Certification Report

EAL 2+ Evaluation of SecureLogix Corporation®

Enterprise Telephony Management (ETM®) System

Version 4.0.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-16
Version: 1.0
Date: 10 April 2003
Pagination: i to iv, 1 to 14

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and associated certificate, has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification Scheme using the Common Methodology for Information Technology Security Evaluation, Version 1.0, for conformance to the Common Criteria for IT Security Evaluation, Version 2.1. This certification report, and associated certificate, applies only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This report, and associated certificate, is not an endorsement of the IT product by the Communications Security Establishment (CSE) or by any other organization that recognizes or gives effect to this report, and associated certificate, and no warranty of the IT product by the CSE or by any other organization that recognizes or gives effect to this report, and 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. Evaluation is performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, managed by the Communications Security Establishment.

A CCEF is a commercial facility that has demonstrated the ability to meet the requirements of the CCS Certification Body for approval to perform Common Criteria evaluations. A significant requirement for such approval is accreditation to the requirements of the *ISO Standard 17025, General requirements for the accreditation of calibration and testing 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 Electronic Warfare Associates–Canada, Limited located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that a product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines and scopes 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 (evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 10 April 2003, 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 Canadian certified products list at:
http://www.cse-cst.gc.ca/en/services/common_criteria/trusted_products.html

This certification report makes reference to the following trademarked names: Windows NT, Windows 98, and Windows 2000 which are registered trademarks of Microsoft Corporation; ETM, TeleAudit, TeleWall, and TeleView which are trademarks or registered trademarks of SecureLogix Corporation; and Solaris which is a registered trademark of Sun Microsystems Inc.

TABLE OF CONTENTS

Executive Summary

The Enterprise Telephony Management (ETM®) System, Version 4.0.1, from SecureLogix Corporation, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

The ETM® System is designed to protect telecommunications lines from abuse and provide extensive auditing capabilities on all telecommunications line traffic. The ETM® System acts as a traffic firewall to protect internal telecommunication resources (telephones, modems, faxes, etc.) from abuse, fraud, and attack. The system is capable of operating in conjunction with a Private Branch Exchange, but is not required to do so.

The system can encrypt communications between components using DES or Triple DES cryptography. The ETM® System implementation of DES and Triple DES was previously validated under the Cryptographic Module Validation Program (refer to certificate numbers 149 and 150 on the DES Validated Implementations list and certificate numbers 89 and 90 on the Triple DES Validated Implementations list).

Electronic Warfare Associates–Canada, Limited is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 8 April 2003, 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 the ETM® System, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the ETM® System are advised to verify that their own environment is consistent with 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[1] for this product indicate that it meets the EAL 2 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 1.0* (with applicable final interpretations), for conformance to the *Common Criteria for IT Security Evaluation, version 2.1*. The following augmentations are claimed:

a. ACM_CAP.3 – Configuration management authorization controls;

b. ACM_SCP.1 – TOE configuration management coverage; and

[1] The evaluation technical report is an internal document to the CCS that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

c. ALC_DVS.1 – Identification of security measures.

The Communications Security Establishment, as the CCS Certification Body, declares that the ETM® System Version 4.0.1 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.

1 Identification of Target of Evaluation

The Target Of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation is the Enterprise Telephony Management (ETM®) System, Version 4.0.1, from SecureLogix Corporation.

This report pertains to the ETM® System Version 4.0.1, comprising:

a. the ETM® Management Server, build 3;

b. the TeleView™ Infrastructure Manager, build 3; and

c. the ETM® appliances (four appliances for analog, T1, ISDN/PRI, and E1 ISDN/PRI telecommunications lines, and one authorization, authentication and accounting (AAA) appliance), with version 4.0.36 software.

2 Product Description

The ETM® System Version 4.0.1 is designed to protect telecommunications lines from abuse and provide extensive auditing capabilities on all telecommunications line traffic. The ETM® System acts as a traffic firewall to protect internal telecommunication resources (telephones, modems, faxes, etc.) from abuse, fraud, and attack. The system is capable of operating in conjunction with a Private Branch Exchange (PBX), but is not required to do so.

Figure 1 in the Security Target (ST) shows a typical configuration for the ETM® System.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the ETM® System is identified in Section 5.1 of the ST.

The following Government of Canada approved algorithms were evaluated for correct implementation in the ETM® System: DES and Triple-DES. As part of the CC evaluation effort, the evaluator made use of the results generated under the Cryptographic Module Validation Program (CMVP). The cryptographic algorithms tested under the CMVP are:

1. Data Encryption Standard (DES), FIPS 46-3 Certificates #149 & #150; and

2. Triple-DES, FIPS 46-3 Certificates #89 and #90.

4 Security Target

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

Title: Security Target for the SecureLogix Corporation® Enterprise Telephony Management (ETM®) System, Version 4.0.1

EWA-Canada Document No: 1443-002-D001, Version 0.6, 7 April 2003

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 1.0*, for conformance to the *Common Criteria for IT Security Evaluation, version 2.1*. The ETM® System Version 4.0.1 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 2 augmented, containing all security assurance requirements from EAL 2, as well as the following:

   1. ACM_CAP.3 – Configuration management authorization controls;
   2. ACM_SCP.1 – TOE configuration management coverage; and
   3. ALC_DVS.1 – Identification of security measures.

6 Security Policy

The ETM® System is a telecommunications firewall that provides the same type of visibility and control over the use of the telephone network that traditional firewalls provide for Transmission Control Protocol/Internet Protocol (TCP/IP) networks. It physically interfaces with each telephone voice or data line in the enterprise and enforces a user-defined security policy based on calling number, called number, time of day, call direction (inbound, outbound), call duration, and call type (voice, fax, modem, modem energy[2], STU III, busy, unanswered, data, or undetermined). The ETM® System also provides an enterprise with the ability to counter the threat of unauthorized access to the data network through user-connected modems.

[2] Applicable only for the appliance models ETM 2100 and ETM 3200.

There are four appliance types corresponding to different types of telecommunications lines: analog, T1, ISDN/PRI, and E1 ISDN/PRI. The analog, T1, ISDN/PRI, and E1 ISDN/PRI appliances control and enforce the information flow security policy on the telecommunication lines based on the rule set and configuration settings downloaded from the ETM® Management Server. These appliances can be configured individually or as a group. There is also an AAA appliance type that is used for authorization, authentication and accounting purposes.

The ETM® System mediates access between local and external telecommunication users based on rules defined by the administrator. Rule sets are created on the ETM® Management Server, then pushed down to the appliances. The appliances allow or deny calls based on their respective rule sets. The default behaviour is to allow any calls not explicitly denied.

The ETM® System provides auditing capabilities on all telecommunications line traffic. It monitors telecommunication traffic and detects events defined by security policies. Upon detection of potential security violations, the ETM® System provides follow-up actions such as alerts and logging.

Administrators may configure the security policy to define which calls will be allowed, which will be terminated and what other actions will take place such as logging events, alerting security personnel (alerts, pages, email, etc.), or forwarding Simple Network Management Protocol (SNMP) messages to network management systems. The ETM® System can force users to access the data network through controlled remote access services and prevent access through user-configured access points. The ETM® System can prevent the misuse of telephone lines for other than their designated functions such as restricting the use of fax lines for voice or modem traffic. A default security policy rule exists to always allow emergency calls (e.g., 911).

A hardware setting exists for the 1000 Series appliances (except the AAA appliance) to determine the default failure-mode behaviour should an ETM® appliance fail (due to a power outage, for example). The ETM® appliances can be configured to fail-safe (allow all calls), or fail-secure (deny all calls). If the AAA appliance fails, the AAA session is terminated and all AAA services are unavailable.

The ETM® System provides security to its appliances from attack through the network. Data is protected from modification or disclosure when it is transmitted between separate parts of the ETM® System, by validating IP address and username and password, and by authenticating communications with a variable handshake. Cryptography is used to protect the confidentiality of data communications. The ETM® System can encrypt communications between components using DES or Triple DES cryptography.

The ETM® System has three security modes to administer the communications with its appliances. The appliances can be set to Low, Medium, or High security modes. The appliance security mode determines whether Telnet access to the appliance is enabled, and

controls the means by which modifications may be made to several security-related configuration items, including those related to networking (e.g., IP address, IP port), encryption (e.g., encryption key, encryption algorithm), and the appliance security mode itself.

7 Assumptions and Clarification of Scope

Consumers of the ETM® System should consider assumptions about usage and environmental settings as requirements for the installation and operating environment. This will ensure the proper and secure operation and functionality of the ETM® System.

7.1 Secure Usage Assumptions

For purposes of this evaluation, the ETM® System administrators are assumed to be trusted and to understand the correct usage of the system within the context of TCP/IP networking and telecommunications systems. The ETM® System must be installed and configured using the guidance specified in the SecureLogix® ETM® System Installation Guide.

7.2 Environmental Assumptions

The following assumptions are made about the operating environment of the TOE:

1. the ETM® System appliances are physically secure;

2. administrators are non-hostile and follow all administrator guidance; however, they are capable of error; and

3. the administrator is knowledgeable of both TCP/IP networking and telecommunication systems.

For more information about the TOE security environment, refer to Section 3 of the ST.

7.3 Clarification of Scope

The administrator responsible for the TOE must ensure that the TOE is delivered, installed, configured, administered, and operated in a manner that maintains its security by following proper security procedures. Compromise of the integrity and/or availability of the TOE may occur as a result of an administrator not following proper security procedures or unwittingly introducing malicious code (e.g., virus, trojan horse) into the system.

The product should be operated within the intended operating environment as specified in the ST (and in the guidance documentation).

In order to ensure that the ETM® System properly enforces the security policy without leaving vulnerabilities due to rule set processing logic, it is important that administrators carefully read and understand the applicable administrative guidance information published by SecureLogix Corporation.

8 Architectural Information

The following are the major ETM® subsystems:

a) ETM® Communication Appliance subsystem:
   1. AAA appliance;
   2. Analog appliance;
   3. T1 appliance;
   4. ISDN-PRI appliance; and
   5. E1 appliance.

b) ETM® Server subsystem:
   1. Audit Reports; and
   2. Appliance Manager/Security Policy Editor.

c) ETM® Client Interface subsystem:
   1. GUI – TeleView™ Infrastructure Manager (console) I/O;
   2. ASCII window (ETM® Commands) I/O;
   3. Telnet (ETM® Commands) I/O; and
   4. RS-232 serial (ETM® Commands) I/O.

Ethernet network links are used to implement communication channels between:

1. the appliances and the ETM® Management Server;
2. the TeleView™ Infrastructure Manager (console) and the ETM® Management Server; and
3. the administrator and appliances (Telnet).

9 Evaluated Configuration

The evaluated configuration for the ETM® System Version 4.0.1 consists of:

1. the ETM® Management Server v4.0.1 build 3 executing on an Intel®-based PC with Windows® NT 4 SP6a, Windows® 2000 SP3, and Sun platform with Solaris™ 7/8 as the operating systems;

2. the administrator TeleView™ Infrastructure Manager v4.0.1 build 3 executing on an Intel®-based PC with Windows® NT 4 SP6a, Windows® 98 (not patched), Windows® 2000 SP3, and Sun platform Solaris™ 7/8 as the operating systems;

3. Java® Virtual Machine software, version 1.3.1.04 on both the ETM® Management Server and the TeleView™ Application hosts;

4. hardware analog appliances software version 4.0.36, hardware model ETM 1010;

5. hardware T1 appliances software version 4.0.36, hardware model ETM 1020, model ETM 2100 or model ETM 3200;

6. hardware ISDN-PRI appliances software version 4.0.36, hardware model ETM 1030, model ETM 2100 or model ETM 3200;

7. hardware E1 ISDN-PRI appliances software version 4.0.36, hardware model ETM 1040, model ETM 2100 or model ETM 3200; and

8. hardware AAA appliances software version 4.0.36, hardware model ETM® 1000.

10 Documentation

The complete documentation for the ETM® System consists of a set of printed guides and in-depth, context-sensitive online Help. The following set of guides is provided with the ETM® System Version 4.0.1 in both printed and electronic (PDF) format:

1. ETM® System v4.0 Concepts Guide;

2. ETM® System v4.0 Installation Guide;

3. ETM® System v4.0 Technical Reference;

4. TeleView™ Infrastructure Manager v4.0 User Guide;

5. TeleWall® Telecom Firewall v4.0 User Guide;

6. TeleAudit® Usage Manager v4.0 User Guide;

7. ETM® System v4.0 Safety and Regulatory Compliance Information;

8. ETM® System v4.0 Minimum System Requirements. (See SecureLogix Knowledge Base at http://support.securelogix.com);

9. Knowledge Base Article #ETM170 ETM® (Enterprise Telephony Management) System v4.0.1 Release Notes;

10. Installing The ETM® System V4.0.1 Applications On Windows/Solaris; and

11. Oracle database installation and configuration articles for the ETM® System v4.0 (See SecureLogix Knowledge Base at http://support.securelogix.com).

Note: The above-listed user guides are applicable to both ETM® System v4.0 (major release) and ETM® System v4.0.1 (maintenance release).

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the ETM® System, including the following areas:

Configuration management: An analysis of the ETM® System development environment and associated documentation was performed. The evaluators found that the ETM® System configuration items were clearly marked, and had the ability to be modified and controlled. The developer's configuration management system was observed during a site visit and found to be mature and well developed. The evaluators found that SecureLogix Corporation® continues to use the Concurrent Versions System (CVS) tool to support software configuration management. This tool is an open source version control system for keeping track of all modifications to project source code files. The evaluators witnessed a CVS demonstration by the developer.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain integrity when distributing versions of the ETM® System to the user's site. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and in sufficient detail to result in a secure configuration.

Design documentation: The evaluators analysed the ETM® System functional specification and high-level design, and determined that they were internally consistent, completely and accurately instantiated all interfaces and security functions, and independently verified that the correspondence mappings between the design documents were correct.

Guidance documentation: The evaluators examined the ETM® System user and administrator guidance documentation and determined that the documentation sufficiently

describes how to securely use and administer the product, and that it was consistent with all other documents supplied for evaluation.

Life-cycle support: The evaluators assessed the development security documentation and determined that it details all security measures used in the development environment that are necessary to protect the confidentiality and integrity of the ETM® System design and implementation.

Vulnerability assessment: The ETM® System Security Target's claims for the strength of function and the developer's vulnerability analysis were validated through independent evaluator analysis. In addition, the evaluator supplemented the developer's vulnerability analysis with their own independent vulnerability analysis, and development of additional penetration tests.

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

12 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing independent penetration tests. During this evaluation, the evaluators developed independent tests by examining the design and guidance documentation, examining the developer's test documentation, and witnessing and performing a sample of the developer tests.

The test philosophy used in this evaluation was to test and evaluate the security features of the ETM® System, as defined in the functional specification. In general, the philosophy used in the establishment of test procedures for the security evaluation of the ETM® System was to prove or disprove the security claims made by the vendor through positive and negative oriented "functional type" testing. Also, the evaluators attempted to defeat the ETM® System and its programmed security policies through "penetration type" testing.

12.1 Testing Coverage

The developer-provided test documentation comprised a test suite and an analysis of both coverage and depth, which were reviewed in detail by the evaluator. The evaluator tests focused on the security functional requirements defined in the ST and the security functions defined in the functional specification.

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 EWA-Canada test goals:

a. Test Goal No. 1: Installation procedures;

b. Test Goal No. 2: System admin functionality;

c. Test Goal No. 3: AAA voice modem functionality;

d. Test Goal No. 4: Call-processing policy execution;

e. Test Goal No. 5: Regression testing based on results from the previous CC evaluation of ETM™ Platform v3.0.1;

f. Test Goal No. 6: Audit;

g. Test Goal No. 7: Secure communication between Client, Server and Appliance;

h. Test Goal No. 8: Vulnerability assessment;

i. Test Goal No. 9: Security modes [High, Medium, Low];

j. Test Case No. 10: Access control;

k. Test Case No. 11: Report generation; and

l. Test Case No. 12: Self-protection mechanisms.

12.2 Penetration Testing

Independent penetration vulnerability tests were devised using the ETM® System vulnerability analysis and associated strength of function analysis, the functional specification, the high-level design, the ST, and the ETM® System user documentation. The tests focused on:

a. running vulnerability analysis tools against each of the target system components;

b. attempting to overflow the open network sockets of each system component;

c. performing port mapping on each system component;

d. monitoring network connections between system components for plaintext readable information; and

e. using high speed Denial-of-Service and flooding tools to test the stability of each system component.

12.3 Conduct of the Testing

The TOE was subjected to an extensive and comprehensive suite of formally documented independent functional and penetration tests. The testing took place at the Developer's facility in San Antonio, Texas, and at the ITSET Facility at Electronic Warfare Associates–

Canada, Limited located in Ottawa, Ontario. The CCS certification body witnessed a portion of this independent testing.

The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are defined and documented in the Evaluation Technical Report (ETR)[3].

12.4 Testing Results

The developer tests and independent functional tests yielded the expected results, giving assurance that the TOE behaves as specified in the ST and the functional specification. The penetration testing received a PASS verdict, as the evaluators were unable to exploit any of the identified potential vulnerabilities of the ETM® System in the intended operating environment while assuming basic levels of attack from both the network and the telco Public Service Telephone Network.

13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 2+** level of assurance, including the augmentations identified in section 5 of this report. All evaluation activities resulted in a PASS verdict. These results are supported by evidence contained in the ETR.

14 Evaluator Comments, Observations and Recommendations

The complete documentation for the ETM® System consists of a multi-volume set of printed guides and in-depth, context-sensitive online Help. The detailed set of guides is provided with the ETM® System in both printed and electronic (PDF and online) format. The ETM® System Concepts Guide provides a useful conceptual and technical overview of the architecture and functionality of the ETM® System, and was written for those familiarizing themselves with the product.

The ETM® System is straightforward to configure, use and integrate into a corporate telephone network.

The reporting capabilities of the ETM® System are extensive and useful.

[3] The Evaluation Technical Report is an internal document to the CCS that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review

15 Acronyms and Abbreviations

Acronym/Abbreviation	Description
AAA	Authorisation, Authentication, and Accounting
CB	Certification Body
CC	Common Criteria for Information Technology Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCRA	Common Criteria Recognition Arrangement
CCS	Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CR	Certification Report
CSE	Communications Security Establishment
CVS	Concurrent Versions System
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ETM	Enterprise Telephony Management
ETR	Evaluation Technical Report
GUI	Graphical User Interface
ISDN	Integrated Services Digital Network
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
PBX	Private Branch Exchange
PC	Personal Computer
PRI	Primary Rate Interface
SNMP	Simple Network Management Protocol
ST	Security Target
STU III	Secure Telephone Unit III
TCP/IP	Transmission Control Protocol/ Internet Protocol
TOE	Target of Evaluation

16 References

This section lists all referenced documentation used as source material in the compilation of this report:

a. Common Criteria for Information Technology Security Evaluation, CCIMB-99-031/032/033, Version 2.1, August 1999.

b. Common Methodology for Information Technology Security Evaluation, CEM-97/017, Part 1: Introduction and general model, Version 0.6, January 1997.

c. Common Methodology for Information Technology Security Evaluation, CEM-99/045, Part 2: Evaluation and Methodology, Version 1.0, August 1999.

d. CCS#4, Technical Oversight, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 1.0, 3 October 2002.

e. Security Target for the SecureLogix Corporation® Enterprise Telephony Management (ETM®) System, Version 4.0.1, 1443-002-D001, Version 0.6, 7 April 2003.

f. Evaluation Technical Report (ETR) SecureLogix Corporation® Enterprise Telephony Management (ETM®) System Version 4.0.1, 1443-006-D001, Version 0.2, 8 April 2003.