Microsoft and partners toughen firmware defense

23 October 2019, by Nancy Cohen

For many people who are not tech professionals, the word "firmware" first appears to them in the negative. News items over the past years have used the word over and over again to report attacks. What is firmware? If software is "soft," is it just another word for hardware?

Firmware is actually "the code that defines the relationship between hardware and software," said Igor Bonifacic in *Engadget*, and it is "vitally important to any computer." The crucial role that hardware manufacturers play, though, is that the firmware is often written by them, he pointed out, rather than by OS developers. "This means there are countless different varieties of firmware, each with their own particular set of quirks and vulnerabilities."

Microsoft's security people have decided that enough is enough with quirks and vulnerabilities. They are springing for tougher requirements, tougher protection against firmware threats. Microsoft along with some hardware partners are looking at solutions to waylay threats against PC firmware.

David Weston, director of OS security at Microsoft, talked fundamentals with Lily Hay Newman in Wired. "Firmware runs at a privileged level. It's the thing that boots up the machine—it plays a critical role. Yet firmware is not integrated into update systems like Windows Updates, and for enterprises their visibility into firmware is generally relatively limited. So it's highly privileged and there's lots of opportunities for bugs."

Their resolve to offer PC protections against targeted firmware drew headlines this week. Now Microsoft OEM partners will be able to pick up on Microsoft's new Secured-core PC initiative.

Brandon Hill in *HotHardware* commented on the unease over malicious actors. "There's no question that we're living in relatively dangerous times with regards to cybersecurity concerns. There isn't a week that goes by that we don't hear of app malware, some large corporation's customers database being raided, or devices themselves being the subject of low-level attacks."

Weston told Microsoft Security site viewers on Monday what this "Secured-core PC" move is all about.

Who: It will affect devices created in partnership with Microsoft's PC manufacturing and silicon partners.

What: A specific set of device requirements applying security best practices of "isolation and minimal trust to the firmware layer, or the device core," that underpins Windows. The devices are designed specifically for industries such as financial services, government, healthcare. Also it's for workers handling sensitive IP, customer and personal data.

How: Microsoft worked with partners to make sure the new capabilities are shipped in devices out of the box.

"Windows 10 now implements System Guard Secure Launch as a key Secured-core PC device requirement to protect the boot process from

firmware attacks."

They turned to capabilities from AMD, Intel and Qualcomm.

Newman elaborated in *Wired*. "Microsoft has worked with AMD, Intel, and Qualcomm to make new central processing unit chips that can run integrity checks during boot in a controlled, cryptographically verified way. Only the chip manufacturers will hold the encryption keys to broker these checks, and they're burned onto the CPUs during manufacturing."

System Guard uses the Dynamic Root of Trust for Measurement (DRTM) capabilities built into silicon from AMD, Intel and Qualcomm.

According to the Microsoft Security site, "System Guard uses the Dynamic Root of Trust for Measurement (DRTM) capabilities that are built into the latest silicon from AMD, Intel, and Qualcomm to enable the system to leverage firmware to start the hardware and then shortly after re-initialize the system into a trusted state by using the OS boot loader and processor capabilities to send the system down a well-known and verifiable code path.

"This mechanism helps limit the trust assigned to firmware and provides powerful mitigation against cutting-edge, targeted threats against firmware. This capability also helps to protect the integrity of the virtualization-based security (VBS) functionality implemented by the hypervisor from firmware compromise. VBS then relies on the hypervisor to isolate sensitive functionality from the rest of the OS which helps to protect the VBS functionality from malware that may have infected the normal OS even with elevated privileges."

OK, then, thanks to Igor Bonifacic in *Engadget*, its readers got an idea of what happens when Secured-core PC is put to work.

Bonifacic: "...a processor's firmware will power up the system as always, but then limit how much the processor trusts its own firmware to define the code path it takes to launch the system. The processor will instead call on Microsoft's bootloader for those instructions. The ultimate goal of the framework is to create a safe and reliable path the processor can take each and every time it boots your computer. One major advantage of this system is that it puts the emphasis on preventing attacks, instead of merely detecting them."

The effort does not stop with hardware protection. There is something called Project-Mu. "Beyond the hardware protection of firmware featured in Secured-core PCs, Microsoft recommends a defense-in-depth approach including security review of code, automatic updates, and attack surface reduction. Microsoft has provided an open-source firmware project called Project-Mu that PC manufacturers can use as a starting point for secure firmware."

Is Secured-core PC the magic bullet? No more worries about hackers staging firmware attacks? Microsoft's Weston is not that naive. "We're never going to say it's impossible that something could be compromised," he said in *Wired*. "But we always want to drive the cost up, so it's prohibitive for most adversaries."

What's next? "One of the first devices that will include Secured-core PC is Microsoft's upcoming Surface Pro X, with devices from Dell, Lenovo and Panasonic to follow," said *Engadget*.

Wired said other models will eventually come out on devices. "Secured-core PCs will also have an identifying sticker, so that you know what you're getting the next time you buy."