National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Delta Security Technologies
Sentinel Model III Computer Security System

Report Number: CCEVS-VR-02-0023
Dated: 13 September 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

Aerospace Corporation

Columbia, Maryland

Common Criteria Testing Laboratory

COACT , Inc.

Columbia, Maryland

National Information Assurance Partnership

Common Criteria Certificate

Delta Security Technologies

The IT product 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 and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. 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 IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name: Sentinel Model III
Evaluation Platform: N/A
Assurance Level: EAL4
Protection Profile Identifier: N/A

Name of CCTL: COACT, Inc.
Validation Report Number: CCEVS-VR-02-0023
Date Issued: 13 September 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

This report documents the NIAP validators' assessment of the evaluation of Sentinel Model III Computer Security System, manufactured by Delta Security Technologies. It presents the evaluation results, their justifications, and the conformance result. This Validation Report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The evaluation was performed by COACT, Inc. CAFÉ Laboratory, and was completed during June 2002. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both written by COACT. The evaluation determined the product to be **Part 2 conformant, Part 3 conformant,** and to meet the requirements of **EAL 4**.

The product allows the (non-simultaneous) sharing of a PC or workstation among users at different sensitivity levels by using traditional "periods processing" techniques. In essence, each user of the workstation is presented with a sanitized machine that is configured in accordance with the resource authorizations for that user and the security level for which he is authorized. This is done by controlling the power to the various devices (e.g., internal hard drive, removable hard drives, USB ports, floppy drive) that are available.

The product implements three distinct and physically separate domains: an *unrestricted* domain, and two *sensitive* domains. In the unrestricted domain, the user has access to the internal hard drive and all of the devices and ports. It is intended that this domain process only non-sensitive data. The other (restricted) domains are each characterized by a removable hard drive (RHDD) that contains the operating system and all of the data and applications for that domain. Each RHDD is labeled at its level, and also for the particular PC/workstation for which it is authorized. Thus, an RHDD may only be used in the PC/workstation for which it is intended, and the user must have an authorization (e.g., clearance) that is equal to the sensitivity level of the RHDD. The Sentinel only provides access control to the domain; it is presumed that all users that are authorized for any given domain have equal access to all the data and resources in the domain. If any further or more fine-grained access control is required (e.g., discretionary access controls), it must be provided by the operating system that is resident on the RHDD.

The product is "standalone;" there are no dependencies on other hardware or software.

The validation team monitored the activities of the evaluation team, participated in team meetings, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans and witnessed evaluator testing, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the Evaluation Technical Report (ETR) and test report. The validation team determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the validation team concludes that COACT's findings are accurate, the conclusions justified, and the conformance claims correct.

2 IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) 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 EAL 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 information needed to completely identify the product, including

- the Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated,
- the Security Target (ST), describing the security features, claims, and assurances of the product,
- the conformance result of the evaluation,
- the organizations and individuals participating in the evaluation

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Delta Security Technologies Sentinel Model III Computer Security System
Protection Profile	Not Applicable
Security Target	Sentinel Security Target, Version 5.6, dated June 2002
Evaluation Technical Report	*Sentinel Model III Computer Security System Evaluation Technical Report*, September 25, 2002, Document No. F4-0802-002(1)
Conformance Result	Part 2 conformant, Part 3 conformant, EAL 4
Sponsor	Delta Security Technologies
Developer	Delta Security Technologies
Evaluators	COACT, Inc. CAFÉ Laboratory
Validators	The Aerospace Corporation

3 SECURITY POLICY

The Sentinel product enforces the following security policies:

3.1 Role Differentiation Policy.

The product supports exactly two roles:

- Authorized Administrator
- Authorized User

The roles are determined by the attributes indicated on a Smart Card and are validated in the logon process. The administrator role is defined by the possession of the role attribute coded onto the user's[1] Smart Card. The authorized administrator is authorized to download the audit records and to set and modify security parameters for users (e.g., change their sensitivity levels, change their passwords).

By definition, anyone with a valid Smart Card that does not contain the administrator attribute is an authorized user. More precisely, an authorized user is any user that has access to the PC/workstation and has a Smart Card that allows access to restricted data and restricted operations.[2] The specific authorizations of authorized users are determined by the sensitivity level and other security attributes recorded on the Smart Card.

3.2 Identification and Authentication Policy.

Each user is issued a Smart Card. When the Smart Card is inserted into the card reader, an embedded code (i.e., the "Machine Authorization Code") is checked against a value stored in the Sentinel (specifically, the "Secure Microcontroller") to determine whether the Smart Card is valid for the specific PC or workstation. This guarantees that the card owner can only exercise his authorizations on a computer with the identical Machine Authorization Code as that stored on the Smart Card.

If the Machine Authorization Code is valid, the user is then required to enter a PIN. This value is encrypted by the Secure Microcontroller and compared to the encrypted value of the PIN that is stored on the Smart Card. If this check is successful, the user is then prompted to enter a personal password which is checked with the one stored on the Smart Card. When this final check succeeds, the user's identity and authorities are established, and the user is prompted to select from a menu of available security profiles (stored on the Smart Card). The profile identifies the user's authorized security level(s) and the components (e.g., NIC, USB ports) that are available at each of the levels authorized.

[1] The more general term, "user," denotes anyone who interacts with the TOE.

[2] This is because there is no restriction to access to the unrestricted domain; anyone who can physically access the machine can gain access to the domain.

3.3 Access Control Policy

The unrestricted domain may be accessed by any authorized user. The unrestricted domain may be set as the default condition when any of the logon checks fail[3] (or when the Smart Card is removed).

The restricted domains are characterized by the ability to access one of two removable hard drives (RHDD), each being labeled with its sensitivity level. An RHDD is available to users authorized access to the domain that includes the specific RHDD. The rules that are enforced for access to a domain include:

- The user must have a clearance equal to the sensitivity level of the RHDD;
- The user must be initiating access to a domain during a time of day when the clearance is in effect (defined by the Time of Day attribute);
- The user must be designated as an authorized user (i.e., not an administrator);
- The RHDD ID must be valid for the PC/workstation in which it will be used.

3.4 Security Management Policy

The following actions are restricted to authorized administrators:

- Download the audit file;
- Control of user PINs (i.e., delete PIN, change PIN).

4 ASSUMPTIONS AND CLARIFICATION OF SCOPE

4.1 Usage Assumptions

The TOE is designed to provide security in an environment in which users need to share (but not simultaneously) the computing resources of a single PC or workstation to process information at different levels of sensitivity. The evaluation results are predicated on the following assumptions concerning the configuration and use of the product:

- There is at least one authorized administrator who is competent and is assigned to administer the TOE;
- There exist procedures for establishing user clearances and authorization for the data and resources of each domain;

4.2 Environmental Assumptions

The following assumptions are made with respect to the environment:

[3] The other allowable default condition is "power-off." The specific default condition is chosen by the user and is set by the vendor when the system is configured, prior to delivery.

- The product is maintained in a controlled facility, with physical security sufficient to prevent theft or access by other than authorized personnel;
- Physical controls are sufficient to prevent unauthorized tampering with the product.

4.3 Clarification of Scope

Certain threats are outside the scope of the product's capabilities to counter, and the product makes no claims of protection against them:

- The product relies on the correctness of the information contained on the Smart Card, and on the integrity of the card itself. However, threats to the Smart Card are outside the scope of the evaluation, and it is presumed that the card is offered reasonable protection and is relatively immune from unsophisticated attacks.
- The assessment of strength and efficacy of the cryptographic algorithms employed are not part of the evaluation.
- It is presumed that each user authorized for a given domain is authorized to access all the resources and data resident in the domain;
- It is further presumed that there exist procedures for protecting the RHDDs consistent with the sensitivity of the data stored on them.

5 ARCHITECTURAL INFORMATION

The Sentinel Computer Security System is adaptable to a wide variety of PCs or workstations. It comprises of a kit of components that is used to modify the particular PC/workstation that needs to be shared and protected. The kit consists of the following components:

- Security Module
- Sensor/Controller Cards
- I/O Controller
- RHDD Drive Frame
- LCD Module
- Back Panel Assembly
- Secure Microcontroller
- NVM Controller Interface

A Smart Card Reader—associated with the Security Module—is used to read the smart cards that are issued to each user, and to verify the security attributes that are associated with the user (e.g., card PIN, password, authorized domains). The security policy is implemented in the Security Module, which determines access to the restricted domains. The physical instantiation of the several domains, along with the activation of the resources that are available in each, is implemented by the Sensor/Controller cards. It does this by providing power to the allowable resources (e.g., NICs, modems, USB ports). The Security Module also stores and controls access to audit data. A number of security events are recorded, and only an authorized administrator is allowed to download the audit data (which is processed off-line).

The minimum authorized restricted domain constitutes access to exactly one of the available RHDDs and the available CD/DVD drives. When an RHDD is installed in the drive frame, signals are generated that allow the Security Module to determine the sensitivity level of the RHDD and whether it is authorized for the specific PC/workstation into which it has been installed. Any mismatch causes the Security Module to default to the unrestricted domain (or the optional power-off state). For example, if the user has selected and is authorized access to a restricted domain but the required RHDD has not been installed, the default state is selected. Likewise, if the user's security attributes (e.g., sensitivity level) does not match that of the installed RHDD, the default state is selected by the Security Module.[4]

When the PC/workstation is first powered on, the Sensor/Controller Card enables power only to the Smart Card Reader, LCD Module, LEDs, and keyboard, latching them directly to the Security Module. All the functions for I&A and access control decisions are then performed by the Security Module before instantiating any domain. After a user is granted access to a domain, all user activity is limited to that domain. The Security Module continually polls the card reader. If the user's Smart Card is removed at any point during a user session, a system reset is initiated.

[4] The full set of conditions that result in the default state are described in the Security Target.

DOCUMENTATION

The following product documentation is provided to consumers:

Sentinel Model III Computer Security System Security Target, Version 5.6, dated June 2002;

Sentinel Model III Computer Security System Installation, Generation, and Start-up Procedures, Version 2.2;

Sentinel Model III Computer Security System Installation Guide, Version 1.2;

Trusted Facility Manual for the Sentinel Model III Computer Security System, Version 2.2;

Security Features User's Guide for the Sentinel Model III Computer Security System, Version 2.2;

Administrator's Guide for AuditX, Version 1.2.

The following additional documentation was employed during the course of the evaluation:

Test scripts for Sentinel Model III Computer Security System;

Sentinel Model III Computer Security System Informal Functional Specification, Version 2.6;

Sentinel Model III Computer Security System High-Level Design, Version 2.6;

Life-Cycle Definition for the Sentinel Model III Computer Security System, Version 1.0.

IT PRODUCT TESTING

5.1 Developer Testing

Developer testing was relatively complete. The developer's test scripts exercise all important security functional requirements. In particular, each of the various combinations of user authorizations and domain allocations are exercised by the vendor test scripts; the vendor tests exercise operation in the unrestricted domain, operation in each of the sensitive domains (i.e., for each of the RHDDs), Identification and Authentication, authorized administrator actions, and access control.

5.2 Evaluator Testing

The evaluator performed the entire vendor test suite, validating that the test results matched the expected results.

The evaluator also devised and executed additional tests:

- Smart Card verification;
- BIOS tests;

- Programming of Smart Cards using the AuditX Utility[5];
- Verification of the inability of user processes to write to shared, non-volatile memory (NVM);
- Additional testing of the access control policy.

All tests gave expected (correct) results. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or security vulnerabilities.

6 EVALUATED CONFIGURATION

The Sentinel product is delivered pre-configured by the developer. Although the purchaser may elect several options, these are installed prior to delivery; the user site neither performs installations nor alters the configuration after the product is delivered.

The evaluated configuration contained the following hardware:

- Security Module
- Sensor/Controller Board
- I/O Controller Board
- RHDD Drive Frame
- LCD Module
- Back Panel Assembly
- Secure Microcontroller
- NVM Control Interface

Additionally, three separate Network Interface Cards (NIC) were installed; one for unclassified (i.e., the *unrestricted* domain), one for *sensitive*, and one for *classified*. Likewise, the removable hard drives (RHDD) were labeled *sensitive* and *classified*.

The developer installs the Security Module source code for the Sentinel product. The default state for I&A and the access control policies may be set to power off or the unrestricted domain. For the evaluated configuration, the product was set to default to the unrestricted domain. Thus, any I&A or access control failures caused the computer to boot up in the unrestricted domain.

[5] Although the AuditX utility is not included in the TOE definition (i.e., not part of the evaluated configuration), the administrator functions supported by this utility were considered sufficiently important that the CCTL chose to verify their operation.

7 RESULTS OF THE EVALUATION[6]

The evaluation determined the product to be **Part 2 conformant, Part 3 conformant,** and to meet the requirements of **EAL 4.** This implies that the product satisfies the security technical requirements specified in *Sentinel Model III Computer Security System Security Target, Version 5.6*, June 2002.

8 EVALUATOR COMMENTS

There are no Evaluator Comments.

9 ANNEXES

There are no annexes to this report.

10 SECURITY TARGET

The ST, *Sentinel Model III Computer Security System Security Target, Version 5.6*, June 2002 is included here by reference.

[6] The terminology in this section is defined in CC Interpretation 008, specifying new language for CC Part 1, section/Clause 5.4.

11 GLOSSARY

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
NIAP	National Information Assurance Program
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVM	Non-Volatile Memory
PP	Protection Profile
RHDD	Removable Hard Drive
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

12 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0

[7] Sentinel Security Target, Version 5.6, June 2002

[8] Sentinel Model III Evaluation Technical Report, August 7 2002; Document No. F4-0802-002

[9] Sentinel Computer Security System Test Report, August 7, 2002; Document No. F4-0802-001