National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme

Validation Report

Xerox Corporation

Xerox CopyCentre C2128/C2636/C3545 Copier and WorkCentre Pro C2128/C2636/C3545 Advanced Multifunction System including Image Overwrite Security

Report Number: CCEVS-VR-05-0121

Dated: 30 September 2005

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

Jean Hung

The MITRE Corporation

Jandria Alexander

The Aerospace Corporation

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 a line of copiers 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 January 2005. 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 2 conformant and Part 3 conformant,** and to meet the requirements of **EAL2**. 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 product family provides copy and copy/print/scan/fax capability. There are two primary configurations of the TOE, although with identical security features; a digital copier (DC) that provides only copy functions, and a multifunction device (MFD) that provides copy, print, scan to email, network scan, and network fax services. DC models have only a single internal hard drive (the Copy Controller HDD), whereas the MFD contains two internal hard drives (the Network Controller HDD and the Copy Controller HDD).

The primary security feature is that of the overwriting of temporary image data that is stored on the internal or optional external hard drive(s). 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 copy, print, network scan, or scan to email function.

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 EAL4 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~~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	Xerox CopyCentre C2128/C2636/C3545 Copier and WorkCentre Pro C2128/C2636/C3545 Advanced Multifunction System[1]including Image Overwrite Security.
Protection Profile	None
Security Target	*Xerox CopyCentre Copier C2128/C2636/C3545 and WorkCentre Pro C2128/C2636/C3545 Advanced Multifunction System including Image Overwrite Security,* Version 1.0, Rev 1.06, August 25, 2005
Evaluation Technical Report	*Xerox CopyCentre Copier C2128/C2636/C3545 and WorkCentre Pro C2128/C2636/C3545 Advanced Multifunction System including Image Overwrite Security,* Version 1.0, September 7, 2005
Conformance Result	Part 2 extended conformant, Part 3 conformant, EAL 2
Sponsor	Xerox Corporation
Developer	Xerox Corporation
Evaluators	Computer Sciences Corporation

[1] For convenience, the product family will be referred to hereafter as DC/MFD, or Digital Copier/ MultiFunction Device.

Validators	Jean Hung of The MITRE Corporation & Jandria Alexander of The Aerospace Corporation

2. SECURITY POLICY

The Xerox product line identified enforces the following security policies:

2.1. Overwrite Policy

The TOE is available in two models; a digital copier or multifunction device copies, prints, with network scan, scan to email, and provides fax capability (MFD). Both models store temporary image data, along with associated files, that are created during any of the supported services on an internal hard drive(s), or optional external hard drive(s). 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, network scan, scan-to-email, or network fax jobs jobs, halts the printer interface and overwrites the contents of the sections for temporary image files. The machine then reboots.[2]

2.2. 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

2.3. Security Management

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 system administrator PIN via the front panel. Also, only system administrators may invoke or abort the ODIO function through the web interface.

3. ASSUMPTIONS

3.1. 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, and all users are authorized for that level of information (although they do not necessarily have access to all

[2] The details of the image overwrite function are slightly different in each of the models. For a more detailed description, please refer to the Security Target (TOE Summary Specification, Sections 6.1.1, and 6.1.2)

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.

3.2. Environmental Assumptions

It is presumed that the TOE has been delivered, installed, and configured in accordance with documented procedures, which includes installation and setup by an authorized Xerox technician..

No explicit assumptions are made relative to physical controls. There will be one or more competent system administrator(s) assigned to manage the TOE and the security of the information it contains.

4. ARCHITECTURAL INFORMATION

The essential elements of the TOE models are:

- Network Controller (MFD only)—processes print, network scan, scan-to-email, and network fax tasks;
- Copy Controller—processes copy tasks;
- User interface (UI)—detects soft and hard button actuations and provides graphical prompts to the user;
- Image Output Terminal (IOT)—performs copy/print paper feeding and transport.

On the MFD models (i.e., WorkCentre C2128/C2636/C3545) copy jobs are submitted via the Local UI directly to the Copy Controller. Print jobs submitted via a client print driver or the Web UI are passed by the Network Controller to the Copy Controller. Once processed by the Copy Controller, copy and print jobs are sent to the Image Output Terminal (IOT). Network scan, scan-to-email, and internet fax jobs are submitted via the Local IU directly to the Network Controller for processing. Each time a job transits or is processed by one of the controllers, temporary image data, consisting of the original data submitted and any additional files created during job processing, is created and stored in the controller HDDs. (Note: Network Scan, scan-to-email, and internet fax jobs are sent directly to the Network Controller without getting stored on the Copy Controller HDD).

On DC models, copy jobs are submitted via the Local UI to the Copy Controller and, after processing, are sent to the Image Output Terminal. Temporary image data, consisting of the original data submitted and any additional files created during the processing of each copy job, is created and stored on the Copy Controller HDD.

On both DC and MFD models, outgoing analog fax jobs are submitted via the Local UI to the Copy Controller, and after processing, are sent to the Embedded Fax subsystem for transmission over the telephone line. Incoming analog fax jobs are passed from the Embedded Fax subsystem

to the Copy Controller, and then to the Image Output Terminal for printing. Temporary image data created during the processing of each fax job is stored on the Copy Controller HDD.

The TOE provides image overwrite functions (TSF_IOWN and TSF_IOWC for the MFD and TSF_IOWC for the DC) to enhance the security of both models. The image overwrite function overwrites temporary document image data as described in DoD Standard 5200.28-M at the completion of each print, network scan, scan-to-email, internet fax (MFD), and copy (MFD/DC) job or *on demand* of the system administrator. A system administrator may use the "on demand" image overwrite security function to clear sensitive information from the Network and Copy Controller HDDs when the MFD is decommissioned, for example. TSF_IOWN overwrites data stored on the Network Controller HDD (MFD) and TSF_IOWC overwrites data stored on the Copy Controller HDD (MFD and DC).

5. 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 that 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;
- User and administrator guidelines;
- Configuration management
- Delivery and installation procedures, and operation guidance;
- Vendor test plans, test suites, and test results;
- Vulnerability assessment documentation and strength of function analyses;
- Security Target

[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 1.0, September 7, 2005.

6. IT PRODUCT TESTING

6.1. Developer Testing

Evaluator analysis of the developer's test plans, test scripts, and test results demonstrate accurate correspondence between the tests identified and the functional specification, and 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.

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.

6.2. 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, running the entire developer test suite. Specifically:

- Image Overwrite Network Controller (TSF_IOWN)
- Image Overwrite Copy Controller (TSF_IOWC)
- Authentication (TSF_AUT)
- Security management (TSF_FMT)

were all tested.

6.2.1. 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. A test was added by the evaluators to validate the system behavior upon a system crash.

6.2.2. 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.

6.2.3. 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).

6.2.4. 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 block unauthorized NetBios connection (i.e., attempt to access the net controller filesystem through NetBios), as well as a number of known attack scenarios (e.g., FTP bounce attack, buffer overflow attempts).

The evaluator run a nikto scan against the TOE to determine if any obvious vulnerabilities with default or sample web server files are revealed by a nikto web server scan. The nikto report was generated and showed two vulnerabilities. The evaluation team attempted to exploit the vulnerabilities that showed in the scan, and found that both vulnerabilities were false positives.

7. EVALUATED CONFIGURATION

Testing was performed on both the Xerox CopyCentre and WorkCentre Pro models with System Software Set 0.001.04.505. The complete listing of firmware and software versions for each element within the product lines can be found in section 2.1 of the Security Target.

There are two versions known as "0.001.04.052" and "0.001.04.505". The 0.001.04.052 version comes on all new copiers before they are shipped from the factory. The 0.001.04.505 version is applied to previous copiers that have already shipped from the factory without 0.001.04.052 on them. The 0.001.04.505 version contains three bits of functionality that are not found in 0.001.04.052.

These changes are clearly spelled out in "Addendum #2" of the Functional Specification (FSP) evidence, included in the "Errata" section of the High-Level Design (HLD), and the ACM documentation for each release agrees with both FSP and HLD (i.e.: the file names and versions that change are logical given the changes to the TOE). These three changes are not security relevant where TSFs are concerned.

Additionally, because the changes are additions (not modifications or deletions), the whole of 0.001.04.052 is contained within 0.001.04.505; therefore a test of 0.001.04.505 constitutes a test of 0.001.04.052.

The evaluation results apply to the Image Overwrite Security for the Xerox CopyCentre C2128/C2636/C3545 Copiers and WorkCentre Pro C2128/C2636/C3545 Advanced Multifunction System.

8. 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.

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

9. VALIDATOR COMMENTS

The TOE of this evaluation and the TOE of Xerox CopyCentre C65/C75/C90 Copier and WorkCentre Pro 65/75/90 Advanced Multifunction System including Image Overwrite Security belong to the same family. One difference is that the TOE of this evaluation supports color features. Although the two evaluations are independent, the TOEs are similar. For further information on the previous evaluation, please refer to Validation Report Number: CCEVS-VR-04-0092.

10. SECURITY TARGET

The ST, *Xerox CopyCentre C2128/C2636/C3545 and WorkCentre Pro C2128/C2636/C3545 Advanced Multifunction System,including Image Overwrite;* Version 1.0, Revision 1.06, August 25, 2005 is included here by reference.

11. 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

12. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.2.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.2.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.2.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.2.

[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, Xerox CopyCentre C2128/C2636/C3545 Copier and WorkCentre Pro C2128/C2636/C3545 Advanced Multifunction System including Overwrite Security; Version 1.0, Revision 1.06, August 25, 2005.

[8] Common Criteria Testing Laboratory Penetration Test Plan and Report, Xerox CopyCentre C2128/C2636/C3545 Copier and WorkCentre Pro C2128/C2636/C3545 Advanced Multifunction System including Image Overwrite Security, September 7, 2005.

[9] CSC Common Criteria Laboratory Independent Test Plan and Report, Xerox CopyCentre C2128/C2636/C3545 Copier and WorkCentre Pro C2128/C2636/C3545 Advanced Multifunction Device including Image Overwrite Security, September 7, 2005.

[10] Evaluation Technical Report for a Target of Evaluation, Xerox CopyCentre C2128/C2636/C3545 Copier and WorkCentre Pro C2128/C2636/C3545 Advanced Multifunction System including Image Overwrite Security, Version 1.0, September 7, 2005.