National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme

Validation Report

National Security Agency

Intrusion Detection System System Protection Profile, Version 1.4, February 4, 2002

Report Number: CCEVS-VR-02-0012

Dated: 1 March 2002

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

Jeffrey Gilliatt
S. Meg Weinberg
Mitretek Systems Inc.,
McLean, VA

Common Criteria Testing Laboratory

Computer Sciences Corporation
Annapolis Junction, MD

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 Intrusion Detection System System Protection Profile
Version Number: 1.4
Assurance Package: EAL2

Name of CCTL: Computer Sciences Corporation
Validation Report Number: CCEVS-VR-02-0012
Date Issued: 1 March 2002

Original Signed

Director
Information Technology Laboratory
National Institute of Standards and Technology

Original Signed

Information Assurance
Director
National Security Agency

Table of Contents

1 Executive Summary

An evaluation of the Intrusion Detection System System, Protection Profile [IDS_SYS_PP], Version 1.4, February 4, 2002 commenced on 10 August 2001 and completed on 31 January 2002. The [IDS_SYS_PP] evaluation was performed by Computer Sciences Corporation in the United States. The evaluation was conducted in accordance with the 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 [IDS_SNS_PP] contains realistic security objectives that are countered by stated threats. The CC class also offers confidence that the Protection Profile is internally consistent, coherent and technically sound. The protection profile identified in this Validation Report 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 Validation Report applies only to the specific version of the protection profile as evaluated. The evaluation has been conducted in accordance with the provision 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 Validation Report 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.

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 [Common Criteria], the CEM [The Common Evaluation Methodology] 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 Guidance to Validators of IT Security Evaluations. 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.

Evaluation Specific Details
Dates of Evaluation: 10 August 2001 – 31 January 2002
Evaluated Product: Intrusion Detection System System, Protection Profile, Version 1.4, February 4, 2002
Developer: Science Applications International Corporation, 7125 Gateway Drive, Suite 300, Columbia, MD 21046 for National Security Agency, 9800 Savage Road, Fort George G. Meade, MD 20755-6000
CCTL: Computer Sciences Corporation, Annapolis Junction, MD.
Evaluation Class: EAL2
Validation Team: Jeffrey Gilliatt, Mitretek Systems Inc.
S. Meg Weinberg, Mitretek Systems, Inc.
Applicable National and International Interpretations: None

2 Identification

Intrusion Detection System System, Protection Profile, Version 1.4, February 4, 2002.

3 Protection Profile Summary

The [IDS_SYS_PP] specifies a set of security functional and assurance requirements for Information Technology (IT) products. An Intrusion Detection System (IDS) monitors an IT System for activity that may inappropriately affect the IT System's assets. An IT System may range from a computer system to a

computer network. An IDS System consists of Sensors, Scanners and Analyzers (i.e., IDS components). Sensors and Scanners collect information regarding IT System activity and vulnerabilities, and they forward the collected information to Analyzers. Analyzers perform intrusion analysis and reporting of the collected information.

[IDS_SYS_PP] conformant products monitor, both real-time and statically, an IT System for activity that may inappropriately affect the IT System's assets and react appropriately. [IDS_SYS_PP] conformant products also provide the ability to protect themselves and their associated data from unauthorized access or modification and ensure accountability for authorized actions.

The [IDS_SYS_PP] provides for a level of protection which is appropriate for IT environments that require detection of malicious and inadvertent attempts to gain inappropriate access to IT resources, where the System can be appropriately protected from hostile attacks. Though products that are [IDS_SYS_PP] conformant can be used to monitor and analyze a system or network in a hostile environment, they are not designed to resist direct, hostile attacks. The [IDS_SYS_PP] does not fully address the threats posed by malicious administrative or system development personnel. This profile is also not intended to result in products that are foolproof and able to detect intrusion attempts by hostile and well-funded attackers. [IDS_SYS_PP] conformant products are suitable for use in both commercial and government environments.

The [IDS_SYS_PP] is generally applicable to products regardless of whether they are embedded, stand-alone, centralized, or distributed. However, it addresses only security requirements and not any special considerations of any particular product design.

4 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

4.1 TOE Threats

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the System’s collection and analysis functions by halting execution of the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit

system privileges to gain access to TOE security functions and data

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

T.FACCNT Unauthorized attempts to access TOE data or security functions may go undetected.

4.2 IT System Threats

T.SCNCFG Improper security configuration settings may exist in the IT System the TOE monitors.

T.SCNMLC Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

T.SCNVUL Vulnerabilities may exist in the IT System the TOE monitors.

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

T.MISUSE Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

T.INADVE Inadvertent activity and access may occur on an IT System the TOE monitors.

T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

5 Security Policy

This section identifies the organizational security policies applicable to the Intrusion Detection System System Protection Profile.

P.DETECT Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

P.MANAGE The TOE shall only be managed by authorized users.

P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

P.INTGTY Data collected and produced by the TOE shall be protected from modification.

P. PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

6 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

6.1 Intended Usage Assumptions

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

6.2 Physical Assumptions

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

6.3 Personnel Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.NOTRST The TOE can only be accessed by authorized users.

7 Security Content of PP

A System is one or more Sensors and/or Scanners, and one or more Analyzers. A System monitors an IT System for activity that may inappropriately affect the IT System's assets, performs analysis on the data it collects, and reacts appropriately. The information collected may be obtained from a variety of sources located on an IT System. Similarly, the response functions may affect one or more targets on the IT System.

Sensors must be able to:

- Collect data about all events as they occur on an IT System. Events may include authentication events; data access events; configuration access events; service requests; network traffic; data introduction; and, start-up and shutdown of audit functions.
- Forward all collected data to an authorised Analyser for data reduction and analysis.

Scanners must be able to:

- Collect static configuration information about an IT System. Configuration information may include detected malicious code, access control configuration, service configuration, authentication configuration, accountability policy configuration, and detected known vulnerabilities.
- Forward all collected configuration information to an authorised Analyser for data reduction and analysis.

Analysers must be able to:

- Receive data from identified Sensors and Scanners.
- Process specified data to make intrusion/vulnerability determinations.
- Respond to identified intrusions/vulnerabilities. Such responses may include report generation, visual signals/alarms, audible signals/alarms, configuration changes, and/or invocation of remote warnings.

All IDS components must be able to:

- Protect themselves and their data from tampering.
- Be configured by an authorised user.
- Produce an audit trail (e.g., configuration changes, component and data accesses).

8 Documentation

The evidence used in this evaluation is based solely upon:

[IDS_SYS_PP]	Intrusion Detection System System, Protection Profile, Version 1.4, February 4, 2002 (and previous versions leading up to this document).

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_PART 1]	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_PUB1] 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_PUB2] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures, Scheme Publication #2, Version 1.5, May 2000.

[CCEVS_PUB3] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Validators of IT Security Evaluations, Scheme Publication #3, Version 1.0, October 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, August 2000.

9 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.