Enhanced Security for Applications and Data In-use

CPU hardening for Application Security

Intel SGX delivers new instructions & memory access changes enabling a ground-breaking security model for developers. Hardware-assisted security has arrived for the application layer.

Introduction

Intel® Software Guard Extensions (Intel® SGX) helps protect selected code and data from disclosure or modification. Developers can partition their application into hardened "enclaves" or trusted execution modules to increase application security. Using this new application-layer trusted execution environment, developers can enable identity & records privacy, secure browsing, DRM, harden endpoint protection, or many high assurance security use cases that need to safely store secrets or protect data.

- **Enhances Confidentiality and Integrity**
  Even in the presence of privileged malware at the OS, BIOS, VMM, or SMM layers

- **Low Learning Curve**
  A familiar OS programming model integrates with the parent application & executes on main CPU

- **Remotely Attest & Provision**
  A relying party can verify an application enclave’s identity and securely provision keys, credentials and other sensitive data into the enclave

- **Help Significantly Reduce Attack Surface**
  Application enclave runs within CPU boundary - enclave data, memory, & I/O is encrypted and protected

**Figure 1**: Empower developers to better protect code and data
The Constraints of Application Security
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 by hackers who have exploited weaknesses to steal sensitive data, credentials, or hijack code for attacks. Software developers have had to rely on the provider’s security architecture with no means to apply a security model designed to fit their own requirements.

A new model is now available that can leverage the strengths of the platform and OS but deliver independence for the developer who understands what application secrets need additional protection. Silicon assisted security has a unique place to augment the OS to deliver new capabilities that help applications protect themselves according to developer needs.

Intel SGX - A New Approach
To address the reality of widespread security holes & compromised systems, Intel set out to design a hardware assisted trusted execution environment to help minimize attack surface. Intel SGX delivers new Intel® Architecture instructions that can be used by applications to set aside private regions of code and data that can help prevent direct attacks on executing code or data stored in memory.

Intel SGX introduces a revolutionary new security architecture that is certain to be the preferred trusted execution environment for security focused application developers.

Developing Intel SGX Applications
In Figure 2, the application design illustrates an SGX application includes two parts: an untrusted component that launches, and a trusted part where production code runs in an encrypted enclave. A developer can create 1-n enclaves that work in concert to support distributed architectures. Many solutions benefit from the additional protection provided by Intel SGX. Solution examples include AI and ML processing, key management, proprietary algorithms, protection of biometrics, etc.

“At Intel SGX offers critical protections for password vault security today and for biometric factor matching.”

– Security Authentication Vendor

Figure 2: Application Partitioning

Figure 3: Runtime Execution

At runtime (see Figure 3), the Intel SGX instructions build & execute the enclave into a special encrypted memory region with restricted entry/exit location defined by the developer. This helps prevent data leakage: Enclave code & data inside the CPU perimeter runs in the clear and enclave data written to disk is encrypted and integrity checked. Helping ensure that no unauthorized access or memory snooping of the enclave is possible. (See Figure 4.)
“Hardware-based security technologies are a top priority for cloud providers aiming to address enterprise scaling challenges. Trusted execution technologies such as Intel SGX are now readily available in a wide range of platforms helping to fuel innovation in the digital security ecosystem and further assist in implementation roll-out.”

–Dimitrios Pavlakis, Industry Analyst, ABI Research

**Attesting Enclaves and Sealing Data**

Currently, device manufacturers and ISVs commonly provision application software and secrets at manufacturing time or via complex field configurations that cannot cryptographically prove application integrity. Intel SGX enables local attestation between enclaves or remote attestation by a Relying Party to help ensure the application has not been compromised.

The encrypted portion of an application is loaded into an enclave where its code and data is measured. An enclave report is sent to the remote application owner’s server which in turn can validate that the enclave report was generated by an authentic Intel processor. (See Figure 5). Upon verification of the enclave identity, the Relying Party can trust the enclave and provision keys, credentials, or other data.

![Figure 5: Attestation and Sealing](image)

Intel SGX includes an instruction for generating a CPU/enclave specific “Sealing Key” that can be used to safely store and retrieve sensitive information that may need to be stored to disk, or protected while outside the enclave.

**Data Center Attestation**

Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) (See Figure 6) allows the enterprise, data center and cloud service providers to build and deliver an attestation service themselves, rather than using the remote attestation from a 3rd party provider. This also removes the need for direct Internet access and allows all provisioning and quote verification to remain on the local network.

**Intel SGX Enables New Security Models and Innovation**

The foundational capability of Intel SGX is to enable software to be significantly less vulnerable to attacks, by providing a higher level of isolation and attestation for program code, data and critical IPs from the OS, applications and hardware on the platform. Intel SGX has been used to enhance security within multiple use cases and applications. Examples of these applications are listed on the following page:
**Engaging Intel SGX Resources**

Intel provides an SDK that is suitable to use with most production implementations. ISVs who want to ship commercial software that uses Intel SGX should follow the steps on the Intel SGX commercial license page to initiate the process of applying for a production license.

The Intel SGX SDK is a collection of APIs, runtime libraries, documentation, sample source code, and tools that allows software developers to create, debug, and deploy Intel SGX enabled applications using C/C++.

As part of the on-boarding process, ISVs & Enterprise developers can obtain an Intel SGX Launch Token and get their application listed on the Intel access list of certified implementations.

---

**INTEL SGX USE CASES**

**Increased Data Protection**
- In-use data in public clouds
- Electronic medical records (EMR)

**Store Keys with More Protections**
- Transport Layer Security (TLS) management for key stores
- Keys with more security protection on local file systems
- Virtual hardware security module (HSM)

**Content with More Protection**
- More security for viewing and sharing of documents
- Enhanced digital rights management (DRM) with more security

**Blockchain**
- Supply chain
- More secure contracts
- Hyperledger Sawtooth*

**Edge**
- Network functions virtualization (NFV)
- Edge routers for IoT
- Edge network appliances

---

**Specifications**

<table>
<thead>
<tr>
<th>REQUIRED HARDWARE</th>
<th>REQUIRED DEVELOPMENT SOFTWARE</th>
<th>SUPPORTED OS</th>
</tr>
</thead>
</table>
| • Intel® Xeon® processor E3-1500 v5 and v6  
• Intel® Xeon® processor E family 2100  
• 6th, 7th, 8th, and 9th generations of the Intel® Core™ processor family  
• Celeron® processor J4105 or J4005 (models that include BIOS with Intel SGX)  
• Intel® Platform Developer Kit for Intel SGX | **Windows:**  
• Microsoft Visual Studio 2015 or 2017 (Intel Parallel Studio is not required any longer).  
**Linux:**  
• GNU toolchain  
• Intel® SGX Eclipse® Plug-in | **Windows**  
• Windows® 10 64 bit November Update (version 1511) or newer  
• Windows® Server 2016/2019  
**Linux**  
• Ubuntu 16.04 LTS Server/Desktop 64-bit version  
• Ubuntu 18.04 LTS Server/Desktop 64-bit version  
• Red Hat® Enterprise Linux® Server 7.4 64-bit version  
• SUSE® Linux Enterprise Server 12 64-bit version  
• CentOS® 7.5 64-bit version  
• Fedora 27 Server 64-bit version |

---

Download Documentation and the SDK at: [software.intel.com/sgx](http://software.intel.com/sgx)

Intel technologies’ features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. Intel and the logo are trademarks of Intel Corporation in the U.S. and/or other countries.

* Other names and brands may be claimed as the property of others.

© 2019 Intel Corporation.