National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems

Report Number: CCEVS-VR-07-0049

Dated: 30 June 2007

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

Mike Allen (Lead Validator)

Jandria Alexander (Senior Validator)

Aerospace Corporation

Columbia, Maryland

Common Criteria Testing Laboratory

Computer Sciences Corporation

Hanover, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems, the target of evaluation (TOE), performed by Computer Sciences Corporation the Common Criteria Testing Laboratory (CCTL). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by Computer Sciences Corporation (CSC) of Hanover, MD in accordance with the United States evaluation scheme and completed on June 18, 2007. The information in this report is largely derived from the ST, the Evaluation Technical Report (ETR) and the functional testing report. The ST was written by Xerox Corporation. The evaluation was performed to conform with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.3, dated August 2005 at Evaluation Assurance Level 2 (EAL 2) and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.3, August 2005.

The TOE is a multi-function device (MFD) with the Image Overwrite Security accessory, the embedded fax accessory, and, in the Pro models, the Network Scanning accessory, all consumer options. The Overwrite Security accessory causes any temporary image files created during a print, network scan, scan-to-email, and LanFax job to be overwritten when those files are no longer needed or “on demand” by the system administrator. Copy and embedded fax jobs do not get written to the Hard Disk Device (HDD). The Network Scanning option utilizes the inherent TOE SSL support to secure the filing of scanned documents on a remote SSL-enabled server.

User image files associated with the Store Print and Scan-to-Mailbox feature may be stored long term for later reprinting. Files are stored in an encrypted partition of the hard disk. These files are overwritten automatically when deleted by the user, or when “on demand” image overwrite is executed by the system administrator.

The Xerox Embedded Fax accessory provides local analog fax capability over Public Switched Telephone Network (PSTN) connections and also enables LanFax jobs. The TOE also provides support for other network security protocols, such as IPSec and SNMPv3, to protect user data. Additionally, the TOE can be configured to filter inbound network traffic based on the provided address or port. Finally, the TOE also maintains an audit log.

To be in the evaluated configuration, the product requires that the Image Overwrite Security and SSL options be enabled.

The TOE makes use of cryptographic modules in order to fulfill some security functions. The Cryptographic modules are certified by the vendor to operate correctly. No independent certification under National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 was performed on this product. In addition, the cryptographic functions of the TOE were not evaluated further during the CC evaluation. **NOTE:** Users should ensure that they select a product that meets their needs, including FIPS 140-2 compliance, if appropriate. Also, the algorithm suite that is used within the TOE (OpenSSL, IPSec and SNMP) is **not** a certified FIPS 140 cryptographic module.

The Xerox WorkCentre / WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems models can be ordered with the following features:

Table 1: Models and Capabilities

(X – included in all configurations; O – product options ordered separately)

	Print	Copy[1]	Network Scan	Embedded Fax[1]	Scan 2 email
WorkCentre 232	x	x	n/a	o	x
WorkCentre 238	x	x	n/a	o	x
WorkCentre 245	x	x	n/a	o	x
WorkCentre 255	x	x	n/a	o	x
WorkCentre 265	x	x	n/a	o	x
WorkCentre 275	x	x	n/a	o	x
WorkCentre Pro 232	x	x	x	o	x
WorkCentre Pro 238	x	x	x	o	x
WorkCentre Pro 245	x	x	x	o	x
WorkCentre Pro 255	x	x	x	o	x
WorkCentre Pro 265	x	x	x	o	x
WorkCentre Pro 275	x	x	x	o	x

[1] Copy and embedded FAX jobs are not spooled to the HDD.

The Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems have the following software installed:

Table 2: Software

Software/Firmware Item	WorkCentre	WorkCentre + PostScript	WorkCentre Pro
System Software	**12.060.17.000**	**14.060.17.00**	**13.060.17.000**
Network Controller Software	**040.022.00115**	**040.022.10115**	**040.022.50115**
UI Software	**012.60.012**	**012.60.012**	**012.60.012**
IOT Software	**50.04.00**	**50.04.00**	**50.04.00**
SIP Software	**12.60.05**	**12.60.05**	**12.60.05**
DADH Software (Options)			
• Normal Mode	**14.00.00**	**14.00.00**	**14.00.00**
• Quiet Mode	**15.12.00**	**15.12.00**	**15.12.00**
FAX Software	**02.28.013**	**02.28.013**	**02.28.013**
Finisher Software (Options)			
• 1K LCSS	**01.27.00**	**01.27.00**	**01.27.00**
• 2K LCSS	**03.20.00**	**03.20.00**	**03.20.00**
• HCSS	**13.38.00**	**13.38.00**	**13.38.00**
• HCSS with BookletMaker	**24.10.00**	**24.10.00**	**24.10.00**
Scanner Software (Options)			
• 232/238/245/255 PPM[1] Models	**17.05.00**	**17.05.00**	**17.05.00**
• 265/275 PPM[1] Models	**04.09.00**	**04.09.00**	**04.09.00**

1.1. Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all International interpretations with effective dates on or before May 1, 2006.

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, 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 conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT 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 3 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 3: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	A) Xerox WorkCentre 232 [OR] B) Xerox WorkCentre 238 [OR] C) Xerox WorkCentre 245 [OR] D) Xerox WorkCentre 255 [OR] E) Xerox WorkCentre 265 [OR] F) Xerox WorkCentre 275 [OR] G) Xerox WorkCentre Pro 232 [OR] H) Xerox WorkCentre Pro 238 [OR] I) Xerox WorkCentre Pro 245 [OR] J) Xerox WorkCentre Pro 255 [OR] K) Xerox WorkCentre Pro 265 [OR] L) Xerox WorkCentre Pro 275
Protection Profile	None
Security Target	*Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems Security Target* Version 1.0, May 24, 2007
Dates of evaluation	December 2006 through May 2007
Evaluation Technical Report	*Evaluation Technical Report for Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems*, Version 1.0, May 24, 2007
Conformance Result	Part 2 and Part 3 EAL 2 augmented with ALC_FLR.3
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 2.3, August 2005
Common Evaluation Methodology (CEM) version	CEM version 2.3, August 2005
Sponsor	Xerox Corporation
Developer	Xerox Corporation
Evaluators	Patti Spicer, Christa Lanzisera and Gregory Bluher of Computer Sciences Corporation
Validation Team	Mike Allen and Jandria Alexander of The Aerospace Corporation

3. SECURITY POLICY

The Xerox product line identified enforces the following security policies:

3.1. Image Overwrite Policy

The WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction System models implement an image overwrite security function (Immediate Image Overwrite (IIO) and On Demand Image Overwrite (ODIO)) that causes temporary image files created during a print, network scan, scan-to-email, or LanFax job to be overwritten automatically at the completion of the job. The "On-Demand" Image Overwrite (ODIO) function can be manually invoked by the system administrator. Both IIO and ODIO use a three pass overwrite procedure as described in DODD 5800.28-M. [Copy and analog fax jobs initiated from the platen do not create files on the Network Controller HDD so no overwrite is needed for these job types.]

Once invoked, ODIO cancels all copy, print, network scan, scan-to-email, LanFax, or analog fax, jobs, halts the printer interface, and overwrites the contents of the sectors used for temporary image files on the internal hard disk drive. The entire machine then reboots. If the System Administrator attempts to activate diagnostics mode while ODIO is in progress, the request will be queued until the ODIO completes and then the system will enter diagnostic mode.

3.2. Identification and Authentication Policy

The WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction System models can identify users via a remote network authentication server. Supported authentication services include Kerberos (Solaris), Kerberos (Windows 2000), NDS (Novell 4.x, 5.x), and SMB (Windows NT.4x/2000). NOTE: The security functionality of these servers was **not** evaluated as part of this evaluation therefore the security of these servers must be certified elsewhere. The system prevents unauthorized use of the installed network options (network scanning, scan-to-email, and LanFax) unless the user is properly authenticated. To access a network service, the user is required to provide a user name and password which is then validated by the remote authentication server. (See Validator Comments on Authentication Servers, Section 10).

To authenticate the system administrator, the WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction System models utilize a simple authentication function accessible through the front panel or web interface. The system administrator must authenticate by entering a 3 to 12 digit PIN prior to being granted access to the tools menu and system administrator functions. The system administrator must change the default PIN after installation is complete. While the system administrator is entering the PIN number, the TOE displays a '*' character for each digit entered to hide the value entered. The authentication mechanism has a PIN space of 12**3 to 12**12. (See Validator PIN Comments, Section 10).

System administrators may also authenticate through a Web user interface that requires the user to enter a PIN and enter "admin" into the username field. The username prompt provided by the web server is not used, but is provided for historical reasons. The only valid string is "admin", which is

hard coded into the web server and cannot be changed. Additional users cannot be added. The TOE does not associate user attribute or privileges based on username.

3.3. Security Management

The WorkCentre/WorkCentre Pro models utilize the front panel software module security mechanisms to allow only authenticated system administrators the capability to enable or disable the TSF_IOW function, change the system administrator PIN, abort ODIO, or manually invoke "On Demand" Image Overwrite. Additionally, the WorkCentre/WorkCentre Pro models utilize the web server authentication mechanism to allow only authenticated system administrators the capability to: manually invoke "On Demand" Image Overwrite; establish a recurrence schedule for "On Demand" image overwrite; enable/disable the audit function; transfer the audit records (if audit is enabled) to a remote trusted IT product; enable/disable SSL; create/upload/download X.509 certificates; enable/disable and configure IPSec tunneling; enable/disable and configure SNMPv3, and enable/disable and configure (specify the IP address and/or IP address range (presumed), port and port range, for remote trusted IT products allowed to connect to the TOE via the network interface) IP filtering] through the SSL enhanced web interface. (See Validator Comments on IP Protocols, Section 10).

The WorkCentre/WorkCentre Pro models restrict the ability to manage administrative functions to the system administrator.

3.4. Cryptographic Support

The WorkCentre/WorkCentre Pro models utilize data encryption (RSA, RC4, DES, TDES) and cryptographic checksum generation and secure hash computation (MD5 and SHA-1), as provided by the OpenSSL cryptographic libraries, to support secure communication between the TOE and remote trusted products. Those packages include provisions for the generation and destruction of cryptographic keys and checksum/hash values and meet the following standards: 3DES – FIPS-42-2, FIPS-74, FIPS-81; MD5 – RFC1321; SHA-1 – FIPS-186, SSLv3, SNMPv3. (See Validator Comments on Cryptographic certification, Section 10).

3.5. Auditing Policy

The WorkCentre/WorkCentre Pro models generate audit logs that track events/actions (e.g., print/scan/fax job submission) to logged in users, and each log entry contains a timestamp. The audit logs are only available to TOE administrators and can be downloaded via the web interface for viewing and analysis.

The audit log tracks system start-up/shutdown, ODIO start/completion, and print, scan, email, local fax, I-Fax (not evaluated), and LanFax jobs. Copy jobs are not tracked. By adopting a policy of regularly downloading and saving the audit logs, users can satisfy the tracking requirements for transmission of data outside of the local environment, as required by such legislation as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, etc.

The Web UI presents the only access to the audit log; the audit log is not viewable from the local UI. The Web UI screen contains a button labeled "Save as Text File" that is viewable by all users. If this button is selected, and the system administrator is not already logged in through the interface, then a system administrator login alert window is presented. Once the system administrator has successfully logged in, then the audit log file becomes downloadable.

3.6. User Data Protection

The WorkCentre/WorkCentre Pro models provide support for SSL through the use of the OpenSSL cryptographic libraries, and allow the TOE to act as either an SSL server, or SSL client, depending on the function the TOE is performing. SSL must be enabled before setting up either IPSec, SNMPv3, or before the system administrator can retrieve the audit log. The SSL functionality also permits the WorkCentre/WorkCentre Pro models to be securely administered from the Web UI, as well as, being used to secure the connection between the TOE and the repository server when utilizing the remote scanning option. The TOE creates and enforces the informal security policy model, "All communications to the Web server will utilize SSL (HTTPS)." (See Validator Comments on IP Protocols, Section 10)

The WorkCentre/WorkCentre Pro models implement the IPSec SFP to ensure user data protection for all objects, information, and operations handled or performed by the TOE through the lpr and port 9100 network interfaces. Printing clients initiate the establishment of a security association with the Multi-Function Device (MFD). The MFD establishes a security association with the printing client using IPSec "tunnel mode." Thereafter, all IP-based traffic to and from this destination will pass through the IPSec tunnel until either end powers down, or resets, after which the tunnel must be reestablished. The use of IPSec tunnel mode for communication with a particular destination is based on the presumed address of the printing client.

The WorkCentre/WorkCentre Pro models utilize data encryption (AES) and cryptographic checksum generation and secure hash computation (SHA-1), as provided by the OpenSSL cryptographic libraries, to support encryption and decryption of designated portions of the hard disk where user files may be stored. Those packages include provisions for the generation and destruction of cryptographic keys and meet the following standards: AES-128-FIPS-197. (See Validator Comments on Cryptographic certification, Section 10).

3.7. Network Management Policy

The WorkCentre/WorkCentre Pro models support SNMPv3 as part of their security solution through the SNMPSec SFP. The SNMPv3 protocol is used to authenticate each SNMP message, as well as provide encryption of the data as described in RFC 3414.

As implemented, both an authentication and privacy (encryption) password must be set up both at the device and at the manager. Both passwords must be a minimum of 8 characters. SNMP uses SHA-1 for authentication and single-DES in Cipher Block Chaining mode for encryption. SNMPv3 utilizes the OpenSSL crypto library for the authentication and encryption functions. (See Validator Comments on IP Protocols, Section 10).

3.8. Network Management Policy

The WorkCentre/WorkCentre Pro models implement a static, host-based firewall that limits network access to the device. The system administrator can control access based on source IP address and/or protocol/port. Access rules can be administered via a secure interface provided by the Web UI.

3.9. Fax-Network Separation

The WorkCentre/WorkCentre Pro models have an architecture that provides separation between the optional FAX processing board and the network controller. This architecture ensures that a malicious user cannot access network resources from the telephone line via the system's optional FAX modem.

4. ASSUMPTIONS

4.1. Physical Security Assumptions

A key environmental assumption is physical security, for it is assumed appropriate physical security protection will be applied to the TOE hardware and software commensurate with the value of the IT assets. Specifically, the TOE is assumed to be located within a facility providing controlled (i.e., employee-only) access to prevent unauthorized physical access to internal parts of the TOE and the TOE serial port.

4.2. Personnel Security Assumptions

It is assumed that all authorized administrators are properly trained, not careless, not willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

4.3. Operational Security Assumptions

It is assumed that all components connected to the network to which the TOE is connected pass data correctly without modification. It is also assumed that the systems that connect to the TOE are under the same management and physical control as the TOE. It is assumed that remote trusted IT entities that communicate with the TOE implement the external half of the communication protocol in accordance with industry standard practice with respect to RFC/other standard compliance (i.e., SSL, SSH, IPSec, SNMPv3) and work as advertised.

4.4. Threats Countered and Not Countered

The TOE is designed to fully or partially counter the following threats:

T.RECOVER	A malicious user may attempt to recover temporary document image data from a print/network scan/email/LanFax job by removing the HDD and using commercially available tools to read its contents. This scenario may occur as part the life-cycle of the MFD (e.g., decommission) or as a more overt action.
T.COMM_SEC	An attacker may break into a communications link between the TOE and a remote trusted IT product in order to intercept, and/or modify, information passed to/from/between the TOE and remote trusted IT product.
T.FAXLINE	A malicious user may attempt to access the internal network (to access data and/or resources) via the FAX telephone line/modem using publicly available tools and equipment (the threat agent does not have access to specialized digital/analog telephone/modem/computer/etc. equipment).

4.5. Organizational Security Policies

The following are applicable organizational security policies:

P.COMMS_SEC	TOE supported network security mechanisms (i.e., HTTPS, IPSec ESP and/or AH, SNMPv3, IP filtering) shall be employed per, and in accordance with, local site security policy.
P.HIPAA_OPT	(Appropriate to organizations under HIPAA oversight) All audit log entries (scan) will be reviewed periodically (the period being local site specific and to be determined by the local audit cyclic period) and in accordance with 45 CFR Subtitle A, Subchapter C, Part 164.530(c),(e),(f) which covers safeguards of information (c), sanctions for those who improperly disclose (e), and mitigation for improper disclosures (f).
P.SSL_ENABLED	Secure Socket Layer network security mechanisms shall be supported by the TOE and enabled.

5. ARCHITECTURAL INFORMATION

5.1. Logical Scope and Boundary

The TOE logical boundary is composed of two distinct security approaches: the architecture of the TOE, and the security functions provided by the TOE.

Architecturally, the TSF cannot be bypassed, corrupted, or otherwise compromised. Whereas the TOE is an MFD and not a general purpose computer, there are no untrusted subjects, or processes, contained therein, and the TSF functions in its own domain (Security Architecture – TSF_ARCH). While not a TSF in the classic sense of the term, the functionality that would be associated with TSF_ARCH is present and represented by the security functional requirements (SFRs) FPT_RVM.1 and FPT_SEP.1 based strictly on the TOE definition and architecture.

The following security functions are controlled by the TOE:

- Image Overwrite (TSF_IOW)
- System Authentication (TSF_SYS_AUT)
- Network Identification (TSF_NET_ID)
- Security Audit (TSF_FAU)
- Cryptographic Support (TSF_FCS)
- User Data Protection – SSL (TSF_FDP_SSL)
- User Data Protection – IP Filtering (TSF_FDP_FILTER)
- User Data Protection – IPSec (TSF_FDP_IPSec)
- Network Management Security (TSF_NET_MGMT)
- FAX Flow Security (TSF_FAX_FLOW)
- Security Management (TSF_FMT)
- User Data Protection - AES (TSF_EXP_UDE)

5.1.1. Image Overwrite (TSF_IOW)

The TOE implements an image overwrite security function, through the Image Overwrite Security accessory, to overwrite temporary files created during the printing, network scan, scan-to-email, and LanFax processes. Temporary files are created as a result of this processing on a reserved section of the hard disk drive. Copy and local FAX jobs do not get written to the HDD. Once the job has completed, the files are automatically overwritten using a three pass overwrite procedure as described in DOD 5200.28-M (Immediate Image Overwrite (IIO) and "On-Demand" Image Overwrite (ODIO)). The overwrite patterns used for stored jobs are the same patterns specified by 5200.28-M; however, since the patterns are written through the encryption algorithm, they get written to the disk as randomized data. The TSF_IOW function, ODIO, can also be invoked manually by the system administrator. A scheduling function allows ODIO to be executed on recurring basis as set up by the System Administrator.

The ODIO is invoked by the System Administrator via the tools menu/web interface. Once invoked, the ODIO cancels all jobs, halts the network interface, and overwrites the contents of the reserved section on the hard disk (it utilizes the same three-pass procedure identified above), and then the network controller reboots. If the System Administrator attempts to activate diagnostics mode while ODIO is in progress, the request will be queued until the ODIO completes and then the system will enter diagnostic mode.

5.1.2. System Authentication (TSF_SYS_AUT)

The TOE utilizes a simple authentication function through the front panel or web interface. The system administrator must authenticate by entering a 3 to 12 digit PIN prior to being granted access to the tools menu and system administration functions (**NOTE**: Xerox security guidance documentation specifies the use of a PIN between 8 and 12 digits). The system administrator must change the default PIN after installation is complete. While the system administrator is entering the PIN number, the TOE displays a '*' character for each digit entered to hide the value entered.

The Web user interface also requires the system administrator to enter a PIN and enter "admin" into the username field. Additional users cannot be added. The TOE does not associate privileged-user attributes or privileges based on username.

5.1.3. Network Identification (TSF_NET_ID)

The TOE can prevent unauthorized use of the installed network options (network scanning, scan-to-email, and LanFax); the network options available are determined (selectable) by the system administrator. To access a network service, the user is required to provide a user name and password, which is then validated by the designated authentication server (a trusted remote IT entity). The user is not required to login to the network; the account is authenticated by the server as a valid user. The remote authentication services supported by the TOE are: LDAP v4, Kerberos (Solaris), Kerberos (Windows 2000), NDS (Novell 4.x, 5.x), and SMB (Windows NT.4x/2000). (See Validator Comments on Authentication Servers, Section 10).

5.1.4. Security Audit (TSF_FAU)

The TOE generates audit logs that track events/actions (e.g., print/scan/fax job submission) to users (based on network login). The audit logs, which are stored locally in a 15000 entry circular log, are available to TOE administrators and can be exported for viewing and analysis. SSL must be configured in order for the system administrator to download the audit records; the downloaded audit records are in comma separated format so that they can be imported into an application such as Microsoft Excel™.

5.1.5. Cryptographic Operations (TSF_FCS)

The TOE utilizes data encryption (RSA, RC4, DES, TDES) and cryptographic checksum generation and secure hash computation (MD5 and SHA-1), as provided by the OpenSSL cryptographic libraries, to support secure communication between the TOE and remote trusted products. Those packages include provisions for the generation and destruction of cryptographic keys and checksum/hash values and meet the following standards: 3DES – FIPS-42-2, FIPS-74, FIPS-81; MD5 – RFC1321; SHA-1 – FIPS-186, SSLv3, SNMPv3.

5.1.6. User Data Protection – SSL (TSF_FDP_SSL)

The TOE provides support for SSL through the use of the OpenSSL cryptographic libraries, and allows the TOE to act as either an SSL server, or SSL client, depending on the function the TOE is performing (SSLSec SFP). SSL must be enabled before setting up either IPSec, SNMPv3, or before the system administrator can retrieve the audit log. The SSL functionality also permits the TOE to be securely administered from the Web UI, as well as being used to secure the connection between the TOE and the repository server when utilizing the remote scanning option. If the system administrator-managed function is enabled, then the TOE creates and enforces the informal security policy model, "All communications to the Web server will utilize SSL (HTTPS)." (See Validator Comments on IP Protocols, Section 10).

5.1.7. User Data Protection – IP Filtering (TSF_FDP_FILTER)

The TOE provides the ability for the system administrator to configure a network information flow control policy based on a configurable rule set. The information flow control policy (IPFilter SFP) is generated by the system administrator specifying a series of rules to "accept," "deny," or "drop" packets. These rules include a listing of IP addresses that will be allowed to communicate with the TOE. Additionally rules can be generated specifying filtering options based on port number given in the received packet.

5.1.8. User Data Protection – IPSec (TSF_FDP_IPSec)

The TOE implements the IPSec SFP to ensure user data protection for all objects, information, and operations handled or performed by the TOE. Printing clients initiate the establishment of a security association with the MFD. The MFD establishes a security association with the printing client using IPSec "tunnel mode." Thereafter, all IP-based traffic to and from this destination will pass through the IPSec tunnel until either end powers down, or resets, after which the tunnel must be reestablished. The use of IPSec tunnel mode for communication with a particular destination is based on the presumed address of the printing client.

5.1.9. Network Management Security (TSF_NET_MGMT)

The TOE supports SNMPv3 as part of its security solution (SNMPSec SFP). The SNMPv3 protocol is used to authenticate each SNMP message, as well as, provide encryption of the data as described in RFC 3414. (See Validator Comments on IP Protocols, Section 10).

5.1.10. FAX Flow Security (TSF_FAX_FLOW)

The TOE is architected to provide separation between the optional FAX processing board and the network controller.

The FAX card plugs directly into the PCI bus of the SIP (Scanner Image Processor) board with the SIP acting as the PCI bus master. The SIP communicates with the network controller via the industry standard FireWire interface, but it is the SIP/FAX interface that provides TSF_FAX_FLOW.

There are two methods of communication between the SIP and the FAX – Command/Response and Image data transfer. Commands and Responses are sent and received via a shared memory block on the FAX card. Image data is transferred using DMA transfer with the SIP acting as the bus master. For outgoing fax the SIP will push image data to the FAX card. For incoming fax the SIP will pull image data from the FAX. The FAX card will inform the SIP when there is a FAX available for collection. Similarly, the SIP will inform the FAX card when it wishes to send a fax out.

5.1.11. Security Management (TSF_FMT)

The TOE restricts access to the configuration of administrative functions to the system administrator by implementing the PrivUserAccess SFP. Under this SFP, the TOE utilizes the front panel software module security mechanisms to allow only the authenticated system administrator the capability to:

- Enable or disable the TSF_IOW function;
- Change the system administrator PIN;
- Abort ODIO;
- Manually invoke “On Demand” Image Overwrite.

The SFP also controls the Web UI connected over a secure connection (https) to allow only the system administrator, the PrivUserAccess SFP, to manage the following security functions:

- Manually invoke “On Demand” image overwrite;
- Establish a recurrence schedule for “On Demand” image overwrite;
- Enable/disable SSL support;
- Enable/disable and configure IPSec tunneling;
- Enable/disable and configure SNMPv3;
- Create/install X.509 certificates;
- Enable/disable and download the audit log;
- Enable/disable and configure (rules) IP filtering.

As indicated above, SSL must be enabled and configured before the system administrator can utilize the secure Web UI to manage IPSec and SNMPv3, and to download the audit log.

5.1.12. User Data Protection - AES (TSF_EXP_UDE)

The TOE utilizes data encryption (AES) and cryptographic checksum generation and secure hash computation (SHA-1), as provided by the OpenSSL cryptographic libraries, to support encryption

and decryption of designated portions of the hard disk where user files may be stored. Those packages include provisions for the generation and destruction of cryptographic keys and meet the following standards: AES-128-FIPS-197.

5.2. Physical Scope and Boundary

The TOE is a Multi-Function Device, shown in **Error! Reference source not found.** Figure 1, which performs printer, copier, scanner, LanFax, embedded analog FAX (optional), and email functions.

The physical scope and boundary of the TOE consists of the Xerox WorkCentre or WorkCentre Pro devices and include installed Xerox accessories. For this evaluation, all models of the TOE will include the Image Overwrite Security accessory and the embedded FAX accessory. In the WorkCentre Pro models the Network Scanning accessory (a software component) is included in the configuration.

*** Also shown are optional paper feeder and finisher**

Figure 1: Physical Boundary

The TOE physical boundary also consists of the Administrative and User Guidance provided on CDs with the device, as well as the Secure Operation guidance provided to consumers through the Xerox web site (www.xerox.com).

6. DOCUMENTATION

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems. Note that not all evidence is available to customers. The following documentation is available to the customer:

- Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems Administrator and User Guidance CD Pack (delivered with the TOE)
- Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems "Read Me First" Flier (delivered with the TOE)
- Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems Secure Operations Guidelines (available at http://www.xerox.com/security)
- Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems Security Target, Version 1.0 (available at the NIAP website)

The remaining evaluation evidence is described in the Evaluation Technical Report developed by Computer Sciences Corporation.

7. IT PRODUCT TESTING

This section describes the testing efforts of the Developer and the evaluation team.

7.1. Developer testing

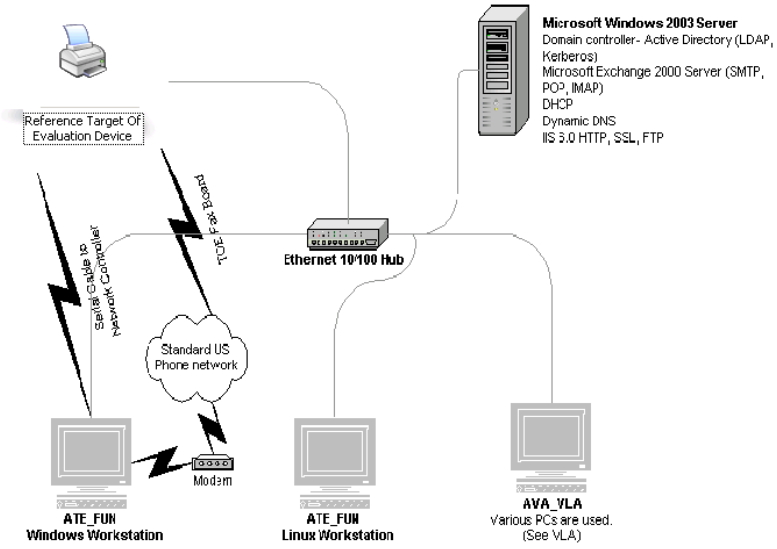
Test procedures were written by the Developer and designed to be conducted using manual interaction with the TOE interfaces. The developer tested 56 of the 165 interfaces to the TOE and in doing so tested all TSFs. A number of system administrator functions were not exercised, but these represent voluntary manual reconfigurations of the TOE and/or its network identity and are not relevant to the security functions of the TOE.

The Developer tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. The Developer's approach to testing is defined in the TOE Test Plan. The expected and actual test results (ATRs) are also included with each of the tests in the TOE Test Procedures. Each test case was assigned an identifier that was used to reference it throughout the testing evidence.

The evaluation team analyzed the Developer's testing to ensure adequate coverage for EAL 2. The evaluation team determined that the Developer's actual test results matched the Developer's expected test results.

The following diagram depicts the test environment that was used by the Developers. The Evaluators assessed that the test environment used by the Developers was appropriate and mirrored a portion of this test configuration during Independent testing.

TOE Environment



7.2. Evaluation team independent testing

The evaluation team conducted independent testing at the CCTL. The TOE was delivered and installed by the Developer. The evaluation team configured the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE while performing work unit ATE_IND.2-2. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Developer's Test Plan as a basis for creating the Independent Test Plan. The evaluation team analyzed the Developer's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions that implement critical security features
- Security functions critical to the TOE's security objectives
- Security functions that gave rise to suspicion regarding the behavior of the security features during the documentation evidence evaluation
- Security functions not tested adequately in the vendor's test plan and procedures

The evaluation team repeated a portion of the Sponsor's test cases and designed additional independent tests. The additional test coverage was determined based on the analysis of the Developer test coverage and the ST.

Each TOE Security Function was exercised at least once, and the evaluation team verified that each test passed.

The security functional requirements in Table 4 were either not tested, or were only partially tested. All other security functional requirements found in the ST were tested by the evaluation team.

Table 4: Not Tested/Partially Tested Requirements

SFR	Rationale
FAU_STG.4	The TOE audit storage capacity is fairly large and the evaluation would not feasibly be able to generate enough audit log entries to exhaust the audit storage capacity.
FCS_CKM.1 (1)	Partially tested by tests that utilized SSL.
FCS_CKM.1 (2)	Partially tested by tests that utilized SSL.
FCS_CKM.2 (1)	Partially tested by tests that utilized SSL.

FCS_CKM.2 (2)	Partially tested by tests that utilized SSL.
FCS_COP.1 (1)	Partially tested by tests that utilized SSL.
FCS_CKM.1 (3)	Partially tested by tests that utilized IPSec.
FCS_COP.1 (3)	Partially tested by tests that utilized IPSec.
FCS_CKM.1 (4)	Partially tested by tests that utilized SNMPv3.
FCS_CKM.4	Partially tested by tests that utilized SSL, IPSec, SNMPv3.

7.3. Vulnerability analysis

The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the Developer Strength of Function analysis, the Developer Vulnerability Analysis, and the evaluation team's Vulnerability Analysis, and the evaluation team's performance of penetration tests.

The Developer performed a Vulnerability Analysis of the TOE to identify any obvious vulnerability in the product and to show that it is not exploitable in the intended environment for the TOE operation. In addition, the evaluation team conducted a sampling of the vulnerability sites claimed by the Sponsor to determine the thoroughness of the analysis.

Based on the results of the Developer's Vulnerability Analysis, the evaluation team devised penetration testing to confirm that the TOE was resistant to penetration attacks performed by an attacker with an expertise level of unsophisticated. The evaluation team conducted testing using the same test configuration that was used for the independent team testing. In addition to the documentation review used in the independent testing, the team used the knowledge gained during independent testing as well as knowledge of publicly available vulnerability information to devise the penetration testing. This resulted in a set of six penetration test areas:

- Background information scanning
- Postscript program execution
- WebUI bypass and misuse
- General resource abuse and denial of service
- Jet Direct misuse and exploitation
- NetBios misuse and exploitation

8. EVALUATED CONFIGURATION

The evaluated configuration of the Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems, as defined in the Security Target, consists of the either a WorkCentre/ WorkCentre Pro 232/238/245/255/265/275 with the Image Overwrite accessory and SSL enabled, and the Embedded Fax present. Please see the Security Target for the TOE's hardware and software components.

The Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems must be configured in accordance with the following Guidance Documents:

- Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Administrator and User CD Pack
- Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems Secure Operations Guidelines (http://www.xerox.com/security)

9. RESULTS OF THE EVALUATION

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 2.3. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.3.

Computer Sciences Corporation has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 2 augmented with ALC_FLR.3. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished on May 29, 2007. A final Validation Oversight Review (VOR) was held on June 18, 2007 and final changes to the VR were completed on June 30, 2007.

10. VALIDATOR COMMENTS

The validation team's observations support the evaluation team's conclusion that the Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems meet the claims stated in the Security Target. The validation team also wishes to add the following caveats to the use of the product and the evaluated configuration.

10.1. Cryptographic Module Certification

The products make use of cryptographic modules in order to fulfill some security functions. The Cryptographic modules used in these products are certified by the vendor and **not** certified under the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 nor certified by Computer Sciences Corporation. Users of these products should ensure that their certification requirements can be satisfied by a product that does not include FIPS 140-2 certified encryption.

10.2. Internet Protocol Certification

These products make use of several internet protocols for remote communication with the devices (SSL, IPSec, SNMPv3, etc.). These protocols, while used during testing, were not confirmed to operate completely in accordance with the appropriate RFC by the CCTL. That is, not all optional parameters specified in the RFC's were tested; therefore the protocols remain self-certified by the vendor.

10.3. System Administrator's PIN Complexity

The complexity of the System Administrator's PIN is limited to twelve characters (0-9, #, *) provided by the device. Users of the products need to ensure that their security "password/PIN" requirements can be satisfied by the twelve-character PIN used on these products.

10.4. Authentication Server Certification

These products make use of an authentication server for some Identification and Authentication functions in support of the TOE. None of these identified supported servers were evaluated as part of this evaluation. The strength of the security of these servers must be determined elsewhere.

11. ANNEXES

None

12. SECURITY TARGET

Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems Security Target, Version 1.0, May 24, 2007.

13. GLOSSARY

- **Administrator:** Role applied to user with full access to all aspects of the Xerox WorkCentre/ WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems. Member of Administrative Users definition.
- **Administrative Users:** This term connotes within this ST an administrative user of the Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems. Members of this grouping term include: Administrator.
- **Attack:** An attack is an exploited threat or an attempt to bypass security controls on a computer. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.
- **Authentication:** Verification of the identity of a user.
- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so

forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14. BIBLIOGRAPHY

1.) Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 2.3, August 2005. CCMB-2005-08-001.

2.) Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements, Version 2.3, August 2005. CCMB-2005-08-002.

3.) Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements, Version 2.3, August 2005. CCMB-2005-08-003.

4.) Common Criteria Project Sponsoring Organisations. Common Criteria Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005 CCMB-2005-08-004.

5.) Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

6.) Xerox Corporation/Computer Sciences Corporation. *Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems Security Target* Version 1.0, May 24, 2007

7.) Computer Sciences Corporation. *Evaluation Technical Report Xerox WorkCentre/WorkCentre Pro 232/238/245/255/265/275 Multifunction Systems*, Version 1.0, May 29, 2007.