

Common Criteria Evaluation

Questions & Answers Xerox and Sharp

Xerox Advanced Multifunction Systems

WorkCentre M35/M45/M55

WorkCentre Pro 35/45/55/65/75/90

WorkCentre Pro C2128/C2636/C3545 Color

CopyCentre 65/75/90

CopyCentre C2128/C2636/C3545 Color

Prepared by:

Larry Kovnat and Betty Ingerson
Xerox Office Group
1530 Jefferson Road – Mail Stop 801-25B
Rochester, New York 14623
USA

©2005 by XEROX CORPORATION. All rights reserved.

Copyright protection claimed includes all forms and matters of copyrightable material and information now allowed by statutory judicial law or hereinafter granted, including without limitation, material generated from the software programs which are displayed on the screen such as icons, screen displays, looks, etc.

Printed in the United States of America.

XEROX® and all Xerox product names mentioned in this publication are trademarks of XEROX CORPORATION. Other company trademarks are also acknowledged.

Changes are periodically made to this document. Changes, technical inaccuracies, and typographic errors will be corrected in subsequent editions.

When it comes to security certification, Xerox believes that a complete system certification provides a better assessment of security than one limited to only a component or kit. This document explains the rationale for this strategy compared to competitive approaches.

Xerox currently has the broadest array of Common Criteria Certified multifunction products in the industry, covering products from 35 to 90 pages per minute:

- WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55
- CopyCentre 65/75/90 and WorkCentre Pro 65/75/90
- CopyCentre C2128/C2636/C3545 and WorkCentre Pro C2128/C2636/C3545, the first color products in the industry to receive Common Criteria Certification.

Also:

- WorkCentre 232/238/245/255/265/275 and WorkCentre Pro 232/238/245/255/265/275, Xerox' newest multifunction products offering the most comprehensive set of security functionality in the industry are currently listed on the NIAP products in evaluation list at: http://niap.nist.gov/cc-scheme/in_evaluation.html#x

All of these Xerox products are certified in the United States under the auspices of the National Information Assurance Partnership (NIAP).

Q: Xerox receives EAL2 Common Criteria Certification (CCC) for its products. Sharp announced that they received EAL4 Certification for the AR-FR4/AR-FR5 Data Security Kit. Doesn't higher a higher EAL mean that the product is more secure?

A: Achieving a higher EAL says little about the security functionality offered by the product or the security of the other subsystems that make up an MFD. The scope of a Common Criteria evaluation varies by manufacturer. Some manufacturers have been able to achieve higher EALs by limiting the scope of the evaluation to only a subset of functions. Xerox is the only manufacturer to certify complete products, not kits or subsets of functionality. The AR-FR4/AR-FR5 Data Security Kit includes only a subset the total MFD functionality.

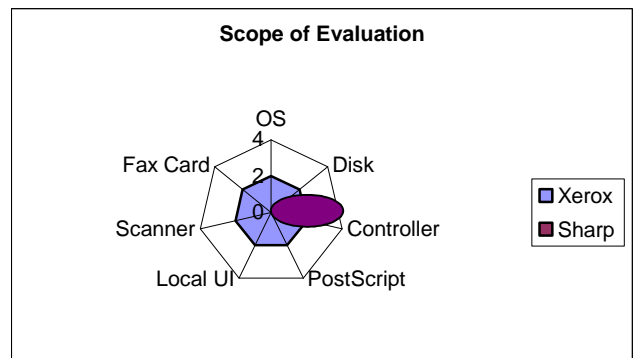
Q: Doesn't the kit control the security functions?

A: Yes, but because it is a subset of the entire MFD functionality, it does not include other potentially vulnerable subsystems.

Q: Are you saying that Sharp excludes potentially vulnerable subsystems from its evaluations?

A: Yes. The easiest way to show the difference is with this graph.

The major subsystems that make up a



Multifunctional Device are labeled on the spokes of the chart. Sharp's certification examined a limited configuration of the controller only. (For example, PostScript was not included.) Sharp chose to look

deeper at one part of the MFD system. Xerox took amore comprehensive approach by including the entire product in the evaluation.

The evaluation assurance level provides an indication of the relative depth to which the developer's documentation is examined. There is more to a Common Criteria (CC) evaluation than the assurance level however. Equally important is the scope of the evaluation or what functionality was actually evaluated. In Sharp's case, only the device controller was evaluated. Xerox had the entire product evaluated.

Q: When you say the entire product was evaluated, what does that mean?

A: Xerox believes that a complete system certification provides a better assessment of security than one limited only to a component or kit. The Target of Evaluation (TOE)¹ or certification scope on the WorkCentre and WorkCentre Pro products includes the Network Controller, the Scanner, the User Interface, and the Marking Engine. Other major components are the PostScript printing subsystem, the Operating System, the internal disk drive, and the Web User Interface. The certification achieved covered the entire device, therefore all of these components were included and tested during the evaluation.

Q: Does every component that is included in the evaluation get tested?

A: Yes, every component of a system that is included in an evaluation is tested for security. If a component is excluded from the evaluation, then it is simply not tested. Evaluating part of a system could mean that other components of the system may contain security flaws that were simply not

tested in the evaluation process. For example, a building may have several security systems such as fire alarms, sprinklers, security access cards, and camera systems. The Xerox security certification tested all aspects of security within the building. The Sharp evaluation tested only one aspect of security.

Q: Are the products to which the AR-FR4/AR-FR5 kits apply still being sold?

A: No. A kit must be evaluated within specific product embodiments. According to the rules of the Common Criteria, if the surrounding system is changed or modified, the kit must be re-evaluated within the new operational environment. The products specified in the AR-FR4/AR-FR5 Security Target are no longer sold in the US.²

Q: Does Sharp have other certifications?

A: Sharp recently received EAL3 certifications for the AR-FR11 and AR-FR12 Data Security Kits.

Q: Can you describe the differences between an EAL2 and EAL3 evaluation?

A: To understand Common Criteria evaluations, you must understand that the evaluations are broken down into seven major assurance classes. Depending on the evaluation level sought, different components of each of these classes is evaluated. The following is a highly condensed summary of the Common Criteria assurance requirements. We will discuss them in the order in which the CC describes them.

1. Configuration Management (CM). CM examines the vendor's CM plan, process, and systems. At EAL2, the CC requires that the vendor use a CM system, and keep track of the configuration items that make up the system. EAL3 adds access control

¹ "Target of Evaluation (TOE) – An IT product or system and its associated guidance documentation that is the subject of an evaluation." See Common Criteria for Information Security Evaluation, Part 1: Introduction and General Model, January 2004, Version 2.2, Revision 256, CCIMB-2004-01-001, pg. 16

² "Sharp Digital Multifunction Device Data Security Kit AR-FR4/AR-FR5", http://www.ipa.go.jp/security/jisec/jisec_e/documents/c0018_est.pdf, Table 3, pg. 4

requirements to the CM system (e.g., who is authorized to make changes), and the requirements for a documented CM plan.

All Xerox factories have received ISO9000 certification, which includes CM requirements. Since Xerox already had received ISO9000 certification, we decided that it was more important to focus on the security operation of the devices being evaluated, rather than to spend any time or expense reevaluating our CM system.

2. Delivery and Operation. Delivery and Operation looks at the procedures for delivering the product from the developer's factory to the end user, and at the procedures for securely installing the device. There are no differences between EAL2 and EAL3 in the D&O class.
3. Development. The developer's design documentation is examined in the Development class. At EAL2 the evaluators check that the developer has used a hierarchical design process, that the system is subdivided into its constituent subsystems, and that all of the external interfaces of the system are documented as to their relevance to security. At EAL3, the internal interaction between subsystems is examined in more detail. The fact that every external interface to the device must be analyzed for relevance to security is extremely important. Since Xerox included the entire device in the evaluation, not only the obvious interfaces such as connectors were examined, but also every protocol that operates over those connectors. Also, every user command that can be entered either at the Local UI or Web UI was examined for relevance to security. In contrast, Sharp limited the TOE to the controller software only. Again, this allows Sharp to assume that the other parts of the system are mediating user

and data inputs for correctness before those commands or data reach the controller. However, since those components are outside of the scope of evaluation, they are never tested for possible compromise. In the Xerox case, every interface, command, and input channel is tested for its resistance to attack or compromise.

4. Guidance Documents. The Guidance class looks at the User and System Administration manuals that the developer provides to the customer. The intent of this class is to ensure that the customer understands the proper use and administration procedures necessary to maintain the security the device. There are no differences between EAL2 and EAL3 in the Guidance class.
5. Life Cycle Support. Life cycle support is not required at EAL2. At EAL3 the evaluators will check the developer's control of the development environment to make sure that only authorized personnel have access to the designs or components during manufacturing.

In 1989 Xerox won the Malcolm Baldrige National Quality Award. Xerox would never have been able to receive such a prestigious award without procedures such as those required by the CC Life Cycle Support assurance class. Again, we decided that it would be better to devote our resources to providing a complete certification. Customers can be assured that Xerox has world-class personnel and IT policies and procedures in place, as evidenced by a long string of industry and quality awards since receiving the NQA.

6. Tests. Simply put, the Testing class verifies that the security functions operate as designed. At EAL2, that means that all of the external interfaces (i.e., user commands, data inputs) are tested to insure that they operate as intended. EAL3 adds an analysis of the

testing to make sure that every security function described in the developer's functional specification maps to a specific test case, and also, that these test cases are sufficient to show that the interfaces between subsystems as defined in the developer's high-level design operate as intended.

By limiting the scope of the evaluation, Sharp limited the number and complexity of the test cases that needed to be developed and analyzed. As previously stated, Xerox tested all of the user and data inputs of the device (literally hundreds of commands and interfaces). In the Sharp case, the evaluation shows that the testing of the controller was formally complete. However, it was limited to the controller only. All of the other inputs of the machine were outside of the scope of evaluation, and were simply assumed to operate correctly.

7. Vulnerability Assessment. The vulnerability class is where penetration testing is done. The entire Xerox system was subjected to penetration testing. At EAL3, this class adds a requirement to analyze the user and system administration documentation for misleading or confusing information. Again, since we included the entire product in the evaluation, all of the functions of the device, and all of the corresponding instructions, would have had to be analyzed. In Sharp's case, the evaluation is limited to the controller, and is further limited only to the enablement and disablement of the Overwrite function. Examining the documentation to enable or disable the Overwrite function cannot be compared to examining the entire package of user and system administration documentation that Xerox provides with its devices.

Q: What did Sharp include and exclude in their evaluation?

A: Sharp's Data Security Kits replace a portion of the controller firmware with new software that adds the disk overwrite function. Sharp does NOT include the Scanner, User Interface, Network Interface, Marking Engine, Fax Interface, or PostScript in the evaluation³.

Q: What is the significance of leaving PostScript out of the evaluation?

A: PostScript is the industry standard page description language. It is in fact a powerful scripting language, and as such, it can be abused by attackers to gain unauthorized access to confidential data. Many exploits against PostScript have been published and are easily available through the web. Sharp excludes PostScript, leaving one of the most popular attack paths for MFD's untested in its products.

Q: Did the evaluators test Sharp's Overwrite function to show that it worked as designed?

A: Yes, both the vendor and the evaluators are required to test the function and show that it operates correctly. Because the scope of the evaluation is limited however, PostScript is excluded from any of the test configurations.

Q: What is penetration testing?

A: Penetration testing is performed by the evaluators to show that "...the TOE is resistant to penetration attacks performed by an attacker."⁴ A penetration attack is an attempt to get access to the multi-function system in order to create a Denial of Service condition, or worse, to execute malicious code that could compromise or

³ Security Targets for Sharp Data Security Kits are available on the Certified Products List of the Japan Information Technology Security Evaluation and Certification Scheme (JISEC), http://www.ipa.go.jp/security/jisec/jisec_e/certfy_list200504.html.

⁴ Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, January 2004, Version 2.2, Revision 256, CCIMB-2004-01-003, pg. 161

destroy data. The intent of penetration testing is to verify that vulnerabilities do not exist in all parts of the system included in the evaluation, not just in the claimed security functions. Any parts of the system that are excluded from the scope of the evaluation by the assumptions made in the Security Target are exempt from penetration testing.

Q: *Is more strenuous penetration testing required at the higher EAL level?*

A: No, the strenuousness and intrusiveness of penetration testing is the same at both EAL2 and EAL3.

Q: *What standards govern the overwrite algorithm?*

A: The Xerox Image Overwrite Security feature complies with DoD 5200.28-M, which specifies an overwrite algorithm. This directive was cancelled when DoD Directive 8500.1 was issued. However, the DoD never issued a replacement overwrite algorithm. Therefore Xerox continues to comply with the previous standard until such time as the DoD specifies a new algorithm.

Sharp's image overwrite algorithm is proprietary.

Q: *Is the Xerox Overwrite feature available on other machines?*

A: Yes, the same Image Overwrite Security feature is available on the CopyCentre C65/C75/C90, WorkCentre M35/M45/M55, and WorkCentre Pro 35/45/55/65/75/90. The Image Overwrite Security feature is also available on the CopyCentre C2128/C2636/C3545 Color Copier and WorkCentre Pro C2128/C2636/C3545 Color Advanced Multifunction System.

Q: *Did Xerox evaluate the Fax function?*

A: Yes, Xerox is the only manufacturer with a CC certification proving that there is complete separation between the Fax telephone interface and Network interface.

Q: *Why is it important to maintain separation between the fax and network interfaces?*

A: There is the risk that an enterprise's network could be compromised through the fax connection, circumventing the firewalls and routers that provide the perimeter defense for the network. In fact, many government and government contractor facilities prohibit the enablement of both functions in any single MFD. The CC certification means that the Xerox product has been tested by an independent third-party and shown to be immune to attacks of this type.

Q: *Xerox periodically issues software patches for its products. What prompted those?*

A: Xerox is the only copier or multifunction vendor that has an active security patch program. Security patches are posted on the Security@Xerox website. Xerox is committed to continually test its products and upgrade the software when security vulnerabilities are discovered. No other manufacturer makes the same level of commitment.

Q: *What new security features are available on the WorkCentre 232/238/245/255/265/275 and WorkCentre Pro 232/238/245/255/265/275?*

A: With the introduction of these products Xerox has raised the bar for security functionality in multifunction devices. Our objective was to completely secure all of the external interfaces of the device through a combination of encryption and network filtering. We refer to this as "Securing the Perimeter".

- Secure Sockets Layer (SSL) is available to secure the web user interface and to allow secure scanning.
- Simple Network Management Protocol ver. 3 (SNMPv3) supports encrypted network device management.
- Internet Protocol Security (IPsec), a unique feature on Xerox MFPs, automatically encrypts the entire connection between the client and the

MFP, ensuring complete security for all printing functions.

- An internal firewall gives the customer complete control over those clients that are authorized to access the device, while blocking all other connection attempts.
- Another unique feature is the inclusion of a security audit log, which tracks all job activity to the logged-in network identity of the user. The audit log can assist those customers concerned with meeting compliance requirements for job tracking mandated by such regulations as HIPAA, GLB, and SarbOx.

Q: When will these products receive certification?

A: A consequence of certifying an entire product is that the evaluations take time. Even at EAL2, a Common Criteria evaluation, especially one conducted within the US NIAP scheme, is very rigorous. We expect to complete the evaluation on the new WorkCentre and WorkCentre Pro 232/238/245/255/265/275 sometime in the second quarter of 2006.