Flaws in Popular SSD Drives Bypass Hardware Disk Encryption

Lawrence Abrams ⋮ 6-7 minutes ⋮ 11/5/2018

Researchers have found flaws that can be exploited to bypass hardware decryption without a password in well known and popular SSD drives.

In a new report titled "Self-encrypting deception: weaknesses in the encryption of solid state drives (SSDs)", researchers Carlo Meijer and Bernard van Gastel from Radboud University explain how they were able to to modify the firmware or use a debugging interface to modify the password validation routine in SSD drives to decrypt hardware encrypted data without a password.

The researchers tested these methods against well known and popular SSD drives such as the Crucial MX100, Crucial MX200, Crucial MX300, Samsung 840 EVO, Samsung 850 EVO, Samsung T3 Portable, and Samsung T5 Portable and were able to illustrate methods to access the encrypted drive's data.

"We have analyzed the hardware full-disk encryption of several SSDs by reverse engineering their firmware," stated the report. "In theory, the security guarantees offered by hardware encryption are similar to or better than software implementations. In reality, we found that many hardware implementations have critical security weaknesses, for many models allowing for complete recovery of the data without knowledge of any secret."

To make matters worse, as Windows' BitLocker software encryption will default to hard drive encryption if supported, it can be bypassed using the same discovered flaws.

Accessing encrypted files without knowing the password

To bypass decryption passwords, the researchers utilized a variety of techniques depending on whether debug ports were available, the ATA Security self-encrypting drive (SED) standard was being used, or if the newer TCG Opal SED specification was being used.

These flaws were responsibly disclosed to Crucial and Samsung to give them time to prepare firmware updates. New firmware is availble for Crucial SSD drives, while Samsung has only released new firmware for their T3 and T5 Portable SSD drives. For their non-portable drives (EVO), they recommend that users utilize software encryption instead.

Crucial MX 100, Crucial MX 200, & Samsung T3 Portable

For the Crucial MX 100, Crucial MX 200, and Samsung T3 Portable SSD drives, the researchers were able to connect to the drive's JTAG debugging interfaces and modify the password validation routine so that it always validates as successful regardless of the password that is entered. This allows them to enter any password and have the drive unlocked.

JTAG Interface

Crucial MX300 SSD Drive

The Crucial MX300 also has a JTAG debugging port, but it is disabled on the drive.

Therefore, the researchers had to rely on a more complicated routine of flashing the device with a modified firmware that allows them to perform various routines, which ultimately allow them to either decrypt the password or authenticate to the device using an empty password.

Samsung 840 EVO and Samsung 850 EVO SSD Drives

Depending on which SED specification is used, the researchers were able to access the encrypted data by either connecting to the JTAG debug port and modifying the password validation routine or by using a wear-level issue that allows that them to recover the cryptographic secrets needed to unlock the drive from a previous unlocked instance.

The Samsung 850 EVO does not have the wear-level issue, so would need to rely on the modification of the password-validation routine through the debug port.

BitLocker fails by defaulting to hardware encryption

Most modern operating systems provide software encryption that allows a user to perform whole disk encryption. While software decryption offered by Linux, macOS, Android, and iOS offer strong software encryption, BitLocker on Windows falls prey to the SSD flaw by defaulting to hardware encryption when available.

When using BitLocker to encrypt a disk in Windows, if the operating system detects a SSD drive with hardware encryption, it will automatically default to using it. This allows drives encrypted by BitLocker using hardware encryption to be decrypted by the same flaws discussed above. BitLocker software encryption on the other hand has no known and verifiable flaws that allow users to bypass password authentication.

In order to prevent the use of SSD hardware encryption, the researchers suggest that users disable its use using a Windows Group Policy at "Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives" called "Configure use of hardware-based encryption for operating system drives".

Windows Policy to disable Hardware Encryption

This policy is also available for removable and fixed data drives and should be disabled for them as well to enforce software encryption.

Before software encryption will be used, after you change these policies you must first completely decrypt the drive and then enable BitLocker again to use software encryption.

Update 11/6/18: Microsoft has issued an advisory related to BitLocker and discovered flaws in SSD hardware encryption. This advisory contains mitigation information

"Microsoft is aware of reports of vulnerabilities in the hardware encryption of certain self-encrypting drives (SEDs). Customers concerned about this issue should consider using the software only encryption provided by BitLocker Drive Encryption™. On Windows computers with self-encrypting drives, BitLocker Drive Encryption™ manages encryption and will use hardware encryption by default. Administrators who want to force software encryption on computers with self-encrypting drives can accomplish this by deploying a Group Policy to override the default behavior. Windows will consult Group Policy to enforce software encryption only at the time of enabling BitLocker."