Tuesday, March 1. 2011

Garbage Collection on SSD makes digital forensics more problematic.

A few days i linked to a paper, that explains why it's hard to really delete all data from an SSD. You will find the link to the paper in that article. In those paper, the authors argued, that the SSD need better mechanisms to securely delete data. A paper from 2010 goes in the opposite direction, argueing that SSD make forensics more difficult due to some tuning tricks used in SSD.

When you look at the paper "Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?", the situation gets a little bit more complex. The document looks from the perspective of people, who try to gather data from disks for example for law enforcement.

The basic problem is: To keep performance at a high level, modern SSDs are using garbage collection. This is a good thing, as writing into an already used block needs twice as long as writing in an empty block. So the internal controller of the SSD runs a garbage collection that erases areas before the free areas is needed. This is done, when the SSD is idling. On page 8 it's
The X axis shows time and the Y axis shows the approximate percentage of the drive that has been zeroed out. In all three SSD runs, around 160 seconds from the log-in time (i.e. around 200 seconds from power-on), the SSD begins to wipe the drive. After approximately 300 seconds from log-in, the SSD consistently appears to pause briefly before continuing. 350 seconds after log-in, the SSD’s pre-existing evidence data has been almost entirely wiped.To comparision: On a quick formated HDD, they were able to recover almost all data.

The problem for the digital forensics is: The disk is doing this after a short time you've powered it up. It just wipe out those blocks it knows they are unused by some clever algorithms. And it gets even worse: When your OS uses the TRIM command, it doesn't have to find out by clever tricks, the OS tells the blocks that can be wiped out and it directly wipe them after the TRIM command when there is some spare on the SSD, as the SSD is doing this on it's own controller. And this is the next problem: You can't do anything top stop besides of powering the device down. Perhaps the only way to get to the data is to use a device like the flash chip reader from the article about secure deletion to circumvent the flash firmware in total. But i don't think a police team can seize the computer and power it down in 300 seconds. However it's still not a secure delete, as they were still able to get fragments from the disk.

The conclusion is really interesting: It seems possible that the golden age for forensic recovery and analysis of deleted data and deleted metadata may now be ending.No wonder law enforcement agency are so keen on having trojans in their repository. Analysing SSD looks like a really futile endeavour.

Posted by Joerg Moellenkamp in General at 18:18

since the (last gen of) ssd's don't export their internal structure (write/delete block sizes),
and i can't see anything in the last available solaris code...
how does solaris/zfs take care of the intrinsic porformance/durability degration when using os based encryption?
i can see how eg. truecrypt loose on ssd's, but the zfs enc approach is quite different. does that mitigate the issue?
Anonymous on Mar 2 2011, 02:21