AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAM

Certification Report

Certificate Number: 2003/27

The Australian Software Company

Destroy 2.01 and Destroy Lite 2.01

Issue 1.0
August 2003

Issued by:

Defence Signals Directorate - Australasian Certification Authority

EXECUTIVE SUMMARY

This report describes the findings of the evaluation of Destroy 2.01 and Destroy Lite 2.01, developed by The Australian Software Company (TASC), to the Common Criteria (CC) Evaluation Assurance Level EAL2+. It concludes that these products have met the target Assurance Level of CC EAL2+, and includes recommendations by the Australasian Certification Authority (ACA) that are specific to the secure use of the Destroy products. The evaluation was performed by LogicaCMG and was completed in July 2003.

Destroy 2.01 and Destroy Lite 2.01 are products which securely sanitise PC hard disks. The products completely overwrite PC hard disks with hexadecimal values 00 and FF. This process is repeated three times for Destroy 2.01 (and once for Destroy Lite 2.01) and then a final write process overwrites the hard disk(s) with random ASCII characters.

The Destroy products (Destroy 2.01 and Destroy Lite 2.01) have been found to uphold the claims made in the Security Target (Ref [12]), and potential customers are urged to consult this document before planning to implement Destroy 2.01 or Destroy Lite 2.01. In particular, the Destroy products have been found to provide the claimed security functionality of user data protection, self protection, audit, and cryptographic support, when configured according to the evaluated configuration.

Ultimately, it is the responsibility of the user to ensure that Destroy 2.01 or Destroy Lite 2.01 meets their requirements. For this reason, it is ***strongly*** recommended that a prospective user of the product obtain a copy of the Security Target (Ref [12]) from the product vendor, and read this Certification Report thoroughly prior to deciding whether to purchase the product.

TABLE OF CONTENTS

Chapter 1 Identification

Intended Audience

This report states the outcome of the IT security evaluation of the TASC products, Destroy 2.01 and Destroy Lite 2.01. It is intended to assist potential customers when judging the suitability of the Destroy products for their particular requirements, and to provide advice to administrators to ensure that the product is used in a secure manner.

This report should be read in conjunction with the Security Target for Destroy 2.01 and Destroy Lite 2.01 (Ref [12]), 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 obtained from TASC.

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 Summary

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Destroy and Destroy Lite
Software Version	Version 2.01
Security Target	Destroy 2.01 and Destroy Lite 2.01 Security Target, Version 1.18, July 2003
Protection Profile	The Security Target does not claim conformance to any PPs
Evaluation Level	CC EAL2+ (augmented with ADV_SPM.1)
Evaluation Technical Report	Evaluation Technical Report for Destroy 2.01 and Destroy Lite 2.01, Issue 1.1, July 2003.
Conformance Result	CC Part 2 Conformant CC Part 3 Augmented
Version of CC	Version 2.1, August 1999
Version of CEM	CEM –99/045, Version 1.0, August 1999
Sponsor	The Australian Software Company
Developer	The Australian Software Company
Evaluation Facility	LogicaCMG
Certifiers	Katrina Johnson, Lachlan Turner, Robert Lee

Description of the TOE

The Target of Evaluation (TOE) consists of two hard disk sanitisation products:

- Destroy 2.01
- Destroy Lite 2.01

The primary role of the TOE (either Destroy 2.01 or Destroy Lite 2.01) is to securely sanitise PC hard disks. The Destroy 2.01 product provides a higher level of confidence in the removal of residual data than Destroy Lite 2.01, due to the more extensive sanitisation process used.

The Destroy products completely overwrite hard disks with the hexadecimal value 00 and the hexadecimal value FF. This process is repeated three times for Destroy 2.01(and only once for Destroy Lite 2.01) and then a final write process overwrites a hard disk with random ASCII characters. The program verifies each known value write process by reading each sector from the hard disk to ensure data has been overwritten. The final random write process is not verified.

Any errors in attempting to read or write to a sector will be reported. At the completion of the disk sanitisation, the Destroy Operator is presented with a summary of the process including notification of any errors and a statement of the overall outcome (success or failure) of the process.

The Destroy products do not write to the floppy disk drive, or to any other types of storage media including tape drives, CD-ROM drives or Zip drives. The programs are executed from write protected bootable floppy disk or CD-ROM.

A Microsoft Windows based utility (Windows 95 or higher, or Windows NT) is a component of both the Destroy 2.01 and Destroy Lite 2.01 products. This utility is termed the Destroy Validation Check (DVC); it provides the ability to conduct integrity checks of the Destroy and Destroy Lite programs to ensure that the programs have not been changed prior to use. The DVC utility uses MD5 hashing to perform the integrity check.

Chapter 2 Security Policy

This section outlines the security policies or rules that the TOE must enforce, or comply with, for correct operation.

Organisational Security Policy

The TOE is designed to be operated in conjunction with the following Organisational Security Policies (OSPs) which must be defined by the owners of the TOE.

The OSP ***P.Disposal*** specifies that the organisation using the TOE must:

- Define an appropriate policy for the identification, disposal and sanitisation of hard disks.
- If the organisation is within the Australian government then the policy should be consistent with the guidelines in ACSI 33 (Ref [1]).

The OSP ***P.Integrity_check*** specifies that the organisation using the TOE must define an appropriate policy stating how often and under what circumstances the integrity of the TOE is to be checked.

TOE Security Policies

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 [12]) does not contain any explicit security policy statements, however, the TOE implements a number of implied TSPs, drawn from the collection of security functional requirements. The TSPs are summarised as follows:

- **Report:** The TOE must notify users of the success or failure of the sanitisation process. Any failure of the TOE functions will be reported to the user to inform the user of the security state of the hard disk.
- **User data protection:** The TOE employs mechanisms to ensure that once a resource (defined as a hard disk) has been de-allocated, any previous information content is made unavailable. Failure of any aspect of the sanitisation process will result in recovery to a secure state (either completing the sanitisation or informing the user of the failure).
- **Protection of the TOE:** The TOE provides a means of detecting loss of integrity that may affect the secure operation of the TOE, and self-testing of the TOE Security Functions.

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 Destroy 2.01 and Destroy Lite 2.01 products took into account the following assumptions about the secure usage of the TOE:

- The Destroy User will follow all policies and procedures defined in the Destroy documentation to ensure the secure usage of Destroy.
- Destroy Users are assumed to be non-hostile and are trusted to perform their duties in a competent manner.
- Destroy will be used to prevent unauthorised access to stored data and potential attackers are assumed to have a medium level of expertise and resources and a medium level of motivation.
- It is assumed that while the Destroy program is in operation, no other software will be active.
- It is assumed that while the Destroy program is in operation, no network connectivity is active for the computer containing the target hard disk(s).
- The Destroy program will be run from a write-protected, bootable device such as a floppy disk.
- The BIOS is configured to know that all hard disks are installed. For IDE hard disks that support the Host Protected Area (HPA) feature the HPA has been reset to the manufacturer's specification or has been removed.

Clarification of Scope

The scope of the evaluation is limited to those claims made in the Security Target (Ref [12]). 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 following security functionality was included in the scope of evaluation:

- Sanitisation functions provided by Destroy 2.01 and Destroy Lite 2.01.
- Reporting functions provided by Destroy 2.01 and Destroy Lite 2.01.
- Integrity checking functions performed by Destroy Validation Check and Destroy Lite Validation Check

Chapter 4 Architectural Information

Destroy 2.01 and Destroy Lite 2.01 each contain the following subsystems:

- **INT 13:** The INT 13 subsystem provides a low-level interface between Destroy and the physical hard disk.
- **BIOS Query Disk Details:** This subsystem works with the INT 13 subsystem to determine the number of hard disks and their actual physical capacity.
- **Write and Verify:** This subsystem interfaces with the INT 13 subsystem, writing to each hard disk and then reading and verifying the information written to each hard disk.
- **User Interface:** This subsystem provides the mechanism for the reporting to the screen information about Destroy such as the BIOS Query disk details, the ongoing progress of the Destroy process and the completion report at the end of the Destroy process. It also provides a mechanism to accept keyboard input to confirm the start of the Destroy process when required.

The Destroy Validation Check program contains the following subsystems:

- **User Interface:** This subsystem allows the user to choose the location of the Destroy executable and then check the located Destroy program. The user interface displays a message indicating whether the key matches an inbuilt Destroy hash key and also displays the calculated hash to the user.
- **File Location:** This subsystem uses a standard Microsoft Windows Application Programming Interface to display a list of current drives available on the computer.
- **MD5 Hash:** This subsystem performs a hash of the Destroy executable located by the User Interface subsystem.

Chapter 5 Documentation

It is important that Destroy 2.01 and Destroy Lite 2.01 are used in accordance with the supplied guidance documentation in order to ensure the secure usage of the TOE. The following is a list of guidance documentation provided by the developer with the product:

- Operations Guide for Destroy Version 2.01 & Destroy Lite Version 2.01 (Ref [13])
  (Ships with Destroy 2.01), or

- Operations Guide for Destroy Lite Version 2.01 (Ref [14])
  (Ships with Destroy Lite 2.01).

The Operations Guide provides the Destroy operator with guidance and information regarding the correct operation of the TOE. It contains a description of all the functions and interfaces available to the administrator of the TOE as well as all the security requirements for the IT environment that are relevant to the administrator.

There are no components that are available to non-administrative users, therefore no additional user-level guidance documentation is provided.

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.
- **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, 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. The evaluators then performed a sample of the developer tests in order to verify that the test results matched those recorded by the developers. In addition, the evaluators drew on this evidence to develop a set of independent tests, expanding on the testing done by the developers.

The functions tested covered the full range of Security Functional Requirements identified in the Security Target (Ref [12]), with the exception of those that rely on cryptographic operations. Whilst the tests devised did ensure that the cryptography was implemented, testing of the actual cryptographic processes is 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.

Penetration Testing

The developers performed a vulnerability analysis of the Destroy products, 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 TASC sources. A number of potential vulnerabilities relevant to the product type were identified and in each case the developers were able to show that the vulnerability was not exploitable in the intended environment.

Based on the information given in the developer's vulnerability analysis, the evaluators were able to devise a suitable penetration test plan for the TOE. In addition, the evaluators performed an independent vulnerability analysis in order to identify any possible vulnerabilities that had not been addressed by the developers. The evaluators found the developer's analysis to be comprehensive, and did not identify any further vulnerabilities.

Upon completion of the penetration testing activity, the evaluators concluded that the TOE, operating in its intended environment, did not display any susceptibility to the identified vulnerabilities

Chapter 7 Evaluated Configuration

Software

The Software elements of the TOE are as follows:

- Destroy 2.01 and Destroy Lite 2.01
- Destroy Validation Check 2.01 and Destroy Lite Validation Check 2.01

Hardware

Destroy 2.01 and Destroy Lite 2.01 require the following hardware:

- An IBM-compatible PC containing the hard disk(s) for sanitisation and capable of running a DOS 7 bootable disk.
- The PC must contain a drive suitable for the supplied media type.

The DVC Integrity checking program is installed on a platform that meets the minimum requirements of:

- IBM-compatible PC running Windows 95 or higher, or, NT 4.0 or higher; and equipped with a drive suitable for the media containing the Destroy or Destroy Lite executable.

Procedures for Determining the Evaluated Version of the TOE

When placing an order for TASC Destroy or Destroy Lite, 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.

The Destroy Operator should ensure that the following information is displayed once the Destroy program starts up:

- Destroy Version 2.01 (or Destroy Lite Version 2.01)
  Copyright (c) 1999-2002 The Australian Software Company Pty Limited
  All rights reserved

To identify the evaluated version of the DVC integrity checker, users should use the [File -> Help -> About] menu option to ensure that they are running either:

- Destroy Validation Check 2.01 (to check Destroy 2.01), or
- Destroy Lite Validation Check 2.01 (to check Destroy Lite 2.01).

Chapter 8 Results of the Evaluation

Evaluation Procedures

The evaluation of the Destroy products 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 [2],[3],[10],[11]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [4]) were also upheld during the evaluation and certification of this product.

Certification Result

The Australasian Certification Authority has determined that Destroy 2.01 and Destroy Lite 2.01 uphold the claims made in the Security Target (Ref [12]) and have met the requirements of the Common Criteria EAL 2 Assurance Level augmented with the ADV_SPM.1 assurance component (EAL2+).

Common Criteria EAL2

EAL2 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 the functional specification, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

EAL2 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.

ADV_SPM.1 Augmentation (+)

Augmentation is a term used in the Common Criteria to describe the addition of ‘assurance components’ to a particular EAL that are not included in the defined EAL packages (each made up of multiple assurance components). Augmentation is denoted by a ‘+’ symbol appended after the EAL (eg. EAL2+).

The ADV_SPM.1 (Informal TOE security policy model) assurance component requires the developer to supply an Informal TOE security policy model that describes the rules and characteristics of all TOE Security Policies that can be modelled.

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

Chapter 9 Recommendations

The following recommendations include information highlighted by the evaluators during the conduct of the evaluation, and during the additional activities performed by the certifiers.

Host Protected Area

The individual responsible for hard disk sanitisation in an organisation should be aware of the possible issues relating to the Host Protected Area of a hard disk.

The Host Protected Area (HPA) is a feature of IDE hard disks that conform to the ATA-4 hard disk standard which is the ANSI standard that details the communication of a hard disk with the computer. The HPA is a reserved area for data storage outside the normal operating system file system and is both read and write protected.

The HPA could potentially be used to store data that would otherwise be erased in the sanitisation process. It is for this reason that DSD strongly recommends that the following procedures be followed in operating the TOE:

- Identify if the disk to be sanitised supports the Host Protected Area feature (IDE ATA-4 and above hard disks).
- Unless the HPA has been utilised by the organisation in a controlled and deliberate manner, the HPA should be reset giving consideration to the possibility that resetting and erasing the contents of the HPA may have an adverse affect on the hard disk. Contact the hard disk manufacturer for further details.

Note: A decision to not reset and erase the HPA should be based on a threat and risk assessment.

Media Disposal Policy

Organisations using this TOE should develop a policy for the identification, sanitisation, declassification and disposal of hard disks. Organisations dealing with Commonwealth data should refer to ACSI 33 (Ref [1]) for further information.

Integrity Check Policy

Organisations using this TOE should note that it has the ability to check the integrity of the executables, however, this checking is not performed automatically. Therefore organisations should develop a policy for the use of this feature and in particular, how often and/or under what circumstances it will be used.

Appendix A Security Target Information

A brief summary of the Security Target (Ref [12]) is given below. Potential purchasers should attempt to obtain a copy of the full Security Target to ensure that the security enforcing functions meet the requirements of their security policy.

Security Objectives for the TOE

Destroy 2.01 and Destroy Lite 2.01 has the following IT Security Objectives:

- The TOE shall prevent unauthorised access to data stored on a hard disk that is to be redeployed, transferred out of the organisation's control, or discarded.
- The TOE shall provide a means of detecting loss of integrity affecting operation.
- The TOE shall provide a means of notifying authorised users of the success and/or failure to sanitise a hard disk that is to be redeployed, transferred out of the organisation's control, or discarded.

Security Objectives for the Environment

Destroy 2.01 and Destroy Lite 2.01 has the following IT Security Objectives for the environment:

- Those responsible for the TOE shall ensure that the TOE is installed, managed and operated in a manner consistent with defined organisational policies and the TOE documentation. In addition, those responsible for the security of the organisation shall ensure that all appropriate background checks, psychological assessments, and security clearances, as required, are conducted for all Destroy Operators.
- Those responsible for the TOE shall ensure that access to the media containing the TOE executable is controlled in a manner consistent with defined organisational policies.
- Those responsible for the TOE shall ensure that the BIOS of the machine containing the hard disks to be sanitised has been correctly configured to know that all hard disks are installed. Those responsible for the TOE shall also ensure that the Host Protected Area (HPA) has been reset to the manufacturer's specification or removed.

Threats

The following threats are addressed by the TOE:

- An unauthorised person attempts to access sensitive data stored on a hard disk that has been redeployed, transferred out of the organisation's control, or discarded.

- An unauthorised person attempts to recover sensitive data remaining after the data has been deleted from a hard disk that has been redeployed, transferred out of the organisation's control, or discarded.

- An unauthorised person attempts to recover sensitive data remaining after formatting of a hard disk that has been redeployed, transferred out of the organisation's control, or discarded.

- An unauthorised person attempts to recover sensitive data from tracks or sectors of a hard disk that are outside of the defined configuration parameters for that hard disk and that has been redeployed, transferred out of the organisation's control, or discarded.

- An unauthorised person attempts to modify the software comprising the TOE to circumvent or disable its security features.

- An authorised user of the TOE executes the software but is unaware of a failure to completely sanitise a hard disk.

The TOE Operating Environment is not required to explicitly address any threats.

Summary of the TOE Security Functional Requirements

The TOE SFRs are outlined below. Full description of these SFRs can be found in Chapter 5 of the Security Target (Ref [12]).

- **Class FAU: Audit**
  - FAU_ARP.1 Security alarms
  - FAU_GEN.1 Audit data generation
  - FAU_SAA.1 Potential violation analysis
- **Class FCS: Cryptographic Support**
  - FCS_COP.1 Cryptographic Operation
- **Class FDP: User Data Protection**
  - FDP_RIP.2 Full residual information protection
- **Class FTP: Protection of the TSF**
  - FPT_AMT.1 Abstract machine testing
  - FPT_PHP.1 Passive detection of physical attack
  - FPT_RCV.4 Function recovery
  - FPT_TST.1 TSF testing

Security Requirements for the IT Environment

There are no security requirements for the IT environment.

Security Requirements for the Non-IT Environment

The following is a list of requirements for the Non-IT environment:

- **Training of Destroy Users** - The TOE environment shall ensure that operators of the TOE are aware of, and if necessary trained, to use the TOE correctly, securely, and in accordance with defined policies.

- **Limiting Physical Access** - The TOE environment shall ensure that physical access to the media containing the TOE software is limited to only those people explicitly authorised access.

- **Verification of BIOS configuration** - The TOE environment shall ensure that operators of the TOE are aware of the need to ensure that the BIOS of the machine containing the hard disks to be sanitised has been correctly configured to know that all hard disks have been installed and procedures are in place to ensure that hard disk(s) with configured Host Protected Area(s) (HPA) have the HPA restored to the manufacturer's specification or the HPA is cleared.

Appendix B Glossary

ACSI 33	Australian Communications - Electronic Security Instruction 33
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ASCII	American Standard Code for Information Interchange
ATA	Advanced Technology Attachment
BIOS	Basic Input/Output System
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HPA	Host Protected Area
IDE	Integrated Drive Electronics
PP	Protection Profile
SFR	Security Functional Requirements
SOF	Strength of Function
ST	Security Target
TASC	The Australian Software Company
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

Appendix C References

[1] Australian Communications - Electronic Security Instruction 33
Defence Signals Directorate
http://www.dsd.gov.au

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

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

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

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model (CC)
CCIMB-99-031, Version 2.1, August 1999

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements (CC)
CCIMB-99-032, Version 2.1, August 1999

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements (CC)
CCIMB-99-033, Version 2.1, August 1999

[8] Common Methodology for Information Technology Security Evaluation (CEM)
CEM-99/045, Version 1.0, August 1999

[9] Destroy 2.01 and Destroy Lite 2.01 Evaluation Technical Report (ETR)
Issue 1.1, July 2003
LogicaCMG
(EVALUATION-IN-CONFIDENCE)

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

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

[12] TASC Destroy 2.01 and Destroy Lite 2.01 Security Target
Version 1.18, July 2003
The Australian Software Company

[13] Operations Guide for Destroy Version 2.01 and Destroy Lite Version 2.01
Document version 1.8, November 2002
The Australian Software Company

[14] Operations Guide for Destroy Lite Version 2.01
Document version 1.7, November 2002
The Australian Software Company