National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme Validation Report

HP LaserJet 9040 MFP System Firmware Version 08.091.3, HP LaserJet 9050 MFP System Firmware Version 08.091.3, HP LaserJet 4345 MFP System Firmware Version 09.091.4, and HP LaserJet CM4730 MFP System Firmware Version 50.021.4

Report Number: CCEVS-VR-VID10297-2008

Dated: 28 February 2008

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

Jerome F. Myers
Dianne M. Hale

Common Criteria Testing Laboratory
COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587

Table of Contents

1 Executive Summary 4
2 Identification 4
2.1 Applicable Interpretations 6
3 TOE Description 6
3.1 Secure Erase 6
3.2 Network and Analog Fax Resource Separation 7
3.3 Identification & Authentication 8
3.4 Security Management 8
4 Assumptions, Threats, and Clarification of Scope 9
4.1 Usage Assumptions 9
4.2 Threats Addressed by the TOE 9
4.3 Threats Addressed by the IT Environment 9
4.4 Clarification of Scope 10
5 Architecture Information 10
6 Evaluated Configuration 11
7 Product Delivery 12
8 IT Product Testing 14
8.1 Evaluator Functional Test Environment 14
8.2 Functional Test Results 15
8.3 Evaluator Independent Testing 15
8.4 Evaluator Penetration Tests 15
8.5 Test Results 16
9 RESULTS OF THE EVALUATION 16
10 VALIDATOR COMMENTS 16
11 Security Target 17
12 List of Acronyms 17
13 Bibliography 17

List of Figures

Figure 1 - MFP System Firmware 11
Figure 2 - Test Configuration/Setup 15

List of Tables

Table 1 - Evaluation Identifier 5

1 Executive Summary

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the HP LaserJet 9040 MFP System Firmware Version 08.091.3, HP LaserJet 9050 MFP System Firmware Version 08.091.3, , HP LaserJet 4345 MFP System Firmware Version 09.091.4, and HP Color LaserJet CM4730 MFP System Firmware Version 50.021.4 at EAL3. 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 22 January 2008. 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) 3resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE is the HP LaserJet 9040 MFP System Firmware Version 08.091.3, HP LaserJet 9050 MFP System Firmware Version 08.091.3, HP LaserJet 4345 MFP System Firmware Version 09.091.4, and HP Color LaserJet CM4730 MFP System Firmware Version 50.021.4.

The TOE is comprised of the MFP System Firmware. It includes the following security functionality:

- Secure Erase Functionality
  - Secure File Erase provides routine real-time erasing of temporary and permanent files stored on the MFP hard drive and Partition 2 of the MFP Compact Flash card during normal operations.
  - Secure Storage Erase erases the entire contents of the MFP hard drive or of Partition 2 of the MFP Compact Flash card.
- Network and Analog Fax Resource Separation.
  - All data coming in through or going out through the analog fax accessory is only fax data with no network information.
  - All incoming fax data is stored or printed securely.
  - All outgoing fax data is only from the scanner.
- Identification & Authentication - Administrators authenticate to the TOE prior to managing security functions.
- Security Management – The TOE allows for security management of Secure Erase functions by requiring restricted access through non-TOE interfaces, which are the only interfaces that can provide these options. This ensures that the secure erase functions are executed as intended by authorized personnel. Only the authenticated and authorized system administrator can enable, disable, or configure the secure file erase or secure storage erase options.

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 Identifier

Evaluation Identifiers for HP LaserJet 9040 MFP System Firmware Version 08.091.3, HP LaserJet 9050 MFP System Firmware Version 08.091.3, HP LaserJet 4345 MFP System Firmware Version 09.091.4, and HP Color LaserJet CM4730 MFP System Firmware Version 50.021.4	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	HP LaserJet 9040 MFP System Firmware Version 08.091.3, HP LaserJet 9050 MFP System Firmware Version 08.091.3, HP LaserJet 4345 MFP System Firmware Version 09.091.4, HP Color LaserJet CM4730 MFP System Firmware Version 50.021.4
Protection Profile	N/A
Security Target	HP LaserJet 9040 MFP System Firmware Version 08.091.3, HP LaserJet 9050 MFP System Firmware Version 08.091.3, HP LaserJet 4345 MFP System Firmware Version 09.091.4, HP Color LaserJet CM4730 MFP System Firmware Version 50.021.4 Security Target, Version 1.5, dated 07 February 2008.
Evaluation Technical Report	Evaluation Technical Report for the HP LaserJet 9040 MFP System Firmware Version 08.091.3, HP LaserJet 9050 MFP System Firmware Version 08.091.3, HP LaserJet 4345 MFP System Firmware Version 09.091.4, HP Color LaserJet CM4730 MFP System Firmware Version 50.021.4. Document No. F3-0108-001, Dated 29 February 2008.
Conformance Result	Part 2 conformant and EAL3 Part 3 conformant
Version of CC	CC Version 2.2 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on January 26, 2006.
Version of CEM	CEM Version 2.2 and all applicable NIAP and International Interpretations effective on November 20, 2007.
Sponsor	Hewlett-Packard Company 11311 Chinden Blvd Boise, ID 83714

Evaluation Identifiers for HP LaserJet 9040 MFP System Firmware Version 08.091.3, HP LaserJet 9050 MFP System Firmware Version 08.091.3, HP LaserJet 4345 MFP System Firmware Version 09.091.4, and HP Color LaserJet CM4730 MFP System Firmware Version 50.021.4	
Developer	Hewlett-Packard Company 11311 Chinden Blvd Boise, ID 83714
Evaluator(s)	**COACT Incorporated** Bob Roland Greg Beaver
Validator(s)	**NIAP CCEVS** Jerome F. Myers Dianne Hale

2.1 Applicable Interpretations

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

NIAP Interpretations

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 TOE Description

The HP LaserJet 9040 MFP System Firmware Version 08.091.3, HP LaserJet 9050 MFP System Firmware Version 08.091.3, HP LaserJet 4345 MFP System Firmware Version 09.091.4, and HP Color LaserJet CM4730 MFP System Firmware Version 50.021.4 consist of the following components of the MFP:

- Secure Erase
- Network and Analog Fax Resource Separation
- Authentication
- Security Management

These components are explained in the subsections below.

3.1 Secure Erase

The TOE protects residual or remnant information (stored or temporary files used to process print, copy, send to email, send to folder, or fax jobs) by rendering it unavailable to all users by performing Secure Erase operations on the Hard Disk Drive or on Partition 2 of the Compact Flash Drive.

- Secure File Erase -Temporary or user files are stored on an MFP hard drive or on Partition 2 of the MFP Compact Flash card during normal operations such as print, copy, scan to email, scan to network folder, and fax. Secure File Erase regulates how the system deletes files. Secure file erase deletes files in real time as jobs of various types (print, copy, send to email, send to folder, or fax) are executed and completed in the system. Secure file erase is called to delete files using one of two optional modes (as configured according to the Security Checklist) for the MFP hard disk drive and one secure mode for Partition 2 of the MFP Compact Flash card:
    - Secure Fast Erase – Secure Fast Erase overwrites all addressable locations on the MFP hard disk drive with a single character, providing sufficient security for most network environments.
    - Secure Sanitizing Erase – Secure Sanitizing Erase overwrites all addressable locations on the MFP hard disk drive with a character followed by its complement followed by a random character, providing a higher level of security for sensitive environments.
    - Secure File Erase for Compact Flash – Secure Erase for Compact Flash overwrites all addressable locations on Partition 2 of the MFP Compact Flash card with a character. Compact flash technology is not magnetic, and it does not exhibit the problem of residual data. When the Secure File Erase setting is configured with either of the secure settings (listed above), the Secure Erase Mode for Compact Flash is used. Note that some Compact Flash devices that are supported by the MFPs can accommodate an erase command. In which case, the erase command is used rather than the overwrite function.

- Secure Storage Erase - Secure Storage Erase deletes files or data on the entire MFP hard drive or on Partition 2 of the Compact Flash Drive. It is executed by an administrator on demand. It does not operate continuously. Secure Storage Erase deletes files on the MFP hard drive or in Partition 2 of the MFP Compact Flash card using the mode selected for Secure File Erase, which is either Secure Fast Erase or Secure Sanitizing Erase. The types of files erased include permanent stored jobs, proof and hold jobs, disk-based fonts, and disk-based macro (forms) files.Note that Secure Storage Erase function for Partition 2 of the MFP Compact Flash card is not the same as that for Secure File Erase. The Secure Storage Erase function treats Partition 2 of the MFP Compact Flash card the same as it treats the MFP hard disk drive. For Secure Fast Erase mode, it overwrites all addressable locations on Partition 2 of the MFP Compact Flash card with one pass. For Secure Sanitize Erase, it overwrites all addressable locations on Partition 2 of the MFP Compact Flash card with three passes.

3.2 Network and Analog Fax Resource Separation

This ST asserts the following properties of MFPs:

- **All data coming through or going out through the Analog Fax Accessory is fax data** - All data that come into or go out of the MFP via the telephone line pass through the fax card. The part of the MFP System Firmware that operates the fax card is a serial modem driver that is exclusive to the fax card. The serial modem driver is also exclusive to fax protocols. No other part of the MFP can open, read, or write to the fax card. The MFP System Firmware cannot allow generalized communication through the fax card. All requests to send or receive fax data occur only through the fax card and are enabled only when a fax session is active. A fax session is active only when the MFP System Firmware has successfully completed fax negotiation with another fax modem. Fax negotiation occurs when a fax modem calls another fax modem, and the two agree on

common capabilities such as resolution, paper size, and format (protocol). Thus, the MFP is capable of processing fax communication only via the fax card, only in fax protocols, and only with another fax modem to which it is connected and communicating through the telephone service.

- **All fax data coming in through the Analog Fax Accessory is stored or printed securely** - When the MFP System Firmware receives a fax transmission, it cleans up the fax data and writes it to a specific directory that is designated only for incoming fax files. The fax receive, fax print, and the hard disk delete functions of the MFP System Firmware are the only entities permitted to access this designated fax directory. The MFP can store incoming fax transmissions for a limited time to allow for printing at a time that is convenient or secure for users. When the MFP prints the fax, the fax print function can only send the file directly from the designated fax directory to the print engine, which is only capable of printing files. Once printing is complete, the MFP System Firmware erases the file using Secure File Erase. Thus, the MFP can do nothing with an incoming fax transmission other than storing it, printing it, and deleting it.
- **All fax data going out is from the scanner** - Data for sending a fax is scanned after command objects are selected in the Control Panel fax UIs. The MFP System Firmware creates a fax job ticket which designates the scan data as a fax job. The MFP System Firmware creates two TIFF versions of the image data each with a different resolution. Then, it writes the two TIFF files to a directory that is designated only for outgoing fax files. There, it stores the files as it opens a fax call and negotiates with a remote fax modem, during which, the resolution is decided. MFP System Firmware sends the TIFF file with the correct resolution to the Fax Card for sending to the remote fax modem. Once the fax is sent, The MFP System Firmware deletes (securely) both TIFF files.The fax directories on the MFP Hard Drive are accessible only by the MFP System Firmware functions that process incoming fax transmissions, process outgoing fax transmissions, or delete files. Incoming fax transmissions can only be stored, printed, and deleted. Outgoing fax transmissions can only be stored, sent to the fax card, and deleted. No other entity is permitted access to read or write to the designated fax directories. Thus, all fax data going out of the MFP is from the scanner.

3.3 Identification & Authentication

This section defines how identification and authentication is handled for secure erase and security management functionality. The MFP (in the evaluation configuration) requires an administrator to authenticate using PML objects (normally invoked from the Jetdirect NIC via SNMPv3 commands) and to provide the File System password before it will allow changes to secure erase options. The TOE compares the user-supplied password to the actual File System password object. If the passwords match, the MFP returns a result of success through PML to the Jetdirect NIC and grants access to the administrator.

The TOE is administered by a single administrative account, which holds an administrative role. Authentication occurs when the administrator provides the File System password.\The TOE allows the administrator to invoke the Secure File Erase and Secure Storage Erase functions via the PML interface. The administrator does this by sending SNMPv3 commands to the Jetdirect NIC, which converts the SNMPv3 commands to PML objects. The TOE processes the PML objects to activate the functions.

3.4 Security Management

The TOE allows for security management of Secure Erase functions by requiring restricted access through non-TOE interfaces, which are the only interfaces that can provide these

options. This ensures that the secure erase functions are executed as intended by authorized personnel. Only the authenticated and authorized system administrator can enable, disable, or configure the secure file erase or secure storage erase options.

The TOE provides only controlled access to these options. Secure Erase functions cannot be executed without the File System password provided by the authorized system administrator.

4 Assumptions, Threats, and Clarification of Scope

4.1 Usage Assumptions

The assumptions listed below are assumed to be met by the environment and operating conditions of the system.

A.NOEVIL	System administrators are competent, non-hostile, not willfully negligent, ongoing, and follow guidance for using the TOE.
A.ENVIRON	The MFP is placed in a physical environment where only trusted personnel can access it. The room in which the MFP is operating is a controlled environment where personnel are identified and authorized for access.
A.INSTALL	The TOE is delivered, installed, and setup in accordance with documented delivery and installation/setup procedures.
A.CHECKLIST	The TOE is configured according to the “HP LaserJet and Color LaserJet MFP Security Checklist.”
A.SECURE_COMMUNICATIONS	Network communications are protected and authenticated.
A.PROCEDURES	Administrators follow established procedures for access, management, administration, and monitoring of the TOE.

4.2 Threats Addressed by the TOE

The TOE addresses the following threats:

T.RESIDUAL	An authorized user may receive residual or remnant information from a previous copy, print, fax, or scan job as the result of a TOE malfunction.
T.TAMPER	An unauthorized person tampers with the TOE and accesses sensitive information from a previous copy, print, fax, or scan job.
T.IMPERSONATE	An unauthorized person gains access to TOE security management functions by impersonating an administrator.
T.FAXLINE	A malicious user attempts to access data or resources via the fax telephone line and modem using publicly available tools and equipment.

4.3 Threats Addressed by the IT Environment

TE.RECOVER	A malicious user attempts to recover document image data from a print job, a network scan job, or an email job by removing hardware, such as the HDD or the Compact Flash, using readily available tools to read its contents.
TE.TAMPER	An unauthorized person attempts to bypass the security mechanism in order to access data or assets on the MFP, to access data or assets on the network, or to disturb or disrupt routine processes on the MFP or on the network.

TE.OPERATION The execution of non-TSF processes such as copying, printing, and digital sending may interfere with TSF processes already running and cause TSF data to be modified, corrupted, or deleted by unauthorized means.

4.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- This evaluation does not verify all claims made in the product's end-user documentation. The verification of the security claims is limited to those claims made in the TOE SFRs and TOE Summary Specification (see ST sections 5.1 and 6 respectively).

- Several network protocols supported by the MFP are excluded from the TOE. Section 2.7 of the ST and Section 7 of this report provides a list of security-related options that are disabled or restricted to the evaluated configuration.

- Although the TOE requires that authorized administrative users be identified and authenticated before accessing audit/configuration information stored on the system, it only provides accountability to the granularity of the administrator role. The TOE provides a single "admin" login and all administrators login in as that role. There are no individual accounts to distinguish between administrators.

5 Architecture Information

The TOE is the MFP System Firmware that resides on Partition 1 of the Compact Flash card, which is mounted on the MFP Formatter Board. The figure below illustrates the physical boundaries and its interactions:

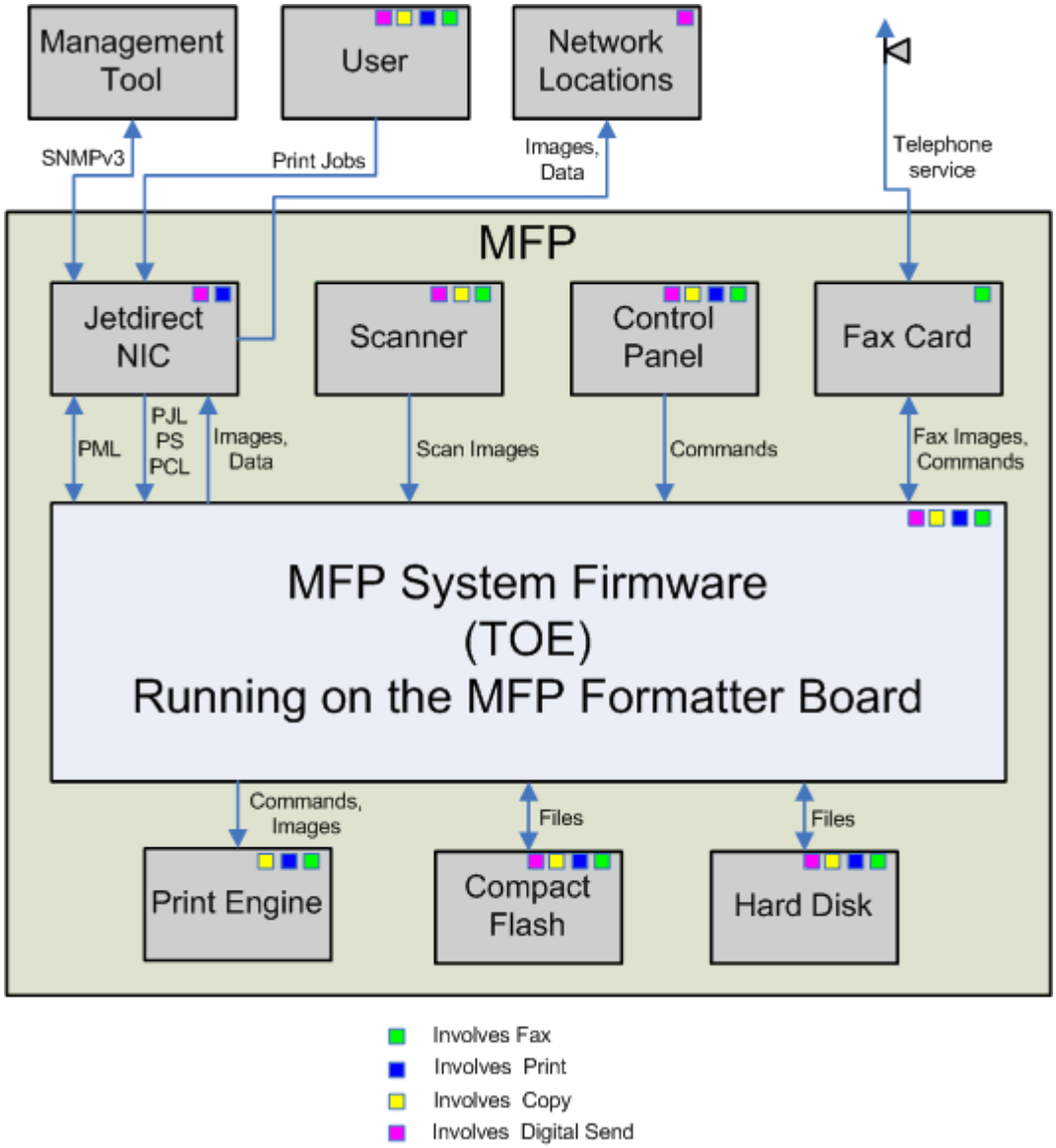

Figure 1 - MFP System Firmware

6 Evaluated Configuration

The evaluated configuration is each of the following MFPs configured according to the "*HP LaserJet and Color LaserJet MFP Security Checklist.*:"

- An HP LaserJet 9040 MFP with firmware version 08.091.3 and analog fax accessory package Q3701A
- An HP LaserJet 9050 MFP with firmware version 08.091.3 and analog fax accessory package Q3701A
- An HP LaserJet CM4730 MFP with firmware version 50.021.4 and analog fax accessory package Q3701A
- An HP LaserJet 4345 MFP with firmware version 09.091.4 and analog fax accessory package Q3701A

In each configuration, the Secure File Erase Mode is configured for Secure Fast Erase or for Secure Sanitizing Erase (as prescribed in the Security Checklist).

The following security-related options are disabled or restricted according to the HP MFP Security Checklist configuration:

- EWS disabled
- Telnet Config disabled
- SLP Config disabled
- FTP printing disabled
- LPD printing disabled
- IPP printing disabled
- MDNS config disabled
- IPV Multicast disabled
- RCFG access disabled
- IPX/SPX disabled
- AppleTalk disabled
- Printer Firmware Update disabled
- Control panel configuration options disabled
- Access via Digital Send Service disabled
- Direct ports (parallel and USB) disabled

7 Product Delivery

The TOE delivery procedure is as follows:

Factory Produced Unit (FPU)s are assembled to form Stock Keeping Units (SKU), which are the products in their basic forms ready for final assembly. SKUs are numbers given to products. SKUs are tailored into versions of the product that meet the needs of specific markets. These product versions are called bundles (thus, the multiple SKUs for each model). Bundles are created for the following reasons:

- To provide choices of configurations, such as fax, Jetdirect, and input/output bins (the evaluated version includes fax and Jetdirect)
- To provide custom features for customers with specific needs

Within the bundles or SKUs, regional options are assigned in order to provide localized versions of the final product. Here are some typical modifications for localizing a product:

- NVRAM settings such as fax country, paper size, display language, symbols, etc. are set to comply with the regional market.
- Localized printed materials (Getting Started Guides, Wall Posters, Errata's, and Control Panel Overlays) and localized CDs are added into the final box.
- Languages on boxes are localized where applicable.
- Localized power and telephony cords are added to the final box.

The HP LaserJet 9040 MFP is delivered with:

A) Digital Sending Software 4.0 disk (not evaluated)
B) HP LaserJet 9040 MFP Support Disk (not evaluated)
C) HP LaserJet 9040 MFP Start Guide
D) HP LaserJet 9040 MFP Diagram/map (not evaluated)
E) Read Me Paper

F) HP Support Paper (not evaluated)
G) Software/documentation CD
   a. Installation Notes
   b. HP LaserJet 9040 MFP User Guide
   c. HP JetDirect Administrators Guide (not evaluated)
   d. HP EWS User Guide (not evaluated)
   e. HP Driver Preconfiguration Guide (not evaluated)
H) HP LaserJet MFP Analog Fax Accessory 300 Fax Guide
I) HP LaserJet 9040 Network Install Guide
J) HP LaserJet 9040 MFP Date/Time Setting Requirements Paper.

The HP LaserJet 9050 MFP is delivered with:

A) HP LaserJet 9050 Network Install Guide
B) HP LaserJet 9050 MFP Date/Time Setting Requirements Paper
C) HP LaserJet 9050 MFP Diagram/map (not evaluated)
D) HP LaserJet MFP Analog Fax Accessory 300 Fax Guide
E) Support Flyer (not evaluated)
F) Software/documentation CD
   a. Installation Notes
   b. HP LaserJet 9050 MFP User Guide
   c. HP JetDirect Administrators Guide (not evaluated)
   d. HP EWS User Guide (not evaluated)
   e. HP Driver Preconfiguration Guide (not evaluated)
G) Getting Started Guide
H) Wall Poster (not evaluated)
I) Digital Sending Software 4.0 disk (not evaluated)
J) READ ME paper

The HP LaserJet CM4730 MFP is delivered with:

A) HP LaserJet CM4730 Network Install Guide
B) HP LaserJet CM4730 MFP Date/Time Setting Requirements Paper
C) HP LaserJet CM4730 MFP Diagram/map (not evaluated)
D) HP LaserJet MFP Analog Fax Accessory 300 Fax Guide
E) Support Flyer (not evaluated)
F) Software/documentation CD
   a. Installation Notes
   b. HP LaserJet CM4730 MFP User Guide
   c. HP JetDirect Administrators Guide (not evaluated)
   d. HP EWS User Guide (not evaluated)
   e. HP Driver Preconfiguration Guide (not evaluated)
G) Getting Started Guide
H) Wall Poster (not evaluated)
I) Digital Sending Software 4.0 disk (not evaluated)
J) READ ME paper

The HP LaserJet 4345 MFP is delivered with:

A) HP LaserJet 4345 Network Install Guide
B) HP LaserJet 4345 MFP Date/Time Setting Requirements Paper
C) HP LaserJet 4345 MFP Diagram/map (not evaluated)
D) HP LaserJet MFP Analog Fax Accessory 300 Fax Guide

E) Support Flyer (not evaluated)
F) Software/documentation CD
   a. Installation Notes
   b. HP LaserJet 4345 MFP User Guide
   c. HP JetDirect Administrators Guide (not evaluated)
   d. HP EWS User Guide (not evaluated)
   e. HP Driver Preconfiguration Guide (not evaluated)
G) Getting Started Guide
H) Wall Poster (not evaluated)
I) Digital Sending Software 4.0 disk (not evaluated)
J) READ ME paper

8 IT Product Testing

Testing was performed January 17 through January 22 2008 at the COACT facilities in Columbia, Maryland. COACT employees performed the tests.

8.1 Evaluator Functional Test Environment

Testing was performed on a test configuration consisting of the following test bed configuration.

The required hardware components are identified below.

A) HP 4345 MFP
B) PC 1 – Setup and Administration computer
C) PC 2 – Linux test computer
D) PC3 – Attack PC
E) Hub

The following software components are required for the TOE functional testing:

A) HP 4345 MFP (IP Address: 192.168.2.4)
   1) System Firmware Version 09.091.4

B) PC 1 – Setup and Administration computer
   1) Microsoft XP Professional
   2) Internet Explorer 7
   3) Web Jet Admin Version 8.1 with Service Pack 5
   4) Java 6 Standard Edition Version 1.6.0
   5) Snag It Version 8.0.0

C) PC 2 – Linux test computer
   1) Debian/Linux 4.0
   2) HP Common Criteria Test Scripts

D) PC3 – Attack PC
   1) Adobe Reader Version 8.0
   2) WinZip Version 10.0 or later
   3) NmapGUI Version 0.2Beta
   4) Snag It Version 8.0.0
   5) WireShark Version 0.99.6a
   6) Nessus Version 3.0.6.1

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

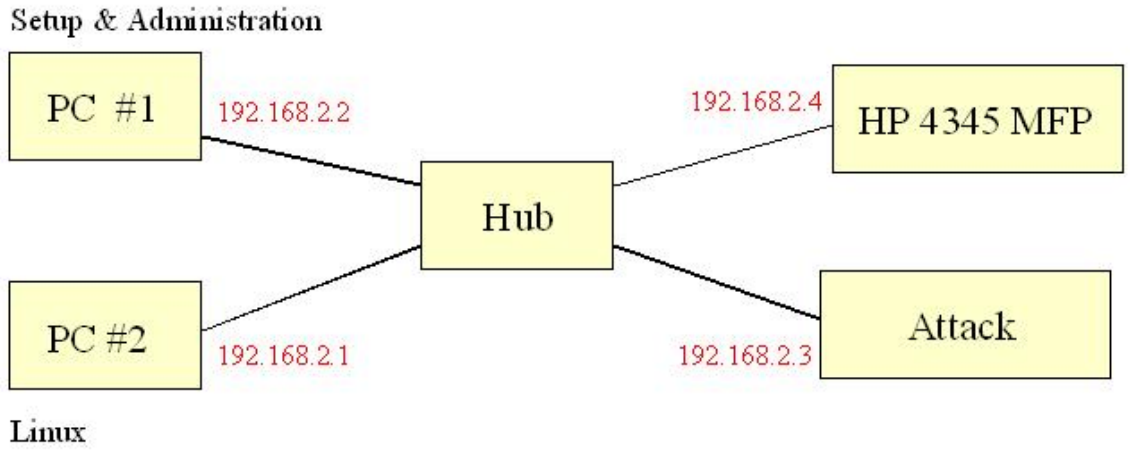

Figure 2 - Test Configuration/Setup

.

8.2 Functional Test Results

The evaluation team executed the nineteen of the twenty-nine developer functional tests. This figure is 66% of the complete developer test suite. This figure falls well with the Common Criteria recommended sample of 20%. The procedures followed to execute these tests and detail the results are presented in the CCTL proprietary report, HP LaserJet 9040 MFP System Firmware Version 08.091.3, HP LaserJet 9050 MFP System Firmware Version 08.091.3, HP LaserJet 4345 MFP System Firmware Version 09.091.4, and HP Color LaserJet CM4730 MFP System Firmware Version 50.021.4 Test Plan F3-0208-001, dated 29 February 2008.

8.3 Evaluator Independent Testing

The evaluation team selected a sample of the vendor tests to be reproduced. The tests selected validated the security functions and the TOE operational status. The purpose of this testing was to provide evidence which indicates that the TSF behaves as expected. Furthermore, this testing provides evidence that indicates that the MFP functionalities related to the TSF behave as expected. This is because the TSF is premised that the MFP, which is the platform of the TOE, correctly performs.

The test environment used for the evaluation team's independent tests was identical with the test configuration used to execute the vendor tests.

8.4 Evaluator Penetration Tests

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:

A) seclists.org
B) Irongeek.com
C) digg.com/security
D) www.securityfocus.com
E) www.antionline.com

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 indicting that the vulnerability is non-exploitable in the intended environment of the TOE.

While verifying the information found in the developer's vulnerability assessment the evaluators conducted a search to verify if additional obvious vulnerabilities exist for the TOE. Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerability.

The evaluator determined that the rationales provided by the developer indicate that the vulnerabilities identified are non-exploitable in the intended environment of the TOE.

8.5 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 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 in the final evaluated version. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

9 RESULTS OF THE EVALUATION

The evaluator devised a test plan and a set of test procedures to test the TOE's mitigation of the identified vulnerabilities by testing the MFP for selected developer identified vulnerabilities.

The results of the testing activities were that all tests gave expected (correct) results. No vulnerabilities were found to be present in the evaluated TOE. The results of the penetration testing are documented in the vendor and CCTL proprietary report, COACT document E3-0108-004, HP LaserJet 9040 MFP System Firmware Version 08.091.3, HP LaserJet 4345 MFP System Firmware Version 09.091.4, HP Color LaserJet CM4730 MFP System Firmware Version 50.021.4 Penetration Test Report, F3-0208-002 dated 29 February 2008.

The evaluation determined that the product meets the requirements for EAL 3. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by COACT Inc.

10 VALIDATOR COMMENTS

The Validators found that the evidence reviewed prior and during the Final Validation Oversight Review (VOR) supported the determination that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. Some limitations and clarifications of the evaluated product, such as the exclusion of certain network protocols, are summarized in Section 4.4 of this document. The Validators agree that the CCTL presented appropriate rationales to support the evaluation results presented in the Evaluation Technical Report for the HP LaserJet 9040 MFP System Firmware Version 08.091.3, HP LaserJet 9050 MFP System Firmware Version 08.091.3, HP LaserJet 4345 MFP System Firmware Version 09.091.4, and HP Color LaserJet CM4730 MFP System Firmware Version 50.021.4. The

Validators conclude that the evaluation and Pass result for the ST and TOE are complete and correct.

11 Security Target

Hewlett-Packard Security Target for HP LaserJet 9040 MFP System Firmware Version 08.091.3, HP LaserJet 9050 MFP System Firmware Version 08.091.3, HP LaserJet 4345 MFP System Firmware Version 09.091.4, and HP Color LaserJet CM4730 MFP System Firmware Version 50.021.4 Version 1.5, dated 07 February 2008 is incorporated here by reference.

12 List of Acronyms

CC.....Common Criteria
EAL3.....Evaluation Assurance Level 3
HDD.....Hard Disk Drive
HP.....Hewlett-Packard
IT.....Information Technology
MFP.....Multifunction Printer
NIAP.....National Information Assurance Partnership
NIC.....Network Interface Card
PML.....Printer Management Language
PP.....Protection Profile
SF.....Security Function
SFP.....Security Function Policy
SFR.....Security Functional Requirement
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