February 26, 2020

Intel Highlights Latest Security Investments at RSA 2020

Announces Compute Lifecycle Assurance Momentum, Previews New Security Capabilities

SAN FRANCISCO--(BUSINESS WIRE)-- At the Intel Security Day event during RSA Conference 2020, Intel underscored its commitment to security with several announcements, including details on security capabilities coming in future products. At Intel, security is a fundamental and foundational element of all aspects of architecture, design and implementation. Together with customers and partners, Intel is building a more trusted foundation in this data-centric world.

This press release features multimedia. View the full release here: https://www.businesswire.com/news/home/20200226005170/en/

Tom Garrison, Intel vice president and general manager of Client Security Strategy and Initiatives, discusses strategy for evolving security in CPUs that have 30 billion transistors and are 1/100th the size of a photon of light, starting with Intel Transparent Supply Chain (Intel TSC) at RSA Conference 2020 in San Francisco on Monday, Feb. 24, 2020. Intel TSC proves transparency of a device's origin and helps establish the foundation for a trusted supply chain. (Credit: Intel Corporation)

"Hardware is the bedrock of any security solution. Just as a physical structure requires a foundation established on bedrock to withstand the forces of nature, security solutions rooted in hardware will provide the greatest opportunity to provide security assurance against current and future threats," said Tom Garrison, Intel vice president and general manager of Client Security Strategy and Initiatives. "Intel hardware, and the assurance and security technologies it brings, help harden the layers above from attack."

More: Intel Security News

Intel customers build solutions and services that depend on the breadth and depth of technologies in the silicon, vertical integration and substantive reach from edge to cloud. It is Intel's mission to provide common security capabilities across all architectures, to help address the ever-increasing sophistication of user experiences.

Data must be protected at rest and in motion. The protection of data is critical to extracting value from it, while delivering uncompromised performance. The next 10 years will see more architecture advancements than the past 50 years.

"Intel is uniquely positioned in the industry to create and deliver truly innovative security technologies that span architectures, memory and interconnect," said John Sell, Intel Fellow and director of Intel Security Architecture and Technology.

Data Platform Protection

As the demand for data-intensive computing grows, there is a need to balance the ease of scaling deployment with the level of data protections. To address customer challenges, new confidential computing capabilities on future data center platforms are expected to offer scale and choice:

- **Application isolation** helps protect data in use with a very narrow attack surface. Already deployed for production data centers and solutions, Intel® Software Guard Extensions (Intel SGX) will expand to a broader range of mainstream data-centric platforms, and is expected to provide larger protected enclaves, extended protections to offload accelerators and improved performance. This will further expand the number of usages able to leverage these advanced application isolation capabilities.
- **VM and container isolation** helps provide protections in virtualized environments, isolating them from each other and from the hypervisor and cloud provider without requiring application code modifications.
- **Full memory encryption** helps better protect against physical memory attacks by providing hardware-based encryption transparent to the operating system and software layers.
- **Intel® Platform Firmware Resilience** is an Intel FPGA-based solution that helps protect the various platform firmware components by monitoring and filtering malicious traffic on the system buses. It also verifies the integrity of platform firmware images before any firmware code is executed and can recover corrupted firmware back to a known good state. When combined with other trusted boot technologies on new platform generations, Intel continues to contribute additional tools to increase resistance against attack and help provide a more trusted foundation for modern cloud and enterprise deployments.

More information can be found on Intel's IT Peer Network.

Compute Lifecycle Assurance Industry Traction

Since its launch in December, Intel's Compute Lifecycle Assurance Initiative has gained traction with customers and ecosystem partners, starting with the foundational offering Intel® Transparent Supply Chain (Intel TSC).

Transparency of a device's origin helps establish the foundation for a trusted supply chain. Intel TSC tools allow platform manufacturers to bind platform information and measurement using the Trusted Computing Group's (TCG) Trusted Platform Module 2.0 (TPM) standard, also referred to as ISO 11889. This allows customers to gain traceability and accountability for platforms with component-level reporting. More information can be found in a blog by Intel's Tom Dodson.

Intel TSC is currently available for customers across Intel vPro® platform-based PCs, Intel® NUC, Intel® Xeon® SP systems, Intel® solid-state drives and certain Intel® Core™ commercial PCs.

To demonstrate Intel's commitment to transparency, measurement and assurance of the supply chain, Intel also enables ecosystem partners with Intel TSC tools. Today, Hyve Solutions, Inspur, Lenovo (client and server), Mitac, Quanta, Supermicro and ZT Systems

have enabled Intel TSC tools. In addition, Intel has active deployments of Intel TSC with enterprise IT and cloud service providers.

“This chain of trust process provides essential traceability based on the TPM,” said Thorsten Stremlau, chair of TCG’s Marketing Work Group. “Bringing component-level traceability to platforms and systems increases confidence and reduces the risk of counterfeit electronic parts while also facilitating procurement standards. This is the right direction for the industry.”

It often takes the industry working together to make technological advancements. Intel has a strong legacy of assisting its customers and industry partners in developing new and innovative ways to improve hardware security. Intel shares knowledge of this experience through its participation and contributions to leading industry initiatives and standards bodies, including the Confidential Computing Consortium under the Linux Foundation, the FIDO Alliance’s IoT Technical Workgroup and the newly expanded Common Weakness Enumeration led by MITRE. Such efforts underscore Intel’s unique capacity to build a more trusted foundation for the industry.

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.

Notices and Disclosures:
Intel technologies may require enabled hardware, software or service activation.
No product or component can be absolutely secure.
Your costs and results may vary.

View source version on businesswire.com:
https://www.businesswire.com/news/home/20200226005170/en/

Megan Phelan
Highwire Public Relations for Intel Corporation
916-834-0802
megan@highwirepr.com

Source: Intel Corporation