SECURITY TARGET

FOR

ENTRUST/TRUEDELETE™

(EAL 1)

Prepared for:

Communications Security Establishment

Prepared by:

CGI Information Systems and Management Consultants Inc.

31 March 1999

Author: CGI Senior Consultant, Mr. Mike Riley
Valid: 31 March 1999
CGI File number: CGI-ITSETF-99-01-ST-04
CB File number: 1999-CGI-02
Issue Number: 1.3
Page Count: 16

Document Change Log

ST Section	Change	Reason for Change	Date Changed
Sec 5.1	Conformance to FDP_RIP	OR CGI-1999-02-01	28 Feb 1999
Title Page	CB Reference Number and Version Number	OR CGI-1999-02-02	16 Feb 1999
Sec 5.1	Clarify description of “file clearing”	OR CGI-1999-02-02	16 Feb 1999
Sec 5.3	Amend security requirements for the IT environment	OR CGI-1999-02-03	20 Feb 1999
Sec 6.1	Clarify TOE Summary Specification	OR CGI-1999-02-04	20 Feb 1999
Sec 6.1	TSS for the assurance requirements	OR CGI-1999-02-05	20 Feb 1999
Sec 6.1	Description of TOE Security Functions	OR CGI-1999-02-11	28 Feb 1999
Sec 1.1	Include Windows ’95 in ST Identification	ST Evaluation	7 March 1999
Sec 1.2	Clarify file clearing (overwrite)	ST Evaluation	7 March 1999
Sec 2	Clarify file clearing (overwrite)	ST Evaluation	7 March 1999
Sec 3.1	Expand Assumptions	ST Evaluation	7 March 1999
Sec 4.2	Trace Back to Threat	ST Evaluation	7 March 1999
Sec 5.1	Clarify file clearing (overwrite)	ST Evaluation	7 March 1999
Sec 6.1	Added to improve	Certifier comments	7 March 1999
Sec 6.2	Re-numbered from 6.1 and revised to clarify file clearing (overwrite)	Addition of 6.1	7 March 1999
Sec 6.3	Re-numbered from 6.2	Addition of 6.1	7 March 1999
Sec 8.2	Added Mapping	ST Evaluation	7 March 1999
Sec 8.4	Added Mapping	ST Evaluation	7 March 1999

ST Section	Change	Reason for Change	Date Changed
Title Page	Revised version number and Date	CSE Observation	31 March 1999
Sec 2	Clarified paging and swap concepts	CSE Observation	31 March 1999

TABLE OF CONTENTS

1 INTRODUCTION

1.1 ST Identification

This document is the security target (ST) for the Common Criteria evaluation of Entrust Technologies "Entrust/TrueDelete version 4.0" program, a component of Entrust/ICE version 4.0 and Entrust/Enterprise Desktop Client, used on a PC (desktop, laptop, notebook) running either Windows '95 or Windows NT 4.0.

1.2 ST Overview

Entrust/TrueDelete makes deleted files unrecoverable by meeting U.S. Department of Defense specifications for file clearing (secure overwriting of file contents prior to file deletion). This standard ensures that information stored in files that are deleted (or left behind in Windows SWAP files) cannot be retrieved or viewed using a disk editor.

1.3 CC Conformance

The TOE is Part 2 conformant, meaning that the functional requirements are only based on the relevant functional components of CC Part 2.

2 TOE DESCRIPTION

A term that often arises during discussions of magnetic media sanitization is "data remanence." Data remanence is the residual magnetic or electrical representation of data that has been in some way erased or overwritten. This residual information may allow data to be reconstructed typically using laborious, time-consuming methods. This usually is a concern only to those processing classified information, but can also be a significant concern for unclassified but sensitive information and for potentially embarrassing comments, which can be unknowingly retained in a file after deletion when using some modern software applications. Often, utility overwrite programs contain an option to overwrite the location of the file to ensure that the chance of recovery of the information from data remanence is very remote.

As well, when users delete files from their computers, they do not often realize that instead of deleting the contents of these files, all that they have deleted is the links, or directory entries, to the files. The information that was contained in the file is not removed from the system until other information is saved that overwrites the same area of the computer disk. This typical method of file deletion enables disk editor products to recover information that has supposedly been "deleted".

Entrust/TrueDelete 4.0, a component of both Entrust/Enterprise Desktop Suite 4.0 and Entrust/ICE 4.0 provides secure file clearing, deletion of temporary files and any information that was stored by the operating system in Windows NT paging files or Windows 95 SWAP file. Entrust/TrueDelete makes deleted information unrecoverable by meeting U.S. Department of Defense specifications for file clearing or overwriting of file contents prior to file deletion. This means that Entrust/TrueDelete completely overwrites the contents of the file to ensure that information originally stored in these deleted files cannot be retrieved or viewed using a disk editor.

3 TOE SECURITY ENVIRONMENT

3.1 Assumptions

The following is the assumption relevant to the security environment:

- Physical Assumptions:

  A.LOCATE – The processing platform of the TOE is assumed to be located within controlled access facilities (for classified processing platforms), which would prevent unauthorized persons access to the disk media. Sensitive but unclassified processing platforms are not always in controlled areas, and in order for the threat below to occur, unauthorized person(s) would require access to the platform.

- Personnel Assumptions:

  A.ATTACK - Attackers are assumed to have a moderate level of expertise, resources and motivation.

- Connectivity Assumptions:

  There are no connectivity assumptions.

- Hardware/Software Assumptions:

  There are no hardware or software assumptions.

3.2 Threats

Most users do not realize that performing a typical delete function on a file in Microsoft Windows 95 and Microsoft Windows NT does not necessarily delete the information contained in that file. The delete function simply removes the directory link to that information, leaving the information accessible on the computer (by disk editor tools) until new information is saved overtop of the original disk space. The threat is as follows:

T.ACCESS – An unauthorized user of the TOE may access information or resources without having permission from the person who owns, or is responsible for, the information.

The asset requiring protection is the information that was intended to be deleted, which was presumed to be sensitive (in the worst case). It needs to be protected from recovery by unauthorized persons (i.e., it is a threat related to confidentiality, not integrity or availability). The threat agents are personnel using a disk utility program who may intentionally or inadvertently be able to read information which was intended to be deleted (and therefore not meant for disclosure). They could, either accidentally or out of malicious intent, recover the information and use the information in a manner harmful or embarrassing to the person who attempted to delete it.

4 SECURITY OBJECTIVES

4.1 Security Objectives for the TOE

The following is the security objective for the TOE, which will minimize the threat noted in section 3.2, that an unauthorized user will access the information:

> *O.OVERWRITE* - The TOE must overwrite deleted information, rendering it unrecoverable by disk recovery programs.

4.2 Security Objectives for the Environment

The TOE is used only to make files unrecoverable under a PC's normal operating conditions, not to declassify floppy or hard disks (because there are elaborate, but well known, laboratory procedures which make it possible to recover information from media long after it has been erased, although this represents a very low risk in most instances). Organizational security procedures must be in effect that prevent the loss of the floppy of physical disk media, which would enable the conduct of these laboratory attacks on the sensitive information. Retaining the disk media under positive inventory control and storage until ready for disposal, and the destruction of the media at that time, are recommended. Disks that had at any time been used for the storage of sensitive information must never be released into an uncontrolled environment (i.e., sold or given, while in a usable state, to unauthorized persons/organizations for their intended re-use or disposal). These objectives will minimize the threat, noted in section 3.2, that an unauthorized user will access the information.

5 IT SECURITY REQUIREMENTS

5.1 Security Functional Requirements

In accordance the security requirement *SFR FDP_RIP.2,* Full Residual Information Protection, subset *SFR FDP_RIP.2.1,* the TSF shall ensure that any previous information content of a resource is made unavailable upon the [*refinement*: deallocation of the resource from] all objects.

The TOE must ensure the protection of residual information (or data remanence), by ensuring that information in deleted files and temporary files cannot be retrieved or viewed using disk editor programs. The TOE must “TrueDelete" any file the user chooses and has the necessary privileges for, and will complete the operation with the selection of "deallocation of the resource”. Available documentation states that the TOE meets the US Department of Defense requirements for file clearing by the overwriting procedure defined in NCSC-TG-025.

The CC Part 2 component, which may be used to express the appropriate requirements, is Access Control – Object Reuse - Protection of residual information in files, memory, etc. - FDP_RIP.1-2. The reader is referred to CC Part 2 Annexes for guidance relating to the use of specific CC Part 2 functional components.

5.2 Security Assurance Requirements

The security assurance requirement for the TOE is Evaluated Assurance Level (EAL) 1 (Functionally Tested) as described in the CC Part 3 and detailed in the following table:

Table 1 - Security Assurance Requirements

Component ID	Component Name
ACM_CAP.1	Version numbers
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance

ATE_IND.1	Independent testing - conformance

5.3 Security Requirements for the IT Environment

There are no security requirements for the IT environment.

6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functions

The TOE performs the following security functions in support of the functional requirements:

> Overwrite of the deleted information and temporary files at least once with a preset pattern of characters to meet the standards for file clearing as specified in the NCSC-TG-025 standard. The default character is 0x55.

6.2 Mapping to TOE Security Functional Requirements

The TOE security function maps to the security requirement *SFR FDP_RIP.2*, Full Residual Information Protection. The *SFR FDP_RIP.2.1*, requires that any previous information content of a resource is made unavailable. File clearing to the NCSC-TG-025 standard accomplishes this.

6.3 Assurance Measures

The TOE is packaged and shipped with an administrator's guide as well as with help files that address the CC requirement for secure installation, generation and start-up procedures. Additional assurance information is provided in the following sub-section.

6.4 Mapping of Assurance Measures to EAL Requirements

6.4.1 Measures Used to Meet Component: ACM_CAP.1

The TOE implements ACM_CAP.1 by including a version number on both the product container and the media (CD-ROM) on which it is provided. Additionally, the TOE software has an “about” option which lists both the version and the Build Number (for further granularity)

6.4.2 Measures Used to Meet Component: ADO_IGS.1

The TOE implements ADO_IGS.1, installation, generation, and start-up procedures, by providing installation instructions on the CD-ROM.

6.4.3 Measures Used to Meet Component: ADV_FSP.1

The TOE ADV_FSP.1 Functional Specification requirement was satisfied by the provision of a Functional Specification document by the vendor and the use of publicly posted information on the vendor's WWW site.

6.4.4 Measures Used to Meet Component: ADV_RCR.1

The TOE implements ADV_RCR.1, informal correspondence demonstration, in the functional specification.

6.4.5 Measures Used to Meet Component: AGD_ADM.1

The TOE implements AGD_ADM.1, administrator guidance, through documentation and help files provided on the TOE CD-ROM and through the vendor's WWW site.

6.4.6 Measures Used to Meet Component: AGD_USR.1

The TOE implements AGD_USR.1, user guidance, through documentation and help files provided on the TOE CD-ROM and through the vendor's WWW site.

6.4.7 Measures Used to Meet Component: ATE_IND.1

The TOE implements ATE_IND.1, independent testing – conformance, by the vendor providing the most recent version of the software to an evaluator for testing.

7 PROTECTION PROFILE CLAIMS

7.1 PP Reference

There are no relevant Protection Profiles for a TOE whose objective is to perform secure overwrite.

8 RATIONALE

8.1 Security Objectives Rationale

O.OVERWRITE - The TOE must overwrite deleted information, rendering it unrecoverable by disk recovery programs.

The security objective of overwriting deleted information, rendering it unrecoverable by disk recovery programs, is satisfactory to address the identified threat of an unauthorized user gaining access to the information without the permission of the owner of the information. By overwriting, disk utilities will be unable to reconstruct or recover the deleted data.

8.2 Security Requirements Rationale

OBJECTIVE	SECURITY FUNCTIONAL REQUIREMENT (CC 2)
O.OVERWRITE	SFR FDP_RIP.2 - Full Residual Information Protection

Overwriting is an effective method of clearing data from magnetic media, one that is recognized by many standards organizations, and the US DoD. As the name implies, overwriting utilizes a program to write (a characters, a complementary character, or a combination of both) onto the location of the media where the file to be sanitized is located. The number of times that media is overwritten depends on the level of sensitivity of the information.

For an EAL 1 assurance, it is sufficient to demonstrate that users will have confidence in correct operation of the TOE in accordance with the available documentation, and the threats are not particularly serious. In this threat scenario, the threat is low for PCs processing classified information, as they are in strictly controlled areas, preventing access by unauthorized persons. In the case of PCs processing lower sensitive information, they are usually in moderately controlled environments (even if only to protect against theft), and the benefit of theft of this information is moderate at best, therefore the threat is low to moderate.

8.3 TOE Summary Specification Rationale

There is only one Security Functional Requirement required (as specified above), as all others are irrelevant.

8.4 PP Claims Rationale

There are no PP compliance issues, as there are no relevant PPs for this TOE.