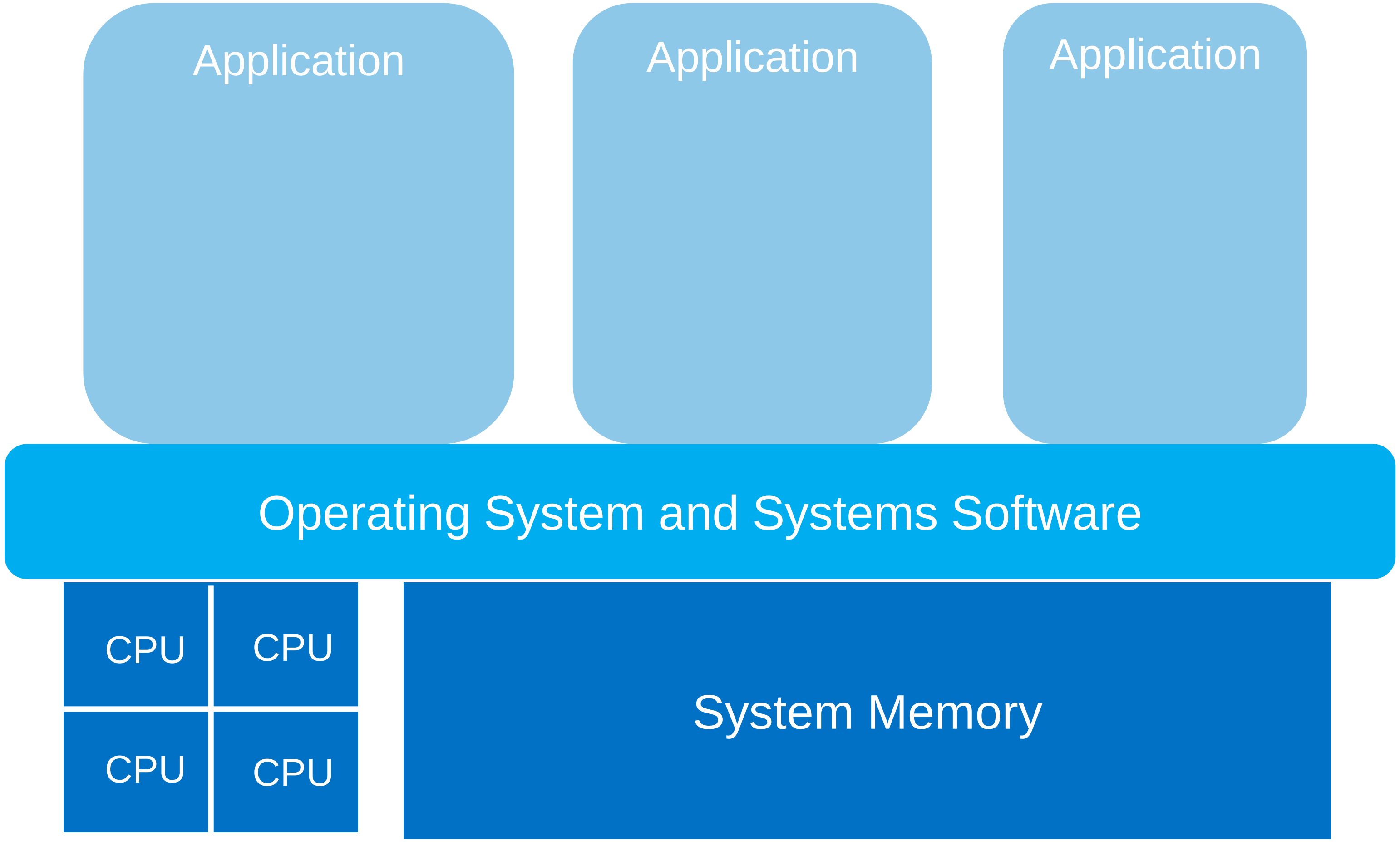
Sealing and Attestation in Intel® Software Guard Extensions (SGX)

Rebekah Leslie-Hurd
Intel® Corporation

January 8th, 2016

A Typical Computing Platform



Platform w/ Software Guard Extensions (SGX)

Secure enclave:

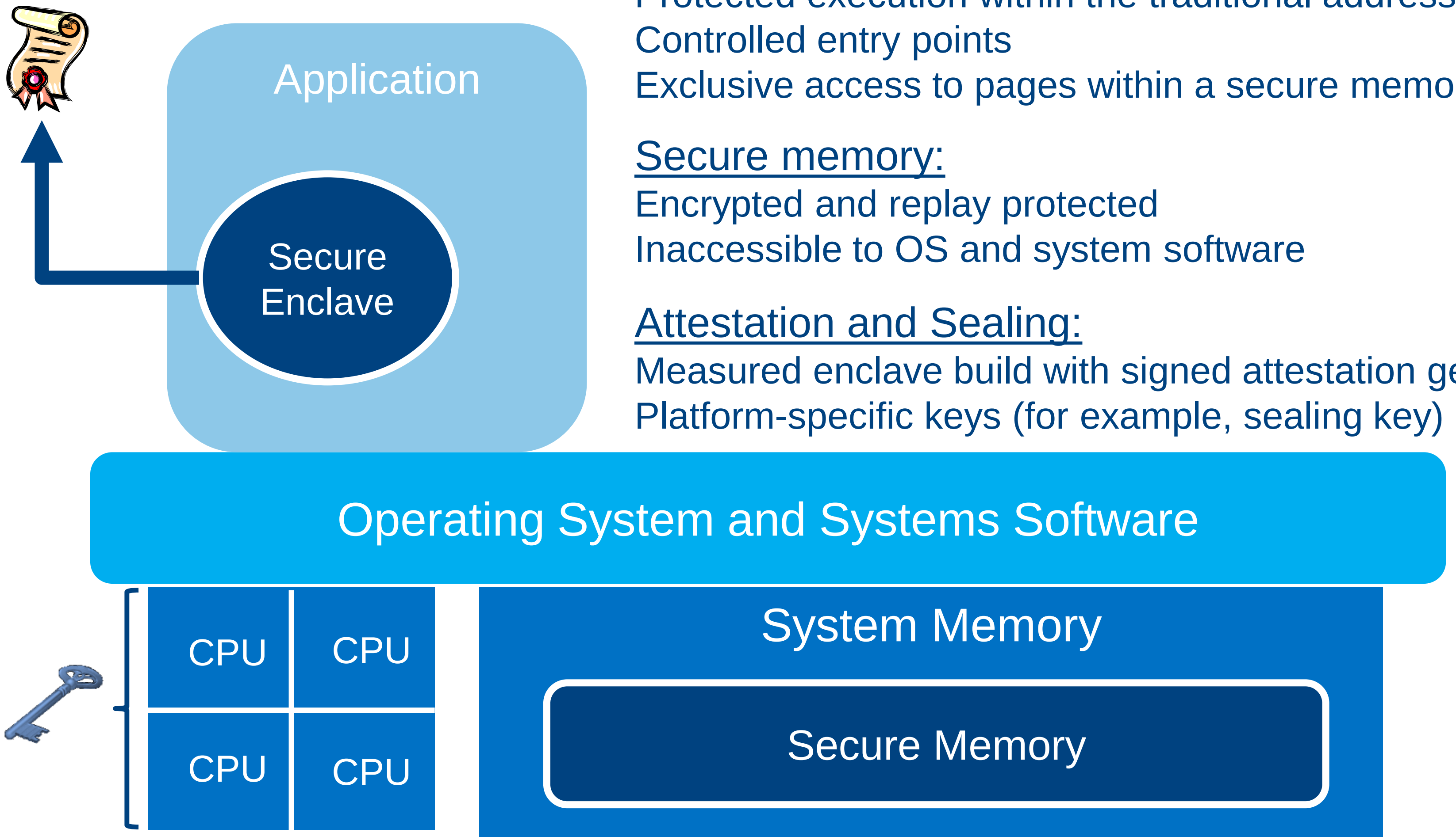
Protected execution within the traditional address space
Controlled entry points
Exclusive access to pages within a secure memory

Secure memory:

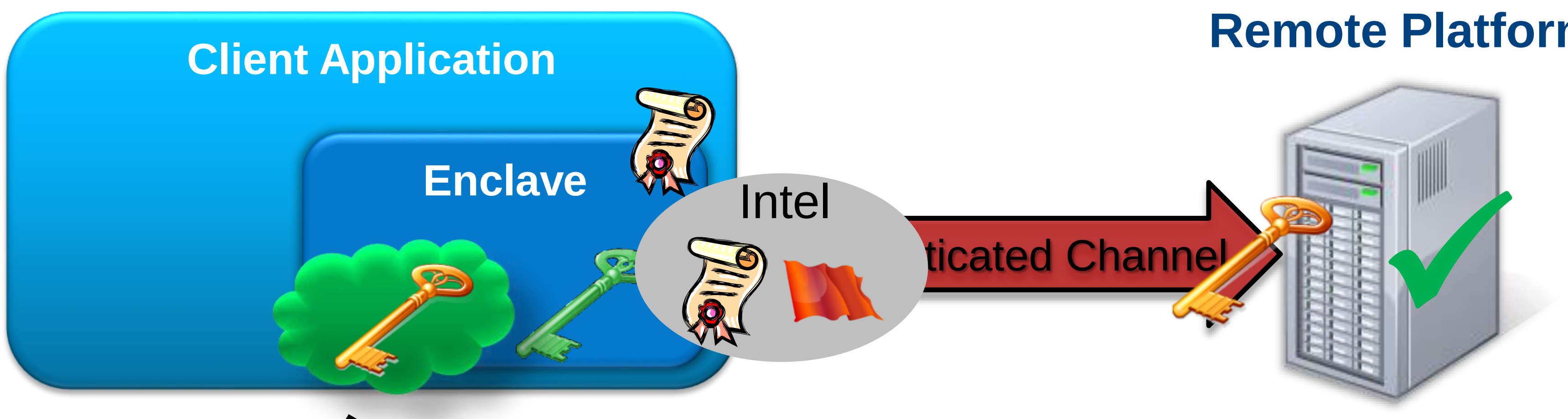
Encrypted and replay protected
Inaccessible to OS and system software

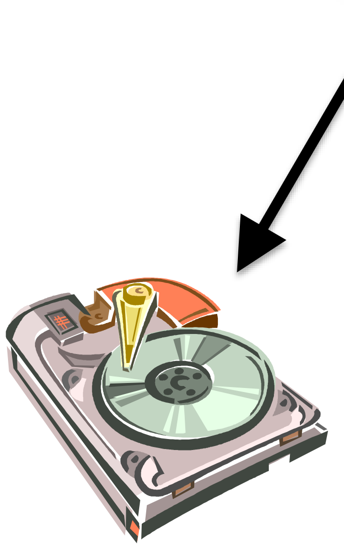
Attestation and Sealing:

Measured enclave build with signed attestation generation
Platform-specific keys (for example, sealing key)



Attestation and Sealing Overview





Enclave is built and **measured**

HW based **attestation** provides evidence that “this is the right application executing on an authentic platform”

Remote platform provisions secrets to the local platform

Enclave uses its platform-specific **sealing** key to store secrets for later use

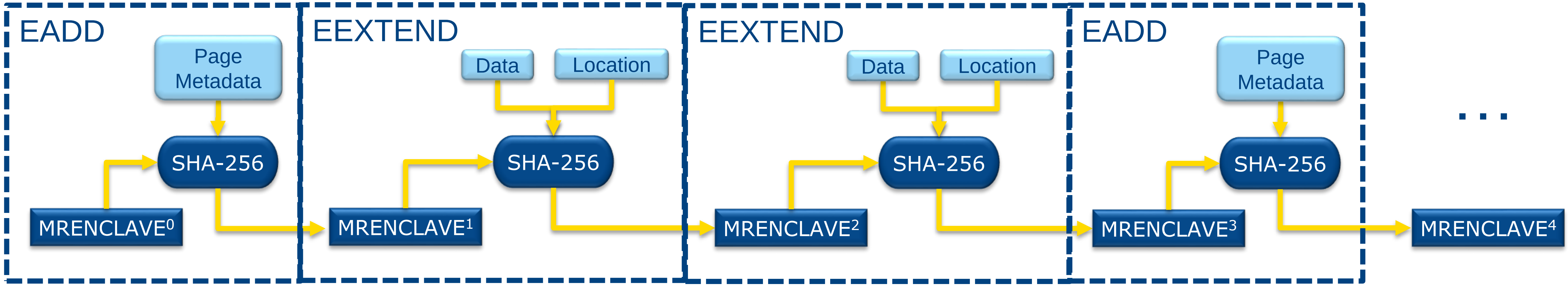
Enclave Measurement

When building an enclave, hardware generates a cryptographic log of the build process

- Code, data, stack, and heap contents
- Location of each page within the enclave
- Security attributes (e.g., page permissions) and enclave capabilities (e.g., debug mode)

Enclave identity (MRENCLAVE) is a 256-bit digest of the log that represents the enclave

- Provided during attestation to remote platform



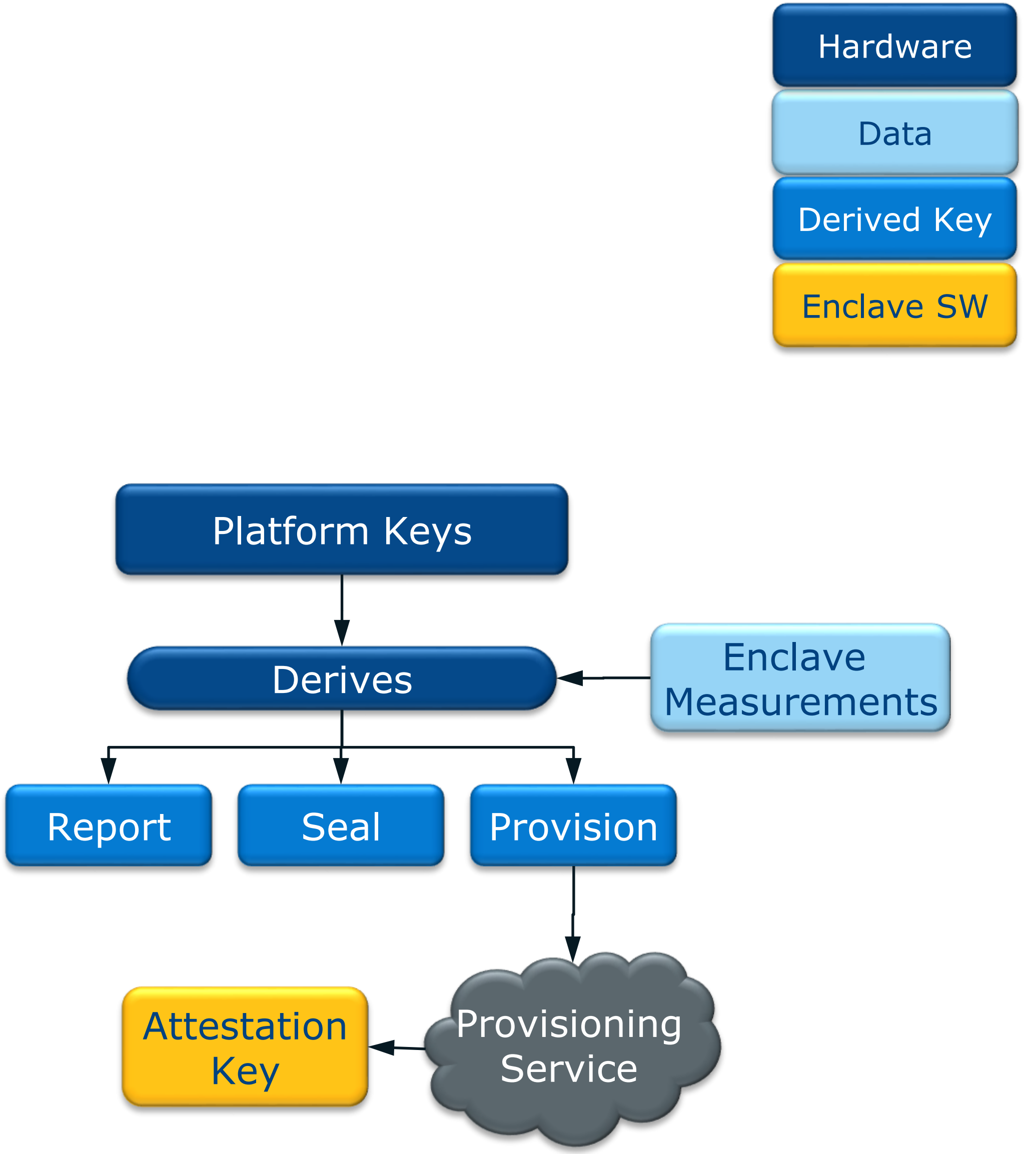
SGX Key Hierarchy

SGX hardware provides unique per-platform keys for various operations

- Seal key for data protection
- Report key for attestation between enclaves
- Provisioning key for negotiating attestation key

Enclave software gains access to platform keys via the EGETKEY instruction

EGETKEY key derivation algorithm uses enclave identity to produce enclave-specific versions of each key type



Attestation

SGX provides both local and remote attestation capabilities

Local attestation allows an enclave to attest its identity and its TCB to another enclave on the *same platform*

Remote attestation allows an enclave to attest its identity and its TCB to another entity *outside of the platform*

Local Attestation

Enclave software uses the EREPORT instruction to construct a hardware-based assertion describing the enclave's identity, called a *report*

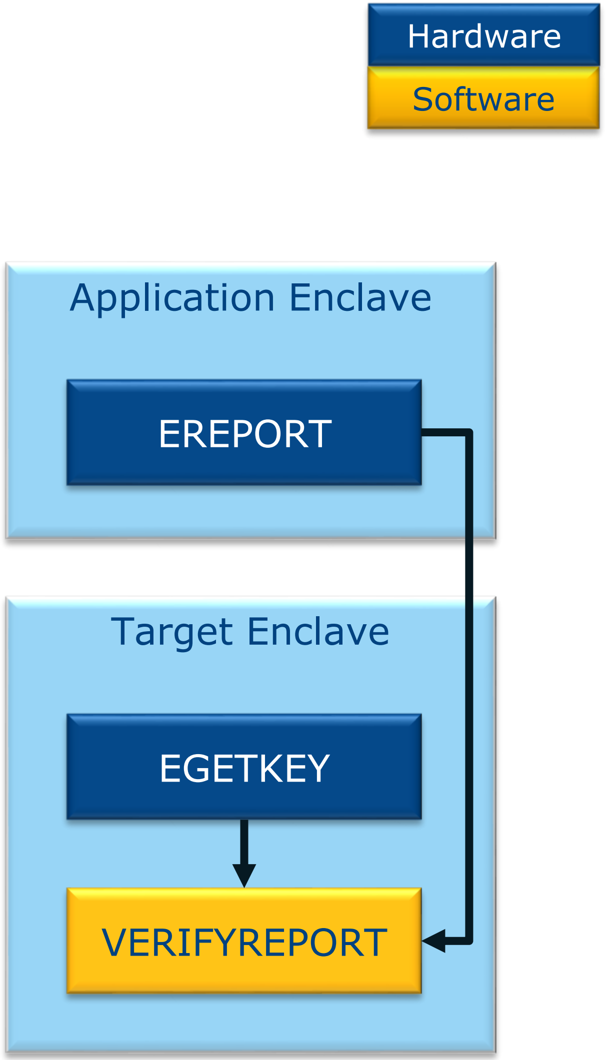
Report contents:

- Enclave attributes
- Enclave measurement
- User-supplied data (e.g., public key)

EREPORT is parameterized by the desired target of the attestation

- Provided by calling enclave
- Report structure is secured by EREPORT using the *report key* of the target enclave

Target enclave uses its report key to verify the report structure (in software)



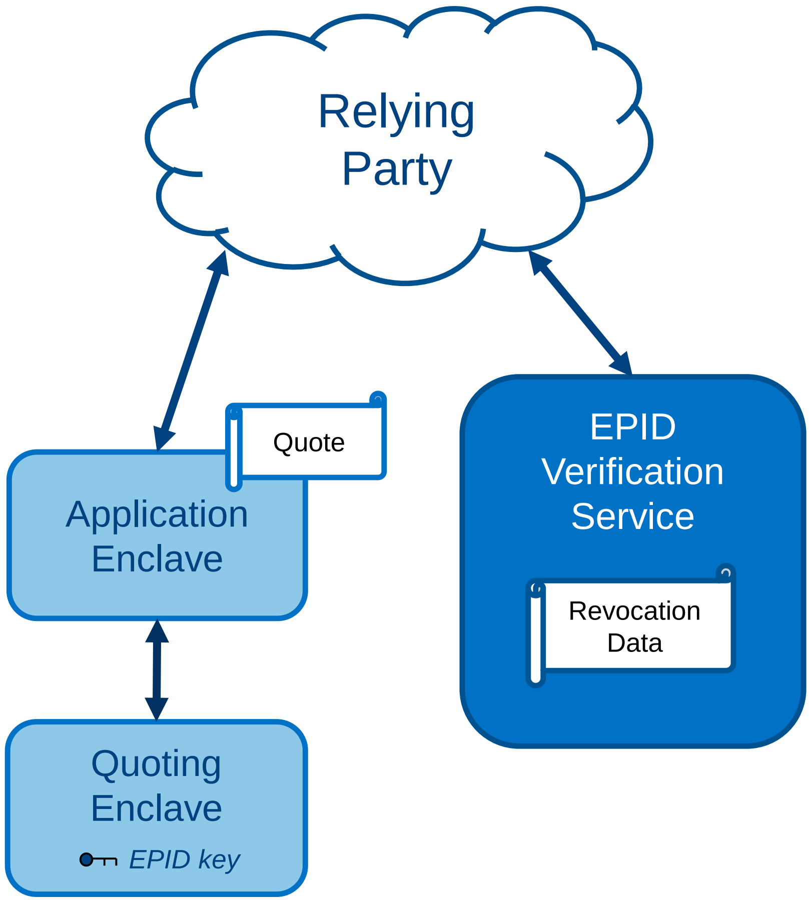
Remote Attestation

Platform identity

- Based on Intel® Enhanced Privacy Identifier (EPID)
  - Group-based anonymous signature scheme
- Provided by Intel® provisioning service

Intel® provides a Quoting Enclave that converts a local attestation into a remote attestation

- Application enclave produces a local report structure that targets the Quoting Enclave
- Quoting Enclave locally verifies the report and is able to determine:
  - Hardware produced the report
  - The application enclave is running on the same hardware platform
- Quoting Enclave signs a quote containing the report data and platform identity



Securely Storing Enclave Secrets

Enclave secrets that live in protected memory are destroyed during enclave tear-down

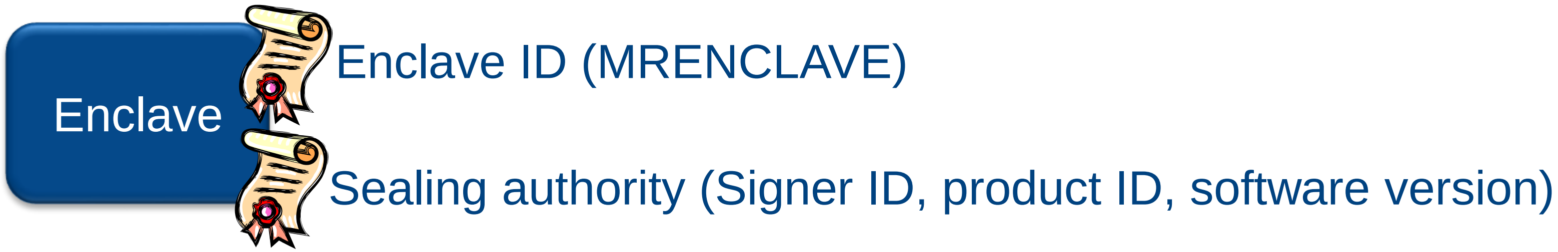
SGX supports the ability to seal secrets to a platform so that enclave data can be cryptographically protected when it is stored outside of the enclave

- EGETKEY returns persistent sealing key that is enclave- and platform-specific

Enclave encrypts data using the sealing key and the software algorithm of its choice before saving it to disk

Enclave Sealing Authority

Each enclave may be signed by a sealing authority



Sealing key may be based on:

- Enclave identity (tied to the current version of the enclave code) or
- Sealing authority (supports secure storage across software upgrades)

Binding to the sealing authority enables the signer to control access to sealed data across versions

- Authorize new enclaves to access old data by signing those enclaves with the same key
- Assign enclave versions to allow upgrades to access existing data while preventing old versions from accessing new data

Conclusions

SGX is an extension to the Intel® instruction set architecture enables developers to run application code within a protected container called an *enclave*

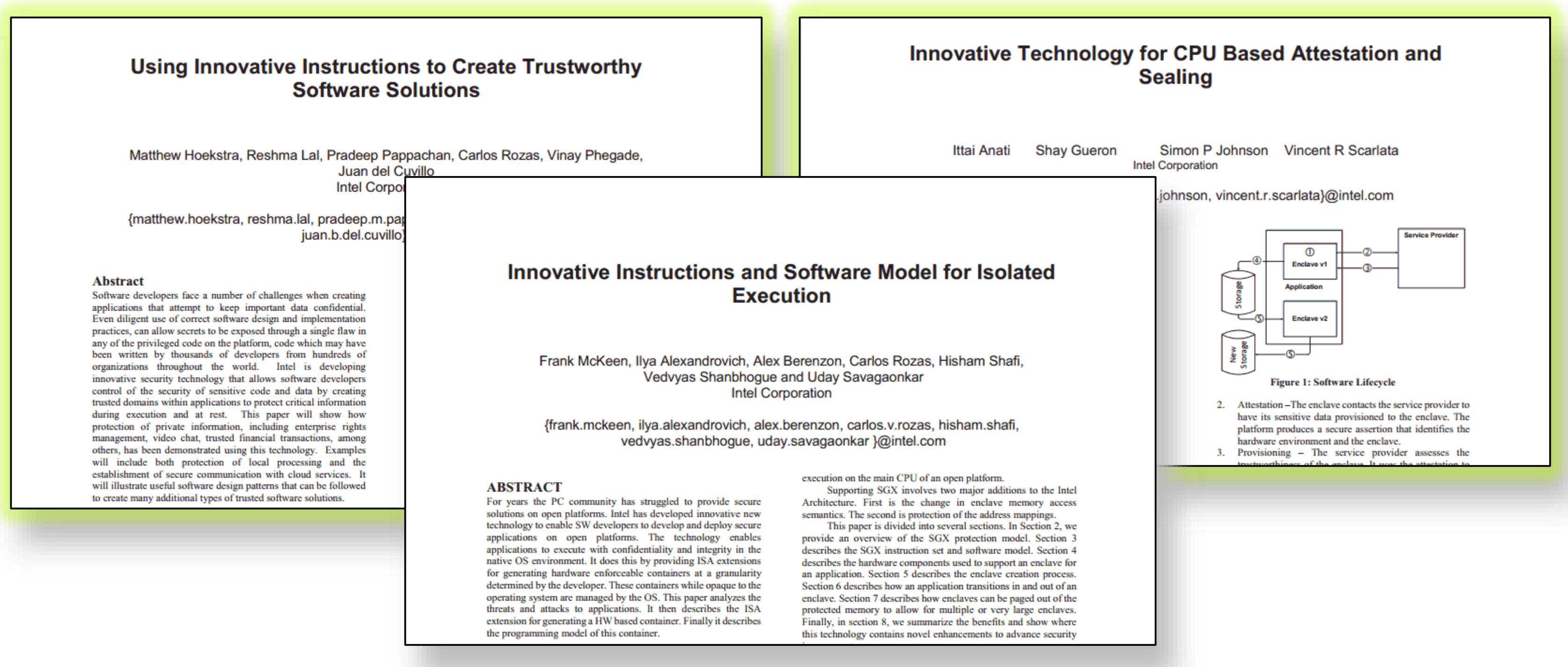
Enclaves are measured during the build process

- Enables hardware to establish the identity of each enclave
- Allows remote parties to validate the integrity of the running software

Local and remote attestation capabilities are combined to enable a remote party to securely provision secrets to an enclave

Data sealing capability enables an enclave to securely store secrets, access stored secrets across software versions, and avoid the overhead of attestation and provisioning during a typical execution

Questions?



Using Innovative Instructions to Create Trustworthy Software Solutions

Matthew Hoekstra, Reshma Lal, Pradeep Pappachan, Carlos Rozas, Vinay Phegade, Juan del Cuvillo
Intel Corpo

{matthew.hoekstra, reshma.lal, pradeep.m.pap
juan.b.del.cuvillo}

Abstract
Software developers face a number of challenges when creating applications that attempt to keep important data confidential. Even diligent use of correct software design and implementation practices, can allow secrets to be exposed through a single flaw in any of the privileged code on the platform, code which may have been written by thousands of developers from hundreds of organizations throughout the world. Intel is developing innovative security technology that allows software developers control of the security of sensitive code and data by creating trusted domains within applications to protect critical information during execution and at rest. This paper will show how protection of private information, including enterprise rights management, video chat, trusted financial transactions, among others, has been demonstrated using this technology. Examples will include both protection of local processing and the establishment of secure communication with cloud services. It will illustrate useful software design patterns that can be followed to create many additional types of trusted software solutions.

Innovative Technology for CPU Based Attestation and Sealing

Ittai Anati Shay Gueron Simon P Johnson Vincent R Scarlata
Intel Corporation

.johnson, vincent.r.scarlata}@intel.com

Figure 1: Software Lifecycle

2. Attestation – The enclave contacts the service provider to have its sensitive data provisioned to the enclave. The platform produces a secure assertion that identifies the hardware environment and the enclave.
3. Provisioning – The service provider assesses the

Innovative Instructions and Software Model for Isolated Execution

Frank McKeen, Ilya Alexandrovich, Alex Berenzon, Carlos Rozas, Hisham Shafi, Vedvyas Shanbhogue and Uday Savagaonkar
Intel Corporation

{frank.mckeen, ilya.alexandrovich, alex.berenzon, carlos.v.rozas, hisham.shafi, vedvyas.shanbhogue, uday.savagaonkar }@intel.com

ABSTRACT
For years the PC community has struggled to provide secure solutions on open platforms. Intel has developed innovative new technology to enable SW developers to develop and deploy secure applications on open platforms. The technology enables applications to execute with confidentiality and integrity in the native OS environment. It does this by providing ISA extensions for generating hardware enforceable containers at a granularity determined by the developer. These containers while opaque to the operating system are managed by the OS. This paper analyzes the threats and attacks to applications. It then describes the ISA extension for generating a HW based container. Finally it describes the programming model of this container.

execution on the main CPU of an open platform.
Supporting SGX involves two major additions to the Intel Architecture. First is the change in enclave memory access semantics. The second is protection of the address mappings.
This paper is divided into several sections. In Section 2, we provide an overview of the SGX protection model. Section 3 describes the SGX instruction set and software model. Section 4 describes the hardware components used to support an enclave for an application. Section 5 describes the enclave creation process. Section 6 describes how an application transitions in and out of an enclave. Section 7 describes how enclaves can be paged out of the protected memory to allow for multiple or very large enclaves. Finally, in section 8, we summarize the benefits and show where this technology contains novel enhancements to advance security

SGX Whitepapers and Programing Reference Manual

- http://software.intel.com/en-us/intel-isa-extensions

Contact

- Rebekah Leslie-Hurd (rebekah.leslie-hurd@intel.com)

Legal Disclaimer

Intel technologies may require enabled hardware, specific software, or services activation. Check with your system manufacturer or retailer.

No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses.