Certification Report

EAL 2+ Evaluation of the

SecureLogix Corporation®

Enterprise Telephony Management (ETM™) Platform Version 3.0.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-10
Version: 1.0
Date: 28 February 2002
Pagination: i to iv, 1 to 20

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 Canadian 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 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 (the Canadian CCS) provides a third-party evaluation service for determining the trustworthiness of IT security products. An evaluation is performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the Canadian CCS Certification Body (CB), managed by the Communications Security Establishment (CSE).

A CCEF is a commercial facility that has demonstrated the ability to meet the requirements of the Canadian CCS CB for approval to perform Common Criteria evaluations. A significant requirement for such approval by the Canadian CCS CB is accreditation to the requirements of the ISO Guide 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 performing the evaluation of the SecureLogix Corporation® Enterprise Telephony Management (ETM™) Platform version 3.0.1 is Electronic Warfare Associates-Canada Limited (EWA-Canada Ltd.) located in Ottawa, Ontario, Canada.

By awarding a certificate, a certifying body asserts, to some degree of confidence, that a product complies with the security requirements specified in its Security Target (ST). A ST is a requirement specification-like document that defines and scopes the evaluation activities. The consumer of certified IT products should review the ST, in addition to the Certification Report (CR), in order to gain an overall understanding of the product. This should specifically include any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (Evaluation Assurance Level) to which it is asserted that the product satisfies its security requirements.

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

Security Target for the SecureLogix Corporation® Enterprise Telephony Management (ETM™) Platform Version 3.0.1
EWA-Canada Document number: 1404-002-D001
Version 2.9
Dated: 14 February 2002

This CR is associated with the Certificate of Product Evaluation dated 28 February 2002.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

This Certification Report (CR) contains the results of the Common Criteria Evaluation Assurance Level 2+ IT Security Evaluation for the SecureLogix Corporation® Enterprise Telephony Management (ETM™) Platform.

The information in this CR is fully substantiated and supported by the evidence contained in the applicable Evaluation Technical Report (ETR), an internal document to the Canadian Common Criteria Evaluation and Certification Scheme (the Canadian CCS), that contains information proprietary to the developer and/or the evaluator. The ETR is not releasable for public review.

The evaluation was carried out in accordance with the rules of the Canadian CCS. The Canadian CCS has established a Certification Body (CB) that is managed by the Communications Security Establishment (CSE).

The goal of this evaluation was to provide third-party analysis and testing of the SecureLogix Corporation® ETM™ Platform. SecureLogix Corporation® sponsored the evaluation. The Common Criteria Evaluation Facility (CCEF) that conducted the evaluation was EWA-Canada Ltd. Evaluation work took place over a 10-month period from April 2001 to February 2002.

The evaluation activities consisted of a comprehensive suite of analysis and testing activities against the requirements of the Common Criteria for Information Technology Security Evaluation (CC) version 2.1, applied using the Common Methodology for Information Technology Security Evaluation (CEM) version 1.0. The CC is an ISO standard (ISO 15408) developed by the multinational Common Criteria Project sponsoring organizations.

The EWA-Canada Information Technology Security Evaluation and Testing (ITSET) facility evaluated different versions of the SecureLogix Corporation® ETM™ Platform as it evolved to meet both production and CC requirements. The final evaluation version of the SecureLogix Corporation® ETM™ Platform (v3.0.1) included the ETM™ Management Server version 3.0.1, the TeleView™ Console version 3.0.l, and the four ETM™ appliances version 3.0.30. Testing was performed at the developer's facility and the EWA-Canada ITSET facility and are defined and documented in the ETR.

The SecureLogix Corporation® ETM™ Platform 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. The SecureLogix Corporation® ETM™ Platform provides an enterprise with the ability to counter the threat of unauthorized access to the data network through user-connected modems. 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, modem, Secure Telephone Unit (STU) III, busy, unanswered, wide-band, undetermined or fax). Through the security policy, users can 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 SecureLogix Corporation® ETM™ Platform can force users to access the

data network through controlled remote access services and prevent access through user-configured access points. The SecureLogix Corporation® ETM™ Platform can also 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. The ETM™ appliances can be installed on either the trunk side or station side of the private branch exchange (PBX). The SecureLogix Corporation® ETM™ Platform is able to provide enterprise-wide visibility into activity and is compatible with multi-vendor and multi-generational PBXs. This enterprise-wide visibility into the complete telephone network provides user insight into resource utilization on an enterprise level providing empirical data to support telecommunications acquisition and reallocation tasks. The SecureLogix Corporation® ETM™ Platform has a distributed architecture that allows the user to remotely manage all aspects of an enterprise-wide deployment of the SecureLogix Corporation® ETM™ Platform including the remote installation of security policies as well as the remote updating of system software simultaneously across the enterprise.

A SecureLogix Corporation® ETM™ Platform consists of the ETM™ Management Server (or many servers for a large organization) and associated appliances that are matched to an organization's telephone systems. The appliances are installed on the telephone circuits and a single ETM™ Management Server can manage multiple appliances or arrays of appliances. The appliances are available in four different types: analog for traditional plain old telephone systems (POTS) and T1, E1 ISDN/PRI, and ISDN/PRI for digital types of telephone lines. The basic processing for security policy enforcement and management for all appliance types is similar, with the main differences being related to telephony signal conditioning and processing within the appliances.

The evaluation of the SecureLogix Corporation® ETM™ Platform demonstrated that this security product conforms to the security functional requirements specified in the Security Target, and that it is conformant to the assurance requirements for Evaluation Assurance Level 2 with the following augmentations:

- ACM_CAP.3 – Authorisation controls
- ACM_SCP.1 – Configuration management coverage
- ALC_DVS.1 – Identification of security measures

The Security Target is a public document that is posted, together with this Certification Report, on the Canadian Certified Products List.

CSE, as the Canadian CCS Certification Body, declares that the SecureLogix Corporation® ETM™ Platform version 3.0.1 evaluation meets all the conditions of the Common Criteria Recognition Arrangement (CCRA) and that the product will be listed on the Certified Products List.

1 Identification

This report pertains to the SecureLogix Corporation® ETM™ Platform version 3.0.1, comprising the ETM™ Management Server, version 3.0.1; the TeleView™ Console, version 3.0.1; and the four ETM™ appliances, Version 3.0.30. The ETM™ Management Server and TeleView™ Console software are available for Windows 2000, Windows NT and Solaris. The TeleView™ Console software is also available for Windows 98. They are both written in the Java programming language and require a Java Virtual Machine to be installed on their host PC. An example of a SecureLogix Corporation® ETM™ Platform configuration is shown in 1.

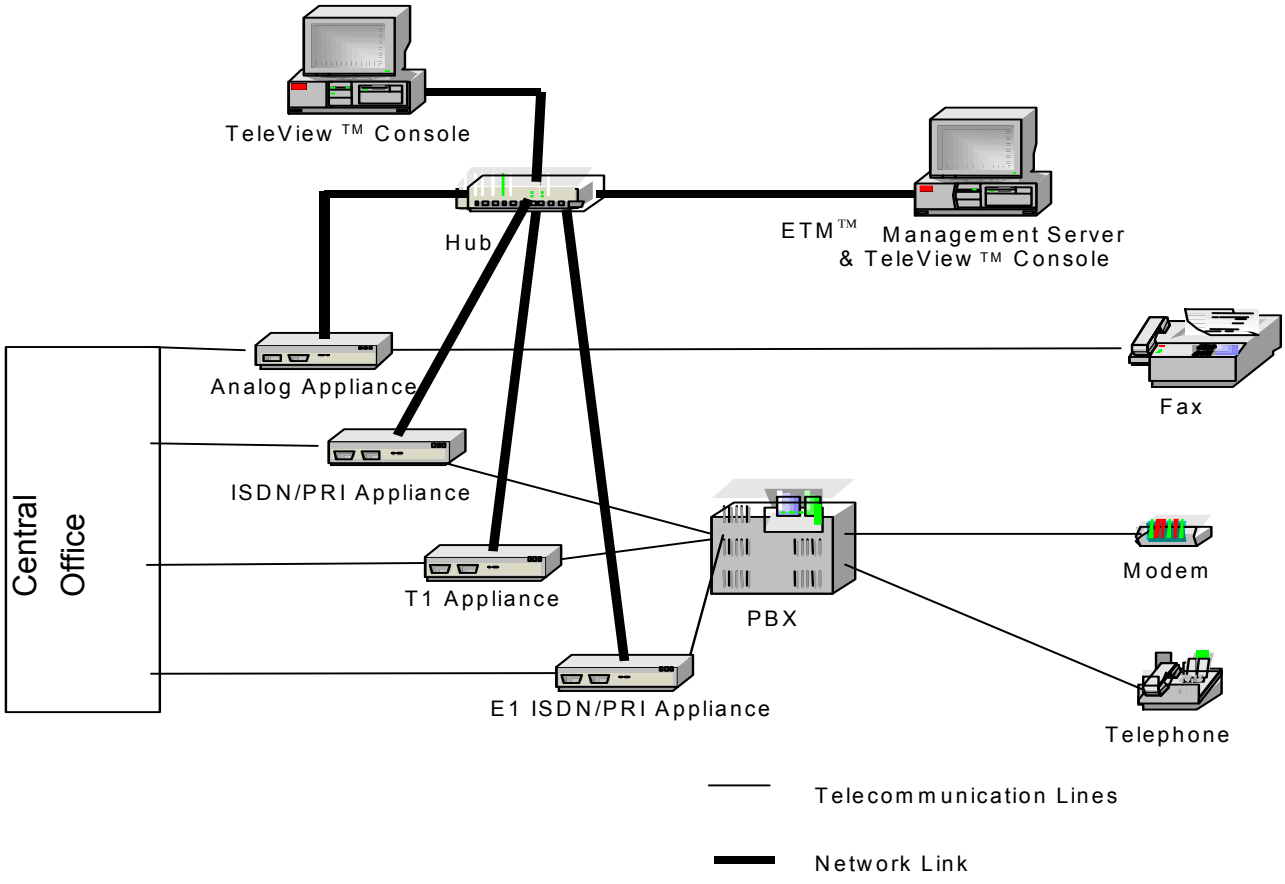

Figure 1: Example SecureLogix Corporation® ETM™ Platform Configuration

2 Security Target

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

Security Target for the SecureLogix Corporation® Enterprise Telephony Management (ETM™) Platform Version 3.0.1
EWA-Canada Document number: 1404-002-D001
Version: 2.9
Dated: 14 February 2002

The ST is a public document that is posted, together with this Certification Report, on the Canadian Certified Products List.

3 Security Policy

The SecureLogix Corporation® ETM™ Platform is a PBX-independent management platform that supports telecommunications security telephony and management applications for real-time visibility, security and control of telecommunications resources across an enterprise.

The SecureLogix Corporation® ETM™ Platform 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. The SecureLogix Corporation® ETM™ Platform is a product that provides an enterprise with the ability to counter the threat of unauthorized access to the data network through user-connected modems. 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, Secure Telephone Unit (STU) III, wideband, busy, unanswered or undetermined).

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

The SecureLogix Corporation® ETM™ Platform is designed to protect telecommunications lines from abuse and provide comprehensive auditing capabilities on all telecommunications line traffic. The ETM™ Platform monitors telecommunication traffic and detects events defined by security policies. Upon detection of potential security violations, the ETM™ Platform provides follow-up actions such as alerts and logging.

Through the security policy, users can 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 SecureLogix Corporation® ETM™ Platform can force users to access the data network through controlled remote access services and prevent access through user-configured access points. The SecureLogix Corporation® ETM™ Platform 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.

The ETM™ appliances can be installed on either the trunk side or station side of the private branch exchange (PBX). They are able to provide enterprise-wide visibility into activity and are compatible with multi-vendor and multi-generation PBXs. This enterprise-wide visibility into the complete telephone network provides user insight into resource utilization on an enterprise level providing empirical data to support telecommunications acquisition and reallocation tasks. The distributed architecture of the SecureLogix Corporation® ETM™ Platform allows the user to remotely manage all aspects of an enterprise-wide deployment, including the remote installation of security policies as well as the remote updating of system software simultaneously across the enterprise.

A hardware setting exists for the 1000 Series appliances 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).

The ETM™ Platform 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™ Platform, 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™ Platform can encrypt communications between components using DES or Triple DES cryptography.

The SecureLogix Corporation® ETM™ Platform has three security modes to administer the communications with its appliances. The appliances can be set to communicate at 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.

In Low security mode, Telnet access to the appliance is enabled and the security-related configuration items can be modified over Telnet, the serial port, or via the ETM™ Management Server. In Medium security mode, Telnet access is disabled. In High security mode, Telnet is disabled and the security-related configuration items can only be modified using the serial port. High security mode requires physical access to the appliance via the serial port to modify the security-related configuration items.

In all security modes, the non security-related settings can be changed from Telnet, the serial port, or from the ETM™ Management Server, provided that the communications type is allowed by the security mode. The user must supply a password before any configuration item, whether security-related or non security-related, can be modified via Telnet or the Serial port.

3.1 SecureLogix Corporation® ETM™ Platform Security Functions

The SecureLogix Corporation® ETM™ Platform provides a large and comprehensive set of security functions to enforce an organization's telephony security policy. These security functions can be grouped into three categories: access control, audit, and human-machine interface. Table 1 lists the Security Functional Requirements specified in the Security Target.

Functional Components	
Identifier	**Name**
FAU_ARP.1	Security alarms
FAU_GEN.1	Audit data generation
FAU_SAA.1	Potential violation analysis
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.1	Protected audit trail storage
FAU_STG.3	Action in case of possible audit data loss
FCS_COP.1	Cryptographic operation
FDP_ACC.1 (1), (2)	Subset access control
FDP_ACF.1 (1), (2)	Security attribute based access control
FDP_IFC.1 (1), (2)	Subset information flow control
FDP_IFF.1 (1), (2)	Simple security attributes
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets

Functional Components	
Identifier	**Name**
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMR.1	Security roles
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_STM.1	Reliable time stamps
FTP_TRP.1	Trusted path

Table 1: Summary of Security Functional Requirements

A brief summary of the security functions claimed by SecureLogix Corporation® is provided in the following sections.

3.1.1 Access Control

Telecommunication calls are allowed/blocked based on call attributes. The administrator creates rules set by configurable security policy, dialing plan and call monitoring definition. The SecureLogix Corporation® ETM™ Platform allows administrators to create rules which allow/block user calls based on calling number, called number, call type (voice, fax, modem, STU III, busy, unanswered, wide-band, undetermined), direction (inbound, outbound), time of day/day of week, and call duration.

Administrators must authenticate using a username and password. The SecureLogix Corporation® ETM™ Platform performs quality checks on the password to ensure only strong ones are accepted. Administrator access to the appliances is provided via the TeleView™ Console, a Telnet server, or a serial port on the appliances. The Telnet access to an appliance can be disabled if desired, and will also be disabled automatically for a period of one hour, by the appliance, if there are six failed logins. The failed login count resets to zero after a successful login. Appliances maintain a file of "allowed" IP addresses and only allow communications from ETM™ Management Servers, which have an allowed IP

address. ETM™ Management Servers have a similar file for communications to remote TeleView™ Consoles.

3.1.2 Audit

The SecureLogix Corporation® ETM™ Platform provides a comprehensive audit capability for the configuration and operation of the appliances. The levels of events to be audited can be set by the administrator. Each audit record contains a unique identification number, date and time stamps, and the appliance or appliance array that originated the record. All call details (numbers, times, telecommunication line specifics, etc.) are recorded and can be viewed in a generated report (from predefined or created templates) or plotted as a graph through the TeleView™ Console.

Audit records concerning telecommunication information flow and appliance status are generated at the appliances. The audit data is then uploaded to the ETM™ Management Server. Each appliance contains a memory card that can store the audit records temporarily if the ETM™ Management Server is unavailable. The memory cards hold the audit data in a circular buffer where it will eventually be overwritten with newer records, however there is sufficient memory to hold multiple days of audit logs even under heavy telecommunications traffic. The ETM™ Platform protects the storage of audit data by managing log file size and location.

3.1.2.1 Audit Reporting Tool

The reporting tool included with the SecureLogix Corporation® ETM™ Platform allows extensive filters to be used to provide fine-grained visibility into the operation of the system and the use of telephone lines.

For example, if a user wishes to see audit records only for modems, the user can search based on call type leaving only modem records.

3.1.3 Human-Machine Interface

For the four appliance types, the SecureLogix Corporation® ETM™ Platform human-machine interface (HMI) allows the administrator to perform the following functions:

- specify rules governing how telecommunication access is mediated;
- specify the level of telecommunications activity displayed; and
- specify what telecommunication activity is logged.

The HMI also provides the user with current and historical views of all calls, and their associated level of activity. Detailed reports and graphs may be generated from the historical data.

The SecureLogix Corporation® ETM™ Platform provides four different user interfaces: a TeleView™ Console (graphical user interface (GUI) for the Security Policy Editor), a real-time ASCII window command line, an RS-232 terminal console, and a Telnet console.

The GUI includes a straightforward and highly intuitive interface for configuring and managing the SecureLogix Corporation® ETM™ Platform. After a short training period for telephony concepts, the ETM™ Platform can be set up and operated by administrators who are inexperienced with the ETM™ Platform within a very short period of time. Of note, the SecureLogix Corporation® ETM™ Platform is capable of providing very fine-grained visibility into, and control over, the activity and traffic on telephony circuits.

The ASCII window, the RS-232 terminal console and the Telnet console can be used for configuring and managing administrative functions of the ETM™ Management Server and appliances.

The ETM™ appliances also include status lights that give real-time indications of their state and current activity.

4 Assumptions and Clarification of Scope

4.1 Environmental Assumptions

The environmental requirements and assumptions for this evaluation are:

- The SecureLogix Corporation® ETM™ Platform appliances are physically secure.
- Network protection mechanisms are in place for the server and TeleView™ Console client as defined by the user and administrator guides.
- Administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
- The administrator is knowledgeable of both TCP/IP networking and telecommunication systems.

4.2 External Interfaces

The SecureLogix Corporation® ETM™ Platform external interfaces are:

- the connections to the telephone lines;
- the TCP/IP network connecting ETM™ Platform components;
- to the TeleSweep Secure® companion product; and
- all of the human-machine interfaces.

The external interfaces are defined in detail in the ST and product documentation.

4.3 Cryptography

The SecureLogix Corporation® ETM™ Platform can be configured to encrypt communications (using DES or Triple DES) between the TCP/IP networked components. The DES and Triple DES algorithms (cryptographic module identifier – National Institute of Standards and Technology (NIST) validated implementation version 3) have been evaluated and approved to the FIPS 46-3 DES and FIPS 81 DES Modes of Operation standards.

Note that the validated version 3 cryptographic modules are being used in the 3.0.1 version of the SecureLogix Corporation® ETM™ Platform.

The following certificates at the following NIST web sites list the applicable NIST DES and Triple DES Validated Implementations:

1. http://csrc.nist.gov/cryptval/des/tripledesval.html
   ETM Platform Version 3 = TDES Certificate #90
   ETM Appliance Version 3 = TDES Certificate #89

2. http://csrc.nist.gov/cryptval/des/desval.html
   ETM Platform Version 3 = DES Certificate #150
   ETM Appliance Version 3 = DES Certificate #149

The ETM™ Platform includes an option to encrypt network communications using DES (by default) or Triple DES (upon request) cryptography. Administrators may also communicate directly to the appliances though a serial port located on the appliances.

5 Architectural Information

The major ETM™ subsystems that implement security features and the external interfaces for the SecureLogix Corporation® ETM™ Platform, and form the High Level Design are:

1. ETM™ Appliances;

2. ETM™ Management Server; and

3. Client Interfaces:

   - TeleView™ Console (includes ASCII window);
   - Telnet Consoles; and
   - RS-232 serial interface to the appliances.

For information regarding the different models of ETM™ Appliances, refer to Section 6 Evaluated Configuration.

The ETM™ Management Server and TeleView™ Console are both written in the Java programming language and require a Java Virtual Machine version 1.3 or higher, to be installed on the host PC.

All appliances are designed by SecureLogix Corporation® using commercially available components and use the Linux 2.4 kernel as the underlying operating system. The types of appliances that are selected and used for specific installations (e.g. analog, T1, E1 ISDN/PRI, or ISDN/PRI) depend on the type of incoming telephony lines. The security policy enforcement logic within each of the appliance types is the same, with the only fundamental differences between the appliances being the signal and waveform conditioning for analog, T1, E1 ISDN/PRI, or ISDN/PRI.

Ethernet network links are used to implement the following communication channels between:

- the appliances and the ETM™ Management Server;
- the TeleView™ Console and the ETM™ Management Server; and
- the administrator and appliances (Telnet).

6 Evaluated Configuration

The evaluated configuration components of the SecureLogix Corporation® ETM™ Platform version 3.0.1 are:

- the ETM™ Management Server version 3.0.1 executing on an Intel based PC with Windows 2000, Windows NT 4 SP6a, or Solaris 7/8 as the operating system;
- the administrator TeleView™ Console version 3.0.1 executing on an Intel based PC with Windows 2000, Windows NT 4 SP6a, Windows 98 (unpatched), or Solaris as the operating system;
- hardware analog appliances software version 3.0.30, model ETM™ 1010;
- hardware T1 appliances software version 3.0.30, hardware Model ETM™ 1020, Model ETM™ 2100, or Model ETM™ 3200;
- hardware E1 ISDN/PRI appliances software version 3.0.30, hardware Model ETM™ 1040, Model ETM™ 2100, or Model ETM™ 3200; and
- hardware ISDN/PRI appliances software version 3.0.30, hardware Model ETM™ 1030, Model ETM™ 2100, or Model ETM™ 3200.

A SecureLogix Corporation® ETM™ Platform consists of the ETM™ Management Server and associated appliances that are matched to an organization's telephone system. The appliances are actually installed on the telephone circuits and a single ETM™ Management Server can manage multiple appliances or arrays of appliances. The appliances are available in different types: analog for traditional analog phone lines, and T1, E1 ISDN/PRI, and ISDN/PRI for digital types of telephone lines. The basic processing for security policy enforcement and management for all appliance types is similar, with the main differences being telephony signal processing within the appliances.

Testing of the evaluated configuration was performed at SecureLogix Corporation® and at the EWA Canada Ltd. ITSET facility. The ITSET facility network is shown in Figure 2. The testing at SecureLogix Corporation® included testing with "live" telephone Central Office interfaces in addition to

simulated calls for all models of appliances and all operating systems.

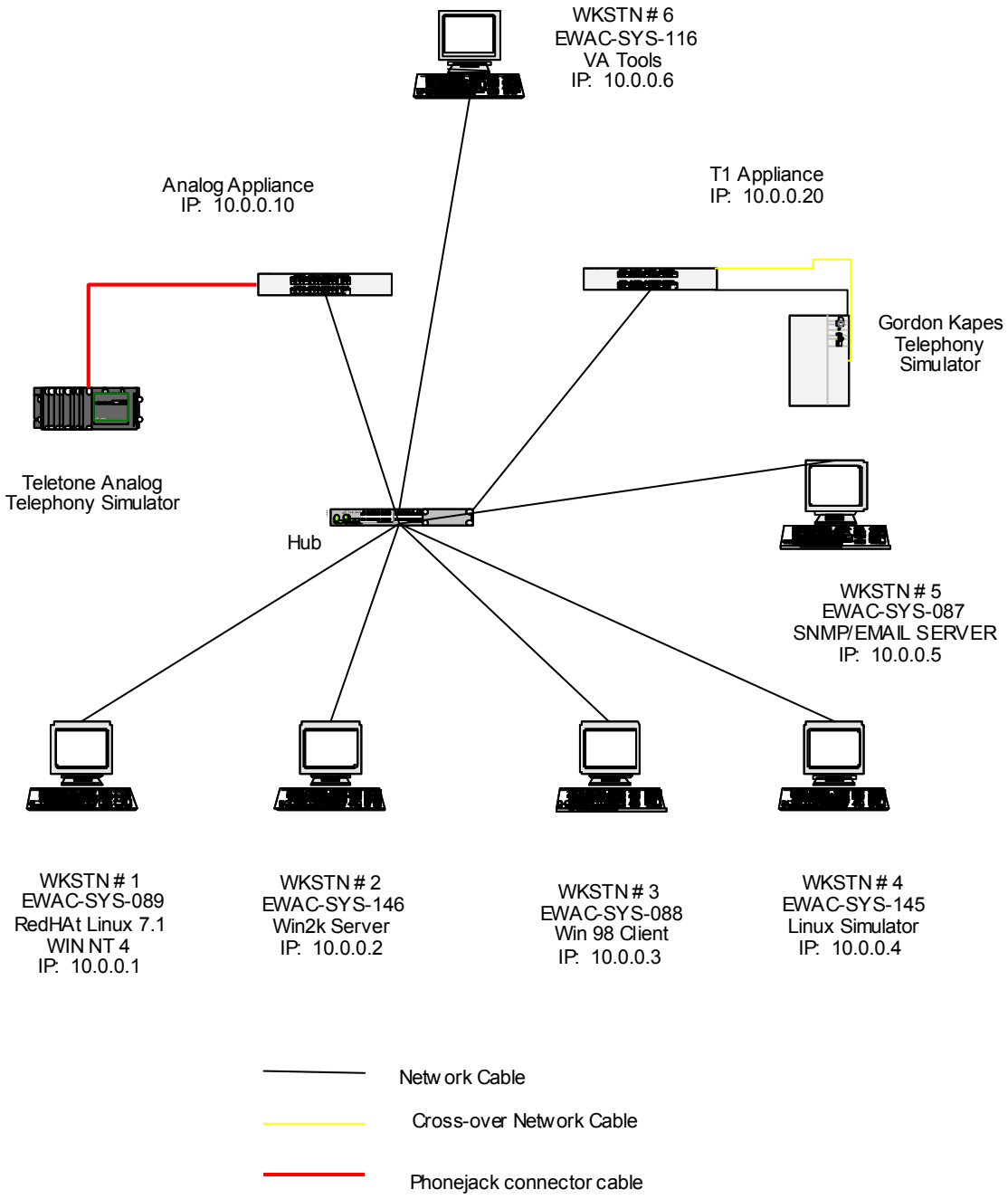

Figure 2: ITSET Facility Network

7 Documentation

7.1 Consumer Documents

The complete documentation for the ETM™ Platform version 3.0.1 consists of a six-volume set of printed guides and in-depth, context-sensitive, online Help. The version number for the document set is v3.0.1 and is comprised of:

- ETM™ Platform Concepts Guide;
- ETM™ Platform Installation and Configuration Guide;
- ETM™ Platform Administration Guide;
- TeleWall® Telecommunications Firewall User Guide;
- TeleAudit® Usage Manager User Guide; and
- ETM™ Platform Safety and Regulatory Compliance Information.

8 Evaluation Analysis Activities

8.1 Scope of Evaluation Analysis Activities

The evaluation involved an analysis of the developer's processes used to develop and support the SecureLogix Corporation® ETM™ Platform and associated documentation. The product documentation and design were considered from a security perspective, along with the associated operational user's manuals and administrative guidance documentation.

The evaluation analysis activities specifically involved a structured evaluation of the product documentation in the following areas:

- Configuration Management (CM);
- Product Delivery and Operation, including secure installation and start-up;
- Development documentation (specifications, design and requirements traceability);
- Administrator and User Guidance documentation;
- Testing (developer's coverage and depth and functional testing);
- Strength of Function (for password mechanisms);
- Vulnerability Assessment for the product; and
- Development Security documentation.

All evaluation activities for the evaluation of the Security Target and the evaluation of the ETM™ Platform resulted in a PASS verdict.

An analysis and examination of the ETM™ Platform product, its development environment and its associated CM documentation was performed. The evaluators found that SecureLogix Corporation continues to use disciplined product development and support processes.

The evaluators examined the user and administrator guidance documentation and determined that they described how to securely use and administer the product.

The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the ETM™ Platform to the user's site.

The evaluators examined 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™ Platform design and implementation.

The ETM™ Platform Security Target's claims for the strength of function and the developer's vulnerability analysis were validated through independent evaluator analysis.

9 Product Testing

9.1 Testing Philosophy

In general there are three aspects to evaluation testing:

- assessing developer tests;
- performing independent tests; and
- performing penetration tests.

For this particular evaluation, the evaluators chose to develop a suite of independent tests by:

- examining the developer's test documentation;
- witnessing and sampling the developer tests;
- independently developing test documentation (e.g., test plan, test procedures, expected results); and
- conducting independent evaluator testing based on the evaluator test plans and procedures and documenting test results.

The test philosophy used in this evaluation was to test and evaluate the security features of the SecureLogix Corporation® ETM™ Platform, as defined in the functional specification. In general, the philosophy used in the establishment of test procedures for the security evaluation of the SecureLogix Corporation® ETM™ Platform 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 SecureLogix Corporation® ETM™ Platform and its programmed security policies through network and telecom "penetration type" testing based on defined Telecom Attacks and Vulnerabilities.

9.2 Testing Coverage

The evaluator's approach to independently test the SecureLogix Corporation® ETM™ Platform was to develop and document tests that covered all security requirements specified in the ST, with emphasis in the form of rigorous testing for a subset of the security requirements. Testing of a subset of security functionality (an approach compliant to the CEM) was appropriate since:

- The SecureLogix Corporation® test documentation was comprehensive and facilitated effective observation of developer testing.

- The developer's laboratory had additional special-purpose telephony test equipment beyond what was available at the EWA-Canada Ltd. ITSET facility.

Resulting from this test coverage approach was the following list of test goals:

- Test Goal 1 - Installation Procedures;
- Test Goal 2 – Security Policy Execution;
- Test Goal 3 – Test Observation Reports (ORs) and Clarification Reports;
- Test Goal 4 – Audit Test;
- Test Goal 5 – Changes to the ETM™ Management Server;
- Test Goal 6 – Secure communication between Client, Server and Appliance;
- Test Goal 7 – Vulnerability Test Procedure;
- Test Goal 8 – Test security posture (H, M, L);
- Test Goal 9 – Fail Safe / Fail Secure;
- Test Goal 10 – Access Control;
- Test Goal 11 – Reports; and
- Test Goal 12 – Self-protection mechanisms.

9.3 Detailed Test Plan and Procedures

The Evaluation Technical Report (ETR) contains detailed test goals, objectives, plans and detailed procedures, along with the expected test results. The ETR is an internal document to the Canadian CCS that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

9.4 Conduct of the Testing

EWA-Canada Ltd. informally tested two different developmental versions of the SecureLogix Corporation® ETM™ Platform to gain product familiarity and to facilitate the evaluation planning process.

The final evaluation version of the SecureLogix Corporation® ETM™ Platform was subjected to an extensive and comprehensive suite of formally documented tests during a three-month period. The testing took place at the Developer's facility and at EWA-Canada Ltd.

The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are defined and documented in the ETR.

Testing covered:

- The customer installation procedures to install the ETM™ Platform – the Management Server and the Appliance set-up.
- Policy creation and installation, call processing, execution of policy rules, and notification (via logs, alerts and emails) of the execution of policy rules.
- Regression testing based on developer resolution of Test Observation reports.
- Audit functionality of the Management Server and the Appliances.
- Verification that encryption secures communications between the client, server and appliance.
- Vulnerability/penetration type tests.
- Different security levels of access into the appliances.
- The Fail Closed (Safe) and Fail Open (Secure) options.
- The ability to create and administer user accounts using the Management Server Software.
- Verification that the reports generated from the security policy logs have correct information, can be configured by the user, and can be saved to file or printed.
- Verification that the ETM™ Platform is fault tolerant and able to detect and recover from errors.

9.5 Testing Results

For all tests, the observed results matched the expected results and confirmed that the security claims, telephony access controls, audit mechanisms and the external interfaces of the product operate as claimed and documented.

In summary, the results of the independent testing by EWA-Canada Ltd. confirmed the following:

- All claims made by SecureLogix Corporation® that related to the ability of the SecureLogix Corporation® ETM™ Platform to mediate access control and traffic on the telephone circuits (by allowing, blocking and auditing calls) were confirmed to be valid, for all types of access control functions.

- All claims made by SecureLogix Corporation® that related to the ability of the SecureLogix Corporation® ETM™ Platform to enforce fine-grained security policy on telephone lines based on source number, destination number, time of day/day of week, call direction (inbound, outbound), and call type (voice, modem, fax, busy, unanswered, wide-band, undetermined or STU III) were confirmed.

- All claims made by SecureLogix Corporation® that related to the ability of the SecureLogix Corporation® ETM™ Platform to audit traffic activity and other events on different telephone circuits were confirmed to be valid for all types of audit events.

- The SecureLogix Corporation® ETM™ Platform effectively terminates and/or audits and logs calls that violate corporate security policy.

- The configurable fail-safe (allow all calls), and fail-secure (deny all calls) failure modes for the SecureLogix Corporation® ETM™ Platform were confirmed to operate as claimed.

- The SecureLogix Corporation® ETM™ Platform can be securely installed on a corporate telephone network (trunk or station side) and managed via a TCP/IP network. It does not introduce any new, known or obvious vulnerability on either the telephone or TCP/IP networks.

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

10 Results of the Evaluation

The evaluation clearly demonstrated that the SecureLogix Corporation® ETM™ Platform merits an Evaluation Assurance Level (EAL) 2+ rating against the requirements of the Common Criteria.

The evaluators found and documented evidence that the SecureLogix Corporation® ETM™ Platform provides the claimed security protection.

The evaluation of the SecureLogix Corporation® ETM™ Platform has determined that it is CC Part 2 conformant to the functional requirements defined in the ST, and CC Part 3 conformant to EAL 2, augmented with the following:

- ACM_CAP.3 – Authorisation controls;
- ACM_SCP.1 – TOE Configuration Management coverage; and
- ALC_DVS.1 – Identification of security measures.

11 Evaluator Comments, Observations and Recommendations

11.1 Developer Briefings

The developer briefings were detailed and comprehensive with respect to the information presented on the product requirements, design and the corporate processes used to develop and support the product.

11.2 Documentation

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

11.3 Recommendation

Corporate users looking for technology to fill a gap in their security protection requirements to include enforcement of security policy on telephone lines are encouraged to consider implementing the SecureLogix® ETM™ Platform.

11.4 Comment on SecureLogix Corporation® Process Maturity

Although it is a relatively young company, SecureLogix Corporation® has instituted a mature set of development processes for their products, which bodes very well for future product development and support. Their systems and software engineering teams are composed of highly experienced, motivated and disciplined staff, most of who have come from very disciplined and demanding standards-based environments.

The engineering efforts of the company are efficient and are highly focused on adopting and integrating best practices and processes into every aspect of their corporate culture for product development, testing and support. As an example of this, SecureLogix Corporation® has a well-developed system for highlighting, tracking and managing all errors, deficiencies and problem rectification issues.

11.5 Configuration

The SecureLogix Corporation® ETM™ Platform is straightforward to configure, use and integrate into a corporate telephone network.

11.6 Product Reporting

The reporting capabilities of the SecureLogix Corporation® ETM™ Platform are extensive and useful.

11.7 Ease of use

For calls that conform to corporate security policy, the fact that the SecureLogix Corporation® ETM™ Platform is installed and operating is completely transparent to users.

12 Glossary

This section expands upon abbreviations and acronyms, and defines vocabulary used in a special way to help increase the readability of this report.

12.1 Abbreviations and acronyms

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
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ETM	Enterprise Telephony Management
ETR	Evaluation Technical Report
GUI	Graphical User Interface
HMI	Human-Machine 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
POTS	Plain Old Telephone System
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

13 References and bibliography

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

1. Common Criteria for Information Technology Security Evaluation, CCIMB-99-031/032/033, Version 2.1, August 1999
2. Common Methodology for Information Technology Security Evaluation, CEM-97/017, Part 1: Introduction and general model, Version 0.6, January 1997
3. Common Methodology for Information Technology Security Evaluation, CEM-99/008, Part 2: Evaluation and Methodology, Version 1.0, August 1999
4. CCS#4, Technical Oversight, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 0.84, 13 April 2000
5. Security Target for the SecureLogix Corporation® Enterprise Telephony Management (ETM™) Platform Version 3.0.1, 1404-002-D001, Version 2.9, 14 February 2002

6. Evaluation Technical Report (ETR) for the SecureLogix Corporation® Enterprise Telephony Management (ETM™) Platform Version 3.0.1, 1404-006-D001, Version 1.4, 14 February 2002