Certification Report

EAL 4 Evaluation of MICROTECH M7245 Revision 7, M7246 Revision 7, and M7248 Revision 4

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-80-CR
Version: 1.0
Date: 26 May 2010
Pagination: i to iii, 1 to 11

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 2.3* for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3.* This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment Canada.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is DOMUS ITSL located in Ottawa, Canada.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 26 May 2010, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

TABLE OF CONTENTS

Executive Summary

MICROTECH M7245 Revision 7, M7246 Revision 7, and M7248 Revision 4 (hereafter referred to as MICROTECH M7245/M7246/M7248), from MICROTECH, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 evaluation.

MICROTECH M7245/M7246/M7248 comprises three rack mountable data channel switch models that operate at the physical level. Data switching capabilities include: RS530 to RS530; RJ45 to RJ45; and 10/100 Base-T to Fibre Optic 1300 nm. The switches may be controlled locally by manually operating the front panel push buttons or remotely via the DB9 Control port located on the rear of the unit. The front panel displays indicate the respective switch position of each data channel and the unit power status.

DOMUS ITSL is the CCEF that conducted the evaluation. This evaluation was completed on 30 April 2010 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for MICROTECH M7245/M7246/M7248, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 4 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation methodology Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the MICROTECH M7245/M7246/M7248 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products List (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 evaluation is MICROTECH M7245 Revision 7, M7246 Revision 7, and M7248 Revision 4 (hereafter referred to as MICROTECH M7245/M7246/M7248), from MICROTECH.

2 TOE Description

MICROTECH M7245/M7246/M7248 comprises three rack mountable data channel switch models that operate at the physical level. Data switching capabilities include: RS530 to RS530; RJ45 to RJ45; and 10/100 Base-T to Fibre Optic 1300 nm. The switches may be controlled locally by manually operating the front panel push buttons or remotely via the DB9 Control port located on the rear of the unit. The front panel displays indicate the respective switch position of each data channel and the unit power status.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for MICROTECH M7245/M7246/M7248 is identified in Section 5 of the Security Target (ST).

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: MICROTECH M7245, M7246 and M7248 Security Target
Version: 1.7
Date: 26 Apr 2010

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation methodology Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3.*

MICROTECH M7245/M7246/M7248 is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2;
b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and
c. Common Criteria EAL 4 conformant, with all security the assurance requirements in the EAL 4 package.

6 Security Policy

MICROTECH M7245/M7246/M7248 implements switching related security policies as well as policies related to data protection, self protection, and security management. Further details on these security policies may be found in Section 5 of the ST.

7 Assumptions and Clarification of Scope

Consumers of MICROTECH M7245/M7246/M7248 should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- Access to the TOE's serial interface is restricted to authorized administrators. If the front panel push buttons are enabled, access to the front panel is also restricted to authorized administrators;
- The Administrator will install and configure the TOE according to the administrator guidance;
- Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going; and
- Users connected to any of the data channel interfaces of the TOE are assumed to possess the necessary privileges to access any information made accessible to them via the TOE switch configuration.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE will be located in an environment that provides physical security and temperature control required for reliable operation.

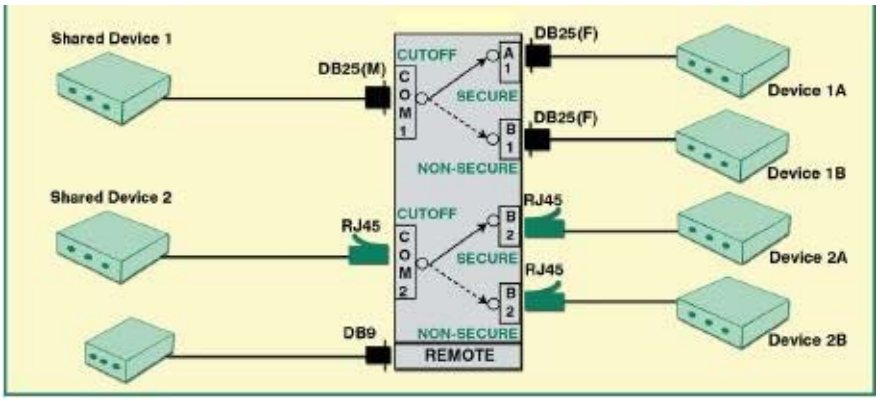
7.3 Clarification of Scope

The TOE does not have the ability to prevent unauthorized access other than by the locking out of the front panel manual push buttons. Only authorized individuals should have physical access to the TOE.

8 Architectural Information

MICROTECH M7245/M7246/M7248 comprises three rack mountable data channel switch models that operate at the physical level. The switches may be controlled locally by manually operating the front panel push buttons or remotely via the DB9 Control port located on the rear of the unit. The front panel displays indicate the respective switch position of each data channel and the unit power status.

Switch architecture is represented in the following M7246 diagram.



Further details about the system architecture are proprietary to the vendor, and are not provided in this report.

9 Evaluated Configuration

The evaluated configuration for MICROTECH M7245/M7246/M7248 comprises:

- M7245 Revision 7 with firmware 724XF.HEX v2.0 and 724XR.HEX v2.0;
- M7246 Revision 7 with firmware 724XR.HEX v2.0; and
- M7248 Revision 4 with firmware 724XR.HEX v2.0.

10 Documentation

The MICROTECH documents provided to the consumer are as follows:

- MODEL 7245 OPERATION GUIDE Revision 5;
- MODEL 7246 OPERATION GUIDE Revision 5;
- MODEL 7248 OPERATION GUIDE Revision 4; and

- Delivery and Operation version D.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of MICROTECH M7245/M7246/M7248, including the following areas:

Configuration management: An analysis of the MICROTECH M7245/M7246/M7248 configuration management system and associated documentation was performed. The evaluators found that the MICROTECH M7245/M7246/M7248 configuration items were clearly marked, and could be modified and controlled, and that the configuration management system supported generation of the TOE. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of MICROTECH M7245/M7246/M7248 during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluator analyzed the MICROTECH M7245/M7246/M7248 functional specification, high-level design, low-level design, security policy model, and a subset of the implementation representation; they determined that the documents are internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluator also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the MICROTECH M7245/M7246/M7248 administrator and user guidance documentation and determined that it sufficiently and unambiguously describes how to securely use and administer the product, and that it is consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the MICROTECH M7245/M7246/M7248 design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

Vulnerability assessment: The evaluators examined the developer's vulnerability analysis for MICROTECH M7245/M7246/M7248 and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of

public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL 4 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[2].

The evaluators analyzed the developer's test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification, TOE design and security architecture description was complete.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach was the following list of DOMUS ITSL test goals:

- Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;
- Self-protection: The objective of this test goal is to determine the TOE's ability to protect itself from improper command sets; and
- Isolation: The objective of this test goal is to determine that the two channels are isolated from one another and meet isolation requirements.

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

12.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and a focused review of all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- Switching: The objectives of this test goal are to determine the effects of simultaneous manual/remote switch configuration and of switch reconfiguration while data is being transmitted; and

- TOE Reset: The objective of this test goal is to determine that switch configuration settings are maintained on a power failure/power reset.

The independent penetration testing did not uncover any exploitable vulnerabilities in the anticipated operating environment.

12.4 Conduct of Testing

The MICROTECH M7245/M7246/M7248 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at DOMUS ITSL. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that MICROTECH M7245/M7246/M7248 behaves as specified in its ST and functional specification.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 4 level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

Consumers should review the security aspects of the intended environment, as detailed in section 3 of the ST.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description

Acronym/Abbreviation/ Initialization	Description
10/100 Base-T	10 Mbit/s, 100 Mbit/s Ethernet over twisted pair
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
DB9	D-subminiature connector
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
RJ45	Ethernet-type computer connectors
RS530	Balanced serial interface standard
ST	Security Target
TOE	Target of Evaluation

16 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.1, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Version 2.3.

c. Common Methodology for Information Technology Security Evaluation Methodology Version 2.3.

d. MICROTECH M7245, M7246 and M7248 Security Target, Version 1.7, 26 Apr 2010.

e. Evaluation Technical Report Version 1.1, 30 Apr 2010.