National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Secure Computing IronMail® Email Security Gateway v6.7 HF2

Report Number: CCEVS-VR-VID10211-2008
Dated: 29 April 2008
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

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Secure Computing IronMail® Secure Email Gateway v6.7 HF2 (hereafter called IronMail v6.7 HF2). It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in February 2008. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Conformant and Part 3 Conformant**, and meets the assurance requirements of EAL 2 augmented with ALC_FLR.2.

The TOE is an email gateway software application. The TOE is physically contained within a special purpose computer with a limited physical interface. This computer device is hereafter referred to as the IronMail® appliance. RFC 822, Multipurpose Internet Mail Extensions (MIME) encoded messages are checked for policy violations and the presence of offensive content. Any message that violates the TOE's notion of security is isolated and acted upon so as to mitigate any threat being posed by it before it reaches the internal network. The TOE is also able to detect and curtail the flow of spam into the internal network in order to ensure the availability of system resources such as storage space and CPU time.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 2.3) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). This Validation Report applies only to the specific version of the TOE 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 provided.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 2 augmented with ALC_FLR.2) have been met.

The technical information included in this report was obtained from the Secure Computing IronMail® Secure Email Gateway v6.7 HF2 Security Target 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 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 Protection Profile to which the product is conformant.

- 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
TOE	Secure Computing IronMail® Email Security Gateway v6.7 HF2 (software only TOE)
Protection Profile	Not applicable
Security Target	IronMail® Secure Email Gateway v6.7 HF2 Security Target, version 86-0947956-G, April 8, 2008
Evaluation Technical Report	Secure Computing IronMail® Email Security Gateway v6.7 HF2 Final Non-Proprietary ETR – Part I Secure Computing IronMail® Email Security Gateway v6.7 HF2 Final Proprietary ETR – Part II
CC Version	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 2.3, August 2005. Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005. Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R. Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.
Conformance Result	CC Part 2 conformant, CC Part 3 conformant
Sponsor	Secure Computing
Developer	Secure Computing
Common Criteria Test Lab	SAIC, Columbia, MD
CCEVS Validators	Scott Shorter, Orion Security Solutions Robin Medlock, MITRE

3. Architectural Information

The TOE can be broadly classified into the following subsystems:

- SMTP Subsystem
- Super Queue Subsystem
- GUI Manager Subsystem
- Auxiliary Services Subsystem

Email messages flow through the TOE from the SMTP Subsystem to the Super Queue Subsystem and then back to the SMTP Subsystem. The GUI Manager Subsystem is used to configure and monitor the TOE, while the Auxiliary Services Subsystem provides supplementary services in the TOE.

The SMTP subsystem is one of the two main subsystems in IronMail®. This subsystem interfaces with external MTAs using the SMTP external interface as described in Section 2.2.1 in [FSP]. Emails are both received and sent through this subsystem by adhering to RFC 2821.

The TOE is based on a fully functional mail server engine and a queuing architecture designed to quickly parse and analyze messages for policy violations. Once accepted by the SMTP interface, messages are written to the hard disk and meta data are inserted into the database. A management and scheduling process known as the “Super Queue” accepts responsibility for each message at this point. Super Queue will spawn multiple copies of itself (based on the hardware model) each with a single processing engine thread that breaks down the message into parts and parses each of them for violations of rules or policies that have been configured by an authorized administrator

The constituent queues that comprise the Super Queue are:

- Rip Queue
- Spam Queue (or Anti-Spam Queue)
- Content Analysis Queue (or Content Filtering Queue)
- Envelope Analysis Queue (or Mail Monitoring Queue)
- Join Queue

TOE queues are components that process messages in an ordered fashion. The queuing architecture scrutinises every message received for harmful content. Once a message has successfully passed the scrutiny of each queue (assuming that no queue had to quarantine, drop, re-route, or take some other action on the message) the message is reassembled and provided to the organization’s internal mail server(s) for delivery to its intended recipient. Each of the queues can be configured to take some action based on a set of rules in the event that a message fails to pass the security policy enforced by the queue.

The Spam Queue technology relies on information obtained from DNS; the DNS server is considered part of the IT environment and can reside on any host on the internal network. It is assumed to always provide reliable information to the TOE.

The GUI Manager subsystem provides a web-based browser interface for the administrators to identify and authorise themselves to the TOE and to configure and maintain the TOE. Users may access the GUI Manager through a web browser by connecting to the IronMail® appliance's configured address using the secure HTTP (or HTTPS) protocol. The TOE provides a unified compliance manager through the GUI Manager. This allows administrators to define, monitor and enforce email policy across all email servers within the organization.

This subsystem depends on Tomcat Application server and APR Web server for its normal functioning. Both Tomcat and APR are outside the scope of the TOE and are in the IT Environment.

The Auxiliary Services Subsystem is not involved directly in the processing of email messages but nevertheless performs a very important task of supplementing the SMTP and Super Queue Subsystems. This subsystem consists of a number of processes supporting services and the logging engine. The following services constitute the Auxiliary Services Subsystem:

- Admin Server
- Scheduling Server
- Health Monitor
- Reporting Server
- Update Services
- Logging Engine
- Database

The evaluated configuration includes an IronMail® appliance that is logically situated between the firewall and the internal mail servers/clients, configured in a manner which ensures that every message that is sent into or out of the internal network always passes through it. The TOE and the Admin workstation and the connection between them are maintained in a physically secure environment.

IronMail® uses "hardened" FreeBSD as its Operating System; the OS is not included in the TOE Scope of Control (TSC). IronMail® provides additional functionality for Anti-virus, Webmail Protection, Corporate Compliance, and System Alert Notification but these are specifically excluded from the scope of evaluation.

The TOE's security functionality depends on security functions provided by the IT environment, as follows:

- Implementation of single-use password-based authentication for Telnet and FTP depends on an external authentication server that validates single-use passwords for a given user identity, using the protocols: RADIUS or SecurID;
- Certificate-based VPN functionality depends on an external Certificate Authority that issues certificates as described in the ST, and makes available certificate revocation information using the protocols: LDAP, HTTP or OCSP.

4. Security Policy

IronMail v6.7 HF2 provides the following security functions:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- TSF Protection

5. Assumptions

The following are assumptions made for the Environment of the TOE:

- The TOE is physically secure.
- The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
- Authorized administrators are non-hostile and follow all administrator guidance.

- All email traffic passes through the TOE.
- DNS information received by the TOE is reliable.
- Integrity of data is maintained by the MySQL database.
- The local administration platform is physically secure.
- The communication path between the TOE and the administrative Windows computer is physically protected.

The following features of the IronMail are excluded from the Common Criteria Evaluation:

- Anti-virus
- Webmail
- POP3
- IMAP4
- Corporate Compliance

6. Documentation

The following documentation is used as evidence for the evaluation of IronPort v6.7 HF2:

CC Assurance	Evidence
Analysis of Correspondence (RCR)	Excel Spreadsheet Part Number RCR-revB
Configuration Management (ACM)	IronMail® Secure Email Gateway v6.7 Configuration Management Plan, Version Date 09 November 2007, Part Number 00-0947957-B
Delivery and Operation (ADO)	IronMail Delivery Procedures, Part Number 00-0947959-B, 9 November 2007
Functional Specification (FSP)	Secure Computing IronMail Setup Guide, Part Number IROP-MN-STUP-67-A
Administration Guide (ADM)	Secure Computing Administration Guide, IronMail Messaging Gateway Security, Version 6.7, Part Number 86-0947656-A, 11/5/2007
Installation Guide (IGS)	Secure Computing IronMail Software Version 6.7.0 Common Criteria Evaluated Configuration Guide, Part number 86-0947968-C Secure Computing IronMail Setup Guide, Part Number IROP-MN-STUP-67-A
High-level Design (HLD)	High Level Design Document, Ironmail® Email Security Gateway 6.7, Part Number: 00-0947961-B
Life Cycle (ALC_FLR)	Secure Computing Engineering Order Procedure Part Number 00-0945165-A Secure Computing IronMail version 6.7 Common Criteria Evaluated Configuration Guide, Part Number 86-0947968-C Secure Computing Engineering Order (EO) / Part Number (PN) Web Form Instruction, Part Number PN: 00-0943763-G, 12/08/2006 Secure Computing Full Product Release Procedure, Part Number PN: 00-0944629-D, 8/23/05 Secure Computing Limited Product Release Procedure, Part Number PN: 00-0943726-F
Security Target (ST)	Secure Computing IronMail® Secure Email Gateway Software Version 6.7 HF2 Security Target, Version 86-0947956-G, 4/8/08
Test Documentation (ATE)	IronMail Email Security Gateway 6.7 HF2 Test Plan, Part Number 00-0947967-C
Vulnerability Analysis (VLA)	IronMail Secure Email Gateway version 6.7 Strength of Function Analysis, Part Number 00-0947969-A, Version Date 12 Dec 2007

CC Assurance	Evidence
	IronMail Secure Email Gateway version 6.7 Vulnerability Analysis, Part Number 00-0947970-A, Version Date: December 20, 2007

7. IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Plan.

The following tests, mapped to TOE security functions, were run and provided to the evaluation team by the developer:

- Security Audit – Logging Test Procedure
- User Data Protection – SMTP Proxy, SMTP Out, GUI Manager, Content Filtering, SpamQ, Mail Monitoring and Logging Test Procedures
- Identification and Authentication – GUI Manager and Logging Test Procedures
- Security Management – GUI Manager and Logging Test Procedures
- TSF Protection – GUI Manager, Logging, SMTP Proxy and SMTP Out Test Procedures

The evaluation team executed all developer tests. In addition, the evaluation team ran additional tests of the Identification and Authentication function and performed a port scan on the TOE environment to identify any potential vulnerability. No vulnerabilities were identified.

8. Evaluated Configuration

The TOE evaluated configuration consists of the IronMail v6.7 HF2 software application running MySQL server version 4.1.21 (installed automatically with the IronMail software) running on the FreeBSD version 6.2 Operating System and IronMail special purpose, rack mounted computer in the IT Environment. The evaluated configuration includes an IronMail® appliance that is logically situated between the firewall and the internal mail servers/clients, configured in a manner which ensures that every message that is sent into or out of the internal network always passes through it. The TOE and the Admin workstation and the connection between them are maintained in a physically secure environment.

IronMail® uses "hardened" FreeBSD as its Operating System; the OS is not included in the TOE Scope of Control (TSC). IronMail® provides additional functionality for Anti-virus, Webmail Protection, and Corporate Compliance but these are specifically excluded from the scope of evaluation.

The TOE must be configured in accordance with the Secure Computing IronMail Software Version 6.7.0 Common Criteria Evaluated Configuration Guide, Part number 86-0947968-C.

9. Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR, Volume II.

Evaluation of the Security Target (ST) (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

Evaluation of the CM capabilities (ACM)

The evaluation team applied each EAL 2 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation.

Evaluation of the Delivery and Operation documents (ADO)
The evaluation team applied each EAL 2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer.

Evaluation of the Development (ADV)
The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

Evaluation of the guidance documents (AGD)
The evaluation team applied each EAL 2 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE.

Evaluation of the Life Cycle Support Activities (ALC)
The evaluation team applied each ALC_FLR.2 CEM work unit. The evaluation team ensured that flaw remediation procedures exist and are in use for reporting and tracking flaws and subsequent fixes.

Evaluation of the Test Documentation and the Test Activity (ATE)
The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE security functional requirements are enforced by the TOE. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team tests and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

Vulnerability Assessment Activity (AVA)
The evaluation team applied each EAL 2 AVA CEM work unit. 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 and the evaluation team's vulnerability analysis and performance of penetration tests.

10. Validator Comments / Recommendations

Administrators should configure OpenSSL to use ciphersuites that correspond to the cryptographic algorithms listed in the Security Target, namely AES, SHA-1 and RSA.

Note that the TOE is capable of detecting and blocking S/MIME and PGP formatted encrypted mail, but other encrypted mail formats and/or steganographic techniques could be used to evade this filter.

11. Annexes

Not applicable

12. Security Target

The security target is the Secure Computing IronMail® Secure Email Gateway Software Version 6.7 HF2 Security Target, Version 86-0947956-G, 4/8/08

13. Glossary

The following definitions are used throughout this document:

Common Criteria Testing Laboratory (CCTL). An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.

Conformance. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.

Evaluation. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.

Evaluation Evidence. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.

Feature. Part of a product that is either included with the product or can be ordered separately.

Target of Evaluation (TOE). A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.

Validation. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.

Validation Body. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14. Bibliography

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

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.

[3] Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R.

[4] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.

[5] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.

[6] Secure Computing IronMail® Email Security Gateway v6.7 HF2 Final Proprietary ETR – Part II.

[7] IronMail® Secure Email Gateway v6.7 HF2 Security Target, version 86-0947956-G, April 8, 2008.

[8] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories. Version 1.0, March 20, 2001.