122-B

CERTIFICATION REPORT No. CRP254

Sipera UC-Sec V4.0 Software
Version 4.0
running on Dell and Portwell / Octeon hardware

Issue 1.0

August 2010

CESG Certification Body
IACS Delivery Office, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.			
Sponsor:	Sipera	Developer:	Sipera
Product and Version:	Sipera UC-Sec v4.0 Software, Version 4.0		
Platform:	Dell and Portwell / Octeon		
Description:	The TOE is a software and OS security solution that implements Unified Communications (UC) routing, firewall, and secure connection to access the UC core network for UC endpoint products, UC network solutions, and UC applications.		
CC Version:	Version 3.1		
CC Part 2:	Extended	CC Part 3:	Conformant
EAL:	EAL3 augmented by ALC_FLR.2		
PP Conformance:	None		
CLEF:	SiVenture		
CC Certificate:	CRP254	Date Certified:	11 August 2010

The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UK Scheme Publication 01 [UKSP01] and 02 [UKSP02P1], [UKSP02P2]. The Scheme has established the CESG Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [ST], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been performed properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement [CCRA] and, as such, this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements[1] contained in the certificate and in this report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. There is no implication of acceptance by other Members of the Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES

The SOGIS MRA logo which appears below confirms that the conformant certificate has been authorised by a Participant to this Agreement and it is the Participant's statement that the certificate has been issued in accordance with the terms of this Agreement.

The judgments[1] contained in the certificate and this Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which carried out the evaluation. Use of the logo does not imply acceptance by other Participants of liability in respect of those judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.

CCRA logo

CC logo

SOGIS MRA logo

[1] All judgements contained in this Certification Report (excluding the *ALC_FLR.2* component) are covered by the CCRA [CCRA] and the MRA [MRA].

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of Sipera UC-Sec V4.0 Software, Version 4.0, to the Sponsor, Sipera Systems, as summarised on page 2 'Certification Statement' of this report, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [ST], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The following product completed evaluation to CC **EAL3** augmented by ALC_FLR.2 on 21 July 2010:

- Sipera UC-Sec V4.0 Software, Version 4.0, running on Dell hardware or Portwell / Octeon hardware.

4. The Developer was Sipera Systems.

5. The evaluated configuration of this product is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration' of this report.

6. An overview of the TOE and its product architecture can be found in Chapter IV 'Product Architecture' of this report. Configuration requirements are specified in Section 1.4.2 of [ST].

Protection Profile Conformance

7. The Security Target [ST] does not claim conformance to any protection profile.

Security Claims

8. The Security Target [ST] fully specifies the TOE's Security Objectives, the Threats which these Objectives counter and the Security Functional Requirements (SFRs) and Security Functions] that refine the Objectives. Most of the SFRs are taken from CC Part 2 [CC2]; use of this standard facilitates comparison with other evaluated products.

9. The TOE security policies are detailed in [ST].

10. The environmental assumptions related to the operating environment are detailed in Chapter III (in 'Environmental Requirements') of this report.

Evaluation Conduct

11. The CESG Certification Body monitored the evaluation which was performed by the SiVenture Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [ST]. The results of this work, completed in July 2010, were reported in the Evaluation Technical Report [ETR].

Conclusions and Recommendations

12. The conclusions of the CESG Certification Body are summarised on page 2 'Certification Statement' of this report.

13. Prospective consumers of Sipera UC-Sec v4.0 Software, Version 4.0, should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST]. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that the SFRs and the evaluated configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

14. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration. Chapter II 'TOE Security Guidance' of this report includes a number of recommendations regarding the secure receipt, installation, configuration and operation of the TOE.

15. In addition, the Evaluators' comments and recommendations are as follows:

a) Any customer should adhere closely to the administrative guidance in order to maintain security.

b) Post-delivery, Sipera should spend up to six months working with the client, prior to 'live' running, to ensure that the software meets the needs of that particular client.

Disclaimers

16. This report is only valid for the evaluated TOE. This is specified in Chapter III 'Evaluated Configuration' of this report.

17. Certification is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability (smaller with higher Evaluation Assurance Levels) that exploitable vulnerabilities may be discovered after an evaluation has been completed. This report reflects the CESG Certification Body's view at the time of certification.

18. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the ETR was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance.

19. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered under an approved Assurance Continuity process by a CCRA certificate-authorising Scheme.

20. All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

II. TOE SECURITY GUIDANCE

Introduction

21. The following sections provide guidance that is of particular relevance to purchasers of the TOE.

Delivery

22. On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised during delivery.

Installation and Guidance Documentation

23. The Installation and Secure Configuration documentation is as follows:

- [INSTALL1];
- [INSTALL2];
- [INSTALL3];
- [GUIDESUP].

24. The User Guide and Administration Guide documentation is as follows:

- [GUIDESUP];
- [AG].

III. EVALUATED CONFIGURATION

TOE Identification

25. The TOE is the Sipera UC-Sec v4.0 Software, Version 4.0, which consists of:

a) the UC-Sec functionality;

b) the EMS centralized management and monitoring console software;

c) the customized Debian Linux OS for EMS; and

d) one of the following:

- the customized Debian Linux OS for the UC-Sec, or
- the customized MontaVista Linux OS for the UC-Sec.

TOE Documentation

26. The relevant guidance documentation for the evaluated configuration is identified in Chapter II (in 'Installation and Guidance Documentation') of this report.

TOE Scope

27. The TOE Scope is defined in the Security Target [ST] Section 1.5.1 and 1.5.2. Functionality that is outside the TOE Scope is defined in [ST] Section 1.5.3.

TOE Configuration

28. The evaluated configuration of the TOE is defined in [ST] Section 1.4.2.

Environmental Requirements

29. The environmental assumptions for the TOE are stated in [ST] Section 3.3.

30. The TOE was evaluated running on Dell hardware and on Portwell / Octeon hardware.

31. The environmental IT configuration is as follows:

a) the UC-Sec hardware appliance appropriate for the intended deployment;

b) the hardware device appropriate for the EMS deployment;

c) UC devices to use the UC network that the TOE protects;

d) call servers on the UC network that the TOE protects;

e) cables, connectors, and switching and routing devices that allow all of the TOE and environmental components to communicate with each other; and

f) an administrator workstation with a web browser.

Test Configuration

32. The Developers used the following configuration for their testing, as shown in Figure 1 below:

a) Hardware Requirement:

- Sipera EMS and UCSec.

b) Software Requirement:

- Sipera Firmware on Universal Serial Bus (USB) memory stick.

c) 3rd Party Server Requirements:

- Cisco Unified Communications Manager 7.0 (CUCM 7.0), Cisco Phone 7941, Webcam for Cisco;
- Skinny Video Call, 7961with Session Initiation Protocol (SIP) and Skinny Call Control Protocol (SCCP) Firmware;
- Steelbelt *Remote Authentication Dial In User Service* (RADIUS) Enterprise Edition V 6.1.0;
- RSA Authentication Manager 6.1;
- RSA TokenID;
- Access Control Server (ACS) Server;
- Syslog Watcher Pro Server;
- OpenSER Version 1.2.2;
- Snom Phones, Xlite Phones for SIP clients;
- Polycom Video Phone;
- Administration Personal Computer (PC); and
- Attacker's PC with SIPp Tools and Xlite Soft phone.

33. The Evaluators used the same configuration for their testing, as shown in Figure 1 below.

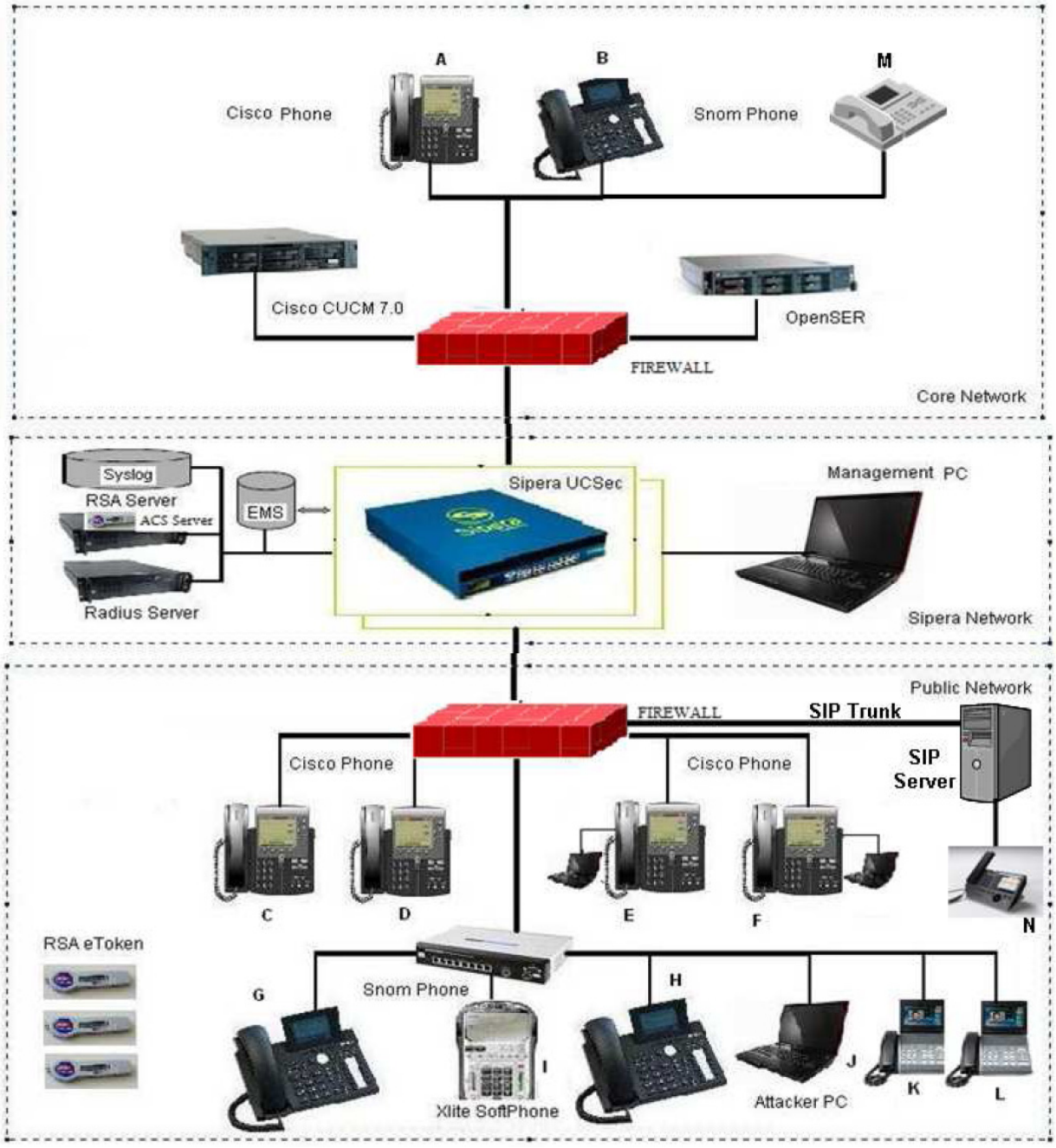

Figure 1 – Developer's and Evaluator's Test Configuration

IV. PRODUCT ARCHITECTURE

Introduction

34. This Chapter gives an overview of the main TOE architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration' of this report.

35. The deployment configuration of the TOE is shown diagrammatically in Figure 2 below.

Product Description and Architecture

36. The TOE consists of the UC-Sec software running on a customized MontaVista *or* Debian Linux OS, and the EMS software running on a second customized Debian Linux OS. The UC-Sec software is the same regardless of the OS used, and provides the main UC routing, firewall, and secure connection functionality for the TOE. The OS chosen is determined by the hardware appliance that the TOE is installed on. Each OS is optimized to suit a different hardware platform. The TOE can be deployed either in a DMZ or in the Core network of an enterprise.

37. EMS is a centralized management console. Administrators can connect to EMS to control and push configurations to one or more UC-Sec devices within the managed network. EMS is also used to manage, monitor, and collect information from each UC-Sec to which it is connected. The EMS provides a GUI based environment to an Administrator to view, monitor, and manage the UC-Sec nodes in real-time.

38. The Web Interface protects itself from tampering by requiring administrators to identify themselves and authenticate their identities before offering any functionality to the administrators. This prevents anyone who is not an authorised administrator from accessing the Web Interface. After an administrator authenticates, the administrator is issued a session ID that corresponds to the administrator's IP address.

39. Only requests from the correct IP address with the session ID are accepted by the TOE. The Web Interface also protects itself by dropping any malformed HTTP messages that could be used by an attacker to bypass the TOE's authentication mechanisms.

40. There is no domain separation for users or administrators. All UC device user traffic is handled by the same iptables application, and is kept in the same data structures. All administrator traffic is served via the same Apache Tomcat web server, and authentication data to the web GUI is stored in the same database. Although the TOE can operate on SIP or SCCP traffic, it cannot operate on both simultaneously. SIP and SCCP traffic are handled by the same iptables application with different rules defined.

TOE Design Subsystems

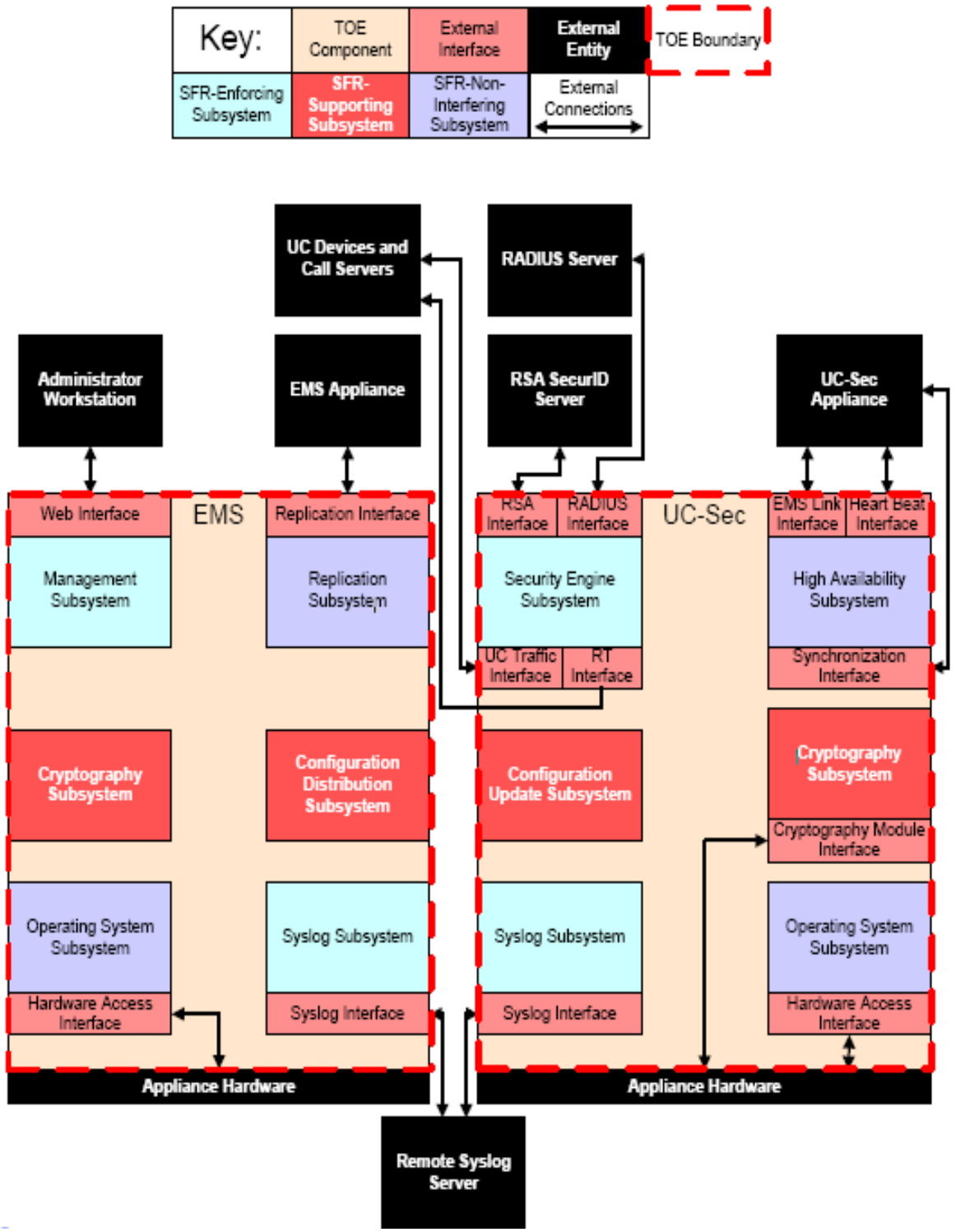

Figure 2 – TOE Subsystems

41. The TOE subsystems, and their security features and functionality, are shown diagrammatically above. A short description of these subsystems is provided as follows:

a) EMS

- Management Subsystem (SFR-enforcing). Provides a web-based GUI that administrators can use to manage one or more UC-Sec appliances.
- Configuration Distribution Subsystem (SFR-supporting). Controls the update process for configurations of UC-Sec appliances on the network.
- Replication Subsystem (SFR-non-interfering).
- Syslog Subsystem (SFR-enforcing). Receives Syslog messages from the other subsystems in the EMS component of the TOE.
- Cryptography Subsystem (SFR-supporting). Provides cryptographic and secure hashing functionality for the EMS component of the TOE.
- Operating System Subsystem (SFR-non-interfering).

b) UC-Sec

- Configuration Update Subsystem (SFR-supporting). Receives update notifications from the Configuration Distribution Subsystem.
- Security Engine Subsystem (SFR-enforcing). Responsible for monitoring UC traffic passing through the TOE and making access decisions on that traffic.
- High Availability Subsystem (SFR-non-interfering).
- Syslog Subsystem (SFR-enforcing). Receives Syslog messages from the other subsystems in the UC-Sec component of the TOE.
- Cryptography Subsystem (SFR-supporting). Provides cryptographic and secure hashing functionality for the UCSec component of the TOE.
- Operating System Subsystem (SFR-non-interfering).

TOE Dependencies

42. The only TOE dependency is:

- The underlying operating system.

TOE Interfaces

43. The external TOE Security Functions Interface (TSFI) is described as follows:

a) EMS

- Web Interface. The Web Interface provides a series of HTML pages that administrators can use to manage the EMS and one or more UC-Sec devices on the network. Communications on the Web Interface occur via Secure Hypertext Transfer Protocol (HTTPS).

b) UC-Sec

- Reverse Turing (RT) Interface. Plays a pre-recorded message to called users informing them that someone is attempting to call them. The message also instructs them to type in a pre-generated random four-digit code to connect the call.

V. TOE TESTING

TOE Testing

44. The Developer's tests covered:

- all SFRs;
- all TOE high-level subsystems, as identified in Chapter IV (in 'TOE Design Subsystems') of this report;
- all Security Functions (SFs);
- the TSFI, as identified in Chapter IV (in 'TOE Interfaces') of this report.

45. The Developer's tests also included those TOE interfaces which are internal to the product and thus had to be exercised indirectly. These interfaces can be seen in the diagram in Chapter IV (in 'TOE Design Subsystems').

46. For each protocol (SIP and SCCP) there are two possible network configurations:

a) De-Militarized Zone (DMZ) – when deployed in the DMZ, the TOE provides its services to UC devices that lie outside the corporate network and must connect remotely to gain access to devices and services within or core network.

b) Core Network – when deployed inside the core network, the TOE provides its services to UC devices operating within the corporate network only.

47. For each of the above two network configurations there are two possible hardware options: Portwell / Octeon or Dell). Therefore for each protocol, tests were carried out four times to cover all of the combinations. See Chapter III (in 'Test Configuration') for the DMZ test set-up.

48. The Evaluators devised and ran a total of 18 independent functional tests, different from those performed by the Developer. No anomalies were found.

49. The Evaluators also devised and ran a total of 12 penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

50. Evaluator testing was carried out on the DMZ network configuration with Portwell / Octeon hardware. See Chapter III in 'Test Configuration' of this report.

51. The Evaluators finished running their penetration tests on 8 July 2010.

Vulnerability Analysis

52. The Evaluators' vulnerability analysis, which preceded penetration testing and was reported in [ETR], was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables, in particular the developer's vulnerability analysis.

Platform Issues

53. The TOE runs on either of the following hardware platforms:

a) Dell;

b) Portwell / Octeon.

VI. REFERENCES

[AG] Administration Guide,
Sipera Systems,
Part Number 010-5423-400-V1.06, Issue 4.0, June 2010.

[CC] Common Criteria for Information Technology Security Evaluation
(comprising Parts 1, 2, 3: [CC1], [CC2], [CC3]).

[CC1] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Maintenance Board,
CCMB-2009-07-001, Version 3.1 R3, July 2009.

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Components,
Common Criteria Maintenance Board,
CCMB-2009-07-002, Version 3.1 R3, July 2009.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Components,
Common Criteria Maintenance Board,
CCMB-2009-07-003, Version 3.1 R3, July 2009.

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security,
Participants in the Arrangement Group,
May 2000.

[CEM] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB-2009-07-004, Version 3.1 R3, July 2009.

[ETR] Evaluation Technical Report,
SiVenture CLEF,
LFV/T010 ETR, Issue 1.1, August 2010.

[GUIDESUP] UC-Sec v4.0 Software Guidance Document Supplement,
Sipera Systems,
Version 1.0, 28 July 2010.

[INSTALL1] UC-Sec-1U Installation Guide Release 4.0,
Sipera Systems,
Part Number 101-5224-400-v1.01, February 2010.

[INSTALL2] UC-Sec-2U Installation Guide Release 4.0,
Sipera Systems,
Part Number 102-5224-400-v1.01, February 2010.

[INSTALL3] Sipera UC-Sec EMS Installation Guide Release 4.0,
Sipera Systems,
Part Number 100-5224-400-v1.01, February 2010.

[MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates,
Management Committee of Agreement Group,
Senior Officials Group – Information Systems Security,
Version 3.0, 8 January 2010 (effective April 2010).

[ST] Security Target: Sipera Systems UC-Sec v4.0 Software,
Sipera Systems,
Issue 1.0, 28 July 2010.

[UKSP00] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
UKSP 00, Issue 1.6, December 2009.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.3, December 2009.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4.2, December 2009.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.4, December 2009.

VII. ABBREVIATIONS

This list of abbreviations is specific to the TOE. It therefore excludes: general IT abbreviations (e.g. GUI, HTML, LAN, PC); standard CC abbreviations (e.g. TOE, TSF) covered in CC Part 1 [CC1]; and UK Scheme abbreviations (e.g. CESG, CLEF) covered in [UKSP00].

Term	Meaning
DMZ	De-Militarized Zone
DNS	Domain Name System
DOS	Denial-Of-Service
DTMF	Dual-Tone Multi Frequency
EMS	Elements Management System
FW	Firewall
HA	High Availability
HTTPS	Secure Hypertext Transfer Protocol
IM	Instant Messaging
IP	Internet Protocol
NAT	Network Address Translation
NTP	Network Time Protocol
PBX	Public Branch Exchange
PIN	Personal Identification Number
RADIUS	Remote Access Dial-In User Service
RT	Reverse Turing
RTP	Real-time Transport Protocol
SCCP	Skinny Client Control Protocol
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SRTP	Secure Real-time Transport Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TLS	Transport Layer Security
U	Unit
UC	Unified Communications
VoIP	Voice over Internet Protocol
WiFi	Wireless Fidelity

This page is intentionally blank.