National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme
Validation Report

Check Point Integrity Agent 6.5.063.145

Report Number: CCEVS-VR-VID10287-2008
Dated: July 23, 2008
Version: 1.0

National Security Agency
Information Assurance Directorate
9600 Savage Road Suite 6757
Fort George G. Meade, MD 20755-6757

Acknowledgements:

The TOE evaluation was sponsored by:

Check Point Software Technologies
650 Townsend, Suite #575
San Francisco, CA 94107

Evaluation Personnel:

Science Applications International Corporation CCTL, Columbia, MD
Terrie Diaz
Tammy Compton
Jasmine Maleki
Jean Petty

Validation Personnel:

Scott Shorter, Orion Security Solutions
Santosh Chokhani, Orion Security Solutions

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Check Point Integrity Agent, version 6.5.063.145. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of Check Point Integrity Agent was performed by the Science Applications International Corporation Common Criteria Testing Laboratory in the United States and was completed in December July 2008. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC's CC consultants, and the ETR and test report used in developing this validation report were written by the SAIC CCTL. The evaluation team determined the product to be Part 2 extended and Part 3 conformant, and concluded that the Common Criteria version 2.3 requirements for Evaluation Assurance Level (EAL) 4 (augmented with ALC_FLR.2, Flaw Reporting Procedures and AVA_VLA.3, Vulnerability Analysis – Moderately Resistant)) have been met.

The Check Point Integrity Agent is a workstation protection application that mediates network communications and scanning for spyware signatures. It can mediate network communications based on network addresses and ports, control outbound network connections from workstation applications, and filter contents of supported instant message protocols. It can scan the host workstation files and registry for spyware based on signatures. Detected spyware is deleted by the TOE.

The TOE's Security Functions are audit, user data protection, identification and authentication, security management, and spyware mitigation.

Figure 1 illustrates the physical configuration of the TOE and IT Environment (TOE shaded in grey).

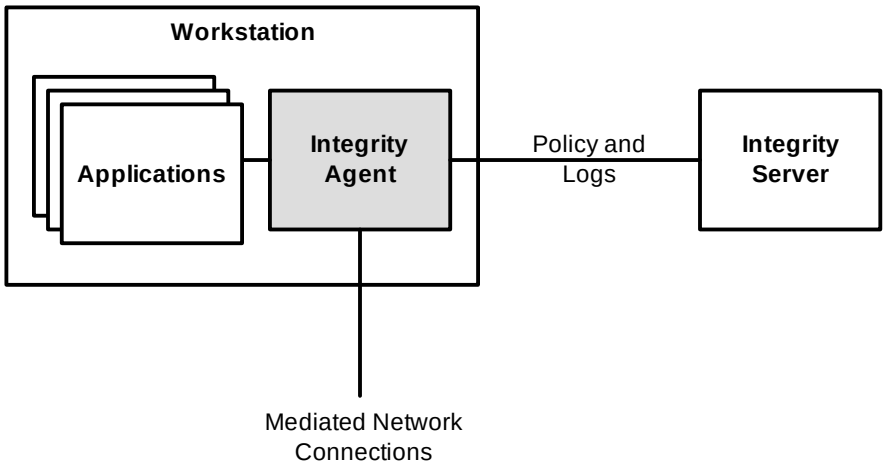

Figure 1 - TOE Configuration

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for EAL 4 evaluation

. Therefore the validation team concludes that the SAIC CCTL findings are accurate, and the conclusions justified.

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 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 listing on the CCEVS 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	Check Point Integrity Agent 6.5.063.145
Security Target	Check Point Integrity Agent 6.5 Security Target, Version 1.2, 6/22/2008
Protection Profiles	N/A
Evaluation Technical Report	• Evaluation Technical Report For Check Point Integrity Agent 6.5.063.145, Part 1 (Non-Proprietary), Version 2.0, 8 December 2006 • Evaluation Technical Report For Check Point Integrity Agent 6.5.063.145, Part 2 (SAIC and Check Point Proprietary), Version 2.0, 23 January 2007
Conformance Result	CC Version 2.3 Part 2 extended, CC Version 2.3 Part 3 conformant, EAL 4 augmented by ALC_FLR.2 and AVA_VLA.3

Item	Identifier
Sponsor	Check Point Software Technologies 650 Townsend, Suite #575 San Francisco, CA 94107
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
CCEVS Validator(s)	Scott Shorter, Orion Security Solutions Santosh Chokhani, Orion Security Solutions

3 Security Policy

The explicit TOE security policy consists of the Personal Firewall Policy that controls network flow to and from the workstation through the TOE. This policy permits or denies outgoing or inbound network flow based on the presumed address of the external subject, protocol, and service.

Note that the TOE also includes features to filter e-mail messages (MailSafe) and Instant Messages (IMSecure). However, filtering content in the context of e-mail and IM protocols is somewhat non-deterministic since the protocols are subject to change and support a wide variety of options that allow content to be hidden or disguised. As such, these features are excluded from this evaluation and the evaluated configuration of the product.

4 Assumptions

The following assumptions about the TOE's operational environment are articulated in the ST:

A.ENVIRONMENT	It is assumed that the hosting IT environment and associated users will not actively seek to disable, bypass, or otherwise impair the TOE security functions.
A.INSTALL	It is assumed that the TOE will be instantiated in its hosting IT environment, according to the TOE installation guidance, such that it can correctly enforce its security policies.
A.MANAGE	It is assumed that the TOE will be managed by authorized users in accordance with the TOE guidance.

5 Architectural Information

The TOE itself is composed of a single subsystem that communicates with the Integrity Server to receive security policy updates and store audit log data. That subsystem is further decomposed into the Integrity Driver that operates on the network stack and filters network communications, the Integrity Service that performs the spyware detection functionality, and the Integrity GUI application that handles configuration and management by human users.

6 Documentation

The following documentation is provided with the product:

- Administrator Console Reference; The Integrity Advance Server User Interface, 1-0283-0600-2005-07-19
- Administrator Guide; Using Integrity Advance Server, 1-0282-0650-2005-09-30
- Installation Guide; Installing, Configuring, and Maintaining Integrity Advance Server, 1-0276-0605-2006-01-03
- User Guide for Integrity Client Software, Version 6.5, ZLD 1-0228-0650-2005-1023
- Integrity Client Management Guide; Deploying and Managing Integrity Flex and Integrity Agent, 1-0281-0600-2005-07-29
- Integrity XML Policy File Reference; A Reference to XML Policy Elements and Attributes,1-0206-0600-25-07-08
- Check Point Integrity Agent 6.5 Security Target, Version 1.2, 06/22/2008

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team.

7.1 Developer Testing

The developer tested the interfaces identified in the high level design documentation and mapped each test to the security function tested. The scope of the developer tests included all TOE Security Functions. The evaluation team determined that the developer's actual test results matched the expected results and witnessed a subset of the tests. Testing consisted of a suite of manual tests.

In particular, developer testing contained the following types of tests, grouped by Security Function:

- Security Management Tests
  - Demonstrate that the local user can apply a policy via the command line interface.
- Spyware Mitigation Tests
  - Demonstrate that spyware scans are performed on the host operating system, and that spyware that is found is removed.
- Audit Tests
  - Demonstrate that audit records are generated when
    - spyware is found and removed,
    - violations of the Personal Firewall Policy are detected, or
    - instant messages are blocked.
  - Demonstrates that audit logs are sent to the authenticated Integrity Server.
- User Data Protection
  - Demonstrate that information flow policies perform as specified in the security functional requirements.
- Identification and Authentication
  - Demonstrates that the Integrity Server must be authenticated before sending security policies to or receiving audit logs from the TOE.

7.2 Evaluation Team Independent Testing

The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the developer test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team also ensured that all subsystem interfaces were tested by the developer. The evaluation team performed a sample of the developer's test suite, representative of the TOE Security Functions, and devised an independent set of team tests and penetration tests.

The independent tests run by the evaluation team included the following types of tests:

- Testing the ability to configure audit settings to log specified event types
- Testing IM filtering of specific services or file types
- Testing that the Integrity Server with invalid credentials cannot receive audit logs or deploy policies
- Testing that the local user can access all security management functionality

7.3 7.3 Moderately Resistant Vulnerability Analysis

Evaluation team testing at NSA was completed in July 2008. Using the results of the VLA.2 evaluation by the CCTL evaluation team, the NSA evaluation team installed the TOE in its evaluated configuration and conducted AVA_VLA.3 vulnerability testing. The NSA evaluation team utilized the same category of tools used by the CCTL for penetration testing, as well as in-house developed tools, which enabled the team to determine that the TOE was resistant to penetration attacks performed by attackers with moderate attack potential.

The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

8 Evaluated Configuration

To operate in the evaluated configuration, the product should be installed with encryption enabled.

9 Flaw Remediation Procedures

Check Point's flaw remediation process provides a mechanism for customers to report issues to the vendor through a web based service request form. If the issue is assessed by the development team to be an actual problem it will be triaged to determine whether it will be addressed in a future release or whether a direct fix is possible. A workaround will be provided, if possible, if the issue will be addressed in a future release.

If a direct fix or workaround is created for the issue, it will be provided directly to the customer who reported the issue, and made available to other users via the SecureKnowledge support site.

10 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 2.3. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.3.

Science Applications International Corporation CCTL has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 4 augmented by ALC_FLR.2 and AVA_VLA.3. A team of validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in July 2008.

11 Validator Comments

The proprietary encryption scheme used between the agent and the server has not been formally evaluated by CCEVS, and it does not use a FIPS 140-2 approved algorithm for symmetric encryption algorithm. Customers requiring FIPS 140-2 approved algorithms must treat the

channel from the Integrity Server to the Integrity Agent as plaintext, and should consider protecting that channel with additional network security protections.

Also, the default configuration uses an SSL ciphersuite that relies on algorithms that are not FIPS 140-2 approved as well. Users may wish to consider hardening the Integrity Server's configuration to require stronger SSL ciphersuites.

SSL is used for authenticating the Integrity Server, but it should be noted that SSL client and server certificates are not checked for revocation. An attacker able to compromise the Integrity Server key and poison a workstation's DNS cache might be able to impersonate the Integrity Server and push bad policies to that workstation, without the administrators being able to revoke the server's credentials. This scenario could be detected if a client disappears from the server's logs, and the system can recover from such a key compromise scenario by reinstalling the server and the TOE.

Of the available features, MailSafe and IMSecure are not subject to evaluation claims in this Security Target and are excluded from the evaluated configuration. Note that these features are effectively disabled by default since filters would need to be explicitly configured in each case.

12 Security Target

Check Point Integrity Agent 6.5 Security Target, Version 1.2, 06/22/2008

13 Bibliography

The validation team used the following documents to prepare the validation report.

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 2005, Version 2.3.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, Version 2.3.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, Version 2.3.

[4] Evaluation Technical Report For Check Point Integrity Agent 6.5.063.145, Part 1 (Non-Proprietary), Version 2.0, 8 December 2006

[5] Evaluation Technical Report For Check Point Integrity Agent 6.5.063.145, Part 2 (SAIC and Check Point Proprietary), Version 2.0, 23 January 2007

[6] Evaluation Team Test Plan For Check Point Integrity Agent 6.5 Final ETR Part 2 Supplement (SAIC and Check Point Proprietary) Version 1.0, 3 November 2006

[7] Evaluation Team Test Report For Check Point Integrity Agent 6.5.063.145 Final ETR Part 2 Supplement (SAIC and Check Point Proprietary) Version 1.0, 15 December 2006

[8] Check Point Integrity Agent 6.5 Test Document, Revision 0.7, November 7, 2006

[9] Check Point Integrity Agent 6.5 Security Target, Version 1.2, 06/22/2008

[10] Common Criteria Evaluation and Validation Scheme for IT Security, *Guidance to Validators of IT Security Evaluations*. Scheme Publication # 3, Version 1.0, January 2002.