National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

Lexmark Multifunction Printer (MFP) Controller Software
Version 907.207b

Report Number: CCEVS-VR-06-0014

Dated: 23 February 2006

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

Thomas P. Murphy
Mitretek Systems
Linthicum Maryland

Dr. Jerome Myers
The Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587

Table of Contents

List of Figures

List of Tables

1 EXECUTIVE SUMMARY

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the Lexmark Multifunction Printer (MFP) Controller Software Version 907.207b at EAL2. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by the CAFE Laboratory of COACT Incorporated, located in Columbia, Maryland. The evaluation was completed on 23 February 2006. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by COACT and submitted to the Validators. The evaluation determined the product conforms to the CC Version 2.2, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 2 resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE is the application software that resides within a network-connected scan unit of a family of Multifunction Printers (MFPs). The TOE executes on a Printed Circuit Board (PCB) with a Linux kernel. Both the PCB and Linux kernel were treated as IT Environment in this evaluation. The TOE typically comes preinstalled on the scan unit from the factory. Setup and installation is performed by a Lexmark representative, and the proper version of the TOE will be installed by that representative during setup and installation if necessary. The scan unit must be mated with a printer in order to be functional. No portions of the printer are part of the TOE.

The security functionality of the TOE includes Fax Communications Control to enforce separation between fax and network data, User Authentication via the touch screen, Device Configuration Protection to enable secure management of the TOE, Touch Screen Lock/Unlock to restrict access to MFP functions, and Partial Self Protection.

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 desire 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 CCEVS' 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.
- The organizations and individuals participating in the evaluation.

Table 1 - Evaluation Identifiers

Evaluation Identifiers for Lexmark Multifunction Printer (MFP) Controller Software Version 907.207b	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Lexmark Multifunction Printer (MFP) Controller Software Version 907.207b
Protection Profile	N/A
Security Target	Lexmark Multifunction Printer (MFP) Controller Software Version 907.207b Security Target, dated March 28, 2006, document number F2-0206-008(1)
Evaluation Technical Report	Lexmark Multifunction Printer (MFP) Controller Software Version 907.207b Evaluation Technical Report, Document No. F2-0206-003(1), Dated March 28, 2006
Conformance Result	Part 2 extended and EAL2 Part 3 conformant
Version of CC	CC Version 2.2 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on December 28, 2004
Version of CEM	CEM Version 2.2 and all applicable NIAP and International Interpretations effective on December 28, 2004
Sponsor	Lexmark, Inc. 740 New Circle Road NW Lexington, KY 40511
Developer	Lexmark, Inc. 740 New Circle Road NW Lexington, KY 40511
Evaluator(s)	**COACT Incorporated** Dawn Adams Greg Beaver Christa Lanzisera
Validator(s)	**NIAP CCEVS** Thomas P. Murphy Dr. Jerome Myers

2.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

I-0407 – Empty Selections or Assignments
I-0418 – Evaluation of the TOE Summary Specification: Part 1 Vs Part 3
I-0426 – Content of PP Claims Rationale
I-0427 – Identification of Standards

International Interpretations

None

3 Security Policy

The TOE resides in the scan unit of a network-connected Multi-Function Printer (MFP). The TOE controls access to MFP functions (copy, email and fax), including a mechanism to lock access to these functions, and provides separation between the fax functionality and any user data from the network. The TOE also provides management functionality to an authorized administrator.

3.1 Device Configuration Protection

The Device Configuration Protection provides the necessary functions to allow an administrator to manage and support the TOE Security Function (TSF). Included in this functionality are the administrator password, user accounts, user passwords, and touch screen lock procedures.

3.2 Fax Communications Control

The TSF ensures that all data transferred through the fax connection is related to an incoming or outgoing fax job by maintaining control of the data that is exchanged. The fax hardware that provides the fax connection is kept in "Facsimile Class 1" mode, which restricts the fax hardware such that it does not manipulate or control the exchanged data. By controlling the data exchange directly, and by not implementing any facility for managing the MFP through this connection, and by not supporting any mechanisms such as telnet or FTP over the fax connection, the TSF protects the MFP's data and configuration settings from exploitation via the fax port.

3.3 User Authentication

The MFP's touch screen interface allows access to up to three types of scan-based operations: scan-to-fax, scan-to-copy, and scan-to-email. When applied to a type of operation, the User Authentication function requires the touch screen user's credentials to be submitted and validated before the TSF gives the touch screen user access to the operation.

3.4 MFP Touch Screen Lock Function

The MFP Touch Screen Lock function allows the MFP's touch screen to be locked, effectively disabling the device's functions: scan-to-fax, scan-to-copy, and scan-to-email.

3.5 TOE Separation

The TOE ensures that all functions are invoked and succeed before the next function may proceed.

3.6 Security Function Strength of Function Claim

The only mechanisms in the TOE for which an SOF claim is required are the Password mechanisms for the Administrative Password, Touch Screen User Authentication Password and Touch Screen Unlock Password, which are SOF-basic.

3.7 Protection Profile Claim

This Security Target does not claim conformance to any registered Protection Profile

4 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's IT Environment. This includes information about the connectivity, personnel, and physical side of the environment plus potential threats.

4.1 Connectivity Assumptions

The TOE is intended for use in areas that have physical control and monitoring. It is assumed that:

- The IT Environment shall preclude HTTP communication between network users and the TOE across the IP network to prevent disclosure of the administrator password.

4.2 Personnel Assumptions

The TOE is intended to be managed by competent non-hostile individuals. It is assumed that:

- System Administrators will follow the MFP guidance.
- Users are not evil, careless, willfully negligent, or hostile.

4.3 Physical Assumptions

The TOE is intended for use in areas that have physical control and monitoring. It is assumed that:

- The TOE will be located within non-hostile facilities.
- The IT Environment is managed and monitored in a secure manner.

4.4 Potential Threats

Potential threats are:

- An unauthorized individual may attempt to gain access to the TOE functions and to TOE resources through either malicious or accidental means.
- A hostile entity may attempt to gain access through a phone connection to TOE resources, or TOE connected networks to retrieve data of value.
- An authorized user may attempt to execute TOE security functions without System Administrator privileges.

5 Clarification of Scope

The TOE is only a portion of the software that resides within the specified Lexmark MFPs. This evaluation focused upon security functionality of the FAX interface to the MFP. This software resides entirely within the scan unit of the MFP. The TOE resides on a hardware platform that executes a version of Linux. The underlying hardware and Linux Operating System were not part of the TOE. Moreover, the network interface to the TOE was considered to be relatively benign. More precisely, IT Environmental requirements were placed on the network interface to the TOE and on the behavior of users of that network interface that precluded malicious attempts to compromise the TOE from the network interfaces of the MFP. The TOE itself does not provide that protection.

6 Architecture Information

The TOE consists of proprietary application software developed by Lexmark. The application software executes on top of a Linux kernel running on a Printed Circuit Board (PCB) in the scan unit of an MFP. Neither Linux nor the PCB is included in the TOE.

6.1 TOE Security Functions

The properties of the TOE necessary for the TOE to provide its security functionality are:

- The TOE will ensure that users gain only authorized access to the TOE.
- The TOE will provide an administrative role to isolate administrative actions.
- The TOE will require users to identify and authenticate themselves before allowing them to access scan-related functions via the touch screen.
- The TSF will provide functions and facilities necessary to support the authorized administrators that are responsible for the management of TOE security.
- The TSF ensures that the fax interface may not be used to access TSF configuration data or user data from the network.

6.2 IT Environment Security Functions

The properties of the IT operational Environment of the TOE necessary for the TOE to be able to provide its security functionality are:

- The IT Environment will ensure that HTTP access to the TOE is not permitted, since such access would permit the administrator password to be passed across the network in cleartext.
- The IT Environment supports non-bypassability and non-interference of the TSF.

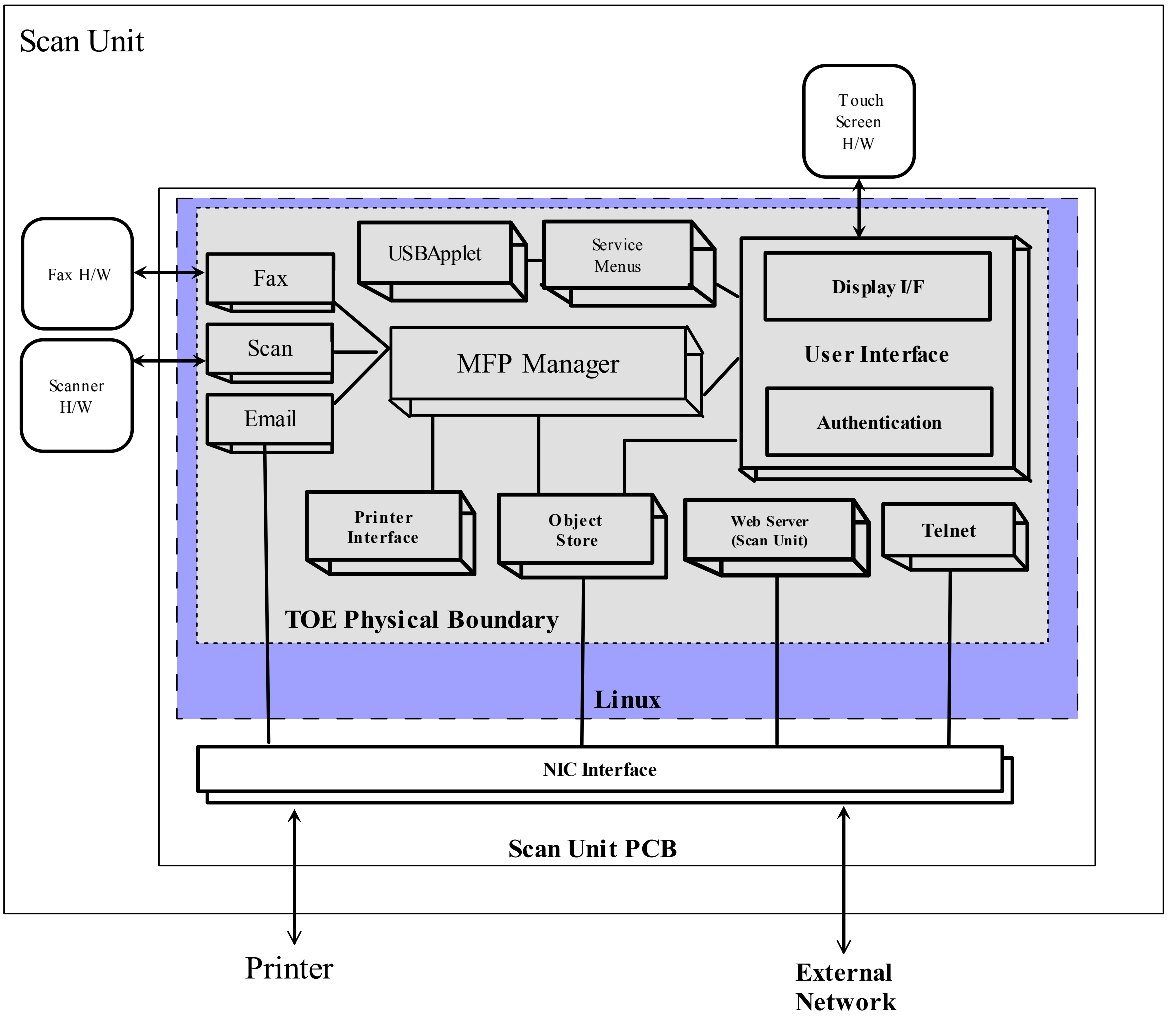
6.3 Physical Boundary

The TOE is normally delivered pre-installed on the hard drive of the scan unit of an MFP. A Lexmark representative is responsible for the installation of the TOE at a customer site; if the evaluated version of the TOE is not pre-installed, the Lexmark representative installs it.

6.4 Logical Boundary

The TOE is divided into multiple modules in the application software. The logical boundary is further described in the following diagram.

Figure 1 - Logical Boundaries Diagram



7 Product Delivery

As stated previously, the TOE is normally delivered pre-installed on the hard drive of the scan unit of an MFP. A Lexmark representative is responsible for the installation of the TOE at a customer site; if the evaluated version of the TOE is not pre-installed, the Lexmark representative installs it. There are eight specific MFP products that share the security functions of the TOE: the Lexmark x634e, x634dte, x762e, x820e, x830e, x832e, and x912e. These products are composed of a scan unit mated with a printer. The following table documents the valid combinations.

Table 2 - MFP Identifiers

MFP Model	Scan Unit Model	Printer Model
X634e	X4500	T634
X634dte	X4500	T634dt
X762e	X4500	C762
X820e	X7500	W820
X830e	X7500	W820

MFP Model	Scan Unit Model	Printer Model
X832e	X7500	W820
X912e	X5500	C912

The TOE delivery included the following items (in addition to the TOE):

- Drivers, Markvision, and Utilities disk
- MFP Setup Guide
- Look What's New document
- Printer Setup Guide
- Safety Information document
- MFP Roadmap document
- Important Notice on Unlocking the Scanner document

The TOE is installed by a Lexmark representative using the Important Information for Common Criteria EAL2 Compliant Operation, P/N 16C0591 EC 4G00931, Version EC4G0093-16C0591.v0.10, a document provided by the Lexmark representative. This document provides information specific to the required configuration to achieve the evaluated configuration stated in the Security Target.

8 IT Product Testing

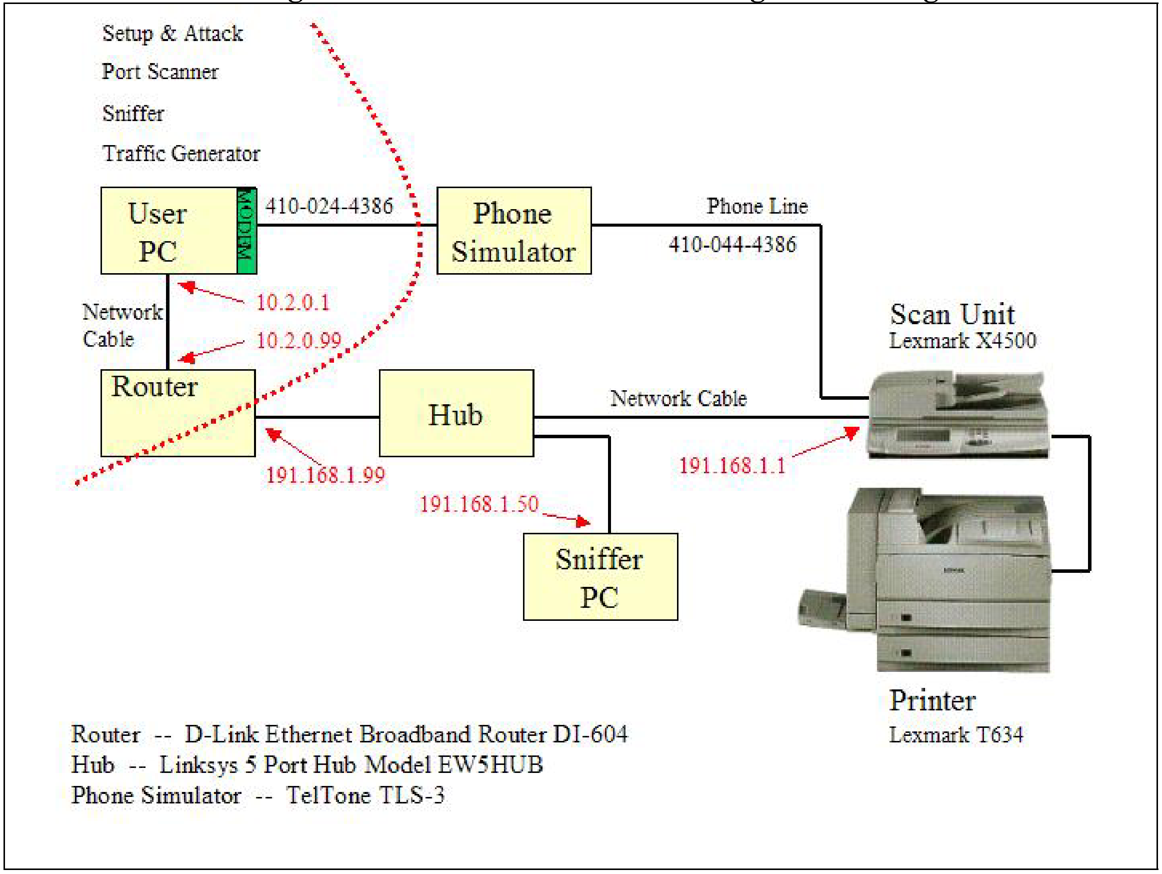
Testing was performed on February 8, 2006 at the COACT Laboratory in Columbia, MD. Three COACT employees performed the tests in the presence of the Lead Validator. All test configurations operated properly and tests were completed in an expeditious manner.

8.1 Evaluator Functional Test Environment

The test configuration used an X4500 scan unit mated with a T634 printer, forming an X634e MFP. Other equipment involved in the testing included a PC to generate print jobs and faxes, a router to filter HTTP traffic between the PC and the MFP, and a phone simulator to provide call control between the PC and MFP.

The following figure graphically displays the test configuration used for functional testing.

Figure 2 - Functional Test Configuration Diagram



8.2 Test Assumptions

The functional test environment/configuration assumes that:

- The TOE has been configured and is operating in the configuration described in the ST. (Note: The router is configured to block HTTP traffic.)
- The Administrator role has been created.
- The Administrator is a trusted user of the TOE.

Lexmark MFP software version 907.207b executes on all of the MFP models identified in Table 2 above.

8.3 TOE Evaluated Configuration Options

The evaluated configuration options were set as follows:

- Internal User Authentication is selected, and applied to all of the user functions accessible via the touch screen operator panel.
- HTTP is enabled.
- FTP is disabled.
- SNMP sets are disabled.
- The NetWare protocol is disabled.
- The AppleTalk protocol is disabled.
- The DLC protocol is disabled.
- The MVP management protocol is disabled.

- An external device (e.g., router) must be placed between the scan unit and all users on the network. The external device must be configured to filter all traffic from the users to the scan unit on ports 80 and 10080 (HTTP).

8.4 Repeated Developer Tests to Confirm Developer Test Results

This section lists tests required to confirm the developer test results. The evaluation team selected five of the thirteen vendor tests to reproduce. The five tests chosen exercise all of the security functions with the exception of TSF Self Protection.

The following list presents the tests:

- 3.1.1 - checks the Fax Communications Control and the Serial Connection to Modem.
- 3.2.2 - checks the User Authentication, Email Icon, and User Credentials Entry Pages.
- 3.3.1 - checks the Device Configuration Protection, the Configuration and Printer Operator Panel page, the System Administrator Credentials Entry Pages on Touch Screen Operator Panel, and the Security Configuration Page.
- 3.4.1 - checks the MFP Touch Screen Lock and the Lock MFP Control.
- 3.4.2 - checks the MFP Touch Screen Lock and the Lock MFP Control, and the Touch Screen Unlocker Password Entry Page.

8.5 Functional Test Results

All tests were performed satisfactorily and the results were as expected. The TOE passed all tests. The procedures followed to execute these tests and detailed results are presented in the Functional Test Report for the Lexmark Multifunction Printer (MFP) Controller Software Version 907.207b, document number F2-0206-004, for Common Criteria EAL2 Evaluation.

8.6 Evaluator Independent Testing

The tests chosen for independent testing allow the evaluation team to exercise the TOE in a different manner than that of the developer's testing. The intent of the independent tests is to give the evaluation team confidence that the TOE operates correctly in a wider range of conditions than would be possible purely using the developer's own efforts, given a fixed level of resource. The selected independent tests allow for a finer level of granularity of testing compared to the developer's testing, or provide additional testing of functions that were not exhaustively tested by the developer. The tests allow specific functions and functionality to be tested. The tests reflect knowledge of the TOE gained from performing other work units in the evaluation. For example, specific TSFI behaviors were identified while performing the ADV work units, and tests have been developed to test specific behaviors.

To determine the independent testing to be performed, the evaluators first assessed the level of developer testing corresponding to all TSFIs. The Independent Tests performed were:

- ET1 - This test shall validate the TOE's ability for the administrator to create a user account, have the user successfully logon, have the user to perform a scan to copy function, and finally have the administrator delete that user account. The ability of the TOE to delete a user by the administrator shall be verified by the user attempting to log in and perform one of the prior privileged tasks.
- ET2 - This test shall validate the TOE's ability to successfully authenticate a user before allowing any other TSF-mediated actions. The obscured password feedback during the authentication process will be validated. A user shall logon and perform a scan to copy

operation. The logged on user shall perform no other actions. The TOE will be tested to validate that the user's session will time out and no other user can gain access to the TOE without first going through the proper logon process.

- ET3 - The Administrator shall enable the Touch Screen Lock function. The Touch Screen Unlockers shall be given the Unlock password. A non-logged on user shall activate the Touch Screen Lock function. A Touch Screen Unlocker shall log on and unlock the function.
- ET4 - The Administrator shall change the passwords for the Administrator, User, and Touch Screen Unlocker's Pin.
- ET5 - This test will verify that only the "MarkNet" administrator is able to change configuration settings.
- ET6 - This test will show that the administrator can still configure the printer when it is locked. Also shows that only the unlock pin can unlock the printer for normal functionality.

8.6.1 Evaluator Independent Test Environment

The test environment used to conduct these tests was the same as that used to reproduce the functional tests.

8.7 Evaluator Independent Test Results

All tests were performed satisfactorily and the results were as expected. The TOE passed all tests. The procedures followed to execute these tests and detailed results are presented in the Functional Test Report for the Lexmark Multifunction Printer (MFP) Controller Software Version 907.207b, document number F2-0206-004.

8.8 Evaluator Penetration Tests

8.8.1 Evaluator Assessment of Developer Analysis

The evaluator examined each of the obvious vulnerabilities identified during the developer's vulnerability analysis. After consulting the sources identified by the developer used during the initial vulnerability analysis, the evaluator consulted other vulnerability relevant sources of information to verify that the developer considered all available information when developing the non-exploitation rationale. These additional sources include:

- https://cirdb.cerias.purdue.edu/coopvdb/public/
- http://www.bugtraq.org/
- http://www.osvdb.org/
- http://xforce.iss.net/
- http://icat.nist.gov/icat.cfm

After verifying that the developer's analysis approach sufficiently included all of the necessary available information regarding the identified vulnerabilities, the evaluator made an assessment of the rationales provided by the developer indicating that the vulnerability was non-exploitable in the intended environment of the TOE. Any possible vulnerability that required further evaluator analysis, such as an Attack Potential Calculation, was identified as suspect.

Of the six vulnerabilities identified by the vendor, the evaluator found one of the developer rationales, describing why a particular possibly relevant vulnerability of the TOE was not exploitable, to be suspect. Therefore the evaluator tested the TOE to ensure the TOE was properly resistant to the relevant vulnerabilities.

8.8.2 Additional Vulnerabilities

While verifying the information found in the developer's vulnerability assessment the evaluator conducted a search to verify if additional obvious vulnerabilities exist for the TOE. This search included examining the websites identified in section 3.1 of this document. Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerabilities. The additional analysis conducted by the evaluator identified two additional vulnerabilities that may possibly be relevant to the TOE:

- Unauthorized persons may be able to use the fax port to generate unauthorized traffic and gain access to the TOE configuration pages in the scan unit
- The use of a postscript sent through the fax may cause the printer to begin to process the postscript file. In this case it may be possible to attack the TOE using the interface that would be opened through the faxline.

However, after confirming that the facsimile protocol used in the TOE is Class 1, it became unnecessary to attempt a postscript attack since postscript is not supported by the Class1 facsimile protocol. Therefore the evaluator tested the TOE to ensure the TOE was properly resistant to the first additional identified vulnerability. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to all the potential vulnerabilities identified by the evaluator.

8.9 Evaluator Penetration Test Identification

As a result of the evaluator's examination of the developer's vulnerability analysis and the independent search for obvious TOE vulnerabilities, the evaluator devised a test plan and a set of test procedures to test the TOE's mitigation of the vulnerabilities. The following Penetration tests were performed by the evaluator:

- #1 - Unauthorized persons may be able to use the fax port to generate unauthorized traffic and gain access to the TOE configuration pages in the scan unit.
- #2 - Attempt to reach the configuration page using ftp, tftp, and telnet protocols.
- #3 - Attempt to reach the configuration page using a browser and the http protocol.
- #4 - Attempt to disrupt the TOE during a fax attempt using ftp.

8.10 Actual Penetration Test Results

The end result of the testing activities was that all tests gave expected (correct) results. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to the all the potential vulnerabilities identified by the evaluator. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

9 RESULTS OF THE EVALUATION

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component. For Fail or

Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence.

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. Section 4, Results of Evaluation, from the document *Evaluation Technical Report for the Lexmark Multifunction Printer (MFP) Controller Software Version 907.207b* contains the verdicts of "PASS" for all the work units.

The evaluation determined that the product meets the requirements for EAL 2. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by COACT Inc.

10. VALIDATOR COMMENTS

As of the time of this evaluation, there is no standard Protection Profile for Multifunction Printers. It is the validators' experience that the security functionality for MFPs that have been evaluated varies so widely that it is hard to compare the results of the evaluations of different MFPs. Until a standard MFP PP is available the security functionality implied by attaching the MFP tag to an evaluation will be nebulous. The focus of the security functionality for this particular evaluated product is the FAX (and associated Console) interface.

The TOE is only a portion of the software that resides within the specified Lexmark MFPs. The software resides entirely within the scan unit of the MFP. The TOE resides on a hardware platform that executes a version of Linux. The underlying hardware and Linux Operating System were not part of the TOE. Moreover, the network interface to the TOE was considered to be relatively benign. More precisely, IT Environmental requirements were placed on the network interface to the TOE and on the behavior of users of that network interface that precluded malicious attempts to compromise the TOE from the network interfaces of the MFP. The TOE itself does not provide that protection; it is provided by the IT Environment. Although some testing was done on the network interface to ensure that obvious direct attacks upon the TOE from the network side would be prevented, a similar analysis was not performed on potential indirect attacks that could be relayed through the TOEs network interface to the attached printer and then redirected back to the internal network interface of the FAX component of the MFP. This does not imply that such attacks exist, those attacks simply were not further analyzed once it was determined that they could not be driven through the user (FAX) interfaces provided by the TOE.

The evaluated version of the TOE requires that the IT Environment be configured to block all HTTP traffic to the network interface of the MFP. Although there is port blocking capability within the network interface of the Linux OS that resides on the actual scan unit that hosts the MFP, that capability cannot be used to block HTTP. A separate component such as the router used in the test configuration is necessary. This is because the HTTP interface on the scan unit needs to be open so the scan unit can communicate with the attached print unit to direct its output to the printer. The validator believes that it is unlikely that the MFP will typically be fielded in this configuration.

11. Security Target

The Security Target document, Lexmark Multifunction Printer (MFP) Controller Software Version 907.207b Security Target dated March 28, 2006 is incorporated here by reference.

12. List of Acronyms

CC	Common Criteria
EAL2	Evaluation Assurance Level 2
IT	Information Technology
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

13. Bibliography

The following list of standards was used in this evaluation:

- Common Criteria for Information Technology Security Evaluation, Part 1 Introduction and General Model, Version 2.2, dated January 2004
- Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements, Version 2.2, dated January 2004
- Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements, Version 2.2, dated January 2004
- Common Methodology for Information Technology Security Evaluation, Part 1, Version 2.2, dated January 2004
- Common Methodology for Information Technology Security Evaluation, Part 2, Version 2.2, dated January 2004
- Guide for the Production of PPs and STs, Version 0.9, dated January 2000