National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

UniShred Pro ® Version 3.3.1

Report Number: CCEVS-VR-02-0030
Dated: 19 December 2002
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team
Richard White
Mitretek Systems Inc.,
Falls Church, VA

Common Criteria Testing Laboratory

Evaluation Team
Cable and Wireless, Inc.
45901 Nokes Boulevard
Sterling, VA 20166

Table of Contents

1 Executive Summary

The evaluation of the Los Altos Technologies UniShred Pro ® Version 3.3.1 was performed by Cable & Wireless CCTL in the United States and was completed on 13 December 2002. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.1 and the Common Methodology for IT Security Evaluation (CEM), Version 1.0.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the UniShred Pro ® product by any agency of the US Government and no warranty of the product is either expressed or implied.

The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The Cable & Wireless evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL1) have been met.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by Cable & Wireless.

1.1 Evaluation Details

Dates of Evaluation: August 22 through December 13, 2002
Evaluated Product: UniShred Pro ® Version 3.3.1
Developer: Los Altos Technologies
CCTL: Cable & Wireless Inc., Sterling VA
Validation Team: Richard White, Mitretek Systems Inc., Falls Church, VA
Evaluation Class: EAL1
PP Conformance: None

1.2 Interpretations

There are no interpretations that apply to this evaluation.

1.3 Threats to Security

The Security Target identified the following threats that the evaluated product addresses:

T.Incomplete_Overwrite: Incomplete Overwrite Operation

An overwrite operation is incompletely performed rendering data still recoverable, and the user performing the overwrite operation has no knowledge of the operation being performed incompletely.

T.Unauthorized_Access: Unauthorized Access to the TOE
An unauthorized individual gains access to the TOE and its resources resulting in the disclosure of the information within the disk media.

2. Identification

2.1 ST and TOE Identification

ST: Los Altos Technologies UniShred Pro ® (EAL1), Version 3.3.1, 19 December 2002.

TOE Identification: UniShred Pro ® Version 3.3.1

CC Identification – *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999, ISO/IEC 15408.

CEM Identification – *Common Evaluation Methodology for Information Technology Security*, Part 1: Introduction and General Model, Version 0.6, January 1997; *Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Version 1.0, August 1999.

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 are 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".
Los Altos UniShred Pro ® provides the capabilities to securely overwrite all existing information residing on either a partition, or entire disk. In addition, the overwriting methods provided conform to various United States Government regulations.
Los Altos UniShred Pro ® also provides capabilities for verifying the successful completion of the overwriting of a partition or disk, as well as, provides reports on the processes. The reports

that are generated, are displayed on-screen, can be archived to a file, and also printed at a later time.
Los Altos UniShred Pro ® operates on the following operating systems:

- Hewlett-Packard's HP/UX 9, 10, and 11
- IBM's AIX 4
- Linux w/ kernel 2.0.x, 2.2.x, and 2.4.x
- SGI's IRIX 6.5.x
- Sun's Solaris 2 and higher

In addition to these defined operating systems, Los Altos UniShred Pro ® also can be operated on any Intel platform PC from a bootable floppy disk, or a bootable CD-ROM, using a supplied, stripped down version of Linux.
Los Altos UniShred Pro ® is a software utility that can be operated from a floppy disk, hard disk, or within a system's internal memory (RAM).

2.2 IT Security Environment

The TOE environment is considered to be secured in that controlled access physically to the TOE is provided. The administrative access to the underlying operating system of the TOE shall be controlled in such a way that secrets used to access UID 0 are not distributed to any individual that is unauthorized for access.

3. Security Policy

3.1 Audit

The audit report management function provides the ability to generate audit reports upon completion of the overwrite and verification functions. The audit report management function also provides the ability to display and store the generated audit reports. For storage options, the Los Altos Technologies UniShred Pro ® Version 3.3.1 can be configured to store audit reports to a hard disk, floppy, or network device. The fifth scenario identified in section 2.3 specifically uses the floppy as an audit report storage option.

The underlying operating system of the Los Altos Technologies UniShred Pro ® Version 3.3.1 provides the capabilities to print the reports using the "lp" command. The underlying operating system also provides the capability to view the reports using a text editor such as *vi*.

When multiple audit reports are generated, they are appended to the same output file. This keeps previous audit data from being overwritten, and allows a user to view or print all audit reports simultaneously from within the same file.

When an overwrite operation is performed, the audit report displays the following information:

a. License number and expiration of license.
b. For the target device, the name, size, vendor name, product number, revision number, serial number, disk type, number of blocks, disk speed, and disk mount status.

c. Overwrite date and time, overwrite pattern, pattern used for each pass and number of passes within the overall pattern, and confirmation of the output report file.
d. Confirmation of each sub-operation being performed for the overall overwrite operation with the time of each sub-operation occurrence, identification of any errors occurred, and confirmation of a complete overwrite of the device.

When a verify operation is performed, the audit report displays the following information:

a. License number and expiration of license.
b. For the target device, the name, size, vendor name, product number, revision number, serial number, disk type, number of blocks, and disk speed.
c. Verification of the pattern performed within the last pass of the full overwrite operation, blocks used, time of the verification operation performed, number of blocks verified, verification of the device being overwritten, and verification of the verify operation being complete.

3.2 Access Control

The access control function enforces access control on the TOE for access to modifying the Los Altos Technologies UniShred Pro ® Version 3.3.1 configuration file, generated audit reports, and executing Los Altos Technologies UniShred Pro ® Version 3.3.1. The access control function is enforced by checking the user identity of the authenticated user to ensure that the user is authenticated as UID 0 or belonging to the administrators group. The access control function is provided by the underlying operating system of Los Altos Technologies UniShred Pro ® Version 3.3.1 and enforces the Los Altos Access Control Policy.

3.3 Identification and Authentication

The identification function provides the capability for a user to authenticate to the TOE. The TOE then checks if the user is authenticated as UID 0 to determine if access to Los Altos Technologies UniShred Pro ® Version 3.3.1 is granted. The identification function is provided by the underlying operating system of Los Altos Technologies UniShred Pro ® Version 3.3.1.

3.4 Overwrite Function

The overwrite function provides the capability to securely overwrite all existing information residing on either a partition or entire disk, using industry known methods for remanence thru the use of a pre-defined set of patterns. A pre-defined pattern provides a variation of overwrite methods with a defined number of times the disk is overwritten in the pre-defined pattern. In addition, the overwrite operation also provides the capability of allowing a user to specify the range of blocks to be overwritten.

The overwrite operation is performed thru the execution of the command, “usp3”, from the command line interface.

3.5 Verification Function

The verification function provides the capability to ensure the successful completion of the overwrite function. The verification function also provides the pattern method performed within the last pass completed in the overwrite function.

Additionally, the verification function provides the capability to read a hard disk.

The verify operation is performed thru the execution of the command, "usp3 --verify", from the command line interface.

4. Assumptions

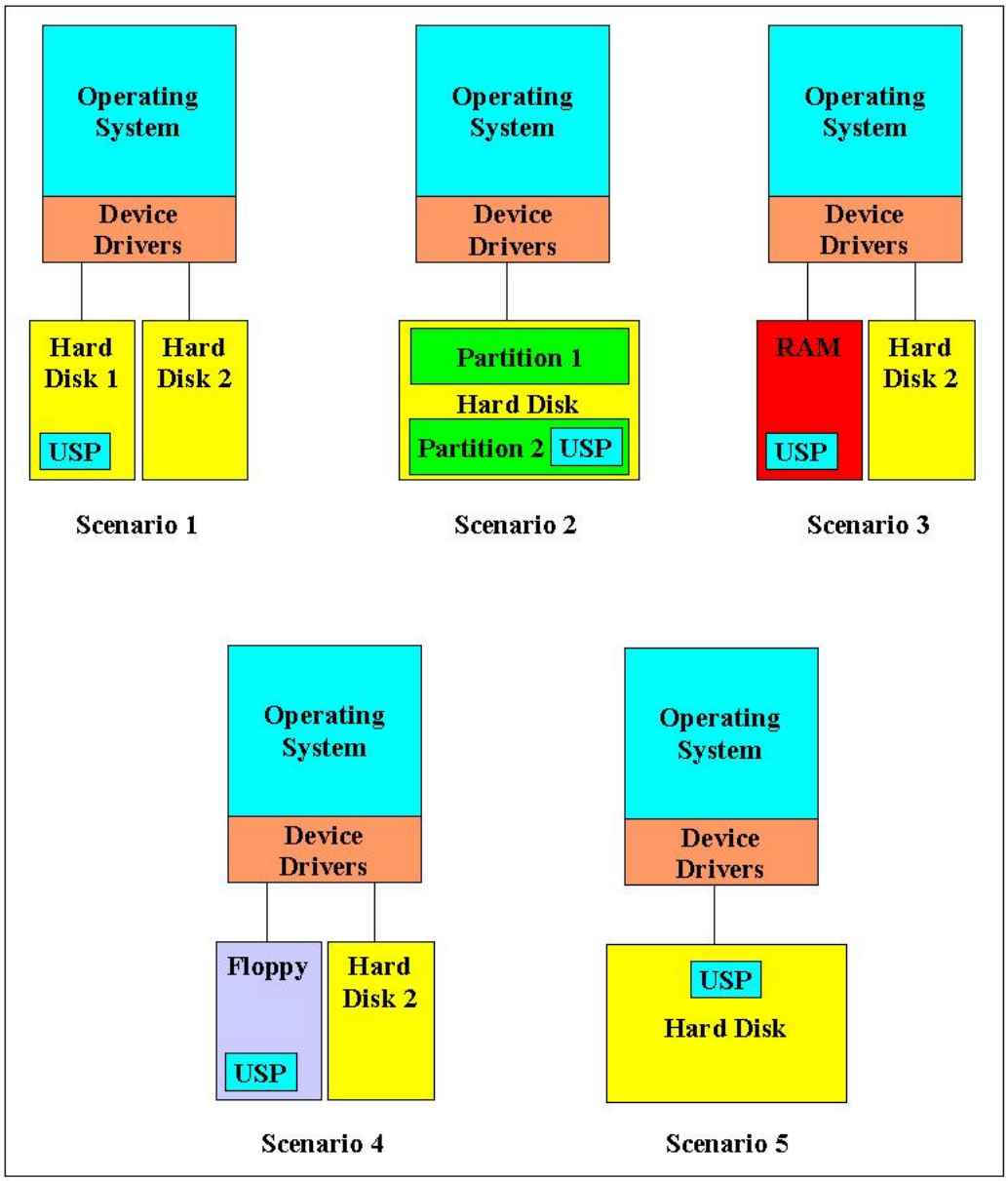
4.1 Personnel Assumptions

A.Admin_Credentials: Disclosure of Administrative Credentials
Administrators (UID 0) of the TOE are assumed not to disclose their authentication credentials to any individual that is not authorized for access to the TOE.

4.2 Physical Assumptions

A.Facility_Access: Controlled Access to TOE Facility
The processing platform in which the TOE resides on is assumed to be located within a facility that provides controlled access, so that unauthorized access to the disk media is prevented.

5. Architectural Information



As shown above, the operating system and Los Altos Technologies UniShred Pro ® Version 3.3.1 are both displayed in a light blue coloration and therefore indicating these two components to be the TOE.

All underlying hardware on which the TOE operates on is not considered to be part of the TOE.

The TOE is not a networked system and executes locally, therefore, a networking interface is not included as a physical TOE or NON-TOE component.

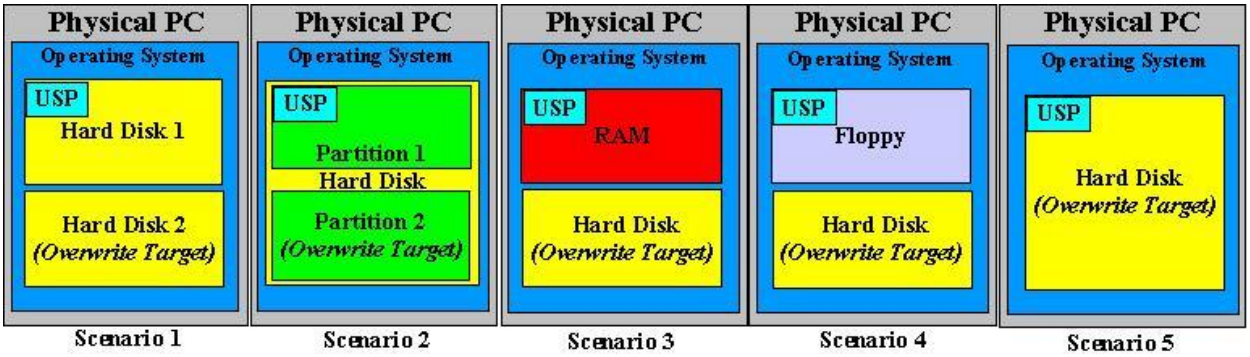
Hardware components not considered part of the TOE, yet at the minimum are required for TOE operation are the following:

- HP HP/UX 9 – 11 Operating Systems
- RAM –24 MB minimum
- Hard Drive Space – 2 MB minimum
- IBM AIX 4.x Operating Systems
- RAM – 32 MB minimum
- Hard Drive Space – 1 MB minimum
- GNU Linux w/ kernel 2.x Operating Systems
- RAM – 32 MB minimum
- Hard Drive Space – 2 MB minimum
- SGI IRIX 6.5.x Operating Systems
- RAM –24 MB minimum
- Hard Drive Space – 2 MB minimum
- SUN Solaris 2.x, 7.x, 8.x, 9.x Operating Systems
- RAM – 24 MB minimum
- Hard Drive Space – 2 MB minimum

Software components considered to be part of the TOE are the following operating systems:

- HP HP/UX 9 – 11 Operating Systems
- IBM AIX 4.x Operating Systems
- GNU Linux w/ kernel 2.x Operating Systems
- SGI IRIX 6.5.x Operating Systems
- SUN Solaris 2.x, 7.x, 8.x, 9.x Operating Systems

Logical Boundaries



The TOE is defined to be the Los Altos Technologies UniShred Pro ® Version 3.3.1 application (USP) and the following operating systems: HP HP/UX 9, HP HP/UX 10, HP HP/UX 11, IBM AIX 4, GNU Linux /w kernel 2.x, SGI IRIX 6.5, SUN Solaris 2, SUN Solaris 7, SUN Solaris 8, and SUN Solaris 9. The identification and access control functionalities are considered the TOE portion of the operating system. Identification provides the capability for users identify themselves to the operating system. Access Control provides the capability for the operating system to control access to operating system resources.

The Physical PC, as shown in the above figure, is not considered part of the TOE. As shown in the above figure, the application, with the defined operating systems, can run in five possible scenarios.

The first scenario provides the ability for USP to overwrite an entire hard disk, while running the application from a separate hard disk.

The second scenario provides the ability for USP to overwrite a partition within a hard disk, while running the application from a separate partition of that same hard disk.

The third scenario provides the ability for USP to overwrite an entire hard disk, while running the application from within the RAM of the residing PC.

The fourth scenario provides the ability for USP to boot from a floppy into a GNU Linux based operating system to provide the same capabilities of overwriting a hard disk. This scenario is only possible on Intel platform machines.

The fifth scenario provides the ability for USP to overwrite the same disk and partition, in which USP resides in. In this case, the audit report would be written to the floppy. However, this scenario is only provided within the Solaris operating systems.

6. Documentation

Purchasers of the Los Altos UniShred Pro ® Version 3.3.1 will receive all OEM instruction and documentation manuals necessary for proper installation, maintenance, and secure use on the specifically requested platform.

7. IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

As this was an EAL 1 evaluation, developer testing was not supplied as part of the documentation.

7.2 Evaluation Team Independent Testing

The Evaluation Team developed independent test sets that covered a range of conditions: some simply verify administrative or user guidance; some exercise boundary conditions that have been troublesome in other products; and some are highly technical flaw hypotheses that seem applicable to Los Altos Technologies UniShred Pro ® Version 3.3.1 platforms. As these scenarios were conducted, the actual tests performed by team members were documented in more detail along with the expected and actual test results. Any associated procedures have also detailed and documented. A total of eleven different test configurations were tested. Each configuration was a single instance of the TOE installed on various platforms. Complete test configuration are contained within section 5 of the UniShred Pro ® Version 3.3.1, Test Report, 12 December 2002.

In addition, the Evaluation Team also tested the installation, generation, and start-up procedures to determine, in accordance with ADO_IGS.1.2E, that those procedures result in a secure configuration.

8. Evaluated Configuration

The evaluated configuration consisted of UniShred Pro ® Version 3.3.1 running on one of the operating systems specified above.

9. Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL1 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The

Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Verdicts were not assigned to assurance classes.

Section 4, Evaluation Results, in the Evaluation Team's ETR, Part 1, states:

The verdicts for each CEM work unit in the ETR sections are each "PASS". Therefore, when configured according to the provided OEM guidance documentation, the UniShred Pro ® (UniShred Pro ® Version 3.3.1) satisfies the Los Altos Technologies, UniShred Pro ® Security Target, Version 1.0b, December 13, 2002.

Section 5, Conclusions and Recommendations, in the Evaluation Team's ETR, Part 1, states:

The TOE was evaluated against the ST and has been found by this evaluation team to be conformant with the ST. The TOE was found to be CC Part 2 Extended and Part 3 Conformant. The overall verdict for this evaluation is a Pass.

10. Validation Comments/Recommendations

The validation team had no recommendations concerning the UniShred Pro ® TOE.

11. Abbreviations

Abbreviations	Long Form
CC	Common Criteria
CEM	Common Evaluation Methodology
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FSP	Functional Specification
I&A	Identification and Authentication
OR	Observation Report
QA	Quality Assurance
SOF	Strength of Function
ST	Security Target (specifically the Security Target for Los Altos Technologies UniShred Pro ® Version 3.3.1)
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSS	TOE Summary Specification
USP	Los Altos Technologies UniShred Pro ® Version 3.3.1

12. Bibliography

The evaluation and validation methodology was drawn from the following:

[CC_PART1] Common Criteria for Information Technology Security Evaluation-Part 1: Introduction and general model, dated August 1999, version 2.1.

[CC_PART2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, dated August 1999, version 2.1.

[CC_PART2A] Common Criteria for Information Technology Security Evaluation Part 2: Annexes, dated August 1999, version 2.1.

[CC_PART3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, dated August 1999, version 2.1.

[CEM_PART 1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[CCEVS_PUB1] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0 May 1999.

[CCEVS_PUB2] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures, Scheme Publication #2, Version 1.5, May 2000.

[CCEVS_PUB3] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Technical Oversight and Validation Procedures, Scheme Publication #3, Version 0.5, February 2001

[CCEVS_PUB 4] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Scheme Publication #4, Version 1, March 20, 2001

[CCEVS_PUB 5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Sponsors of IT Security Evaluations, Scheme Publication #5, Version 1.0, August 2000.