Common Criteria
Evaluation
Questions & Answers
Xerox and Canon

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

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 is the only manufacturer to certify entire multifunction devices. Xerox devices are certified at EAL2. Canon announced that they received EAL2 Certification for the imageRUNNER 4570/3570/2870/2270 series. What is the difference between Xerox and Canon evaluations?*

A: The scope of a Common Criteria evaluation varies by manufacturer. Xerox is the only manufacturer to certify complete products, not kits or subsets of functionality. The iR4570/iR3570/iR2870/iR2270 Security Kit includes only a subset the total MFD functionality. The easiest way to show the difference is with the graph shown here.

Scope of Evaluation
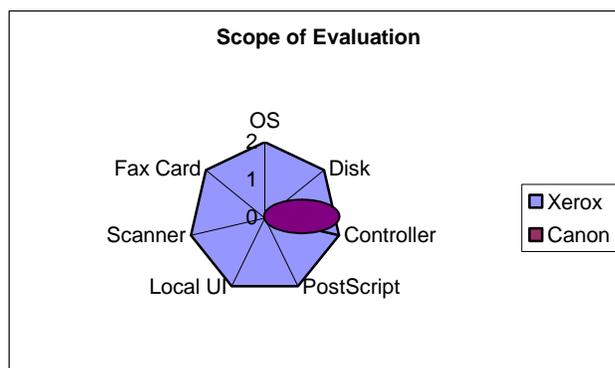
The major subsystems that make up a Multifunctional Device are labeled on the spokes of the chart. Canon's certification examined a limited configuration of the controller only. (For example, PostScript was not included.) Canon chose to evaluate one part of the MFD system. Xerox took a more comprehensive 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 firmware 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 Canon evaluation tested only one aspect of security.

Q: *What did Canon include and exclude in their evaluation?*

A: Canon's Security Kits replace a portion of the controller firmware with new software that adds the disk overwrite function. Canon does NOT include the Scanner, User

Interface, Network Interface, Marking Engine, Fax Interface, or PostScript in the evaluation[2].

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. Canon excludes PostScript, leaving one of the most popular attack paths for MFD's untested in its products.

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. 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."[3] 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

---

[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] iR4570/iR3570/iR2870/iR2270 Security Target, http://www.ipa.go.jp/security/jisec/jisec_e/c0020_it4029_ecvr.htm

[3] 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

Security Target are exempt from penetration testing.

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.

Canon'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: *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.