Certification Report

EAL 2 Evaluation of Network Chemistry Inc.

Network Chemistry RFprotect™ Distributed v6.1.2, RFprotect™ Sensor v6.1.22, and RFprotect™ Mobile v6.1.2

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-66-CR
Version: 1.0
Date: 15 May 2007
Pagination: i to v, 1 to 12

DISCLAIMER

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

FOREWORD

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

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO 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, Ltd. located in Ottawa, Ontario.

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

This certification report is associated with the certificate of product evaluation dated 15 May 2007, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at: http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and on the official Common Criteria Program website at http://www.commoncriteriaportal.org/

This certification report makes reference to the following trademarked or registered trademarks:

- RFprotect™ is a trademark symbol of Network Chemistry Inc.
- Microsoft, and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries,
- CVE is a trademark of MITRE Corporation,
- Intel and Pentium are registered trademarks of Intel,
- Linux is a registered trademark of Linus Torvalds. Inc.
- Red Hat is a registered trademark of Red Hat, Inc.
- SANS is a trademark of SANS/ESCAL.
- Sun and Solaris are trademarks of Sun Microsystems, Inc. in the United States and other countries,
- UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

TABLE OF CONTENTS

Executive Summary

The Network Chemistry RFprotect™ Distributed v6.1.2, RFprotect™ Sensor v6.1.22, and RFprotect™ Mobile v6.1.2, from Network Chemistry Inc. (hereafter referred to as RFprotect™) is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) EAL 2 evaluation.

The RFprotect™ is a wireless intrusion detection system (IDS) coupled with intrusion prevention functionality. This system uses wireless network sensors to detect and respond to suspicious activity and to determine the impact of network attacks, based on collected forensic data. It analyzes the authorized wireless network, checking for and responding to identified vulnerabilities. Wireless intrusion prevention capabilities allow the RFprotect™ to prevent "rogue" wireless stations (including wireless access points, wireless network clients, and ad-hoc wireless devices) from operating within the range of the product, and to neutralize threats after identification of an attack by terminating an attacker's wireless session.

Electronic Warfare Associates-Canada, Ltd. is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 19 April 2007 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 RFprotect™, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 2 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*.

The Communications Security Establishment, as the CCS Certification Body, declares that the RFprotect™ evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) at http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-

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

e.html and on the official International Common Criteria Program website at http://www.commoncriteriaportal.org.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level EAL 2 evaluation is the Network Chemistry RFprotect™ Distributed v6.1.2, RFprotect™ Sensor v6.1.22, and RFprotect™ Mobile v6.1.2, from Network Chemistry Inc. (hereafter referred to as RFprotect™).

2 TOE Description

The RFprotect™ is a wireless intrusion detection and prevention system which uses wireless sensors to collect information about target systems and networks. The system contains an analyzer component to support analysis of the data and to initiate actions in response to its findings.

The following TOE components can be instantiated on separate inter-dependent devices to form the first TOE configuration, or they can be combined onto one device (typically a mobile laptop workstation) to form the second TOE configuration:

a. The RFprotect™ Server is a software package which is installed on standard server hardware and functions as the central management and analysis server for the RFprotect™ system;
b. The RFprotect™ Sensor is a self-contained appliance which is used to scan the channels defined in the 802.11 wireless networking specifications for unauthorized, malicious, or otherwise suspicious traffic, report its findings back to the RFprotect™ Server, and respond to unauthorized or undesirable network traffic as directed by the Server;
c. The RFprotect™ Client is a software package which is installed on standard Personal Computer (PC) hardware and is used to manage the Server and the Sensors and to view reports on wireless network activity; and
d. The RFprotect™ Mobile software is made up of functionality from RFprotect™ Sensor, RFprotect™ Server and RFprotect™ Mobile Client. It is installed on a standard PC workstation, typically a laptop computer, to provide mobility.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the RFprotect™ is identified in Section 5 of the Security Target (ST).

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature: Title: Network Chemistry RFprotect™ Distributed v6.1.2, RFprotect™ Sensor v6.1.22, and RFprotect™ Mobile v6.1.2 Security Target, Version: 1.0, Date: 16 April 2007.

5 Common Criteria Conformance

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

The RFprotect™ is:

a. Common Criteria Part 2 extended; with functional requirements based 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 conformant, with all the security assurance requirements in the EAL 2 package.

6 Security Policy

The following statements are representative of the Security Policy:

Authentication. Users must authenticate to the RFprotect™ to be able to access its security functions, event data, and audit data. A user authenticating to the RFprotect™ must provide a user name and password for a valid user account. The RFprotect™ implements role based access control. A role is assigned to an administrator when the administrator account is created. Login is not permitted if there is no associated role for the administrator.

Protection of Data Transmitted Between RFprotect™ Components. All TOE Security Function (TSF) data communicated between the physically-separated components of the Sensor and the Server is protected from disclosure by using direct protection via Network Chemistry's implementation of AES. The Sensor and Server are configured with a shared secret to validate their identity and protect their communications.

NOTE: Assessment of Network Chemistry's AES implementation did not form part of this CC evaluation and was not separately validated under the Cryptographic Module Validation Program.

For security policy enforcement please refer to the RFprotect™ Security Target.

7 Assumptions and Clarification of Scope

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

7.1 Secure Usage Assumptions

The following Secure Usage assumptions are listed in the ST:

- There will be one or more competent individuals assigned to manage the RFprotect™ and the security information it contains;
- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the RFprotect™ documentation; and
- The TOE can only be accessed by authorized administrators.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The host machine upon which RFprotect™ is installed resides in a physically secure location and only authorized individuals are granted physical access to the host;
- The RFprotect™ hardware and software critical to security enforcement by the TOE will be protected from unauthorized physical access;
- The RFprotect™ is appropriately scalable to the IT System the TOE monitors;
- The RFprotect™ has access to all the IT System data it needs; and
- The RFprotect™ will be installed such that all network traffic will flow through it.

For more information about the RFprotect™ security environment, refer to Section 3 of the ST (TOE Security Environment).

7.3 Clarification of Scope

The RFprotect™ provides a level of protection that is appropriate for a non-hostile and well-managed user community. It is designed to protect its user community against inadvertent or casual attempts to breach system security. It is not intended for situations in which hostile and well-funded attackers use sophisticated attacks from within the physical zone.

NOTE: Assessment of Network Chemistry's AES implementation did not form part of this CC evaluation and was not separately validated under the Cryptographic Module Validation Program.

8 Architectural Information

The RFprotect™ is composed of the following component subsystems:

a. RFprotect™ Sensor

The sensor is a self-contained, purpose build hardware appliance that contains an RF radio and processor that operates the ipOS 6.8 operating system, licensed from Ubicom, Inc. The Sensor is used to scan the channels defined in the 802.11 wireless networking specifications for unauthorized, malicious, or otherwise suspicious traffic, report its findings back to the RFprotect Server, and respond to unauthorized or undesirable network traffic as directed by the Server.

.

b. RFprotect™ Mobile

The RFprotect Mobile software is made up of functionality from RFprotect Sensor, RFprotect Server and RFprotect Mobile Client. It is installed on a standard PC workstation, typically a laptop computer, to provide mobility. RFprotect™ Mobile is fitted with a Peripheral Component Interconnect (PCI) card as part of the TOE environment. This is currently a commercial-off-the-shelf card with the Atheros AR5004X chipset; however any Atheros chipset may be used to communicate with the modified version of the Atheros driver used in RFprotect™ Mobile.

c. RFprotect™ Server

The RFprotect Server is a software package which is installed on standard server hardware and functions as the central management and analysis server for the RFprotect system. The Server provides scanning policies to the RFprotect Sensors deployed on the local network and receives wireless traffic reports from them. The Server stores the reports from all of the Sensors on the network and continuously analyzes the complete wireless traffic dataset. If the complete dataset indicates that suspicious or malicious activity is or may be occurring, the Server may be configured to respond by instructing one or more Sensors to take appropriate actions to mitigate the threat. The Server allows authorized users to view events generated by the Sensors via the RFprotect Client software.

d. RFprotect™ Client

The RFprotect Client is a software package which is installed on standard Personal Computer (PC) hardware. It is used to manage the Server and the Sensors and to view reports on wireless network activity. The Client provides a Graphical User Interface (GUI) to manage users and their associated roles, system policies, and alarms associated with specific events. It also provides a means to view the status of all deployed Sensors and can display reports generated by the Server to provide summary information about attacks, activity graphs, and analysis of event trends.

9 Evaluated Configuration

The RFprotect™ Security Target defines the following systems in the evaluated configuration:

a. Distributed; and

b. Mobile.

There are three components which combine to form the first evaluated configuration:

- RFProtect Sensor
- RFProtect Server running on either of the following OS:
    i. Windows (XP Professional Service Pack 2 or Windows 2003 Server Service Pack 1)
    ii. Linux (Redhat Enterprise 9, Fedora Core 3, or SUSE Enterprise 9.1)
- RFProtect Client running on either of the following OS:
    i. Windows XP Professional Service Pack 2
    ii. Windows 2003 Server Service Pack 1

Functionality of the three components can be combined on one device (typically a mobile laptop) to form the second configuration using either Windows XP Professional Service Pack 2 or Windows 2003 Server Service Pack 1.

The correct configuration is described in detail in the RFprotect™ Distributed Users Guide chapter 1.

10 Documentation

The Network Chemistry Inc. documents provided to the consumer are as follows:

a. Network Chemistry RFprotect™ Distributed 6.1.2 Release Notes;

b. Network Chemistry RFprotect™ Sensor User Manual 802.11a/b/g;

c. Network Chemistry RFprotect™ Distributed 6 Quick Start Guide;

d. Network Chemistry RFprotect™ Distributed User Guide;

e. Network Chemistry RFprotect™ Mobile 6.1.2 Release Notes;

f. Administrator Guidance Supplement; and

g. Installation Guide 6.1.2 Supplement.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the Network Chemistry RFprotect™ Distributed v6.1.2, RFprotect™ Sensor v6.1.22, and RFprotect™ Mobile v6.1.2, including the following areas:

Configuration management: An analysis of the RFprotect™ CM system and associated documentation was performed. The evaluators found that the RFprotect™ configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

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

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

Guidance documents: The evaluators examined the RFprotect™ user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Vulnerability assessment: The RFprotect™ ST's strength of function claims were validated through independent evaluator analysis. The evaluators also validated the developer's vulnerability analysis and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

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

12 ITS Product Testing

Testing at EAL2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing independent penetration tests.

12.1 Assessment of Developer Tests

The evaluators verified that the developer had met their testing responsibilities by reviewing the developer's test plan, test approach, test procedure and test results, and examining their test evidence, as documented in the Evaluation Technical Report (ETR)[2].

The evaluators analyzed the developer's test coverage analysis, and found that the correspondence between tests identified in the developer's test documentation and the functional specification was complete and accurate.

12.2 Independent Functional Testing

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

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. These tests focused on:

- Identification and authentication;
- Audit;
- Security Management;
- Basic product functionality.

12.3 Independent Penetration Testing

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

- Generic vulnerabilities;
- Bypassing;
- Tampering; and
- Direct attacks.

The evaluator conducted a port scan of the RFprotect™. The only ports found to be open were ones that would be expected. The evaluator used a publicly available tool to scan the

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

RFprotect™ for weaknesses, and none were found. The evaluator also used a publicly available packet capture tool to examine output from the RFprotect™ during startup, shutdown and normal operations. The evaluator searched the captured results in an attempt to extract information which might be useful to a potential attacker; no useful information was uncovered. In addition, the evaluator performed direct attacks on the RFprotect™, attempting to bypass or break the TOE's database mechanism.

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

12.4 Conduct of Testing

The RFprotect™ was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the ITSET Facility at EWA-Canada located in Ottawa, Ontario. The CCS Certification Body witnessed a portion of the independent testing.

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

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the RFprotect™ behaves as specified in its ST and functional specification. The penetration testing resulted in a **PASS** verdict, as the evaluators were unable to exploit any of the identified potential vulnerabilities in the RFprotect™ in its intended operating environment.

13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 2** level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The complete documentation for the RFprotect™ includes a comprehensive Installation and Users Guide.

The RFprotect™ is straightforward to configure, use and integrate into a corporate network.

Network Chemistry Inc. Configuration Management (CM) and Quality Assurance (QA) provide the requisite controls for managing all CM/QA activities.

15 Glossary

This section expands any acronyms, abbreviations and initializations used in this report.

15.1 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
ACLs	Access Control Lists
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CIAC	Computer Incident Advisory Capability
CPL	Certified Products list
CM	Configuration Management
CSE	Communications Security Establishment
CVE	Common Vulnerabilities and Exposures
DoD	Department of Defense
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IAVM	Information Assurance Vulnerability Management
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NIST	National Institute of Standards and Technology
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories Canada
PCI	Peripheral Component Interconnect
QA	Quality Assurance
SANS	SysAdmin, Audit, Network, Security
SFP	Security Function Policy
SNMP	Simple Network Management Protocol
ST	Security Target
TOE	Target of Evaluation

Acronym/Abbreviation/ Initialization	Description
TSF	TOE Security Function
US-CERT	United States Computer Emergency Readiness Team

16 References

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

a. Canadian Common Criteria Evaluation and Certification Scheme (CCS) and CCS Publication #4, Technical Oversight, Version 1.0.

b. Common Criteria for Information Technology Security Evaluation, version 2.3 Revision 326, December 2004.

c. Common Methodology for Information Technology Security Evaluation, CEM, version 2.3 Revision 326, December 2004.

d. Network Chemistry RFprotect™ Distributed v6.1.2, RFprotect™ Sensor v6.1.22, and RFprotect™ Mobile v6.1.2 Security Target, Revision No. 1.0, 16 April 2007.

e. Evaluation Technical Report (ETR) Network Chemistry RFprotect™ Distributed v6.1.2, RFprotect™ Sensor v6.1.22, and RFprotect™ Mobile v6.1.2, EAL 2 Evaluation, Common Criteria Evaluation Number: 383-4-66, Document No. 1527-000-D002, Version 1.2, 19 April 2007.