Common Criteria Evaluation Questions & Answers

Xerox Advanced Multifunction Systems

WorkCentre M35/M45/M55
WorkCentre Pro 35/45/55

Written by:
Larry Kovnat and Betty Ingerson

Prepared by:

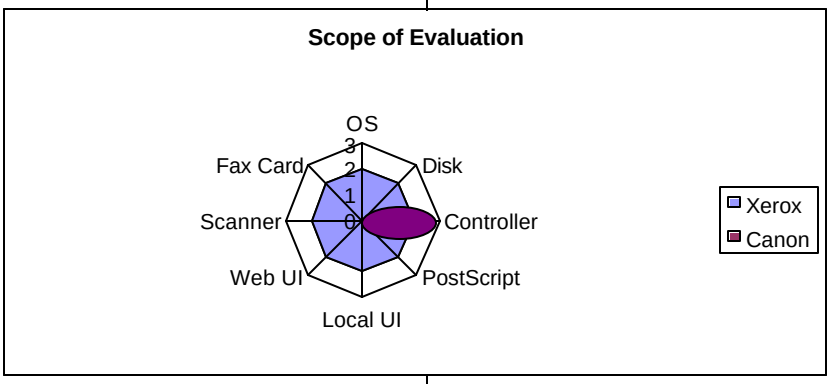
Xerox Creative Communications Group
800 Phillips Road, Bldg. 0845-17S
Webster, New York 14580
USA

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.

Q: *Xerox received EAL2 Common Criteria Certification (CCC) for the WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55. Canon has announced that they received EAL3 Certification for the imageRUNNER 2200/2800/3300. What is the difference between EAL2 and EAL3 Certification?*

A: The easiest way to show the difference is with the graph shown here. The major subsystems that make up a Multifunctional Device are labeled on the spokes of the chart. Canon's certification examined a limited configuration of the controller only. (For example, PostScript was not included.) Canon 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 Canon'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: 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 eval-uation 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 Canon evaluation tested only one aspect of security.

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

[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

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 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, Canon limited the TOE to the controller software only. Again, this allows Canon 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 than 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, Canon 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 Canon 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 Canon'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 Canon include and exclude in their evaluation?*

A: As stated in the Security Target for the Canon imageRUNNER 2200/2800/3300[2], "The TOE is the software that drives the imageRUNNER copier and contains the Complete Erase feature." Canon did NOT include the Scanner, User Interface, Marking Engine, or the controller Operating System (OS) in the evaluation.[3]. 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.

Q: *Isn't the controller really the "brains" of the system? Aren't all the security functions contained within it?*

A: Yes, the controller is the "brains" of the system, but it must rely on the other subsystems to implement the security functions it controls. For example, the Canon Overwrite function is contained in a subroutine of the controller software. The controller software is essentially application software that is invoked by the OS. Therefore, the implementation of the security function must rely on the correct operation of the interface between the controller application level software and the OS, and also on the proper operation of the OS when reading and writing to the disk drive. So not all security functions are

[2] Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-Usen50.06 with Security Kit B1 Security Target, Doc. No. F3-0504-001(2), 28-June-2004, Chapter 2, http://niap.nist.gov/cc-scheme/st/ST_VID1010-ST.pdf

[3] See Canon Security Target, Figure 2, diagram of "TOE Physical Boundary", pg 5, and Sec. 2.4, pg. 6

contained within the controller, and may depend on components in other supporting subsystems.

Q: *Did the evaluators test Canon'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. However, when evaluating the overwrite function, the security target specifically excluded penetration testing of the application software/OS interface, or of the OS itself. The Canon evaluation "…assumes [that] the operating system and device drivers are the only way to access the file system and will correctly execute functions to read, write, and delete files."[4] In other words, the testing results depend on an assumption that the OS operates as intended under all circumstances. This allows the testers to exclude a variety of circumstances that could cause the OS not to behave correctly.

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."[5] 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 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 limiting assumptions did Canon make to bound their evaluation?*

A: Canon assumes that the environment where the product is installed will provide adequate physical security to prevent attackers from removing the disk drive.[6] Remember that the Canon Target of Evaluation (TOE) is the controller software, and it is not possible for software alone to protect itself from physical attack. Canon was therefore required to state this assumption explicitly. Xerox specifies that its devices be used in accordance with standard office environment operating conditions. Since the TOE is the entire machine, simply installing the machine in accordance with its specifications is sufficient to guarantee the physical integrity of the device. No explicit assumption on physical security is required.

Perhaps even more important is that the Canon evaluation assumes that users represent a low threat of attack. As stated in the Canon ST, "Attackers are assumed not to use sophisticated attack methods to attempt to compromise the TOE security functions"[7]. Xerox does not make this limiting assumption. The assumption in the Xerox evaluation is that "…users are not expected to be trustworthy."[8] An untrusted user represents a higher level of threat than one specifically assumed to be a "low threat". Consequently, Xerox has been tested against a stronger threat level.

[4] See Canon Security Target, Chapter 3, IT Environment Assumption AE.OS, pg. 8
[5] 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
[6] See Canon Security Target, Chapter 3, Physical Environment Assumption AE.PHYSICAL, pg. 8
[7] See Canon Security Target, Chapter 3, Personnel Environment Assumption AE.LOWTHREAT, pg. 7
[8] See Xerox Validation Report, pg. 6

Q: *The Canon evaluation does not include PostScript or the Web user interface?*

A: That is correct. The Canon product was tested with only PCL enabled.[9] PostScript was not tested at all.

Since the Canon Overwrite feature can only be administered from the Local UI, that is all that was tested. The Xerox Overwrite feature can be administered from both the Local UI and the Web UI. Because of this, the Xerox Web UI was tested. Therefore, the Canon machine was not tested to see if a hacker could exploit the machine and/or the customer's network via the Web user interface on the device.

Q: *Are there other differences between the Xerox Overwrite Feature and the Canon 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. Canon 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 during manufacturing, or the customer can install the feature on existing machines, offering flexibility to adapt to changing requirements. The Canon feature can only be installed by a Canon Service Technician (CST).
- The Xerox Image Overwrite Security feature can be administered remotely from the System Administrator's workstation. The Canon Overwrite feature must be administered from the Local User Interface.
- The System Administrator PIN is variable from 3 to 12 characters. Canon restricts the PIN length to only 7 characters.

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 and WorkCentre Pro 65/75/90. These products are currently undergoing Common Criteria evaluation[10]. When the evaluation is completed later this year, Xerox will have the broadest line of Common Criteria certified products, from 35 ppm to 90 ppm, of any manufacturer. The Image Overwrite Security feature is also available on the CopyCentre C32/C40 Color Copier and WorkCentre Pro 32/40 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 three product families mentioned in the previous answer. At this point, only the WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55 have been evaluated and certified. However, customers can be sure that the same level of protection and functionality is delivered in the other products.

[9] Common Criteria Evaluation and Validation Scheme Validation Report, Canon imageRUNNER 2200/2800/3300 Series Software Version iR2200N-Usen50.06 with Security Kit B1, CCEVS-VR-04-0063, 28-June-2004, pg. 7, Installed System Software, http://niap.nist.gov/cc-scheme/st/ST_VID1010-VR.pdf

[10] See NIAP "Products in Evaluation" list at http://niap.nist.gov/cc-scheme/in_evaluation.html

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. Thus, customers can feel confident that they can achieve the cost reductions of asset consolidation provided by the Xerox WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55, without compromising security.

Q: *Xerox recently issued several software patches for the WorkCentre M35/M45/M55 and WorkCentre Pro 35/45/55. What prompted that?*

A: Xerox issued two patches that must be installed on the devices to bring them into certified configuration.[11] These were the direct result of penetration testing performed both by Xerox and the evaluation laboratory, and they illustrate a very important point. Unlike Canon, the Xerox evaluation specifically tested the PostScript interpreter and the Web user interface.

[11] The patches are available on the Xerox Security Web site at http://www.xerox.com/go/xrx/template/009.jsp?view=Feature&ed_name=Security_at_Xerox_Bulletins&Xcntry=USA&Xlang=en_US