Data Protection: Solid State Drives and Data at Rest

July 6, 2020

xerox™

Document Version: 1.0 (July 2020).

Preface

This document is intended to provide users of Xerox® products equipped with solid-state storage media, accurate information to help them evaluate security risks associated with image data (data at rest) contained on these devices.

Contents

1. Overview of Solid-State Technology

Xerox® Products and Storage Media

Xerox® single and multi-function products are devices that contain a computer and the necessary software that allows them to accomplish the many productivity-enhancing tasks that have become required in today's workplace. These internal computers may have conventional disk drives (HDD), solid-state drives (SSD), secure digital cards (SD) or other non-volatile storage where job image data may be temporarily written during processing. Some Xerox® products may support a combination of these components.

From the introduction of the first digital products, we recognized the risk of retained data being inappropriately discovered from non-volatile memory, and has built protections into the devices to help safeguard this data

Benefits of SSD Technology

As solid-state technology has become more sophisticated and cost effective, certain Xerox® products are now taking advantage of its benefits. SSDs are mass storage devices that use NAND-based Flash memory instead of the spinning magnetic media disks used in conventional, earlier technology drives. SSDs are much more energy efficient, transfer data faster, and, as there are no moving parts, are not susceptible to mechanical issues. Faster drive performance means reduced device start times, enhanced data handling, and faster response which improves end user productivity.

Data Protection

Xerox® products use solid-state memory to temporarily store (buffer) user document data for print, scan, email, fax, and certain copy operations, and, unless specifically stored for future reuse by the user (Print with Saved Job type, Scan To Mailbox, Fax Mailbox, etc.), releases this temporary data at the completion of the operation. To protect data stored in the solid-state memory, Advanced Encryption Standard (AES) encryption is employed, using a 256-bit encryption key.

HOW SECURE IS AES ENCRYPTION?

AES is the strongest encryption commercially available. Using a 256-bit key, offers $1.1x10^{77}$ possible key combinations. According to a popular solid-state drive manufacturer, defeating AES encryption with a smaller, 128-bit key, would take $1.02x10^{18}$ years, or approximately 1 billion billion years; using a 256 bit key it would take $3.31x10^{56}$ years, an exponentially longer period of time. To put this in perspective, scientists estimate the Universe is only about 13.75 billion years old and Earth about 4.54 billion years old.

AES encryption is therefore, considered to be unbreakable, and is enabled as a standard feature on Xerox® products containing solid-state memory. Encryption keys are never stored on the encrypted drive, so any memory elements on an SSD removed from a Xerox® product are strongly protected.

2. Performance Features

How SSDs Provide Enhanced Performance

Prompt response to commands is critical to user efficiency. Maintaining responsive memory performance is, therefore, an important consideration. The solid-state devices used in Xerox® devices employ two important features to maintain performance at a peak level.
In order to understand these features, it is necessary to understand that data is stored in memory 'pages'. A number of 'pages' make up a data 'block'. While solid-state memory permits writing data by 'page', it does not permit erasing at the page level.

TRIM

The first feature is called TRIM. This is an operation which marks data pages as deleted when they are no longer needed and are therefore free to contain new data. TRIM is done automatically during periods when the solid-state memory is not actively being used. Making these deletes in the background maintains the memory at peak operating speed.

GARBAGE COLLECTION

The second feature is called Garbage Collection. When a sufficient number of pages are deleted by TRIM, Garbage Collection allows entire 'blocks' of memory to be erased as a group. This process is also done in the background which serves to minimize and balance wear on the solid-state memory elements.

JOB DATA REMOVAL (ALTALINK C81XX AND B81XX)

The Xerox® AltaLink B81xx and C81xx device administrator can also initiate a feature called 'Job Data Removal', accessible via the local or web user interface, 'on demand', or on a 'scheduled' basis. When initiated, this feature can delete either temporary files (associated with normal print, scan fax operations) using the 'standard' setting, or temporary files and files specifically stored for later use by the user (e.g. Print with Saved Job type, Scan to Mailbox, Fax Mailbox, etc.)

These features make it extremely difficult to discover any encrypted data that has been buffered or stored to the solid-state drive. It should be noted however that because the drive is encrypted such data would be unreadable due to security of AES 256-bit encryption discussed earlier.