SOLUTION BRIEF

Application Code Security
Intel® Software Guard Extensions

Hardware-Assisted Security for High-Value Information

Numecent, Bromium, and wolfSSL employ Intel® Software Guard Extensions (Intel® SGX) to create more secure, next-generation solutions

Developers have long been constrained by the security capabilities that major platform providers have exposed for application development. These same capabilities are also well known to hackers, who have exploited weaknesses to steal sensitive data and credentials, or hijack code for attacks. Until now, developers have been forced to rely on the provider's security architecture, with no way to apply a security model designed to fit their own requirements after a platform release has shipped.

Recognizing the need for a new model that protects selected code and data from disclosure or modification, Intel designed Intel® Software Guard Extensions (Intel® SGX), a hardware-assisted trusted execution environment with the smallest possible attack surface. With Intel SGX, developers can partition their application into CPU-hardened "enclaves," or protected areas of execution, that increase security even on compromised platforms. Using this new application-layer trusted execution environment allows developers to enable identity and records privacy, secure browsing, DRM, harden end point protection, or any high assurance security use case that needs to safely store secrets or protect data.

Intel SGX is an Intel® technology for application developers who are seeking to protect select code and data from disclosure or modification. Intel SGX makes such protections possible through the use of enclaves. Application code can be put into an enclave by special instructions and software made available to developers via the Intel SGX SDK. The SDK is a collection of APIs, libraries, documentation, sample source code, and tools that allows software developers to create and debug Intel SGX-enabled applications in C/C++.

Forward-thinking technology leaders in a wide variety of services are incorporating Intel SGX into their solutions, including Intel® software vendor partners Numecent, Bromium, and wolfSSL. As successful prototypes become market-ready products, the promise of hardware-assisted security is becoming a reality for the application layer.

Numecent: Enhancing the Security of Innovative, Cloud-Based Application Delivery

Numecent, a pioneer and technology leader in secure application delivery, was an early adopter of Intel SGX, incorporating it into its signature Cloudpaging* product. Cloudpaging, which was founded around application virtualization technology and further enhanced to bring additional capabilities and robustness to application delivery, compartmentalizes Windows* applications so they can be securely delivered to the desktop for native execution. Requiring as little as 10 percent of the application on the desktop to run—and then paging the rest of the application from the cloud on demand—Cloudpaging can reduce the digital delivery time of any native application by between 20 and 100x by previrtualizing the asset to be delivered.

Intel SGX improved Cloudpaging's already-stellar application delivery security by allowing Numecent to run its DRM engine inside the enclave, providing an extra level of hardware-based security that gives the company's clients even more confidence. Additionally, Intel SGX works with the attestation server to prohibit end users from doing "time rollbacks" that would violate license agreements.

The company views Intel SGX as a competitive differentiator, and plans to leverage and market its features as an additional level of security for its partners going forward.

Bromium: Protecting Online Credentials

Founded in 2010 with a mission to restore trust in computing and an expert in securing PCs and Macs* by design, Bromium uses proprietary microvirtualization technology to automatically and instantly isolate all user tasks and the associated content—such as an email attachment, webpage, or executable—in a microvirtual machine. This secure container is automatically discarded when the user closes a web session or document. As a result, malware that might enter the micro-VM through these threat vectors cannot compromise the operating system, applications, data, or network.

Although Bromium Endpoint Protection can monitor the host (desktop) for signs of compromise using the same LAVA technology that provides precise forensics for introspection of micro-VMs, the company's goal is to enhance the protection of the host from, for example, "east-west" attacks. Ultimately, Bromium wants to protect high-value information on the end point (e.g., credentials)—even in instances in which malware might completely own the end point and could potentially steal secrets and access the enterprise. The company chose Intel SGX to help them achieve this objective.

In a prototype shared at IDF 2016, Bromium has isolated—within an Intel SGX enclave—the user's credential store and their password manager in the browser. The result is that malware on an end point desktop cannot access high-value information. With the success of the prototype, which Bromium was able to get up and running in just a few days thanks to Intel's powerful toolkit, the company is moving forward with productizing the solution and building it into their core product.

Hardware-Assisted Security Has Arrived for the Application Layer

Intel® Software Guard Extensions (Intel® SGX) delivers 17 new Intel® architecture instruction sets and memory access changes that can be used by applications to set aside private regions of code and data, preventing direct attacks on executing code or data stored in memory. Application code can be put into an enclave by special instructions and software made available to developers via the Intel SGX SDK, a collection of APIs, libraries, documentation, sample source code, and tools that allows software developers to create and debug Intel SGX-enabled applications in C/C++.

wolfSSL: A Natural Fit for Secure SSL Cryptography

With an emphasis on speed, size, portability, features, and standards compliance, wolfSSL focuses on providing lightweight and embedded security solutions. Its products are open source and are included in many types of network applications and devices, including smart devices on automobiles, IP phones, mobile phones, routers, printers, and credit card scanners.

wolfSSL recently received an Intel SGX software development kit, and has been working diligently to add support for wolfSSL's wolfCrypt library. Proof of concept took about two weeks, testing was straightforward, and the company was happy with the amount of control and transparency SGX provided. Early results are promising, and the company is moving forward with its plan to release this support to the public in the near future.

The Preferred Trusted Execution Environment

Hardware-assisted security has a unique ability to augment the OS and deliver new capabilities that help applications protect themselves according to developer needs. This revolutionary new security architecture is poised to become the preferred trusted execution environment for security-focused application developers.

Learn More

Engage Intel SGX resources and download documentation and the SDK at **software.intel.com/sgx.**