A MICRON TECHNICAL MARKETING BRIEF

Protecting Your SSD and Your Data

Secure Your SSD's Firmware Against Ever-Growing Threats

Overview

In the last few years, data security has emerged as one of the most important issues in IT. Daily, we create, store and transmit multiple exabytes (10^{18} bytes) of data. Much of that data is private or at least sensitive, some of it carries tremendous financial or monetary value, and some is downright invaluable and/or irreplaceable, such as classified government data that could damage national security if compromised in any way.

Figure 1: Data security is among the most important issues facing IT professionals today.

Micron has responded to the need for data security by designing and manufacturing self-encrypting drives (SEDs) for both client computing and enterprise data centers. While encryption is a key component in securing data at rest on an SSD, security should not stop there. As described in this brief, Micron implements several other features in our SSDs — even our non-encrypted products — to ensure that the drives are secure and only accessible to authorized users.

The Expanding Attack Surface

The growing sophistication of data attacks is a prime motivator in Micron's efforts to secure our SSDs. Data security experts describe an attack surface as all of the possible methods, routes and vectors through which attackers can enter a computing or data storage system. A larger figurative attack surface implies more potential vulnerabilities. For data storage systems, this attack surface has expanded in ways that were unimaginable only a few years ago.

A good example of the expanding surface is the ability to attack and compromise SSD or HDD firmware. Firmware is the code set that controls the operation of a drive. While firmware is coded very much like software, it is stored and run differently; and unlike software, designers rarely expect to change firmware — if ever. If all goes as planned, the source code for firmware never leaves the control of the manufacturer. The firmware is stored on the SSD only in binary form, which is illegible to humans. The binary includes a checksum so that any attempt to make a bitwise change to the binary results in broken, unusable code. Knowing which bits to change in the binary code is nearly impossible.

Exposing Firmware Vulnerabilities

Traditionally, we think of the software compilation process as a one-way operation. However, the recent advances in computing power that have done such amazing things for our daily lives have also enabled attackers to do some incredibly harmful things. For example, it may be possible to reverse-engineer a binary file to extract the source code — which could enable a very powerful computer to reconstruct

enough of the source code to get legible assembler-level code. From there, a capable coding team could make workable code that could be modified to change the behavior of the drive. Perhaps the attacker could force the drive to create a hidden storage area, unknown to the user, where OS-level malware could hide sensitive data. Or, perhaps the attacker could disable encryption or steal passwords via this hypothetical firmware vulnerability.

In years past, these possibilities were beyond imagination, but reports indicate that such attacks may have already occurred. While Micron has never demonstrated or replicated such an attack, its mere possibility mandates a response by device manufacturers. Fortunately, Micron's engineers have come up with a way to identify when firmware has been tampered with — and to prevent that firmware from being installed on a Micron SSD using digital signatures.

Digital Signatures for Firmware

Digitally signed software is becoming very familiar to software users, and digital signatures are now essential to the security solution for storage devices. Figure 2 shows a software notification with Micron's corporate signature. Micron uses the industry-accepted RSA cryptosystem to create, manage and secure our industry-recognized signatures. When a Micron executable file runs in an OS, the OS reads and displays that signature so the user can verify that the software comes from a recognized vendor.

Figure 2: Software identifies itself as published by Micron. Firmware can do the same.

Firmware can self-identify in a very similar way. After the code is compiled, a recognized and unique signature is appended to our firmware binaries, completing the firmware build process. This signature helps Micron ensure that only a signed, approved firmware binary is downloaded to our SSDs.

Though rare, we sometimes make updates to firmware that are beneficial to deployed drives in the field. If field updates are necessary, we strive to make this process easy and safe for the end user.

Micron Firmware Update Process

The firmware update process is fairly straightforward. Each drive interface — such as SATA, SAS or NVMe — has a well-defined command sequence that sends a new binary code to the storage device, commanding it to replace the drive's current firmware. To ensure this command doesn't deliver incorrect firmware, the drive checks the target firmware for the correct model number and consistent drive type. And if an older firmware version could expose the drive to a known security vulnerability, we restrict any changes that would allow the firmware to revert, or roll back, to older versions.

Did You Know?

Micron firmware updates are never used to change features on the SSD. For example, an encrypted drive cannot be converted to a non-encrypted drive during a firmware update.

The digital signature also ensures that the firmware has not been tampered with and is not counterfeit. When a drive in the field receives the DOWNLOAD-FIRMWARE command, it first reads the new target binary code and compares the signature against the expected value. If the new signature doesn't match the expected value, the firmware is rejected, rendering the attack unsuccessful.

Validating Security at Boot Time

Microsoft has led an industry effort to institute a new OS feature, called secure boot, which they implemented in their most recent OS, Windows® 10. Secure boot improves overall system security using digital signatures in a similar fashion to Micron's firmware protections. When enabled, secure boot identifies signatures of known-good software to help the system resist attacks by malware installed in the OS during a previous session. The goal is to prevent the installation and execution of what is known as a "rootkit." A rootkit-based attack replaces the OS bootloader with malicious code. One common rootkit attack installs code that detects and records password entries via a keystroke logger, which poses obvious security risks.

Micron's SSDs perform a very similar boot check. When the SSD powers up, the drive performs a self-check of the integrity of the drive's firmware image. This SSD secure boot is a double-check that ensures no invalid firmware has been loaded. When firmware is securely downloaded (either in the factory or in the field after a correct digital signature check), the firmware computes a message authentication code (MAC). This value is calculated using an SHA-3 algorithm, RSA signature-checking or another industry-accepted method. After the MAC is calculated, it is encrypted and stored in nonvolatile memory. During the power-up boot phase, the drive recalculates the MAC for the firmware image that is being booted and compares it to the MAC stored when the code was first installed. If the two values match, the boot process continues.

In the rare case that the two MACs do not match, it is a clear sign that the firmware has been compromised, and the boot process stops. Unfortunately, user data is now inaccessible, and the drive may have to be returned to the factory for recovery. We believe that any attack on an SSD's firmware makes it too dangerous to continue normal operations.

Conclusion

Ensuring the security of user data and protecting the integrity of SSD firmware against attacks is a top priority for Micron. The safest data storage devices include full encryption of user data, but even when encryption is not used, data security is still of the utmost importance. Micron's encrypted and non-encrypted SSDs include features that protect the integrity of the SSD firmware, providing added protection of user data.