Advisory on Solid State Disks (SSDs) / Digital Security, Radboud University / 5-11-2018

Carlo Meijer and Bernard van Gastel

SUMMARY *Solid State Disks (SSDs) often implement hardware full-disk encryption in a way known as Self-Encrypting Drives (SEDs). Several implementations of SEDs have been analysed by reverse engineering their firmware. Many have security vulnerabilities that allow for full recovery of the data without knowledge of any secret when you have physical access to the drive.*

BitLocker, bundled with Microsoft Windows, relies exclusively on hardware full-disk encryption if the drive indicates support for it. Thus, for these drives, data protected by BitLocker is also compromised.

Hardware encryption has, at best, security guarantees similar to those of software encryption. However, in practice, they often fall short. Users should not rely solely on hardware encryption offered by SSDs for data confidentiality. As such, we recommend hardware encryption users to employ also a software full-disk encryption solution, preferably an open-source and audited one.

Background

A standard for Self-Encrypting Drives (SEDs) is TCG Opal. Several implementations exist, e.g. WinMagic SecureDoc, WAVE Embassy, and even BitLocker (built into Microsoft Windows). In case a drive indicates supports for TCG Opal, BitLocker will switch off its software encryption and delegate the encryption entirely to the drive.

Hardware-based full-disk encryption implemented in SEDs are generally considered more secure than software encryption. However, this is not the case. SEDs do not address well-known weaknesses in software encryption: they don't protect against data exfiltration through malware, and they don't protect against an attacker with physical presence while the device is in operation; rather than extracting secret key information from RAM, an attacker may hot-plug the drive. Therefore, at best, hardware-based full-disk encryption is equivalent to software encryption in terms of security guarantees.

Research results

We analysed the full-disk encryption implementation of several SEDs from different vendors through reverse engineering of their firmware. Combined, these vendors cover roughly half of the SSDs sold today. We found that critical security vulnerabilities in the drives studied exist. It is in many cases possible to recover the contents of the drive without knowledge of any password or secret key, thereby bypassing the encryption entirely.

These security issues were identified using public information and around €100 of evaluation devices. The examined SSDs were bought via regular retail channels. It is quite difficult to discover these problems from scratch. However, once the nature of the issues is known, there is a risk that the exploitation of these flaws will be automated by others, making abuse easier. Note that Radboud University will not release this kind of exploitation tool (see 'Responsible disclosure').

We define two classes of vulnerabilities. The first one is identified as **CVE-2018-12037** and is characterised by the absence of cryptographic binding between the password provided by the end user and the cryptographic key used for the encryption of user data. As such, the confidentiality of the user data does not depend on secrets, and thus can be recovered by an attacker who has code execution on the drive's controller (achievable through, e.g. JTAG, memory corruption, storage chip contents manipulation, and fault injection). Devices confirmed to be affected: Crucial (Micron) MX100, MX200, MX300, and Samsung T3 and T5 portable. Finally, Samsung 840 EVO and 850 EVO are found to be vulnerable in case ATA security in High mode is used. Data recovery attacks have been successfully performed in practice.

The second class of vulnerabilities, identified as **CVE-2018-12038**, is characterised by key information stored within a wear-levelled storage chip. As such, multiple writes issued to the same logical sector may result in writes to different physical sectors. In case the end user setting a password, the unprotected key information is overwritten on a logical level with an encrypted variant. However, the unprotected key information may still exist within the storage chip. The Samsung 840 EVO is confirmed to be affected. A data recovery attack has been successfully performed in practice.

Mitigation

Users should **not rely solely on hardware encryption offered by SSDs for data confidentiality**. To warrant data confidentiality, we recommend hardware encryption users to employ also a software full-disk encryption solution, preferably an open-source and audited one. In particular, VeraCrypt allows for in-place encryption while the operating system is running, and can co-exist with hardware encryption.

Conceptually, it is possible that the issues found can be solved through firmware updates. Unfortunately, at the time of writing, all drives found vulnerable either do not have firmware updates available, or do, but they inadequately address the issues. Furthermore, it is difficult to assess if future updates will correctly solve the issues. Therefore, we believe that updating drive firmware is not a proper alternative to using additional protection mechanisms such as software encryption.

In case users are using BitLocker, a Group Policy setting exists that prevents it from configuring new drives through TCG Opal, and uses software encryption instead[1]. However, this has no effect on already-deployed drives. Only an entirely new installation, including setting the Group Policy correctly and securely erasing the internal drive, enforces software encryption. VeraCrypt can be an alternative solution for these existing installations, as it offers in-place encryptions.

Responsible disclosure

To properly handle the situation, the university contacted the National Cyber Security Centre (NCSC) of the Netherlands. Both manufacturers were informed of this security problem in April 2018 by the NCSC. The university provided details to both manufacturers to enable them to fix their product.

When discovering a security flaw, there is always a dilemma on how to handle this information. Immediate publication of the details could encourage attacks and inflict damage. Keeping the flaw secret for an extended period could mean that necessary steps to counter the vulnerability are not taken, while people and organisations are still at risk. It is common practice in the security community to try to strike a balance between these concerns, and reveal flaws after up to 180 days after the manufacturers of the affected products were informed. This practice, known as responsible disclosure, is used by default by Radboud University.

Publication

The researchers have started the process to publish the scientific aspects of their findings in the academic literature. A preliminary version was published on 5 November 2018 on the website of the Radboud University. Once the peer-review process has been completed, a final version will be published in the academic literature. This publication is and will not be a guide on how to break into SSDs.

[1] See `https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj679890(v=ws.11)#configure-use-of-hardware-based-encryption-for-fixed-data-drives`.