www.zdnet.com /article/flaws-in-self-encrypting-ssds-let-attackers-bypass-disk-encryption/

Flaws in self-encrypting SSDs let attackers bypass disk encryption

Written by Catalin Cimpanu, Contributor Nov. 5, 2018 at 9:05 a.m. PT ⋮ 6-8 minutes

A glitched rendering of a Samsung SSD T3 model

Original photo by Samsung

Researchers at Radboud University in the Netherlands have revealed today vulnerabilities in some solid-state drives (SSDs) that allow an attacker to bypass the disk encryption feature and access the local data without knowing the user-chosen disk encryption password.

The vulnerabilities only affect SSD models that support hardware-based encryption, where the disk encryption operations are carried out via a local built-in chip, separate from the main CPU.

Such devices are also known as self-encrypting drives (SEDs) and have become popular in recent years after software-level full disk encryption was proven vulnerable to attacks where intruders would steal the encryption password from the computer's RAM.

Security

-
-
-
-
-

But in a new academic paper published today, two Radboud researchers, Carlo Meijer and Bernard van Gastel, say they've identified vulnerabilities in the firmware of SEDs.

These vulnerabilities affect "ATA security" and "TCG Opal," two specifications for the implementation of hardware-based encryption on SEDs.

The two say that the SEDs they've analyzed, allowed users to set a password that decrypted their data, but also came with support for a so-called "master password" that was set by the SED vendor.

Any attacker who read an SED's manual can use this master password to gain access to the user's encrypted password, effectively bypassing the user's custom password.

The only way users would be safe was if they either changed the master password or if they 'd configure the SED's Master Password Capability setting to "Maximum," which effectively disables it.

But the master password issue was only one of multiple flaws researchers discovered. The research duo also found that due to improper implementations of the ATA security and TCG Opal specifications, the user-chosen password and the actual disk encryption key (DEK) were not cryptographically linked.

In other words, an attacker can grab the DEK value --which is stored inside the SED's chip-- and use it to decrypt the local data without needing to know the actual user password.

"Absence of this [cryptographically linking] property is catastrophic," researchers said. "Indeed, the protection of the user data then no longer depends on secrets. All the information required to recover the user data is stored on the drive itself and can be retrieved."

Other issues are detailed in the researchers' paper, titled "*Self-encrypting deception: weaknesses in the encryption of solid state drives (SSDs)*," which can be downloaded in PDF format from here.

Due to limited access to SSDs, Meijer and van Gastel said they've only tested their findings on a small number of devices, listed in the table below, but found that all were vulnerable.

Image: Meijeir et al.

They tested both internal and external (portable USB-based) SSDs with support for hardware-based encryption, and they believe that other makes and models from many other vendors may be vulnerable as well.

The researchers made their findings in April this year, and since then, they've worked with the Netherlands' National Cyber Security Centre (NCSC) to notify all affected vendors.

Both SSD vendors whose products they've tested --Crucial (Micron) and Samsung-- have released firmware updates to address the reported flaws.

But the reported issues go far deeper than researchers initially realized, and especially for Windows users, who are in more danger than others.

This is because of the default behavior of Windows BitLocker, a software-level full disk encryption system included in the Windows OS.

According to researchers, whenever BitLocker detects a hardware-based encryption capable device, the application defers the data encryption process to the hardware device and will not encrypt the user's data at the software level.

Taking into account the researchers' findings, this means that many BitLocker users may actually be exposing their encrypted data if they're using one of the vulnerable Crucial and Samsung SSDs, or many of the yet-to-be-discovered vulnerable SSDs that rely on fault ATA security and TCG Opal implementations.

The good news for Windows users is that BitLocker's encryption can be forced to work at the software level via a Group Policy setting. According to a Microsoft security advisory, "switching to software encryption on that drive will require that the drive be unencrypted first and then re-encrypted using software encryption."

Until other research groups probe more SED-based SSDs for the flaws they found, the two Radboud researchers recommend that users employ a software-level full disk encryption system, like VeraCrypt, to safeguard their data, instead of relying on the more newer hardware-based solutions.

In addition, because the root of the problem resides in how vendors have implemented hardware-level encryption specifications, the two researchers have also advised the TCG working group to "publish a reference implementation of Opal to aid developers," and also make this sample implementation public so security researchers can probe it for vulnerabilities.

This will ensure that future SEDs will implement the Opal specification in a correct manner where the user's data cannot be recovered after cursory reverse engineering sessions.

"The complexity of TCG Opal contributes to the difficulty of implementing the cryptography in SEDs," researchers said. "From a security perspective, standards should favor simplicity over a high number of features."

Article updated on November 6 with a link to the Microsoft ADV180028 security advisory. A previous version of this article stated that users would have had to reformat SSDs to enforce BitLocker's software-level encryption, as advised by the Radboud researchers. This has been corrected with the information provided in the Microsoft advisory.

Best budget SSD: 960GB PNY CS900

Related coverage:

- Hackers are increasingly destroying logs to hide attacks
- Intel CPUs impacted by new PortSmash side-channel vulnerability
- Intel Foreshadow exploits: How to protect yourself TechRepublic
- US charges China, Taiwan firms with stealing Micron's DRAM technology
- 'Hack the Pentagon' bug bounty expands to include critical systems CNET
- Cisco zero-day exploited in the wild to crash and reload devices