Xerox Product Data Overwrite Security Whitepaper

June 29, 2017

© 2017 Xerox Corporation. All rights reserved. Xerox®, Xerox and Design® and FreeFlow® are trademarks of Xerox Corporation in the United States and/or other countries.

Other company trademarks are also acknowledged.

Document Version: 1.0 (June 2017)

Introduction

Xerox multifunction devices have the ability to permanently erase and securely overwrite customer image data contained on the hard drive of a device.

This document describes the process used for secure overwrite in Xerox products, and how it complies with secure overwrite requirements documented in NIST publication SP.800-88r1 and DOD NISPOM 5220.22-M.

Note: This information is valid only for ConnectKey, AltaLink and VersaLink products. Details of the implementation in earlier Xerox products may differ.

NIST SP.800-88r1 Overwrite Requirement

As documented in Table 5 regarding ATA Hard Disk Drives:

Clear

Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.

Purge

Four options are available:

1. Use one of the ATA Sanitize Device feature set commands, if supported, to perform a Sanitize operation. One or both of the following options may be available:

    a. The overwrite EXT command. Apply one write pass of a fixed pattern across the media surface. Some examples of fixed patterns include all zeros or a pseudorandom pattern. A single write pass should suffice to purge the media. Optionally: Instead of one write pass, use three total write passes of a pseudorandom pattern, leveraging the invert option so that the second write pass is the inverted version of the pattern specified.

    b. If the device supports encryption and the technical specifications described in this document have been satisfied, the Cryptographic Erase (also known as CRYPTO SCRAMBLE EXT) command. Optionally: After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Secure Erase or the Clear procedure could alternatively be applied following Cryptographic Erase.

2. Use the ATA Security feature set's SECURE ERASE UNIT command, if support, in Enhanced Erase mode. The ATA Sanitize Device feature set commands are preferred

over the over the ATA Security feature set SECURITY ERASE UNIT command when supported by the ATA device.

3. Cryptographic Erase through the Trusted Computing Group (TCG) Opal Security Subsystem Class (SSC) or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed (if the requirements described in this document have been satisfied). Refer to the TCG and device manufacturers for more information.

Optionally: After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Secure Erase or the Clear procedure could alternatively be applied following Cryptographic Erase.

4. Degauss in an organizationally approved automatic degausser or disassemble the hard disk drive and Purge the enclosed platters with an organizationally approved degaussing wand.

Department of Defense NISPOM 5220.22-M Common Requirements

As documented in Chapter 8. Information Systems Security. This is an older standard but some Xerox documentation may still reference it.

8-301. Clearing and Sanitization. Instructions on clearing, sanitization and release of IS media shall be issued by the accrediting CSA.

a. **Clearing.** Clearing is the process of eradicating the data on media before reusing the media in an environment that provides an acceptable level of protection for the data that was on the media before clearing. All internal memory, buffer, or other reusable memory shall be cleared to effectively deny access to previously stored information.

b. **Sanitization.** Sanitization is the process of removing the data from media before reusing the media in an environment that does not provide an acceptable level of protection for the data that was in the media before sanitizing. IS resources shall be sanitized before they are released from classified information controls or released for use at a lower classification level.

Xerox Overwrite Process

The process used to overwrite data in ConnectKey, AltaLink and VersaLink products complies with NIST SP.800-88-r1 Purge option 1a. This process meets or exceeds the requirements of the Clear function. The process also complies with DOD NISPOM 5220.22-M section 8-301.

This process may be invoked at the end of a job (IIO), where it will overwrite the files used for that job, or on demand (ODIO), where it will overwrite temporary user image data files. The on demand feature can be scheduled as well. It can also optionally overwrite fax dial directories and fax mailboxes:

1. When the operation is started, a start indication is recorded in the audit log.
2. This process is executed on multiple partitions, depending on the type of overwrite enabled.
3. A single pattern is written to the entire partition.
4. The inverse of the pattern above (ones-complement) is written to the entire partition.
5. A unique new pattern is then written to the entire partition.
6. Starting at a random starting position, 10% of the partition is sampled for the occurrence of the last pattern. The 10% block is continuous.
7. If the sample check fails, then the operation terminates, and indicates a failed condition via a persistent message on the device user interface. When the device restarts, this message persists until an overwrite procedure is repeated. A failed indication will be recorded in the audit log.
8. If the sample succeeds, then the next partition in the list is used, and the process repeats, at step 3).
9. When all the partitions in the list have completed, a “success” is recorded, and the device is rebooted.
10. After the reboot, the device may print a confirmation sheet, if it was enabled.
11. The success or failure of the process is recorded in the audit log.

References

NIST Special Publication 800-88r1:
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

DOD NISPOM 5220-22-M: http://www.dss.mil/documents/odaa/nispom2006-5220.pdf