Product brief

Intel Platform Security Technologies
Intel® Software Guard Extensions

Enhanced Security Features for Applications and Data In-use

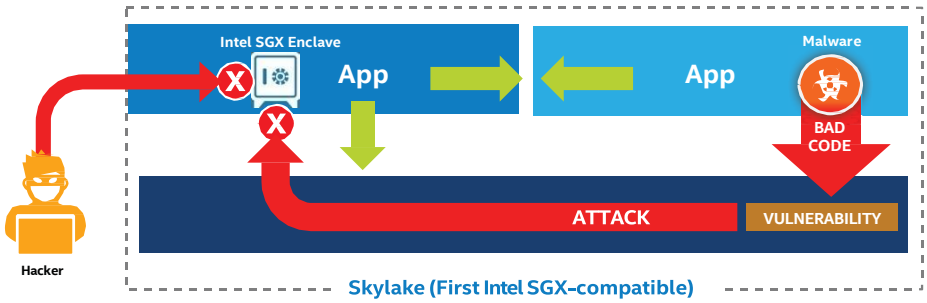
CPU hardening for Enhanced Application Security

Intel SGX delivers new instructions and memory access changes enabling a ground-breaking security model for developers. Hardware-assisted security technologies have 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 help increase application security (see Figure 1). Using this new application-layer trusted execution environment, developers can enable increased identity and records privacy, more secure browsing, DRM, hardened endpoint protection, and many high assurance security use cases that need to more 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 and executes on main CPU
- **Remotely Attest & Provision**
  A relying party can verify an application enclave's identity and more securely provision keys, credentials and other sensitive data into the enclave
- **Help Significantly Reduce Attack Surface**
  The application runs and creates the enclave which is placed in trusted memory.



Intel SGX Capable System

Figure 1: Empower developers to better protect code and data

"Intel SGX offers critical protections for password vault security today and for biometric factor matching."

– Security Authentication Vendor

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

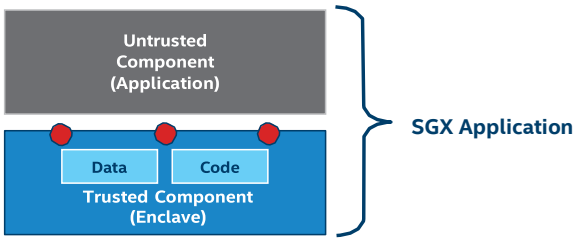


Figure 2: Application Partitioning

Developing Intel SGX Applications

In Figure 2, the application design illustrates an Intel SGX application that includes two parts: an untrusted component that launches, and a trusted part where production code runs in an 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.

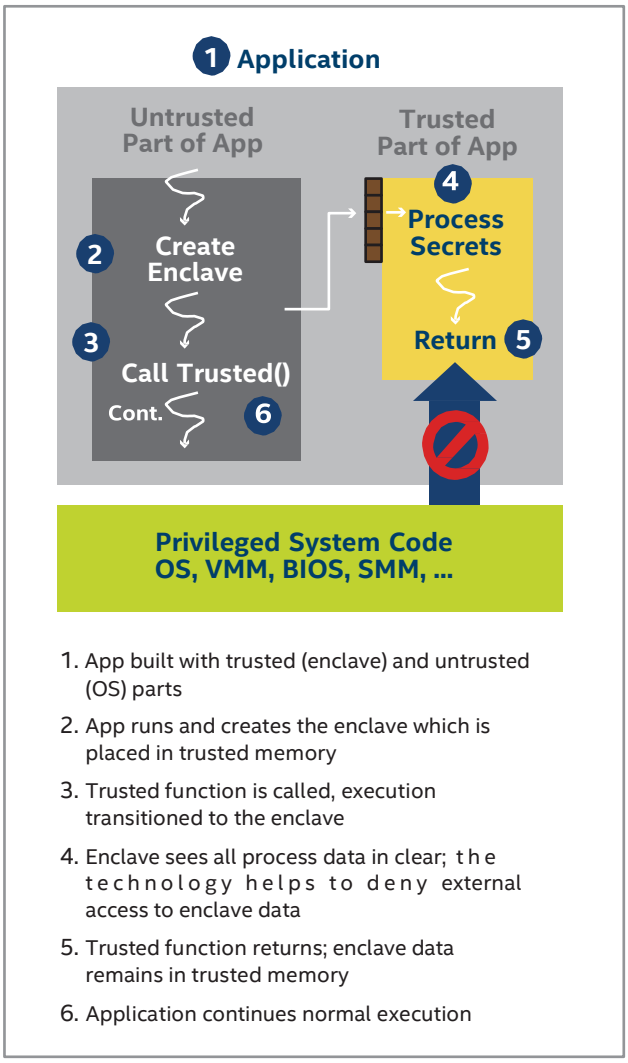


Figure 3: Runtime Execution

At runtime (see Figure 3), the Intel SGX instructions build and 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 and data inside the CPU perimeter runs in the clear, and enclave data written to memory is encrypted and integrity checked, helping provide some assurance that no unauthorized access or memory snooping of the enclave occurs. (See Figure 4.)

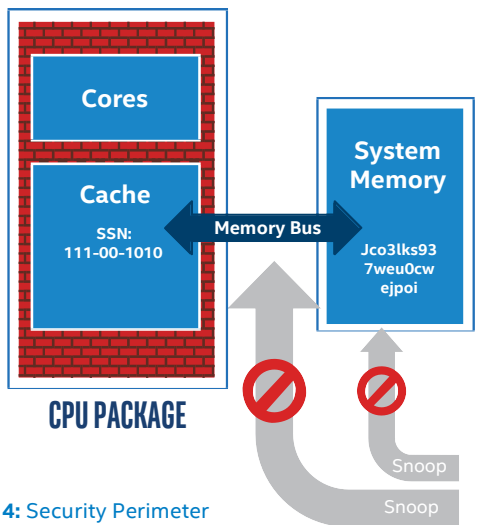


Figure 4: Security Perimeter

"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

Reference here

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 portion of an application is loaded into an enclave where its code and data are 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 have more trust in the enclave and provision keys, credentials, or other data.

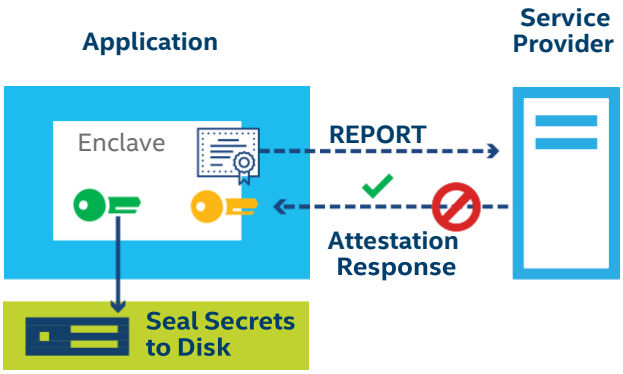


Figure 5: Attestation and Sealing

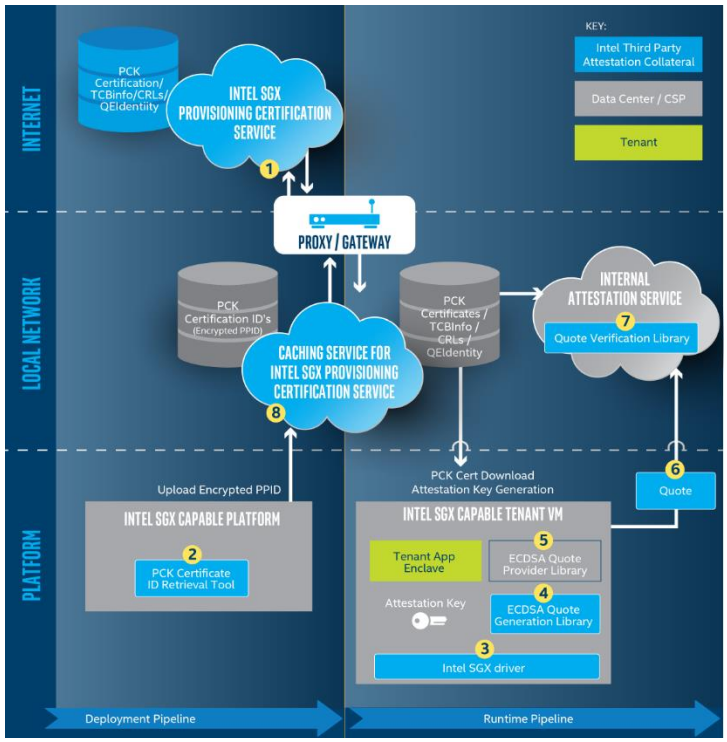


Figure 6: Intel® SGX Data Center Attestation Primitives

Intel SGX includes an instruction for generating a CPU/ enclave specific "Sealing Key" that can be used to more 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 Helps Enable New Security Models and Innovation

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

USE CASES

Key Management
Use enclaves to help manage cryptographic keys and provide HSM-like functionality.

Blockchain
Help increase privacy and security for transaction processing, consensus, smart contracts and key storage.

Privacy Enhancing Analytics and Workloads
Provide additional privacy and enable isolation for multi-party joint computation on sensitive data.

Applications at Runtime
Run unmodified applications within enclaves.

Hardware-Enhanced Content Protection
Help content owners protect their IP, through unaltered or unmodified streaming.

Enhanced Application and Data Protection
Help secure code execution with data isolation for increased protection.

Edge Computing
Help secure IoT edge devices to cloud and client communications.

Digital Wallet
More defense to help secure payments and transactions.

Communications and Messaging
Help secure communications between sender and recipient.

Intel SGX Resources

Intel provides an SDK that is suitable to use with many 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.

Intel SGX commercial license information:
https://software.intel.com/sgx/request-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++.

Intel SGX SDK:
https://software.intel.com/sgx/sdk

As part of the on-boarding process, ISVs and Enterprise developers can apply for and obtain permission for their enclave(s) to be added to the Intel access list of certified implementations.

We remind the reader that no product or component can be absolutely secure.

Specifications

REQUIRED HARDWARE

- 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

REQUIRED DEVELOPMENT SOFTWARE

Windows:

- Microsoft Visual Studio* 2015 or 2017 (Intel Parallel Studio is not required any longer).

Linux:

- GNU* toolchain
- Intel® SGX Eclipse* Plug-in

SUPPORTED OS

Windows

- Window* 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**