential intrusions that must be acknowledged by the IDS Administrator. The IDS Administrator must also manage the IDS specific functions including, but not limited to, what data is collected and what analyses will be performed. The TOE must ensure that storage of the IDS audit log is handled in such a way that no data will be lost.

3.2 Cryptography and Trusted Path

For a TOE that uses cryptographic functionality to achieve its security objectives, a number of requirements are levied on the cryptographic implementation, including the requirement

for FIPS 140-2 validation, minimum symmetric key strength of 128 bits, and numerous additional cryptographic requirements. Cryptography can be used to achieve a trusted path for administrators to manage the TOE, as well as for communications between physically separate TOE components.

ST authors are required to specify all cryptographic algorithms used by the TOE, and provide reference to their FIPS 140-2 validation certificates (i.e. the FIPS 140-2 CAVP algorithm certificates, not the FIPS 140-2 cryptomodule certificates)[1].

The ST must also describe how all keys are generated, including the RNG implementation, the source of the entropy to seed that RNG. Any key tests that are performed (e.g. RSA primality tests) should be added by the ST author as a refinement of FCS_CKM.1.1(2).

Specification of the precise key distribution algorithm is not required by the PP, but highly recommended, at least in the TOE. It is stated that the algorithm must comply with certain NIST publications.

Rigorous key management requirements are stated, including key error detection checks, encrypted storage of persistent keys, and destruction of non-persistent keys.

3.3 Identification and Authentication

Both administrators and TOE components must be identified and authenticated before the TOE will perform any actions on their behalf.

3.4 Administration

The PP define four separate administrative roles: Cryptographic Administrator, Audit Administrator, IDS Administrator and Security Administrator. The Cryptographic Administrator is responsible for the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the TOE. The Audit Administrator is responsible for the regular review and management of the TOE's audit data. The Security Administrator is responsible for all other administrative tasks (e.g., creating the TOE security policy) not addressed by the other three administrative roles. The IDS Administrator is solely responsible for regular review of the IDS audit data. The IDS Administrator is also in charge of managing all IDS data.

4 Threats, Assumptions and Policies

4.1 Threats

T.ADMIN_ERROR	An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.

[1] Which suffices as evidence the algorithms were tested for the CC evaluation.

T.AUDIT_COMPROMISE	A malicious user or process may view audit records, cause audit records and IDS audit records to be lost or modified, or prevent future audit records and IDS 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.EAVESDROP	A malicious user or process may observe or modify user or TSF data transmitted between physically separated parts of the TOE.
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 it was transmitted during the course of legitimate use).
T.RESIDUAL_DATA	A user or a process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
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.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.UNIDENTIFIED_INTRUSIONS	The IDS Administrator may fail to notice potential intrusions, thus limiting the IDS Administrator's ability to identify and take action against a possible intrusion.
T.UNAUTHORIZED_ACCESS	A user may gain access to user data for which they are not authorized according to the TOE security policy.

T.UNKNOWN_STATE	When the TOE is initially started or restarted after a failure, the security state of the TOE may be unknown.

4.2 Assumptions

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.

4.3 Policies

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.COMPONENT_IDENTITY	The IDS Administrator will give each TOE component that provides a scanning, sensing, or analyzing capability a unique component Identification (ID).
P.CRYPTOGRAPHIC_FUNCTIONS	The TOE shall provide cryptographic functions for its own use, including encryption/decryption and digital signature operations.
P.CRYPTOGRAPHY_VALIDATED	Where the TOE requires FIPS-approved security functions, only National Institute of Standards Technology Federal Information Processing Standard Publication (NIST FIPS) validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key distribution, and random number generation services).
P.IDS_DATA_COLLECTION	IDS audit events based on data collected from IT System resources will be created.
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.

5 Architectural Information

The Protection Profile specifies a set of security functional and assurance requirements for Intrusion Detection System products. An IDS monitors an Information Technology (IT)

System for activity that may inappropriately affect the IT System. An IT System may range from a computer system to a computer network. An IDS consists of a sensing capability, an analysis capability and an optional but recommended scanning capability. Sensing and scanning capabilities collect information regarding IT System activity and vulnerabilities, which is then analyzed. Sensing is meant to be a passive capability and scanning is an active capability.

Analyzing capabilities perform intrusion analysis and further categorization of the collected information. Scanning capabilities are optional because a base IDS only needs the capability to sense data from the IT environment being monitored and to have the capability to analyze the sensed data. The Security Target (ST) author is responsible for defining what components comprise the system. One or more components can provide the set of capabilities that are described in this document.

IDS Analyzer components support the ability to receive IDS data from the sensing and/or scanning capabilities and then apply analytical processes to derive conclusions about possible intrusions. IDS Analyzer products also provide the ability to protect themselves and their associated data from unauthorized access and modification and ensure accountability for each user's actions. The IDS Analyzer PP provides for a level of protection which is appropriate for IT environments that require detection of malicious and inadvertent attempts to gain unauthorized access to IT resources, and where the IDS can be appropriately protected from hostile attacks.

IDS Scanner components support the ability to statically monitor a set of IT resources in order to identify events that may be indicative of potential vulnerabilities in or misuse of those IT resources. IDS Scanner PP-conformant products also provide the ability to protect themselves and their associated data from unauthorized access and modification and ensure accountability for each user's actions.

IDS Sensor components support the ability to monitor a set of IT resources in order to identify events that may be indicative of potential vulnerabilities in or misuse of those IT resources. IDS Sensor PP-conformant products also provide the ability to protect themselves and their associated data from unauthorized access and modification and ensure accountability for each user's actions.

IDS System components support the ability to monitor, analyze, and manage a set of IT system resources in order to identify events that may be indicative of potential vulnerabilities in or misuse of those IT resources. IDS System PP-conformant products also provide the ability to protect themselves and their associated data from unauthorized access and modification and ensure accountability for each user's actions.

The assurance requirements were originally based upon Evaluated Assurance Level (EAL) 4. In order to gain the necessary level of assurance for medium robustness environments explicit requirements have been created for some families in the ADV class both to remove ambiguity in the existing ADV requirements as well as to provide greater assurance than that associated with EAL4. The assurance requirements are presented in Section 5.3. At

the present time, a Target of Evaluation (TOE) certified against one of the PPs would have an evaluation result that is outside the scope of mutual recognition. However, this situation may change when Common Criteria (CC) version 3 is adopted (assuming the intent is to use the ADV updates currently under development), which will enhance the usability of the PPs outside of the United States (US).

The PPs are applicable to products regardless of whether they are self-contained, or distributed. In addition, they address only security requirements and not any special considerations of any particular product design or interoperability.

6 Documentation

- U.S. Government Protection Profile Intrusion Detection System – System For Medium Robustness Environments, Version 1.0, April 2, 2006
- U.S. Government Protection Profile Intrusion Detection System – System For Medium Robustness Environments Evaluation Technical Report, March 16, 2007, Document No. E4-0207-001
- U.S. Government Protection Profile Intrusion Detection System – System For Medium Robustness Environments Evaluation Technical Report, May 30, 2007, Document No. E4-0307-008

7 Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the APE section of the CC and the CEM. The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of the APE assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the PP.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., APE) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone, electronic mail, and meetings. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. No constraints were identified in performing this evaluation, and only the assumptions identified above were followed.

Chapter 4, Results of Evaluation, in each of the respective ETRs, states:

"*U.S. Government Protection Profile Intrusion Detection System – System For Medium Robustness Environments* was successfully evaluated."

8 Validator Comments/Recommendations

Considerable effort was devoted to getting the cryptographic requirement written in a useful manner. It should be noted that although the PP mandates the implementation of SHA-256 or stronger hash function, for protocols that require SHA-1, the ST can of course be extended as necessary.

Many organizations purchasing products that comply with the PPs may have additional policies that supplement the PP, for example a certificate policy that states operational procedures for key management. To the extent possible, stating such requirements, when procedural rather than technical, was kept to a minimum.

It should be noted that there are fewer requirements for IDS audit data than for system audit data. This was deemed acceptable since the PP is intended to be a clean slate upon which implementation specific STs can be developed. Enumeration of the types of IDS audit records, and their mechanisms for protection and storage will be critical to a well developed Security Target.

The cryptographic requirements in some ways exceed those of FIPS 140-2, so a CCTL ***may not*** use FIPS 140-2 cryptomodule validation as a substitute for testing of those requirements. See FCS_CKM_EXP.2 for an example.