National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Xerox Corporation

Image Overwrite Security for Xerox WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55 Advanced Multifunction System

Report Number: CCEVS-VR-04-0060

Dated: 28 May 2004

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

Aerospace Corporation

Columbia, Maryland

Common Criteria Testing Laboratory

Computer Sciences Corporation

Annapolis Junction, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the evaluation of Xerox Corporation Image Overwrite Security for its copier/printer and Multifunction Systems. It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The evaluation was performed by Computer Sciences Corporation (CSC), and was completed during May 2004. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both written by CSC. The evaluation determined the product to be **Part 3 conformant,** and to meet the requirements of **EAL 2**. The product is not conformant with any published Protection Profiles, but rather is targeted to satisfy the needs for protection of residual information as defined by DoD Standard 5200.28-M. The Security Target contains one explicitly stated security functional requirement (specifying the separation of the Fax function from the network controller); all other security functional requirements are derived from Part 2 of the Common Criteria.

The product family provides copy/print and copy/print/scan/fax capability. The primary security feature is that of the overwriting of temporary image data that is stored on the internal hard drive. The overwrite function is automatically invoked at the completion of each job, and can also be invoked on demand by an authorized administrator. The overwrite function prevents image data from remaining on the hard drive after the completion of any print, network scan, or scan to email function.[1]

[1] Neither copy nor fax processing result in data being stored on the hard drive.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Image Overwrite Security for the WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55 Advanced Multifunction System[2]
Protection Profile	None
Security Target	*Image Overwrite Security for the WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55 Advanced Multifunction System*, Version 1.0, Rev 1.27 dated April 29 2004
Evaluation Technical Report	*Image Overwrite Security for the WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55 Advanced Multifunction System,* Version 1.1 dated April 29, 2004
Conformance Result	Part 3 conformant, EAL 2
Sponsor	Xerox Corporation
Developer	Xerox Corporation
Evaluators	Computer Sciences Corporation
Validators	The Aerospace Corporation

[2] For convenience, the product family will be referred to hereafter as the MFD, or MultiFunction Device.

3. SECURITY POLICY

The Xerox product enforces the following security policies:

3.1. Overwrite Policy.

The TOE is a multifunction device that copies and prints, with network scan, scan to email, and fax capability. The MFD stores temporary image data, along with associated files, that is created during print, network scan, or scan to email on an internal hard drive. The image data and associated files are overwritten—as prescribed in DoD Standard 5200.28M, using a three-pass procedure—automatically at the completion of each job that writes temporary files to the hard drive.

Additionally, an administrator may invoke the overwrite function on demand (i.e., ODIO; On-Demand Image Overwrite). ODIO cancels all print jobs, halts the printer interface (network), mounts the spool partition as a raw partition, overwrites the spool partition, and then reboots.

3.2. Identification and Authentication Policy.

Because the TOE is essentially a shared office product, there are no users identified, as such. Anyone who can access the MFD—either physically or through the network interface—can exercise its capabilities. Administrators, however, are authenticated via a PIN that may be entered either through the keypad or the network interface. Only administrators have the authority to invoke management functions; to enable or disable the automatic overwrite function, invoke/abort the ODIO function, and change the PIN.

3.3. Fax Card – Network Controller Separation

The TOE architecture is such as to provide separation between the processing board for the fax function and the network controller that spools temporary files to the hard drive. The fax function is both physically and logically independent of the other MFD functions. As noted, fax processing is implemented on separate hardware, and the fax interface responds only to fax carrier protocols (i.e., T.30 protocol signals). No mechanism exists to transfer arbitrary data between the fax card and the network controller.

4. ASSUMPTIONS

4.1. Usage Assumptions

The system is expected to be used in what has traditionally been known as “a relatively benign environment.” That is, all the information on the system is at the same level of sensitivity, all users are authorized for that level of information (although do not necessarily have access to all the data). However, users are not expected to be trustworthy; they may make attempts to bypass system security controls or otherwise exceed their authorizations to data and system resources.

Administrators are assumed to be trusted (i.e., non-malicious) and competent to carry out their responsibilities.

4.2. Environmental Assumptions

It is presumed that the MFD has been delivered, installed, and configured in accordance with documented procedures.

No explicit assumptions are made relative to physical controls. However, the system is essentially a piece of standard office equipment. As such, it would be accorded the kind of physical controls associated with the specific environment in which it is located. The implicit assumption is that control of access to the MFD is consistent with the level of sensitivity of the data that is being processed. For example, the controls on physical access would be different on a military installation than in a commercial office facility.

5. ARCHITECTURAL INFORMATION

The TOE is a single system (i.e., the MFD) which consists of six subsystems. The more significant, in terms of the evaluation are:

- Integrated Network Controller Module (INCM). This subsystem contains the Network Controller, Electronic Subsystem Disk, and power supply, It is the Network Controller that spools the document to be printed or scanned to the hard drive;
- Scanner Image Processor (SIP), which provides the copy, administrative, and diagnostic services (also referred to as the Copy Controller);
- Graphical User Interface (GUI), which detects soft button actuations and provides both text and graphical prompts to the user. The GUI behavior is implemented in a software module known as UIClient.
- Fax card. This is a fully-functional subsystem. The implementation of fax capability is completely independent of the other MFD functions (i.e., copy, scan, print, etc.); the fax processing board and the Network Controller are separate hardware elements. Additionally, the fax function does not use the hard drive to store data or temporary files.

The remaining subsystems provide mechanical transport of originals and functions such as xerography and paper handling.

6. DOCUMENTATION

Because the MFD provides no user security services, there is no user documentation other than the normal guidance relative to the functional features of the device. Furthermore, the TOE is installed and configured by trained Xerox technicians. As a result, no consumer-oriented installation, startup, and configuration guidance is needed.

However, there is guidance provided for the administrator which identifies the responsibilities and functions available to the administrator.

During the course of the evaluation, the CCTL had access to an extensive amount of documentation and evidence[3], covering:

- Interface specifications;
- Design details and system internals;
- Configuration management
- Delivery procedures and operation guidance;
- Vendor test plans, test suites, and test results;
- Vulnerability assessment documentation and strength of function analyses;
- Security Target

7. IT PRODUCT TESTING

7.1. Developer Testing

Evaluator analysis of the developer's test plans, test scripts, and test results demonstrate that the developer's testing is adequate to satisfy the requirements of EAL2.

The developer's tests were largely focused on the externally visible behavior of the TOE, with security testing covering the automatic overwrite, on-demand overwrite (i.e., ODIO) changing of the administrator's PIN, and the authentication function. Although some interfaces to the authentication function—notably, the web interface—were not tested, these were deemed by the evaluators to be indirect interfaces to the security function.

Additionally, the developer performed testing to verify that the fax function is logically separate from the other MFD functions, accepting only fax carrier protocols.

[3] A complete list of the documentation used during the evaluation is included in Section 3.5 of the *Evaluation Technical Report for a Target of Evaluation*, Version 1.1, April 29, 2004.

For each of the developer tests, the evaluators analyzed the test procedures to determine whether the procedures were relevant to, and sufficient for the function being tested. They also verified that the test documentation showed results that were consistent with the expected results for each test script.

7.1.1. Evaluator Testing

Although the developer's testing was considered adequate, the evaluators also tested each of the security functions as defined in the Security Target. Specifically:

- Image overwrite
- Authentication
- Security management
- Information flow (i.e., the separation of fax jobs from print/scan/copy functions).

The evaluators also executed a number of tests to determine whether the TOE is vulnerable to attacks aimed at bypassing the security functions or subverting the basic protection mechanisms.

7.1.2. Overwrite

Developer tests were reproduced. Additionally, the overwrite function was checked—by examining the contents of the hard drive—to verify that both the automatic overwrite and the on-demand overwrite (i.e., ODIO) result in the directory being cleared and the image data and associated temporary files being overwritten.

7.1.3. Authentication

Evaluator tests were performed using both the keypad and the web interface to verify that the administrator authentication function performs as specified in the TOE specifications, and that the administrator can perform no authorized functions prior to authentication.

7.1.4. Security Management

The evaluators performed tests to verify the functioning of the administrator functions, and the consistency of the administrator's PIN between subsystems (i.e., keypad and web interface).

7.1.5. Information Flow

Here also, the developer's tests were reproduced. Evaluator testing was performed to demonstrate that the fax function is both physically and logically independent of the other MFD functions, and specifically, to verify that only fax protocols are accepted via this interface.

7.1.6. Vulnerability Testing

The purpose of vulnerability testing is to determine the existence and exploitability of flaws or weaknesses in the MFD. The evaluators tested the ability of the TOE to handle unrecognized files (e.g., .doc files), as well as a number of known attack scenarios (e.g., FTP bounce attack, buffer overflow attempts).

During initial testing, a vulnerability was discovered that involved the ability to introduce arbitrary Postscript files, leading to some serious consequences. Although it could be argued that the vulnerabilities were out of scope in terms of the definitions and assumptions for an EAL2 evaluation, the Postscript vulnerability was deemed serious enough that the developer was asked to address the problem. As a result, patches were issued (i.e., Patch 4 and Patch 5). With these patches installed, a subsequent round of vulnerability testing was performed, and it was determined that the vulnerabilities of concern were effectively countered.

8. EVALUATED CONFIGURATION

Testing was performed on the Xerox WorkCentre Pro with System Software Set 3.084.016.000 with patches 4 and 5 installed.

The evaluation results apply to the Image Overwrite Security for the Xerox WorkCentre M35/M45/M55 Copier/Printer and WorkCentre Pro 35/45/55 Advanced Multifunction System.

9. RESULTS OF THE EVALUATION[4]

The TOE was found to provide the capabilities defined by the Security Target, and to satisfy all the requirements of EAL2.

10. EVALUATOR COMMENTS

There are no Evaluator Comments.

11. SECURITY TARGET

The ST, *Image Overwrite Security for the Xerox WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55 Advanced Multifunction System;* Version 1.0, Revision 1.27, 29 April 2004 is included here by reference.

[4] The terminology in this section is defined in CC Interpretation 008, specifying new language for CC Part 1, section/Clause 5.4.

12. GLOSSARY

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
MFD	Multifunction Device
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

13. BIBLIOGRAPHY

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

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

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

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

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

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

[7] Security Target, Overwrite Security for the Xerox WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55 Advanced Multifunction System; Version 1.0, Revision 1.27, 29 April 2004.

[8] Common Criteria Testing Laboratory Penetration Test Plan and Report, Xerox WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55 Advanced Multifunction System, April 16 2004.

[9] CSC Common Criteria Evaluation Laboratory Independent Test Plan and Report, Xerox WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55 Advanced Multifunction System, April 22 2004.

[10] Evaluation Technical Report, for the Windows 2000 Product, Part 2 (Proprietary), Version 1.0, October 4 2002.

[11] Evaluation Technical Report for a Target of Evaluation, Xerox WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55 Advanced Multifunction System, Version 1.1, April 29 2004.