XEROX®

Technology | Document Management | Consulting Services

Xerox Security

Common Criteria Evaluation

Questions & Answers
Xerox and Ricoh

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

Printed in the United States of America.

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.

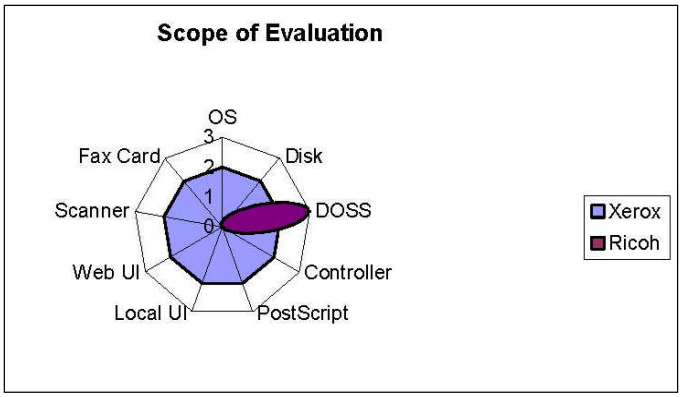
Also:

- 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. Ricoh has announced that they received EAL3 certification for the Data Overwrite Security System (DOSS). What are the differences between the two evaluations?

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



The major subsystems that make up a Multifunctional Device are labeled on the spokes of the chart. Ricoh examined a software security module that is only one component of the system controller. Security professionals know that it is critical to address all aspects of security. Xerox took a balanced, comprehensive approach to security by including the entire product in the evaluation. Ricoh chose to look deeper at only one part of the complete MFD system. While we believe that the balanced approach is wiser, each customer must make a choice based on his or her own environment.

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

A: Xerox included the entire product in the evaluation. To quote from the NIAP[1] validator's report for the WorkCentre product[2] ,"The TOE[3] is a single system (i.e.

[1] National Information Assurance Partnership

[2] Common Criteria Evaluation and Validation Scheme Validation Report, Image Overwrite Security for Xerox WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55 Advanced Multifunction System, CCEVS-VR-04-0060, 28-

the MFD (Multifunction Device))". Any MFD system can be divided into several major components, among which are 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. Since the Xerox evaluation covered the entire device, all of these components were included and tested for security during the evaluation. Ricoh only tested DOSS.

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 the security within the building. The Ricoh evaluation tested only one aspect of security.

Q: Xerox was evaluated at EAL2 while Ricoh was evaluated at EAL3. Is EAL3 better than EAL2?

A: The evaluation assurance level gives 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, but sometimes more difficult to understand, is the scope of the evaluation, or in other words, what functionality was actually evaluated. In Ricoh's case, only DOSS was evaluated. In contrast, Xerox had the entire product evaluated.

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 7 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 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 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. ISO9000 certification also specifies CM requirements, and in some cases these are more stringent than what is required at EAL3. 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

May-2004, pg. 7, http://niap.nist.gov/cc-scheme/st/ST_VID2016-VR.pdf

[3] "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

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, Ricoh limited the TOE to the HSM software only. Again, this allows Ricoh 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 Baldridge 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. 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. Whether EAL2 or EAL3, there is no difference between the level of independent testing that the CC requires the evaluators to conduct.

   By limiting the scope of the evaluation, Ricoh 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 Ricoh case, the evaluation shows that the controller testing was formally complete. However, it was limited to the HSM software 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. As discussed previously, the entire Xerox system was subjected to

penetration testing. The strenuousness and intrusiveness of penetration testing is the same at both EAL2 and EAL3. 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, were analyzed. In Ricoh's case, installing DOSS enables it. It can only be disabled by removing the DOSS module. Therefore there is no administration guidance, and this part of the evaluation becomes trivial.

Q: What did Ricoh include in their evaluation?

A: As stated in the Security Target for the Security SW Module for Ricoh's Multi-Functional-Printers[4], the TOE is defined as the Hard Disk Security Module (HSM), which is "a software module executed on MFP hardware". The Data Overwrite Security System (DOSS) functionality is implemented by the HSM, whose sole responsibility is to overwrite residual image data on the disk. The TOE does not include the Common Service Module (CSM) that implements the functionality of the multifunctional system, which is where the web server subsystem is located. Ricoh also did not include the Scanner, the User Interface, or the Marking Engine in its evaluation. More importantly, Ricoh did not include the controller Operating System (OS) in the evaluation.[5] The operating system in any computer system has primary responsibility for controlling the data transfers between all of the memory devices in the system, including the disk drive. The Ricoh evaluation therefore must base its conclusions on an assumption that the OS will operate correctly in all circumstances, rather than on actual testing.

Q: Did the evaluation of the Ricoh product test the Overwrite function to show that it worked as designed?

A: Yes, but the testing was limited only to the function of the HSM. In Section 5 of the evaluation report[6], the HSM is more explicitly defined to consist of three software subsystems as defined in the High-Level Design, and in Section 7, it says that the testing that was done corresponds to these three subsystems. Because the TOE is limited only to the HSM software module, Ricoh is specifically excluding penetration testing of the application software/OS interface, or of the OS itself.

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".[7] A penetration attack, for example, is an attempt by an attacker 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 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.

[4] https://www.secure.trusted-site.de/certuvit/pdf/9234BE.pdf

[5] See Ricoh Security Target, "Figure 1: Physical Boundary of the TOE", Sec. 2.7, pg. 12

[6] TUVIT-DSZ-CC-9234, Sec. 5, pg. B-10, and Sec. 7, pg. B-11, https://www.secure.trusted-site.de/certuvit/pdf/9234BE.pdf

[7] 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

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: The Ricoh evaluation does not includePostScript or the web user interface?

A: No. It is limited only the overwrite function performed by the HSM.

Q: Are there other differences between the Xerox Overwrite Feature and the Ricoh Overwrite Feature?

A: Yes there are several differences:

- The Xerox Image Overwrite Security feature overwrites files immediately at the completion of the job. Also, overwrite of the entire user data spool partition on the disk can be manually invoked. Ricoh only provides the immediate overwrite capability.
- 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.
- The Xerox Image Overwrite Security feature can be installed either during manufacturing, or the customer can install the feature on existing machines. The Ricoh feature can only be installed by a Ricoh Service Technician (CST) or at the factory. Additionally, DOSS can only be installed at the time of machine installation. No post-sale upgrades are available.
- The Xerox Image Overwrite Security feature can be administered remotely from the System Administrator's workstation. In Ricoh's case, DOSS is enabled when it is installed. It can only be disabled by removing the DOSS module.

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: *Is the same actual software used to implement Image Overwrite Security on all these different models?*

A: Xerox employs a platform architecture. This means that the same controller software is reused among multiple products. In the case of Image Overwrite Security, the same actual software is used in all product families mentioned in the previous answer.

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.