AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAM

Certification Report

Certificate Number: 2003/28

Oullim Information Technology Inc.

SECUREWORKS 3.0

Issue 1.0
September 2003

Issued by:

Defence Signals Directorate - Australasian Certification Authority

Executive Summary

This report describes the findings of the evaluation of the SECUREWORKS 3.0 product, developed by Oullim Information Technology Inc., to the Common Criteria (CC) Evaluation Assurance Level EAL3. The report concludes that the product has met the target assurance level of CC EAL3, and includes recommendations by the Australasian Certification Authority (ACA) that are specific to the secure use of the product. The evaluation was performed by LogicaCMG and was completed on 4 September 2003.

SECUREWORKS 3.0 is a software application designed to protect organisational assets in a network environment. In particular, it provides facilities to control the movement of information between networks. The product consists of two major components:

- **Firewall Server:** Software that is responsible for implementing security policy rules. This component is composed of a kernel driver that implements the security policy rules, an authentication server that authenticates administrators and users, a log server that manages the audit record, and an application gateway that provides application level filtering.

- **Administration Server:** Software that manages the security policy rules. This module provides a HTTP interface that can be accessed via a web browser. With the web browser interface, the administrator can access the Administration Server locally and monitor the SECUREWORKS System.

SECUREWORKS 3.0 has been found to uphold the claims made in the Security Target (Ref [10]), and potential customers are urged to consult this document before planning to implement the product. In particular, SECUREWORKS 3.0 has been found to provide the claimed security functionality of user data protection, protection of the TSF, security audit, identification and authentication, security management, privacy and cryptographic support, when configured according to the evaluated configuration.

Ultimately, it is the responsibility of the user to ensure that SECUREWORKS 3.0 meets their requirements. For this reason, it is ***strongly*** recommended that prospective users of the product download a copy of the Security Target (Ref [10]) from www.dsd.gov.au or alternatively obtain a copy directly from the product vendor, and read this Certification Report thoroughly prior to deciding whether to implement the product.

Table of Contents

Chapter 1 Introduction

Intended Audience

This certification report states the outcome of the IT security evaluation of the Oullim Information Technology Inc ("Oullim"), SECUREWORKS 3.0 product. It is intended to assist potential users when judging the suitability of the product for their particular requirements.

This report should be read in conjunction with the Security Target for SECUREWORKS 3.0 (Ref [10]), which provides a full description of the security requirements and specifications that were used as the basis of the evaluation. A copy of the Security Target can be downloaded from www.dsd.gov.au or obtained directly from Oullim.

Identification

Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to Chapter 7: Evaluated Configuration.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	SECUREWORKS 3.0
Software Version	SECUREWORKS 3.0 release 4
Security Target	Security Target for SECUREWORKS 3.0, Document Version 1.41, September 2003
Protection Profile Claims	U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999. U.S. Department of Defense Application-Level Firewall Protection Profile for Basic Robustness Environments, Version 1.0, June 22, 2000.
Evaluation Level	CC EAL 3
Conformance Result	CC Part 2 Conformant CC Part 3 Conformant
Evaluation Technical Report	SECUREWORKS 3.0 Firewall Evaluation Technical Report, Version 1.1, September 2003.
Version of CC	CC Version 2.1, August 1999, Incorporated with Interpretations as of 2002-02-28.
Version of CEM	CEM-99/045 Version 1.0, August 1999, Incorporated with Interpretations as of 2002-02-28
Sponsor	Oullim Information Technology Inc.
Developer	Oullim Information Technology Inc.
Evaluation Facility	LogicaCMG
Certifiers	Katrina Johnson, Lachlan Turner, Richard Helliwell

Description of the TOE

The Target of Evaluation (TOE) is called SECUREWORKS 3.0 and its primary role is to provide both traffic-filter and application-level gateway services between an internal and external network. The TOE is designed to provide facilities to control the movement of information between these networks in accordance with a defined security policy set by the organisation.

SECUREWORKS 3.0 uses a hybrid technology of dynamic packet filtering and an application gateway (proxies) to control and monitor the information flow of IP packets through the TOE. The packet filtering functions provide for traffic filtering based upon packet attributes available at the transport and network protocol layers. For application gateway filtering, the packet content is examined to determine if it complies with rules that have been established by an administrator of the TOE. SECUREWORKS 3.0 provides a number of application proxies that have been included within the scope of the evaluation to provide the application gateway filtering capability. The inclusion of application proxies provides the capability to perform application gateway filtering based on certain application-specific features. For example, the FTP proxy included within the scope of the evaluation can be configured to allow only a subset of valid FTP commands through to an FTP server located on the internal network.

For further information on the specific hardware and software components included in the evaluated configuration refer to Chapter 7: Evaluated Configuration, or Section 2.3.1 of the Security Target (Ref [10]).

Chapter 2 Security Policy

The TOE Security Policies (TSPs) define the security policies that the TOE must comply with in order to enforce the security functional requirements. The Security Target (Ref [10]) contains four explicit security policy statements AUTHENTICATEDSFP,UNAUTHENTICATEDSFP, AUTHENTICATED_FILTER SFP and UNAUTHENTICATED_PROXY SFP. In addition, the TOE implements a number of implied TSPs, drawn from the collection of security functional requirements. The TSPs are summarised as follows:

- **Identification and Authentication:** Administrators and End-Users need to be identified to establish their rights to administer the security functions of the TOE and access proxy services. Authentication of Administrators and End-Users is achieved through application either of two password-based authentication mechanisms. The TOE also enforces policy on authentication failures.

- **Privacy:** A privacy policy is implemented to limit the information about the IP configuration of the internal network that is available on the external network.

- **Audit:** An audit policy is implemented that allows for the management, logging and detection of security relevant events applicable to the secure management and operation of the TOE.

- **Cryptography:** Encryption mechanisms support the self-protection functions of the TOE to detect changes to the TOE configuration. Cryptographic mechanisms are selected such that they are suitable to provide necessary security characteristics for the intended use of the functions that the mechanisms are applied.

- **Security Management:** The TOE effectively manages and controls security attributes associated with the TOE's information flow control policies. The TOE maintains the roles of Authorised Administrator and enforces policy on static attribute initialisation.

- **Protection of the TSF:** The TOE maintains a separate security domain for its own execution, executes a suite of self-tests and ensures that TOE security functions cannot be by-passed such that TSP is appropriately enforced at all times.

Chapter 3 Intended Environment for the TOE

This section outlines the requirements and assumptions that govern the intended environment in which the TOE is designed to operate, and for which the TOE has been evaluated, and clarifies the scope of the evaluation. Organisations wishing to implement the TOE in its evaluated configuration should review the evaluation scope to confirm that all the required functionality has been included in the evaluation, and must ensure that any assumed conditions are met in their operational environment.

Secure Usage Assumptions

The evaluation of the SECUREWORKS 3.0 product took into account the following assumptions about the secure usage of the TOE:

- The TOE is physically secure.
- The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
- The TOE does not host public data.
- Information cannot flow among the internal and external networks unless it passes through the TOE.
- Authorised Administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
- The TOE only executes security relevant applications and only stores data for its secure operation. The operating system upon which the TOE executes has been hardened to restrict general-purpose computing capabilities and storage.
- Human users (End Users) within the physical secure boundary protecting the TOE may only attempt to access the TOE directly, via its console.
- Human Users (Administrators) cannot access the TOE remotely from the internal or external networks.
- Only the Authorized Administrators may have an account on the TOE host system.

Clarification of Scope

The scope of the evaluation is limited to those claims made in the Security Target (Ref [10]). All security related claims in the Security Target were evaluated by LogicaCMG as a component of the evaluation. A summary of the Security Target is provided in Appendix A of this Certification Report. The evaluated configuration for the TOE is provided in Chapter 7: Evaluated Configuration.

The TOE provides the following evaluated security functionality:

- **Security Audit:** The TOE provides logging for all activities pertaining to the actions to or through the product. The TOE also records events pertaining to accessing of security management functions. The Security Audit function can be configured to provide alarms to Authorised Administrators and access to the audit trail is restricted to that role. A search facility based on keyword, time, source and destination address is included within the Security Audit function.

- **Information Flow Control:** The TOE controls all packet flow between the internal and external networks as defined by security policy rules set by an Authorised Administrator of the TOE. Control of packet flow is performed through a kernel driver that inspects packets and is supported by application-level proxies for FTP, HTTP, SMTP, NNTP, POP3, Telnet, RLOGIN, IMAP4 and H.323. These are the only application proxies included within the scope of the evaluation.

- **Identification and Authentication:** The TOE implements an authentication server that provides both password and single-use authentication mechanisms for End Users and Authorised Administrators. Identification and Authentication can be performed at both the packet-level and application gateway level and is supported by authentication failure handling mechanisms.

- **Security Management:** The TOE provides a Management Module for maintaining and managing all security attributes associated with the provision of the IT security functions. Access to the Management Module is restricted to Authorised Administrators who can perform the following functions: Account Management; Viewing and Querying Security Logs; Defining Security Policy Rules; and Alarm Configuration.

- **Protection of Security Functions:** The Administration Server component of the TOE constantly checks the status of other firewall daemons to ensure that all services that should be running are invoked and operational and cannot be bypassed. The Administration Server also provides functionality to detect integrity errors in critical TOE and underlying system files.

Potential users of the TOE are advised that an extensive set of functions and services **have not been evaluated** as part of the evaluation of SECUREWORKS 3.0. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration. The functions and services that have not been included as part of the evaluation is provided below:

- Encrypting functions of SSL Protocol;

- Remote Administration;

- Virus filtering;

- High Availability;

- SecurID Authentication capability;

- Harmful Site Filtering Setup;
- Virtual Private Network (VPN) Module
- Redirect NAT, Exclude NAT;
- Integration with ASEN product;
- Telnet Session Capture;
- Check Integrity on Start-up;
- Store FTP Transfer Files;
- OTP (One Time Password) calculator for Windows;
- RADIUS Server;
- SNMP Trap Occurrence;
- SQL NET/NET8 Application Gateway;
- CGI Security Check;
- Operating System Password Authentication;
- SecureDNS;
- StreamWorks Application Gateway;
- HTTP Proxy Keep-Alive function;
- HTTP Allow extended methods;
- Web Cache;
- Webtrends Log Analysis Server functions;
- Authentication via LDAP;
- Open SSL cryptographic library except those mechanisms support OTP functions;
- Network Interface Card Management;
- Routing Table Management;
- Routing Protocol RIP Management;
- ARP (Address Request Protocol) Management;
- Remote LogServer;

- Authentication methods for users not registered with SECUREWORKS;
- CA (Certificate Authority) functions;
- Text Administration (Command Line Interface);
- User: Frame protocol (PPP+SLIP);
- Policy Rules relating to Confidentiality;
- Telnet and Rlogin Application Gateway Authentication Function;
- H.323 Application Gateway max session and timeout function;
- SMTP Application Gateway max mail size limit function; and
- IPSec Fragment option.

Chapter 4 TOE Architecture

SECUREWORKS 3.0 consists of the following major architectural components:

- **Firewall Server:** Software that provides the application gateway and packet filter firewall functionality and comprises the following sub-components:
    - **Authentication Server;**
    - **Audit Server;**
    - **Kernel Driver; and**
    - **Application Gateways (proxies).**
- **Administration Server:** Software that is used to securely manage the functions and services provided by the TOE, and to view audit trail information. A web-browser provides the management interface to the Administration Server.

The developer's high-level design identified two subsystems of the TOE, which each implement the security functionality. They are described as follows:

- **Firewall Server:** Provides the application gateway and packet filter firewall functionality in the following sub-components:
    - **Authentication Server:** The Authentication Server provides functionality for managing user authentication requests from either an Application Gateway (proxy) or a user of the TOE.
    - **Audit Server:** The Audit Server provides the functionality for managing the TOE audit functions. Audit events generated by TOE components are handled by the Audit Server and written to an audit database. The Audit Server may be configured to raise security alarms for Administrator defined security events.
    - **Kernel Driver:** The Kernel Driver provides the dynamic packet filtering functionality and network address translation. The Kernel Driver either allows or denies packets received on the network interfaces of the TOE based on Administrator defined Security Policy Rules.
    - **Application Gateway (proxies):** The Application Gateways (proxies) provide the application-level filtering functionality of the TOE. These proxies understand the syntax of application-specific data and can filter network traffic based upon application-specific attributes. Only a defined set of proxies have been included within the scope of evaluation.

- **Administration Server:** Software that is used to securely manage the functions and services provided by the TOE, and to view audit trail information. A web-browser provides the management interface to the Administration Server.

Chapter 5 Documentation

It is important that SECUREWORKS 3.0 is used in accordance with the guidance documentation in order to ensure the secure usage of the TOE. The following documentation is provides with the product:

- SECUREWORKS 3.0 Evaluated Configuration Installation Guide, Oullim Information Technology Inc (Ref [12])

- SECUREWORKS 3.0 Installation Guide, Oullim Information Technology Inc, Version 1.20 (Ref [13])

- SECUREWORKS 3.0 Operation Guide, Oullim Information Technology Inc, Version 1.18 (Ref [14]).

- SECUREWORKS 3.0 User Guide, Oullim Information Technology Inc, Version 1.12 (Ref [15])

The SECUREWORKS 3.0 Evaluated Configuration Installation Guide (Ref [12]) and SECUREWORKS 3.0 Installation Guide (Ref [13]) together are intended to provide the Authorised Administrator with the guidance and information required to install and configure the TOE in a secure manner.

The SECUREWORKS 3.0 Operation Guide (Ref [14]) is intended to provide the Authorised Administrator with guidance on the secure operation of SECUREWORKS 3.0.

The end-user is supplied with the SECUREWORKS 3.0 User Guide (Ref [15]) to provide the effective guidance for using the TOE in a secure manner.

Chapter 6 IT Product Testing

The objectives associated with the testing phase of evaluation can be placed into the following categories:

- **Functional testing:** Tests performed to ensure that the TOE operates according to its specification and is able to meet the requirements stated in the Security Target (Ref [10]).
- **Penetration testing:** Tests conducted to identify exploitable vulnerabilities in the TOE's intended operational environment.

Functional Testing

In this phase the evaluators analysed evidence of the developer's testing effort, including test coverage and depth analyses, test plans and procedures, and expected and actual results, to gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE. In addition, the evaluators drew on this evidence to develop a set of independent tests, comprising a sample of the developer tests, in order to verify that the test results matched those recorded by the developers. The functional testing effort also included a selection of independent functional tests that expanded on the testing done by the developers.

The functional testing effort covered the full range of Security Functional Requirements identified in the Security Target (Ref [10]), with the exception of those that rely on cryptographic operations. Whilst the tests devised did ensure that the cryptography was being implemented, testing of the actual cryptographic processes is considered the responsibility of the national cryptographic authority. In Australia, the cryptographic functions have been evaluated by the Defence Signals Directorate, as the national authority, and found suitable for Australian and New Zealand Government use. Australian and New Zealand Government users should carefully read the Cryptography section in Chapter 9: Recommendations.

Penetration Testing

The developers performed a vulnerability analysis of SECUREWORKS 3.0, in order to identify any obvious vulnerabilities in the product and to show that they are not exploitable in the intended environment for the TOE. This analysis included a search for possible vulnerability sources in the evaluation deliverables, the intended TOE environment, public domain sources and internal Oullim sources. A number of potential vulnerabilities, relevant to the product type, were identified. In each case the developers were able to show that the vulnerability was not exploitable in the TOE's intended operation environment. .

Based on the information given in the developer's vulnerability analysis, the evaluators were able to devise a penetration test plan that would test that the TOE is resistant to penetration attacks performed by an attacker with low attack potential. Upon completion of the penetration testing activity, the evaluators concluded that the TOE did not display any susceptibility to vulnerabilities obtained from the developer in the intended environment.

Chapter 7 Evaluated Configuration

The TOE is comprised of the following software components:

- SECUREWORKS 3.0 Firewall Server
- SECUREWORKS 3.0 Administration Server

The TOE requires the following minimum hardware:

- SunSparc with 256Mb Memory, 8GB Hard Disk space, 2 Network Interface Cards and D.A.T. Backup Device;
- SUN Solaris 5.8 for Sparc;
- Netscape 6.1 (or higher) to interface with Administration Server; and
- Unix OTP (One Time Password) Calculator.

Procedures for Determining the Evaluated Version of the TOE

When placing an order for SECUREWORKS 3.0, purchasers should make it clear to their supplier that they wish to receive the evaluated product. They should then receive the correct software and documentation to allow them to configure the product in accordance with the evaluated configuration.

Oullim has a stringent set of procedures to ensure that the integrity of the TOE is maintained throughout the delivery process. A check is made of the TOE to ensure that it has been correctly published before securely sealing it in a box with a Proof of Licence Certificate (PLC) and delivered to the purchaser. An Electronic Proof of Licence Certificate (EPLC) is sent separately to the purchaser.

To ensure that the TOE is genuine, the purchaser must check the integrity of the security tape and that the details of the PLC match the EPLC. After the purchaser confirms the delivery, the TOE is registered electronically. An authorised Security Engineer will then assist in the to installation of the product.

Chapter 8 Results of the Evaluation

Evaluation Procedures

The evaluation of SECUREWORKS 3.0 was conducted using the Common Criteria for Information Technology Security Evaluation (Refs [5] to [8]), under the procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [1] to [4]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [9]) were also upheld during the evaluation and certification of this product.

Certification Result

After due consideration of the Evaluation Technical Report (Ref [11]) produced by the evaluators and the conduct of the evaluation as witnessed by the certifiers, the Australasian Certification Authority has determined that SECUREWORKS 3.0 upholds the claims made in the Security Target (Ref [10]) and has met the requirements of:

- the U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999;
- the U.S. Department of Defense Application-Level Firewall Protection Profile for Basic Robustness Environments, Version 1.0, June 22, 2000; and
- the Common Criteria EAL3 assurance level.

Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability that exploitable vulnerabilities remain undiscovered.

Common Criteria EAL3

EAL3 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE to understand the security behaviour.

The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis and evidence of a developer search for vulnerabilities.

EAL3 also provides assurance through the use of development environment controls, TOE configuration management, and evidence of secure delivery procedures.

A detailed explanation of the assurance requirements for EAL3 can be found in the Common Criteria, Part 3 (Ref [7]).

General Observations

The certifiers would like to acknowledge the invaluable assistance provided by LogicaCMG and Oullim's staff during the evaluation. The successful completion of this evaluation was made possible by their cooperation, technical assistance and attention to issues raised during the process.

Chapter 9 Recommendations

The following recommendations include information highlighted by the evaluators during their analysis of the developer's deliverables, during the conduct of the evaluation, and during the additional activities performed by the certifiers.

Scope of the Certificate

The certificate applies only to SECUREWORKS 3.0 software on those hardware platforms identified in Chapter 7: Evaluated Configuration of this report. This certificate is only valid when SECUREWORKS 3.0 is installed and configured in its evaluated configuration as described in Chapter 7 and in accordance with the SECUREWORKS 3.0 Evaluated Configuration Installation Guide (Ref [12]) and the SECUREWORKS 3.0 Installation Guide (Ref [13]) documents.

SECUREWORKS 3.0 should only be used in accordance with the intended environment described in Chapter 3: Intended Environment for the TOE and Chapter 3 of the Security Target (Ref [10]).

Installation and Configuration Guide

Potential purchasers of the TOE are strongly recommended to review and follow all relevant installation and configuration guidance provided by Oullim for SECUREWORKS 3.0. Additionally, purchasers should ensure that their end-users follow guidance provided in both the SECUREWORKS 3.0 User Guide (Ref [15]) and that Authorised Administrators follow procedures described in the SECUREWORKS 3.0 Operation Guide (Ref [14]), the SECUREWORKS 3.0 Installation Guide (Ref [13]) and the SECUREWORKS 3.0 Evaluated Configuration Installation Guide (Ref [12]).

Cryptography

The evaluation of the cryptographic functions of SECUREWORKS 3.0 is beyond the scope of the Common Criteria evaluation, and has been undertaken as a separate process by the Defence Signals Directorate, the national cryptographic authority for Australia. The cryptographic functions of SECUREWORKS 3.0 have been found to be suitable for Australian Government use.

Australian and New Zealand Government users wishing to implement the TOE should take the following recommendations into account when planning their operational environment:

- **Message digesting/hashing:** SECUREWORKS 3.0 supports both SHA-1 and MD5 for hashing functions. MD-5 is used for the One-Time Password authentication mechanism of the TOE and the SHA-1 for file integrity checking. Both these algorithms are considered appropriate for Australian Government use.

Passwords

Potential purchasers should be aware that the TOE provides for authentication of End Users and Authorised Administrators through password based mechanisms. While the TOE provides functionality for the selection of good quality passwords, potential purchasers should ensure that appropriate policies and procedures are in place for the appropriate handling of TOE passwords within the organisation.

Further, potential purchasers considering implementation of proxies requiring password-based authentication should give consideration to the operational threat environment relating to the TOE, and their requirements for protection of passwords in transit between the End User and the TOE.

Employment within Australian Government Networks

Australian Government consumers should refer to Australian Communications-Electronic Security Instruction (ACSI) 33 when considering using this product for separating networks of different classification to ensure that the assurance level is appropriate for the intended application.

NTP Timesource

The TOE relies upon synchronisation with an effective NTP time source for the generation of an audit trail and implementation of policy rules that are time dependent (such as restriction on access based on time of day). Consumers should ensure that the NTP time source used by the TOE is appropriately protected to ensure that a reliable NTP time source is available to the TOE at all times.

Appendix A Security Target Information

A brief summary of the Security Target (Ref [10]) is given below. Potential purchasers should obtain a copy of the full Security Target to ensure that the security enforcing functions meet the requirements of their security policy. A copy of the Security Target can be downloaded from www.dsd.gov.au or obtained directly from Oullim.

Security Objectives for the TOE

SECUREWORKS 3.0 upholds the following summarised IT Security Objectives:

- The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.

- The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.

- The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, disallowing passage of non-conformant protocols and ensuring that residual information from a previous information flow is not transmitted in any way.

- Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.

- The TOE must protect itself against attempts by unauthorised users to bypass, deactivate, or tamper with TOE security functions.

- The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.

- The TOE must provide user accountability for information flows through the TOE and for authorised administrator use of security functions related to audit.

- The TOE must provide functionality that enables an authorised administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

- The TOE must provide the means for an authorised administrator to control and limit access to TOE security functions by an authorised external IT entity.

- The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities.

- The TOE must ensure that an Authorised Administrator can prevent users on the external network determining the IP address of the users on the internal network.

- The TOE must provide detecting violations and alerting potential violations as configured by an Authorised Administrator.

Security Objectives for the Environment

SECUREWORKS 3.0 has the following summarised IT Security Objectives for the environment:

- The TOE is physically secure.

- The threat of malicious attacks aimed at discovering vulnerabilities is considered low.

- The TOE does not host public data.

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

- Information cannot flow among the internal and external networks unless it passes through the TOE.

- The TOE must be delivered, installed, administered and operated in a manner that maintains security.

- Authorised Administrators are trained as to establishment and maintenance of security policy rules and practices.

- TOE only executes security relevant applications and only stores data required for its secure operation. The operating system upon which the TOE executes has been hardened to restrict general-purpose computing capabilities and storage.

- Human users (End Users) within the physically secure boundary protecting the TOE may only access the TOE directly via its console.

- Human users (Administrators) cannot access the TOE remotely from the internal or external networks.

- Only Authorised Administrators may have an account on the TOE host system.

Threats

SECUREWORKS 3.0 addresses the following threats:

- An unauthorised person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

- An unauthorised person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.

- An unauthorised person may use valid identification and authentication data obtained to access functions provided by the TOE.

- An unauthorized person on an external network may attempt to bypass the information flow control policy by disguising authentication data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on an internal network.

- An unauthorised person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.

- Because of a flaw in the TOE functioning, an unauthorised person may gather residual information from a previous information flow or internal TOE data by monitoring the padding information flows from the TOE.

- Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.

- An unauthorised person may read, modify, or destroy security critical TOE configuration data.

- An unauthorised person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.

- The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

- With knowledge of the real IP addresses of external IT entities on the internal network, an unauthorised person may determine enough information about the internal network to affect the internal network in an undesirable observation.

- A threat agent may cause auditable events to go undetected.

SECUREWORKS 3.0 environment addressed the following threats:

- The TOE may be inadvertently configured, used, and administered in an insecure manner by a human user.

Summary of the TOE Security Functional Requirements

The SECUREWORKS 3.0 SFRs are given below. Full description of these SFRs can be found in Section 5.1 of the Security Target (Ref [10]).

- Class FAU: Audit
  - FAU_ARP.1: Security alarms
  - FAU_GEN.1: Audit data generation
  - FAU_GEN.2: User identity association
  - 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.4: Prevention of audit data loss
- Class FCS: Cryptographic support
  - FCS_COP.1: Cryptographic operation
- Class FDP: User data protection
  - FDP_IFC.1: Subset information flow control
  - FDP_IFF.1: Simple security attributes
  - FDP_RIP.1: Subset residual information protection
- Class FIA: Identification and Authentication
  - FIA_AFL.1: Authentication failure handling
  - FIA_ATD.1: User attribute definition
  - FIA_UAU.1: Timing of authentication
  - FIA_UAU.4: Single-use authentication mechanisms
  - FIA_UAU.5: Multiple authentication mechanisms
  - FIA_UID.2: User identification before any action
- Class FMT: Security Management

  - 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_MTD.2: Management limits on TSF data
  - FMT_SMF.1: Specification of management functions
  - FMT_SMR.1: Security management roles

- Class FPR: Privacy
  - FPR_PSE.1: Pseudonymity
- Class FPT: Protection of the TSF
  - FPT_AMT.1: Abstract machine testing
  - FPT_RVM.1: Non-bypassibility of the TSP
  - FPT_SEP.1: TSF domain separation
  - FPT_STM.1: Reliable time stamps
  - FPT_TST.1: TSF testing

Security Requirements for the IT Environment

None included.

Security Requirements for the Non-IT Environment

None included.

Appendix B Acronyms

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OULLIM	Oullim Information Technology Inc
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

Appendix C References

[1] AISEP Publication No.1- Description of the AISEP
AP 1, Version 2.0, February 2001
Defence Signals Directorate

[2] AISEP Publication No.2 - The Licensing of the AISEFs
AP 2, Version 2.1, February 2001
Defence Signals Directorate

[3] Manual of Computer Security Evaluation Part I - Evaluation Procedures
EM 4, Issue 1.0, April 1995
Defence Signals Directorate
(EVALUATION-IN-CONFIDENCE)

[4] Manual of Computer Security Evaluations Part II - Evaluation Tools and Techniques
EM 5, Issue 1.0, April 1995
Defence Signals Directorate
(EVALUATION-IN-CONFIDENCE)

[5] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 2.1, August 1999, CCIMB-99-031, Incorporated with interpretations as of 2002-02-28

[6] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements (CC), Version 2.1, August 1999, CCIMB-99-032, Incorporated with interpretations as of 2002-02-28

[7] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (CC), Version 2.1, August 1999, CCIMB-99-033, Incorporated with interpretations as of 2002-02-28

[8] Common Methodology for Information Technology Security Evaluation (CEM), Version 1.0, August 1999, CEM-99/045, Incorporated with interpretations as of 2002-02-28

[9] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000

[10] SECUREWORKS 3.0 Security Target
Document Version 1.41,
September 2003
Oullim Information Technology Inc.

[11] SECUREWORKS 3.0 Evaluation Technical Report (ETR)
Version 1.1, September 2003
LogicaCMG
(EVALUATION-IN-CONFIDENCE)

[12] SECUREWORKS 3.0 Evaluated Configuration Installation Guide
Oullim Information Technology Inc.

[13] SECUREWORKS 3.0 Installation Guide
Version 1.20
Oullim Information Technology Inc.

[14] SECUREWORKS 3.0 Operation Guide
Version 1.18
Oullim Information Technology Inc.

[15] SECUREWORKS 3.0 User Guide
Version 1.12
Oullim Information Technology Inc.