National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

BAE Systems Information Technology Military Message Handling System (MMHS) Filters – v1.1.1

Report Number: **CCEVS-VR-06-0010**
Dated: **24 April 2006**
Version: **1.5**

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

BAE Systems Information Technology Military Message Handling System (MMHS) Filters – v1.1.1

CCEVS-VR-06-0010

ACKNOWLEDGEMENTS

Validation Team

Richard Murphy
Mitretek Systems
Falls Church, Virginia

Common Criteria Testing Laboratory

Debra Baker
Elise Berger
Jean Petty
Kris Rogers
Mark Whitaker
Jenifer Wierum
Dragua Zenelaj
CygnaCom Solutions
McLean, Virginia

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) Validator's assessment of the evaluation of the BAE Systems Military Message Handling System (MMHS) Filters v1.1.1. 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 the MMHS Filters v1.1.1 was performed by CygnaCom Solutions Common Criteria Testing Laboratory in the United States and was completed during February 2006. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both written by CygnaCom.

The evaluation was carried out in accordance to the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. MMHS Filters v1.1.1 was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 2.2. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.2. CygnaCom Solutions determined that the product meets the security criteria in the Security Target, which specifies an assurance level of Evaluation Assurance Level (EAL) 4. The evaluation team determined the product to be Part 2 conformant and Part 3 conformant, and concluded that the Common Criteria requirements for EAL 4 have been met.

The TOE is a set of software modules that are used in conjunction with the Canadian Department of National Defense (DND) MMHS Trusted Guard, which is a system designed to securely connect highly classified computer networks with unclassified computer networks. The MMHS Trusted Guard resides at the entrance to secure enclaves and provides enclave-level security at this boundary by enforcing system and site-specific security policies governing the transfer of electronic messages between workstations within a classified enclave and workstations outside of the classified enclave. Unclassified external mail messaging systems use the Trusted Gateway (TGW) and the Secret external messaging systems use the Multi-Function Gateway (MFGW). Both of these systems, TGW and MFGW, include the MMHS as a gateway subsystem to enforce the security policy decisions related to the release of incoming and outgoing MMHS messages. The Target of Evaluation (TOE) is a portion of the MMHS, i.e., six message filters within the MMHS. It operates within the Content Validation Server portion of the MMHS and provides a set of security functions that permit filtering of messages that pass through the MMHS to implement a set of security policies within the MMHS.

The evaluation considered only the MMHS Filters software components, running on a MMHS Trusted Guard platform, which runs the EAL5 certified XTS-400 Trusted Operating System. There are several components provided by the underlying system that

the TOE depends upon but which are outside the evaluation boundary. These components include the XTS-400 operating system and the MMHS Trusted Guard application as well as several parsing and validation libraries. This evaluation does not demonstrate assurance for these components.

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, 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 an EAL4 evaluation. Therefore the validation team concludes that the CygnaCom findings are accurate, and the conclusions justified.

2 Identification

TOE: BAE Systems Information Technology Military Message Handling System (MMHS) Filters, v1.1.1

Evaluated Software: BAE Systems Information Technology Military Message Handling System (MMHS) Filters, v1.1.1

Developer: BAE Systems Information Technology
2525 Network Place
Herndon, VA 20171 USA

CCTL: CygnaCom Solutions
7925 Jones Branch Drive, Suite 5200
McLean, VA 22102

Validation Team: Richard Murphy, Mitretek Systems, Inc.

CC Identification: *Common Criteria for Information Technology Security Evaluation,* Version 2.2, January 2004 [CCV2.2].

CEM Identification: *Common Methodology for Information Technology Security Evaluation,* Version 2.2, Evaluation Methodology, January 2004 [CEMV2.2].

Interpretations: All CCIMB interpretations as of the date of the Kick-off meeting held on October 8, 2004, were considered during the evaluation. As the product is sold internationally, no NIAP interpretations were considered. The only CCIMB interpretation for CC version

2.2, interpretation 137, does not apply as FIA_USB is not included in the TOE.

3 Security Policy

The TOE assists in the enforcement of three information flow policies by managing user data in the form of electronic mail messages. The TOE validates the contents of messages to verify their security level, passing this information to the environment in the form of the Trusted Guard, which then uses that information to make information flow control decisions. The TOE does not enforce the security policies; it evaluates information provided to it by the environment and provides a policy decision back to the environment, which then enforces the policy. The security policy decisions that the TOE supports include:

- **No Signed Receipts Request Filter.** Disallow messages which require a receipt.
- **Min-Max Filter.** Disallow messages with security labels below the message recipient's minimum clearance level or above the domain's maximum clearance level. This filter uses the message's label, the recipient's minimum security clearance, and the domain's maximum security clearance provided to the filter by the environment and returns an indication whether the policy permits the user to receive the message.
- **Message Precedence (Routine or Lower) Filter.** Allow only messages with routine precedence. This filter uses precedence information supplied by the environment and returns an indication of the message precedence.
- **Valid Message Format Filter.** Allow only properly formatted mail messages. This filter is performed first, using a message parser that is part of the IT environment. The filter returns an indication of the results of that parser.
- **Security Label (Protected B or Lower) Filter.** Allow only messages marked at one of the security levels: Unclassified, Protected A, or Protected B. This filter uses security label information provided by the environment and will cause messages without valid labels to be rejected, and messages above a particular level to be rejected.
- **No Attachment Filter.** Disallow messages with more than one P772 body part. This filter uses the number of body parts returned by the message parser (which is part of the IT environment) to return an indicator of the presence of a message attachment.

These filters support three security policies:

- **P.MAILONLY:** Disallow receipts, verify precedence level, and verify that a message is properly formatted.
- **P.LABELFILTER:** Only allow mail messages with proper security labels and acceptable user clearance to pass.
- **P.MOD_NOATTACHMENT:** Do not permit attachments.

The security functional requirements for the TOE and the IT environment are documented in section 5 of the ST. A summary of the SFRs for the TOE and IT environment are included in the tables below.

TOE Security Functional Requirements

Class FDP: User Data Protection	
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple Security Attributes

IT Environment Security Functional Requirements

Class FIA: Identification and Authentication	
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
Class FMT: Security Management	
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security Roles

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL4 assurance requirements:

ADO_DEL.2 Detection of modification
ADO_IGS.1 Installation, generation, and start-up procedures
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

4.2 Environmental Assumptions

The environmental assumptions listed in the following table are required to ensure the security of the TOE.

Environmental Assumptions

Assumption	Description
A.CONFIG	It is assumed that the TOE will be properly configured and maintained as defined in the MMHS Guard guidance documentation.
A.OSPROTECT	It is assumed that all filter application files and directories are protected from unauthorised access by the underlying

Assumption	Description
	trusted operating system evaluated at Common Criteria Evaluation Assurance Level 5 or higher.
A.NO_TOE_BYPASS	It is assumed that the information cannot flow between different domains without passing through the TOE.

4.3 Clarification of Scope

The TOE evaluated configuration consists of the TOE running within the MMHS guard application running on the EAL5 certified XTS-400 Trusted Operating System. This product is required to be in the IT environment but it is not within the scope of the TOE. The environment provides several complex libraries that are used for message parsing (such as the S/MIME and ASN.1 libraries). The TOE relies upon those to operate properly if it is going to provide valid results. These libraries were not considered to be in the scope of the TOE for the purpose of this evaluation.

The TOE and the TSF are identical. The logical boundary of the TOE includes the six filters described in section 3. The physical boundary of the TOE is the software that implements the six filters; the TOE environment is the entire MMHS guard application running on the XTS-400 Trusted Operating System.

5 Architectural Information

The TOE is a set of software modules that are used in conjunction with the Canadian Department of National Defense (DND) MMHS Trusted Guard, which is a system designed to securely connect highly classified computer networks with unclassified computer networks. The Target of Evaluation (TOE) is a portion of the MMHS, i.e., six message filters within the MMHS. It operates within the Content Validation Server portion of the MMHS and provides a set of security functions that permit filtering of messages that pass through the MMHS to implement a set of security policies within the MMHS.

6 Documentation

The following is a list of the end-user documentation that was used to support this evaluation:

- BAE Systems Information Technology Military Message Handling System (MMHS) Filters – v1.1 Common Criteria Security Target, Version 3.0.
- MMHS Trusted Guard Version 1.1.1 Installation Guide FS02-011-06
- MMHS Trusted Guard Trusted Facility Manual, version FS01-211-01

7 IT Product Testing

7.1 Developer Testing

The vendor testing covered all of the security functions described in section 6.1 of the ST. These functions exercised each of the filters and verified the returned security policy results for each of the security policies (P.MAILONLY, P.LABELFILTER, and P.MOD_NOATTACHMENT.) The evaluators verified that each SFR had a corresponding test case and verified that the vendor testing approach was adequate to test and verify the behavior of the SFRs. A determination that the testing was systematic is supported by the evaluators demonstrating complete coverage for expected SFR behaviour. The correspondence between the test coverage and the functional specification was verified.

The evaluation team executed independent tests to verify proper behavior of the SFRs by first executing all vendor test cases. The TOE was installed using the vendor-supplied documentation. The Vendor test cases, which are manual tests, were performed and verified. These tests were executed using the developer test plan step-by-step guidance. The output from each of the tests was recorded by the test team as evidence. The test report demonstrates complete coverage for all TSF interfaces by the developer tests.

The evaluation team determined that the developer's actual test results matched the vendor's expected results.

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 and high level design. The evaluation team performed the developer's test suite and devised an independent set of team tests and penetration tests. The developer tests were focused on testing the MMHS Trusted Guard according to a specific security

policy (default policy only) required by their customer; therefore, the goal of the independent functional tests was to test the TOE beyond that default security policy. Testing the TOE by sending messages to multiple receipts was another area where the developer testing was not completed; therefore the evaluation team repeated some of the developer tests by sending messages to multiple recipients.

Team testing was performed to ensure that manipulation of the contents of user messages did not permit means of bypassing the TSF. There were some functional problems noted during the team testing (some rejected messages did not result in a rejection message being returned to the sender) but these did not allow information flow in contradiction of security policy. These issues will be investigated by the developer for a future product release. Team testing manipulated messages in several ways to attempt to provide coverage for all TSF interfaces and did not find any instances of policy violation. The evaluation team executed penetration tests with the objective to observe the behavior of the TOE (the 6 filters) by passing bad parameters, or impermissible values.

Penetration testing was performed to ensure that certain forms of misconfiguration of the Guard (invalid security policy specification) did not permit messages to violate policy.

7.3 Strength of Function

The Strength of Function requirements were not applicable for this TOE. The threat level for the TOE authentication function is assumed to be **SOF-basic**. Strength of function applies only to non-cryptographic, probabilistic or permutational mechanisms. The SOF requirement applies to the identification and authentication functionality within the TOE and for this TOE the environment handles the identification and authentication functionality.

7.4 Vulnerability Analysis

The vendor searched for publicly known vulnerabilities specifically related to the TOE. No publicly-known vulnerabilities specific to the evaluated version of MMHS Message Filters were found. The following public domain sources were used to identify and search for relevant vulnerabilities:

- Common Vulnerabilities and Exposures (CVE) (http://www.cve.mitre.org/)
- National Vulnerability Database (http://nvd.nist.gov/nvd.cfm)
- US-CERT Vulnerability Notes Database (http://www.kb.cert.org/vuls/)

The evaluation team accepted the vendor's analysis as reasonable that the MMHS Trusted Guard and the XTS-400 STOP 6.1.E OS have the following properties which make most of publicly vulnerabilities inapplicable:

- MMHS Trusted Guard does not contain the SNMP, FTP server, telnet server, Web server, NFS network services;

- MMHS Trusted Guard does not include internet name translation;
- MMHS Trusted Guard does not include SSL, SSH, Kerberos, IPsec, or any other network security mechanism (other than the old checksums and sequence numbers built into the low protocols);
- MMHS Trusted Guard does not allow logins across a network.
- The Ethernet controllers are "dumb" in that they do not implement protocols above layer 2 and have no capability to route traffic between ports.

The evaluation team also agreed with the vendor's analysis that the XTS-400 STOP 6.1.E OS protects the TOE from some of the well-known vulnerabilities such as unprotected files with TSF data, unprotected ports, guessing accounts that do not require I&A, and default passwords.

The assumed level of expertise of the attacker is unsophisticated, with access to only standard equipment and public information about the product. The specific threats that the TOE is designed to counter are listed in section 3.2 of the ST.

8 Evaluated Configuration

The evaluated configuration includes MMHS (Military Message Handling System) Filters Version 1.1.1 software. The logical boundary of the TOE and the TSF boundary are identical. There is no TSF data maintained by the TSF.

9 Results of the Evaluation

The evaluation team performed the applicable Common Evaluation Methodology activities according to a CygnaCom proprietary methodology. As issues were raised during the evaluation process, observations were documented and provided to the sponsor for correction. Incremental ETRs were released to document the progress of the ST and TOE evaluations. The evaluation team provided rationale for each verdict as part of their final ETR, describing the steps that were executed for each work unit, including the source of information used to make an evaluation conclusion. The ETR provided detailed rationale for each evaluation decision.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC, Version 2.2; CEM, Version 2.2, and all applicable International Interpretations in effect on October 8, 2004.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. 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.

The evaluation determined that the product meets the assurance requirements of EAL 4. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom. The security assurance requirements are displayed in the following table.

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ACM_AUT.1	Partial CM Automation
ACM_CAP.4	Generation support and acceptance procedures
ACM_SCP.2	Problem tracking CM coverage
ADO_DEL.2	Detection of modification
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.2	Fully defined external interfaces
ADV_HLD.2	Security enforcing high-level design
ADV_IMP.1	Subset of the implementation of the TSF
ADV_LLD.1	Descriptive low-level design
ADV_RCR.1	Informal correspondence demonstration
ADV_SPM.1	Informal TOE security policy model
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.1	Identification of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: high-level design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_MSU.2	Validation of analysis
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.2	Independent vulnerability analysis

The Validation Team agreed with the conclusion of the CygnaCom Evaluation Team, and recommended to CCEVS Management that an EAL4 certificate rating be issued for MMHS Message Filters.

10 Validator Comments/Recommendations

The Validation team used vendor-supplied documentation to familiarize themselves with the TOE usage and environment. The Validator used a combination of communications with the evaluation team (largely via electronic mail), records review, and review of the final ETR results to verify the results of the evaluation team's analysis. The evaluation team responded to Validator queries in a timely manner. No deficiencies were found in the execution of the CEM work units.

No significant issues were found during the validation. The evaluation team responded quickly to all validation team requests and observations.

The TOE functional requirements do not include Reference Mediation (FPT_RVM) or Domain Separation (FPT_SEP). The consequence of this is that the TOE is not known to be self-protecting.

11 Security Target

The security target for The MMHS Filters is contained within the document *BAE Systems Information Technology Military Message Handling System (MMHS) Filters – v1.11 Common Criteria Security Target, Version 3.0* dated April 23, 2006 [ST]. The ST is compliant with the *Specification of Security Targets* requirements found within Annex A of Part 1 of the CC [CCV2.2].

The document identifies the security functional requirements necessary to implement Access Control security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 4.

12 Glossary

Acronym	Expansion
CC	*Common Criteria for Information Technology Security Evaluation.* [Note: Within this Validation Report, CC always means Version 2.2, dated January, 2004.]
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CCIMB	Common Criteria Interpretations Management Board
DND	Department of National Defense
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
MMHS	Military Message Handling System
NIAP	National Information Assurance Partnership
PP	Protection Profile

SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

13 Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap.nist.gov/cc-scheme).

CCEVS Documents

[CCV2.2] *Common Criteria for Information Technology Security Evaluation*, CCIMB-2004-01-002, Version 2.2, January 2004.

[CEMV2.2] *Common Methodology for Information Technology Security Evaluation*, Version 2.2, Part 2: Evaluation Methodology, January 2004.

[CCEVS3] *Guidance to Validators of IT Security Evaluations*, Version 1.0, February 2000.

[CCEVS4] *Guidance to Common Criteria Testing Laboratories*, Draft, Version 1.0, March 2000.

Other Documents

[ST] *BAE Systems Information Technology Military Message Handling System (MMHS) Filters – v1.1.1 Common Criteria Security Target, Version 3.0*, April 23, 2006.