

UCSD report finds issues with wiping data on SSDs

By Rafael Ruffolo

8 March 2011

IT World Canada

A recent study by the University of California, San Diego finds that the internal architecture of newer solid-state drives make them more difficult to sanitize than traditional hard disk drives. Find out why

It is more difficult to wipe data from a solid-state drive than on a traditional hard disk drive, according to a new study from the University of California, San Diego.

The report found that overwriting data and using built-in secure erase commands or other software tools are unreliable and, in some cases, result in the data remaining completely in one piece.

Michael Wei, a PhD student at the school's Department of Computer Science and Engineering and lead researcher on the project, said the reason sanitizing single files on SSD is more difficult than on a traditional hard drive is because there is no erase command on the operating system for an administrator to use. Instead, he said, the operating system must use write commands, which are at the mercy of the flash translation layer.

"It's like a game of Plinko," Wei said. "You're basically dropping a write down to the FTL, hoping it will land on your file. When you want to erase the whole drive, if you write to it enough times, you'll probably cover the entire drive, but not always."

He added that if any administrator wants to make sure they don't overwrite useful data, they are much more limited.

"Worse yet, chunks of the file you want to delete might be bunched together with data you want to keep, which results in large amounts of leftover data," Wei said.

The report found that single file sanitization, which is the ability to destroy a specific file on an unencrypted disk, is virtually impossible on SSDs. The researchers also claim that even the most effective file destruction practices will leave about 4 per cent of data behind.

The findings, Wei said, should compel IT leaders to re-evaluate their end-of-life policies.

"Many businesses outsource their data disposal, and data disposal companies often 'recycle' and resell used hardware," he said. "A data disposal company unaware of the different internal architecture of SSDs may apply hard drive overwriting techniques to an SSD, 'certify' the drives as sanitized and resell them, inadvertently exposing confidential data."

For UCSD's team of researchers, understanding and controlling the entire data lifecycle is critical to data security.

This theme is also a key component in your company's larger disaster recovery strategy.

John Riddell, head of operations manager of Minneapolis-based Kroll Ontrack Inc.'s Toronto data recovery lab, said most organizations do not have proper policies in place when they're getting rid of hardware, including storage systems.

"That's where we usually see the problem, at the end of the line," he added.

Often times, a company will simply format their hard drives to the original factory settings before off-loading the gear, Riddell said. "They think they're doing the right thing, but they're not," he said.

In their report, the UCSD researchers also advised users to encrypt their entire disks prior to use the SSDs. That way disks can be safely purged by deleting the encryption keys.