August 21, 2019

Intel Editorial: Intel Joins Industry Consortium to Accelerate Confidential Computing

Intel to Contribute Intel SGX SDK to New Community to Help Simplify Secure Enclave Development and Deployment

SANTA CLARA, Calif.--(BUSINESS WIRE)-- The following is an opinion editorial by Lorie Wigle of Intel Corporation.

This press release features multimedia. View the full release here: https://www.businesswire.com/news/home/20190821005140/en/

Lorie Wigle is vice president in the Architecture, Graphics and Software Group and general manager of Platform Security Product Management at Intel Corporation. (Credit: Intel Corporation)

Leaders in information and infrastructure security are well versed in protecting data at-rest or in-flight through a variety of methods. However, data being actively processed in memory is another matter. Whether running on your own servers on-prem, in an edge deployment, or in the heart of a cloud service provider's data center, this "in-use" data is almost always unencrypted and potentially vulnerable.

Intel's commitment to helping customers and the ecosystem at large with data protection is why we and other industry leaders are coming together to form a new Confidential Computing Consortium under the Linux Foundation. We're proud to be a founding member of this new industry group dedicated to making confidential computing practices, such as the protection of data in-use, easier to adopt in today's multi-cloud world.

Confidential Computing Protects Data In-Use

Confidential computing may take multiple forms, but early use cases rely on trusted execution environments (TEE), also called trusted enclaves, where data and operations are isolated and protected from any other software, including the operating system and cloud service stack. Combined with encrypted data storage and transmission methods, TEEs can create an end-to-end protection architecture for your most sensitive data.

Enterprises and cloud service providers can apply confidential computing to a wide range of workloads. The most popular of the early use cases use the trusted enclave for key protection and crypto-operations. But trusted enclaves can be used to protect any type of highly sensitive information. For example, healthcare analytics can be performed so that the enclave protects any data that may contain personally identifiable information, thus keeping results anonymous.

Companies that wish to run their applications in the public cloud but don't want their most valuable software IP visible to other software or the cloud provider can run their proprietary algorithms inside an enclave. Multiple untrusted parties can share transactions but protect their confidential or proprietary data from the other parties by using enclaves. Any time sensitive data is in use, there may be an opportunity to use confidential computing to better protect it.

Intel SGX – The Hardware Engine Powering Confidential Computing

The Confidential Computing Consortium is initially focused on common programming models and enclave portability, but the Consortium doesn't prescribe the hardware mechanism necessary for creating and protecting the enclave. That's where Intel® Software Guard Extensions (Intel® SGX) comes in.

Intel SGX is a hardware-based technology that helps protect data in-use by establishing protected enclaves in memory so only authorized application code can access sensitive data. Unlike full memory encryption technologies that leave the data within the attack surface of the OS and cloud stack, Intel SGX allows a specific application to create its own protected enclave with a direct interface to the hardware, limiting access and minimizing the overall performance impact for both the application and any other virtual machines (VMs) or tenants on the server.

Intel SGX provides hardware-based encryption for data in-use protection at the application level with the smallest attack surface. Intel SGX is available today on Intel® Xeon® processor E-2100 family, and is used in confidential computing services from Microsoft Azure*, IBM Cloud Data Guard*, Baidu*, Alibaba Cloud* and Equinix*. Later this year, we will release a PCI-Express add-in card that will enable Intel SGX in multi-socket Intel Xeon Scalable servers. And Intel SGX will continue to be rolled out across our mainstream Xeon platforms in upcoming generations.

As part of today's announcement of the new Confidential Computing Consortium, I am pleased to share that we are contributing the Intel SGX SDK to this new community to help simplify secure enclave development and deployment.

The launch of the Confidential Computing Consortium is a big step in bringing this powerful security capability to a broader audience, and we are committed to working with our ecosystem customers to ease use and portability of confidential computing for developers and IT pros. We invite developers to learn about how to integrate Intel SGX into their applications and cloud services today, and the future of the consortium at its website.

Lorie Wigle is vice president in the Architecture, Graphics and Software Group and general manager of Platform Security Product Management at Intel Corporation.

About Intel

Intel (NASDAQ: INTC), a leader in the semiconductor industry, is shaping the data-centric future with computing and communications technology that is the foundation of the world's innovations. The company's engineering expertise is helping address the world's greatest challenges as well as helping secure, power and connect billions of devices and the infrastructure of the smart, connected world – from the cloud to the network to the edge and everything in between. Find more information about Intel at newsroom.intel.com and intel.com.

Intel and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

View source version on businesswire.com:
https://www.businesswire.com/news/home/20190821005140/en/

Megan Grasty
Highwire Public Relations
megan@highwirepr.com
916-834-0802

Source: Intel Corporation