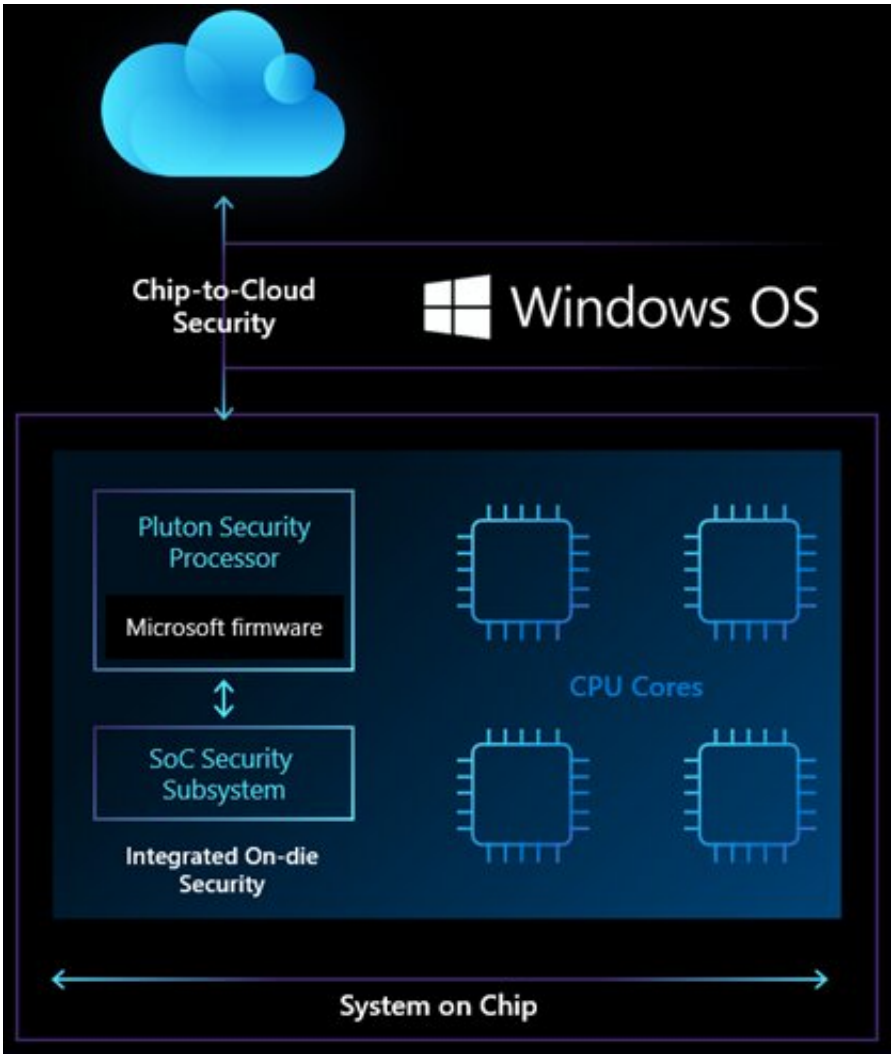
Microsoft teams with chip makers on new super secure processor

November 18 2020, by Peter Grad



Credit: Microsoft

Microsoft unveiled a new chip design Tuesday that it says will usher in a new era of security on Windows PCs.

Partnering with chip manufacturing giants Intel, AMD and Qualcomm, Microsoft says a new security component, Pluton, will be constructed directly into the CPU instead of residing on its own in the current Trusted Platform Module. The TPM has long been used to store hardware and cryptographic keys.

The technology is based upon a security approach that Microsoft launched nearly a decade ago in Xbox gaming consoles. The popular gaming system is a rare example of popular product that has been extraordinarily successful in fending off hackers. The same principles were applied to Microsoft's internet-of-things service Azure Sphere, which along with Xbox helped the company refine its defense line against intruders.

Pluton marks another milestone for Microsoft, which pledged in 2018 to redesign its processors to offer better security in the wake of revelations of the potentially catastrophic Spectre and Meltdown flaws. Those vulnerabilities exposed virtually all computer chips manufactured for the past 20 years to malicious activity.

Hackers had been taking advantage of weakness in the channels between TPM and CPU. The TPM had grown so efficient at protecting the integrity of a system—it powers Windows Hello fingerprint, facial recognition and PIN processes, as well as BitLocker drive encryption—that hackers increasingly directed their attentions towards cracking the bus interface hat connects security components to the CPU.

Pluton will now store all sensitive data within the processor itself, effectively isolating credentials, user identities, encryption keys and other personal data from all other computer hardware. This will provide

"an unprecedented level of security" for Windows users, according to David Weston, Microsoft's director of enterprise and operating system security.

"The Microsoft Pluton design will create a much tighter integration between the hardware and the Windows operating system at the CPU that will reduce the available attack surface," said Weston. "What we've done here is we've said, let's not change the nature of the PC ecosystem—keep the choice, keep the customer variety. But when it matters, which is where your encryption keys are stored, how you boot the system, now Microsoft writes the code for Pluton and works with Intel or others to get it signed and delivered. So there are fewer people involved, and the PC is going to be more secure for it."

He added, "The fact that Microsoft designed a processor and Intel is putting it in their CPU—that's like a head-exploding concept."

The process of security updates will also be improved with the introduction of Pluton. Currently, Windows updates are provided from numerous providers, sometimes leading to patching problems. But under Pluton, security updates will be seamlessly integrated with the Windows Update process, popularly known as Patch Tuesdays.
"This is a better, stronger, faster, more consistent TPM," Weston said of Pluton.

No release date has been set for the new processor.

More information: www.microsoft.com/security/blo … ture-of-windows-pcs/