



Intel® Software Guard Extensions(Intel® SGX), Instructions and Programming Model

Frank McKeen, Ilya Alexandrovich, Alex
Berenzon, Carlos Rozas, Vedvyas Shanbhogue,
Uday Savagaonkar

June 24, 2013

Legal Disclaimers

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: <http://www.intel.com/design/literature.htm>

No computer system can provide absolute security under all conditions. Built-in security features available on select Intel® processors may require additional software, hardware, services and/or an Internet connection. Results may vary depending upon configuration. Consult your system manufacturer for more details.

Intel®, the Intel® Logo, Intel® Inside, Intel® Core™, Intel® Atom™, and Intel® Xeon® 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.

Intel® compilers, associated libraries and associated development tools may or may not optimize to the same degree for non-Intel microprocessors for optimizations that are not unique to Intel microprocessors. These optimizations include Intel® Streaming SIMD Extensions 2 (Intel® SSE2), Intel® Streaming SIMD Extensions 3 (Intel® SSE3), and Supplemental Streaming SIMD Extensions 3 (Intel® SSSE3) instruction sets and other optimizations. Intel does not guarantee the availability, functionality, or effectiveness of any optimization on microprocessors not manufactured by Intel. Microprocessor-dependent optimizations in this product are intended for use with Intel microprocessors.

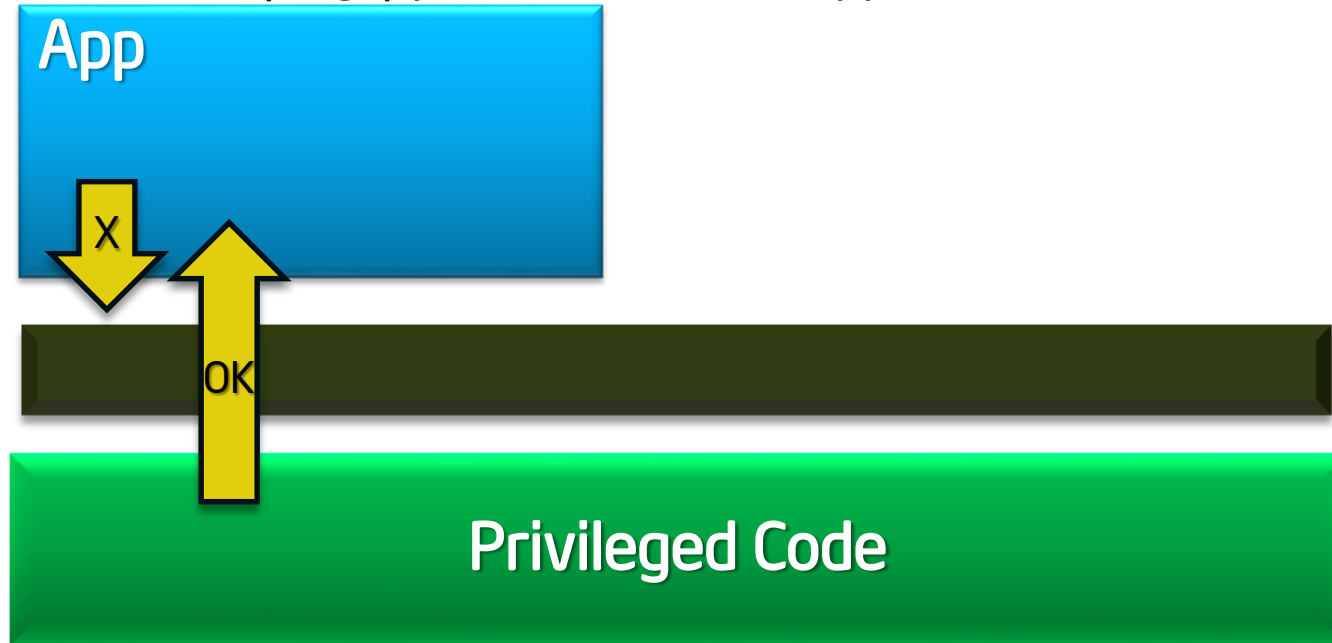
Copyright © 2013 Intel® Corporation

Outline

- Problem Statement
- Attack Surface and Overview
- Programming environment
 - System programming view
 - Day in the life of an enclave
- SGX protected memory paging
 - Evictions
 - Loads
- Off Chip protections
- Summary

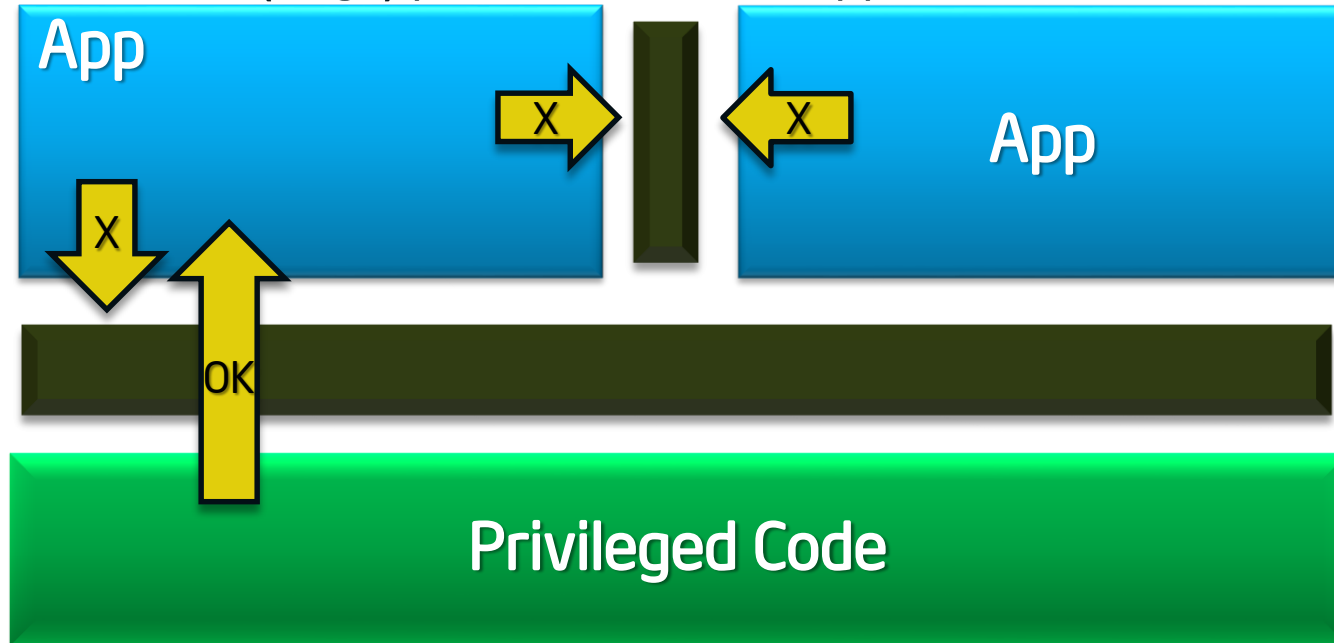
The Basic Issue: Why Aren't Compute Devices Trustworthy?

Protected Mode (rings) protects OS from apps ...



The Basic Issue: Why Aren't Compute Devices Trustworthy?

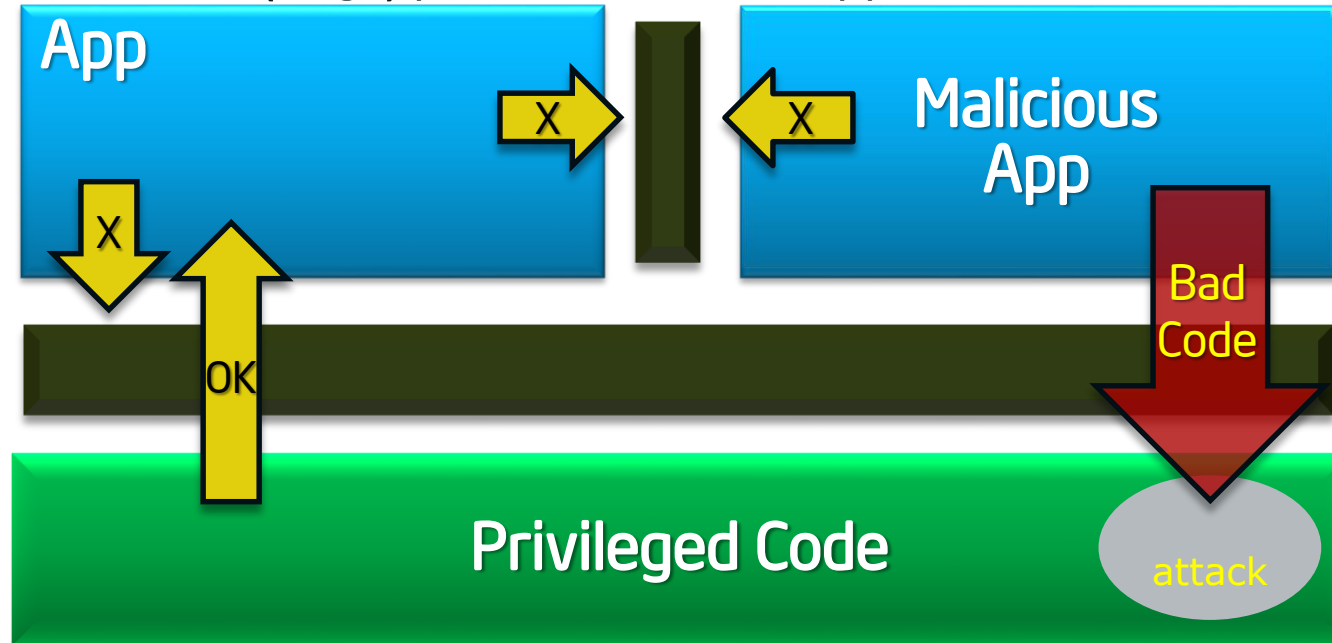
Protected Mode (rings) protects OS from apps ...



... and apps from each other ...

The Basic Issue: Why Aren't Compute Devices Trustworthy?

Protected Mode (rings) protects OS from apps ...

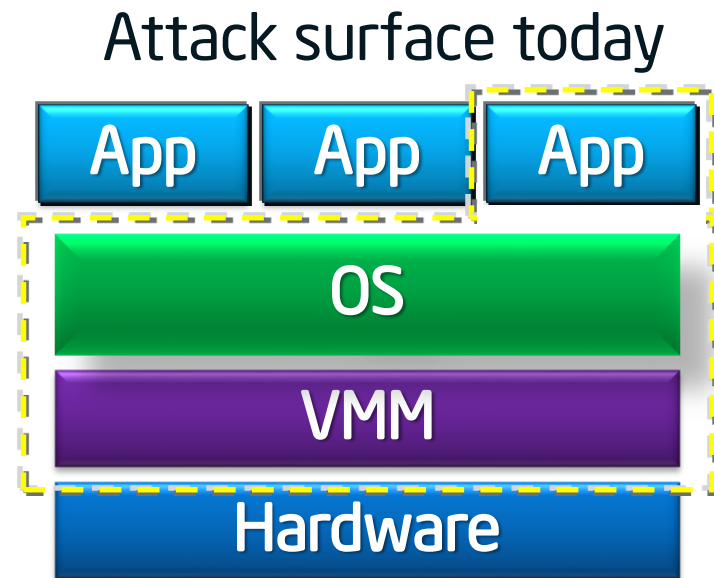



... and apps from each other ...

... UNTIL a malicious app exploits a flaw to gain full privileges and then tampers with the OS or other apps

Apps not protected from privileged code attacks

Reduced attack surface with Intel® SGX



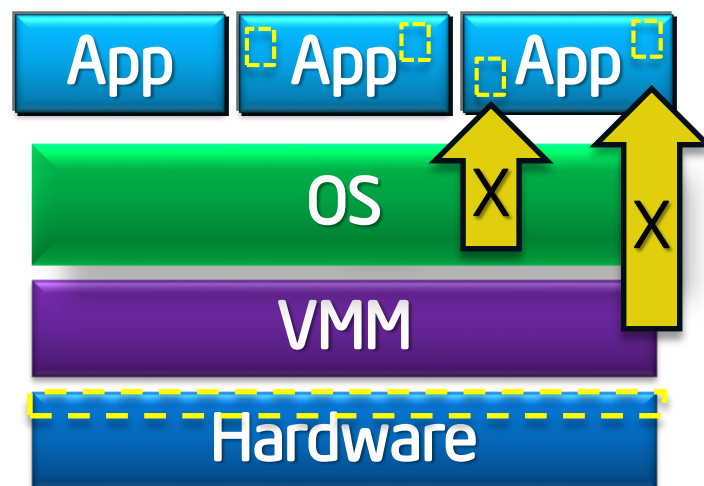
Attack Surface 

Reduced attack surface with Intel® SGX

Application gains ability to defend its own secrets

- Smallest attack surface (App + processor)
- Malware that subverts OS/VMM, BIOS, Drivers etc. cannot steal app secrets

Attack surface with Intel® SGX



Attack Surface 

Reduced attack surface with Intel® SGX

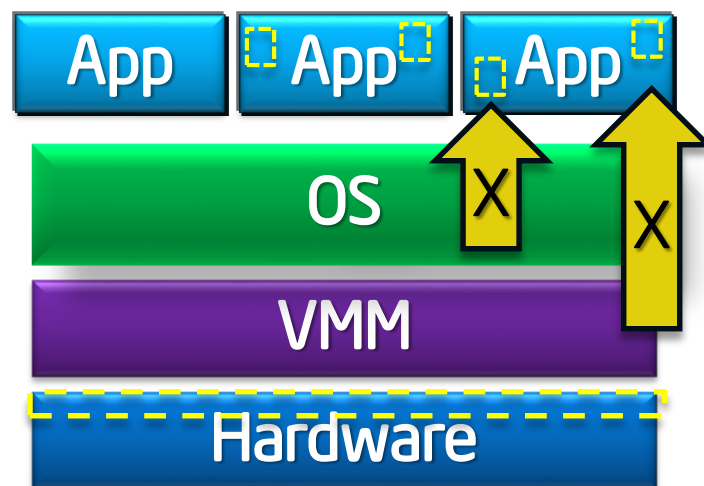
Application gains ability to defend its own secrets

- Smallest attack surface (App + processor)
- Malware that subverts OS/VMM, BIOS, Drivers etc. cannot steal app secrets

Familiar development/debug

- Single application environment
- Build on existing ecosystem expertise

Attack surface with Intel® SGX



Attack Surface 

Reduced attack surface with Intel® SGX

Application gains ability to defend its own secrets

- Smallest attack surface (App + processor)
- Malware that subverts OS/VMM, BIOS, Drivers etc. cannot steal app secrets

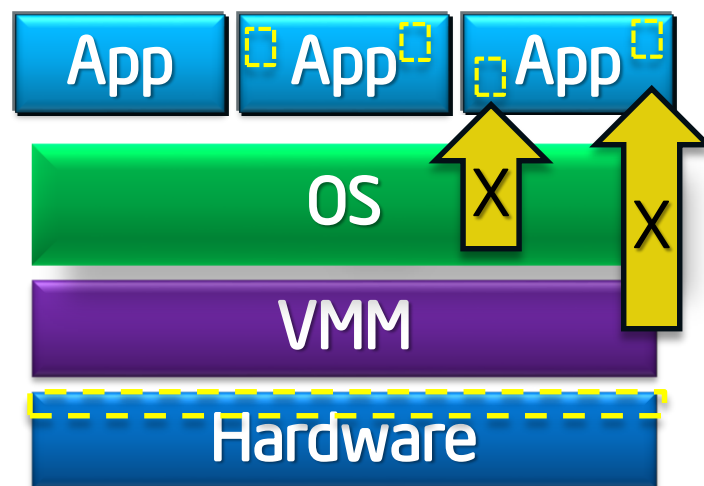
Familiar development/debug

- Single application environment
- Build on existing ecosystem expertise

Familiar deployment model

- Trusted applications can be distributed and updated by app developers as needed

Attack surface with Intel® SGX

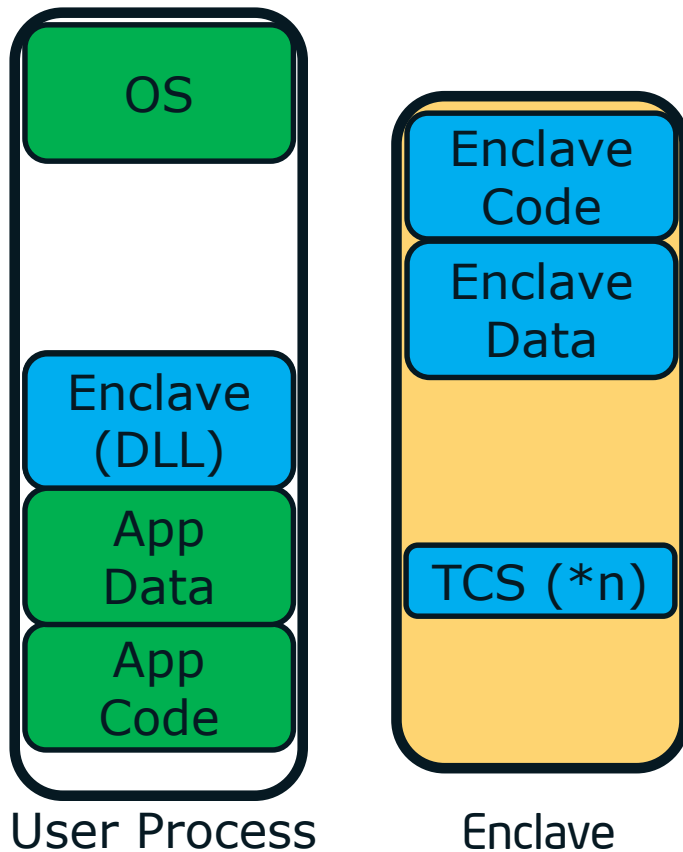


Attack Surface 

Scalable security within mainstream environment

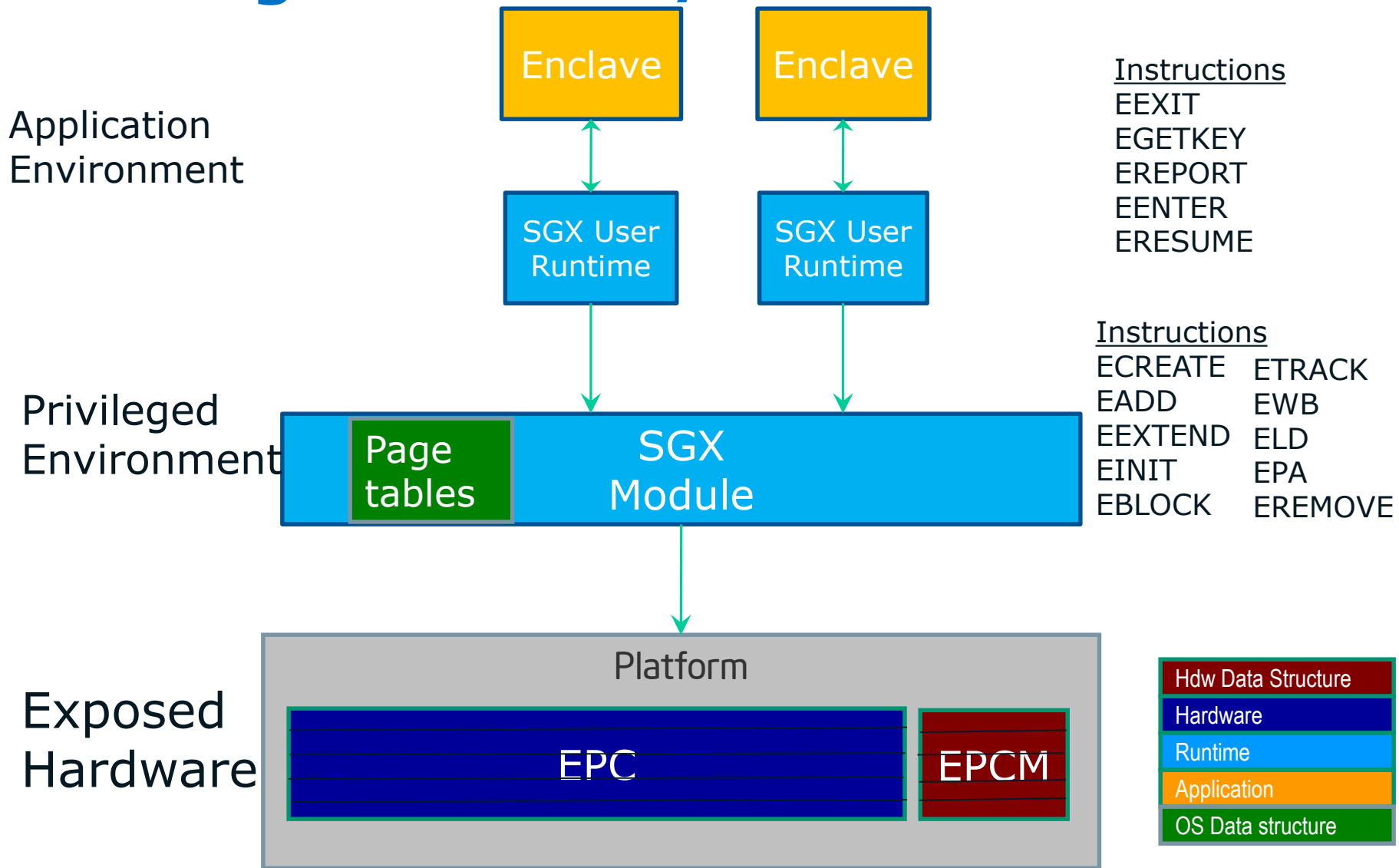
SGX Programming Environment

Protected execution environment embedded in a process



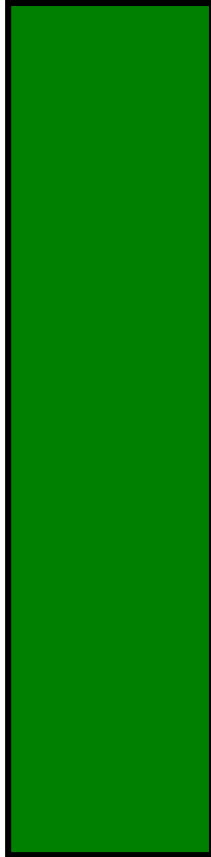
With its own code and data
Provide Confidentiality
Provide integrity
With controlled entry points
Supporting multiple threads
With full access to app memory

SGX High-level HW/SW Picture



Life Cycle of An Enclave

Virtual Addr Space



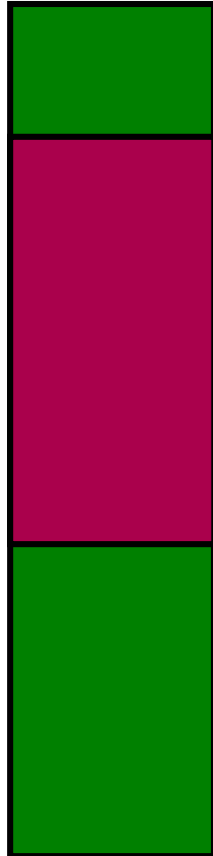
Physical Addr Space



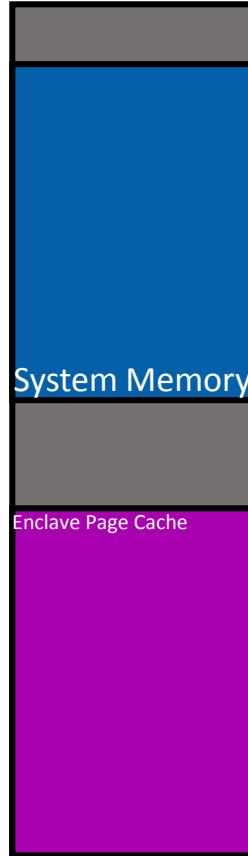
Build

Life Cycle of An Enclave

Virtual Addr Space



Physical Addr Space



ECREATE (Range)

Build

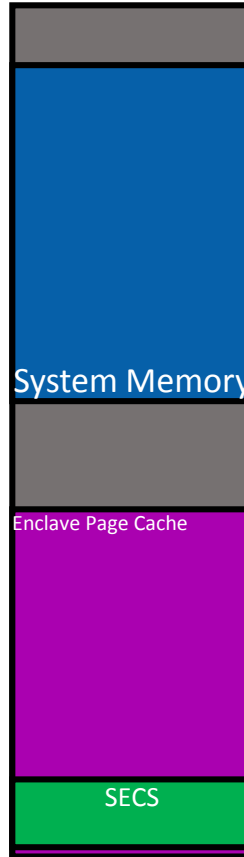


Life Cycle of An Enclave

Virtual Addr Space



Physical Addr Space



ECREATE (Range)

Build

MRENCLAVE

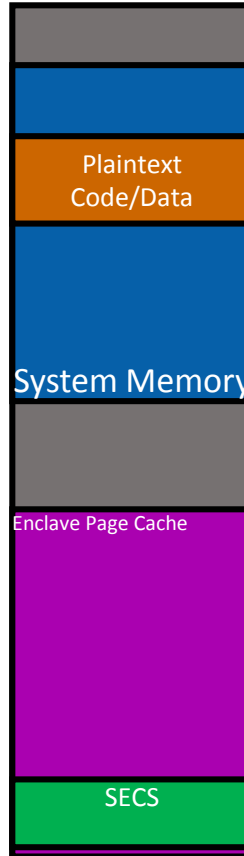


Life Cycle of An Enclave

Virtual Addr Space



Physical Addr Space



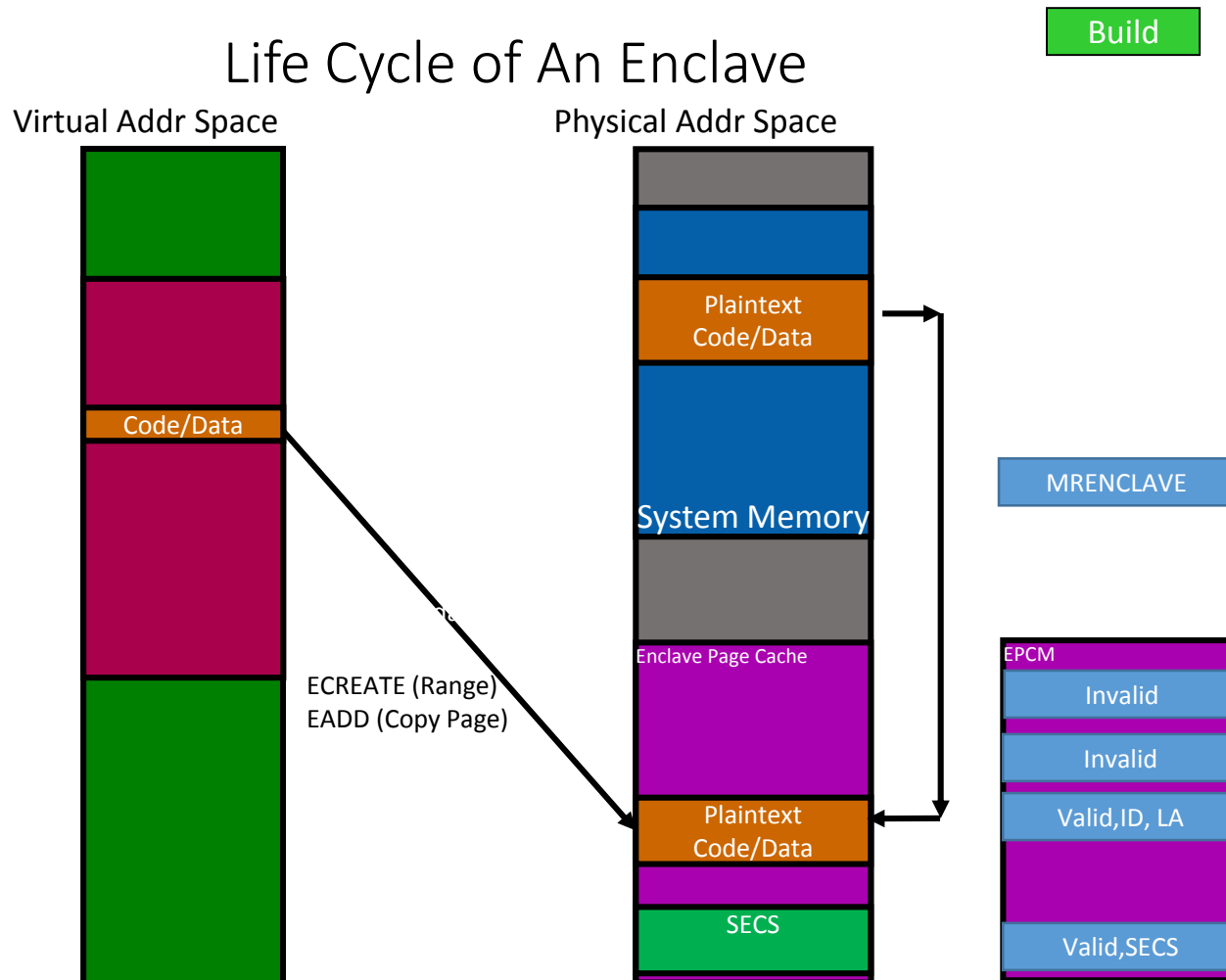
ECREATE (Range)

Build

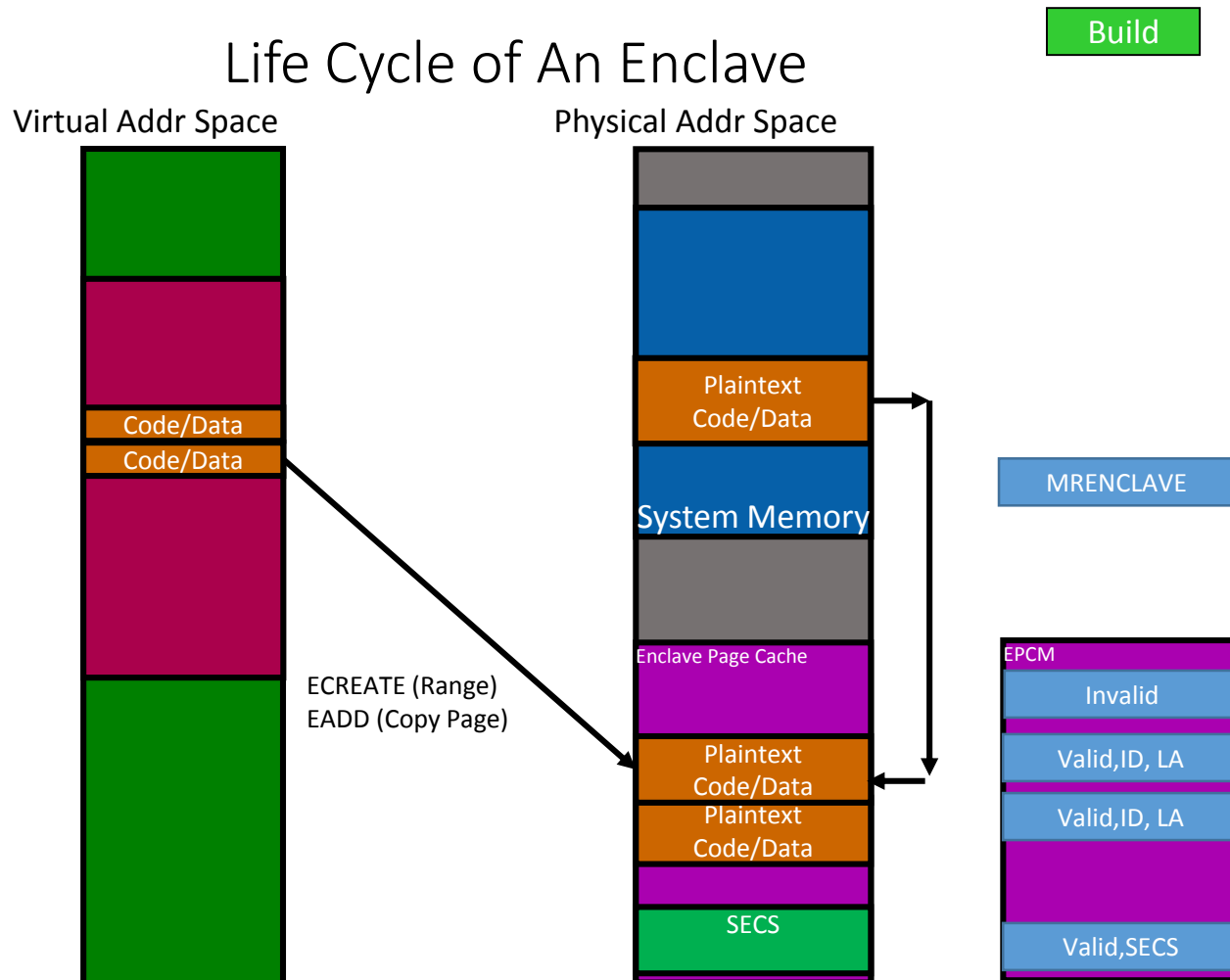
MRENCLAVE



Life Cycle of An Enclave

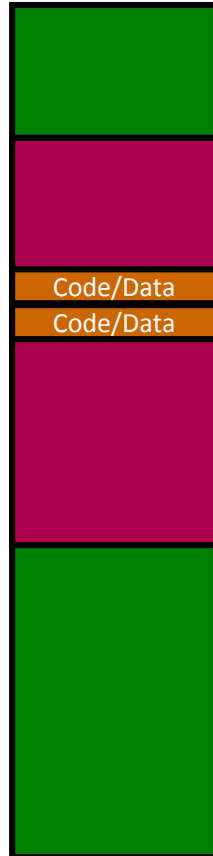


Life Cycle of An Enclave



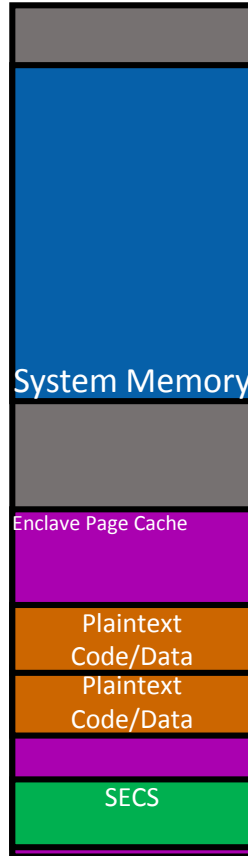
Life Cycle of An Enclave

Virtual Addr Space



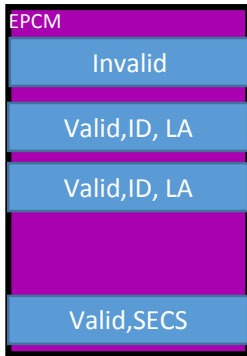
ECREATE (Range)
EADD (Copy Page)
EEXTEND

Physical Addr Space

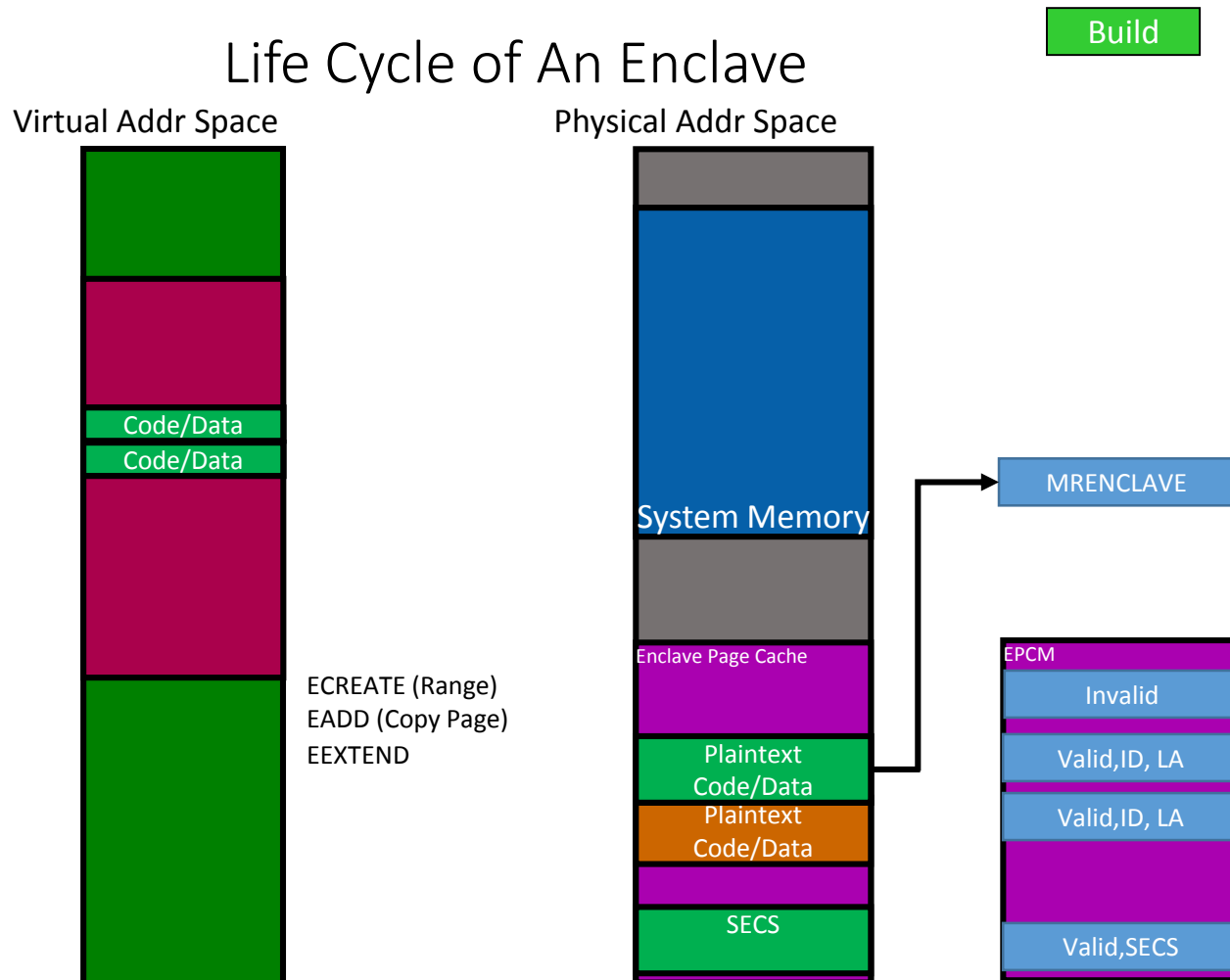


Build

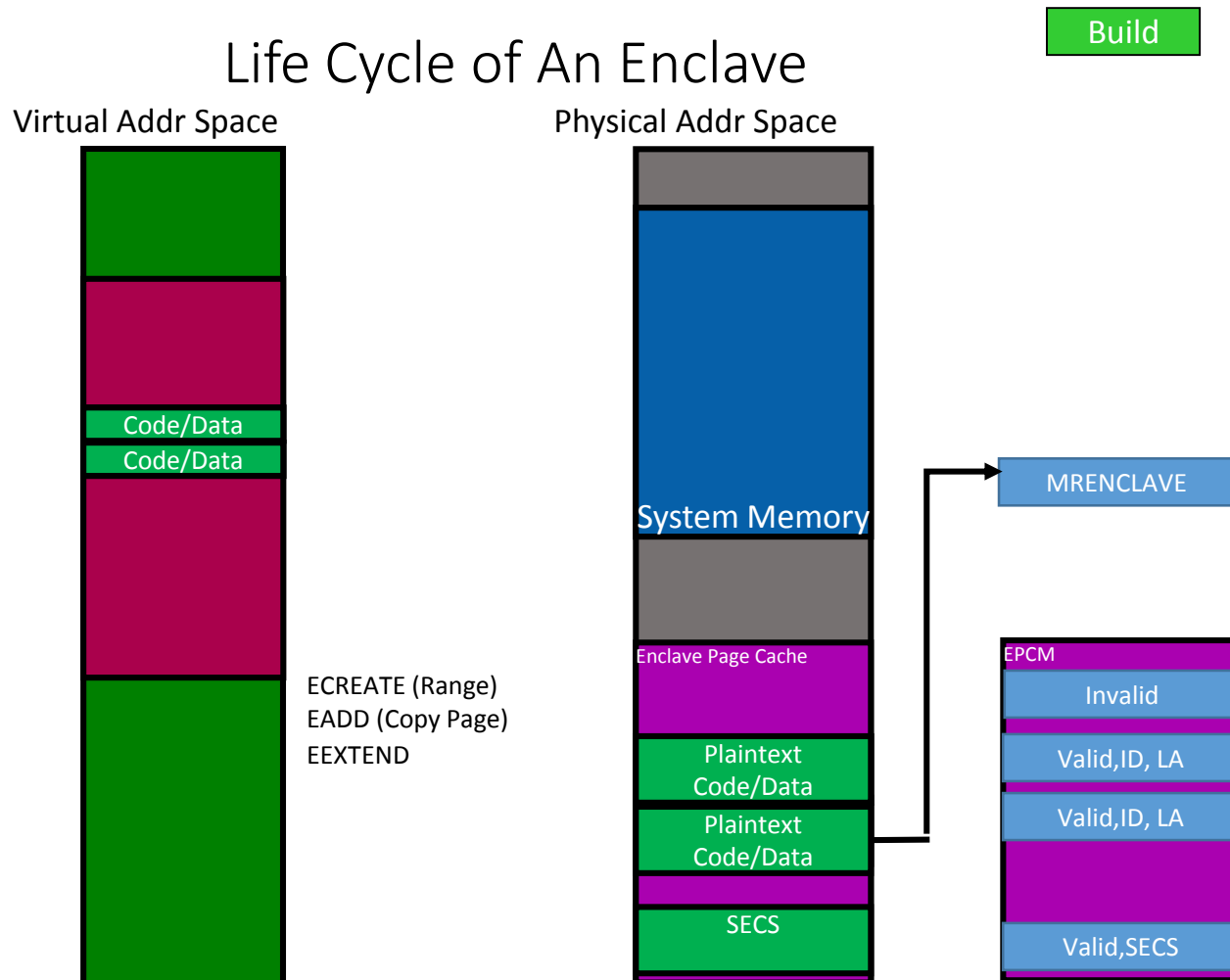
MRENCLAVE



Life Cycle of An Enclave

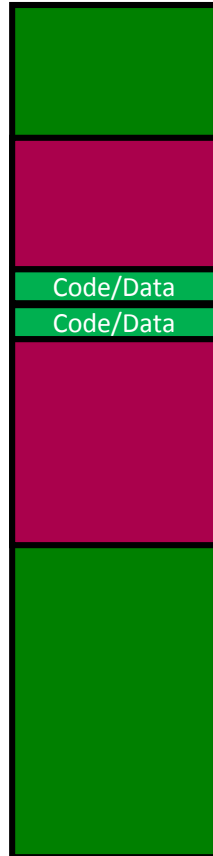


Life Cycle of An Enclave



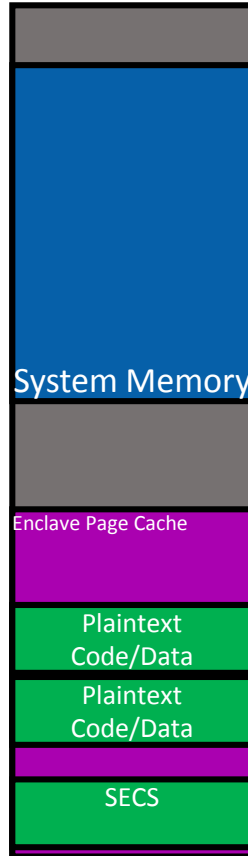
Life Cycle of An Enclave

Virtual Addr Space



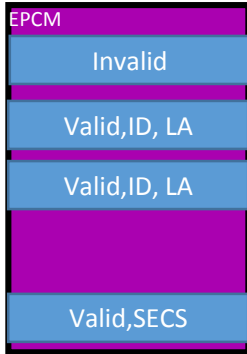
ECREATE (Range)
EADD (Copy Page)
EEXTEND
EINIT

Physical Addr Space



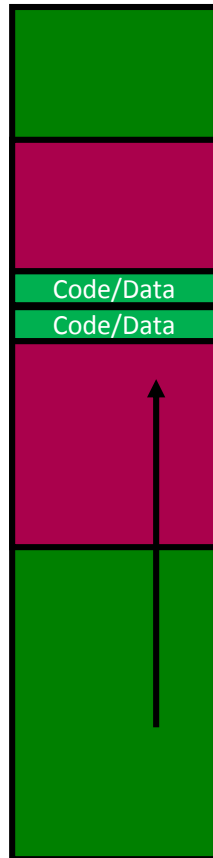
Build

MRENCLAVE



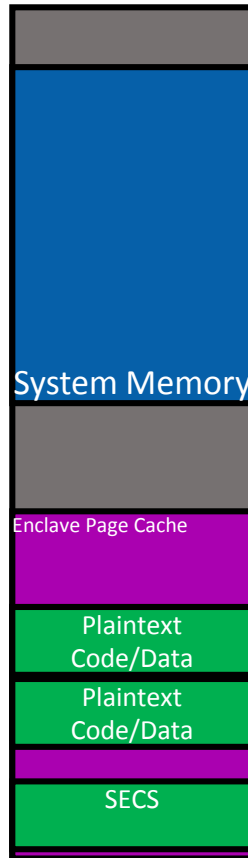
Life Cycle of An Enclave

Virtual Addr Space



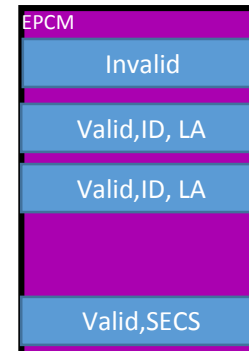
ECREATE (Range)
EADD (Copy Page)
EEXTEND
EINIT
EENTER

Physical Addr Space



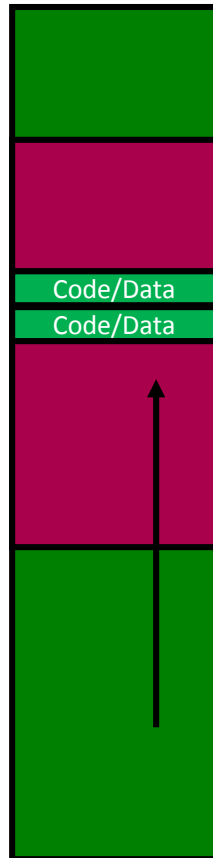
Build

MRENCLAVE



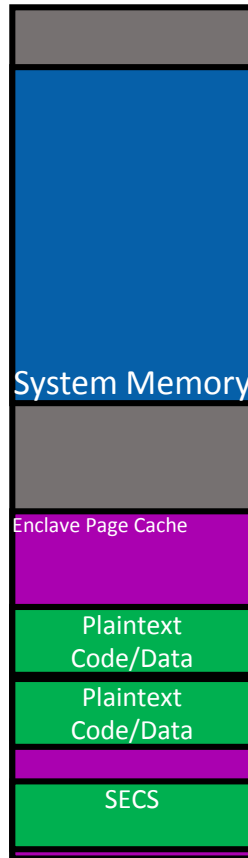
Life Cycle of An Enclave

Virtual Addr Space



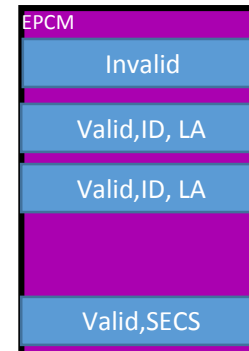
ECREATE (Range)
EADD (Copy Page)
EEXTEND
EINIT
EENTER

Physical Addr Space



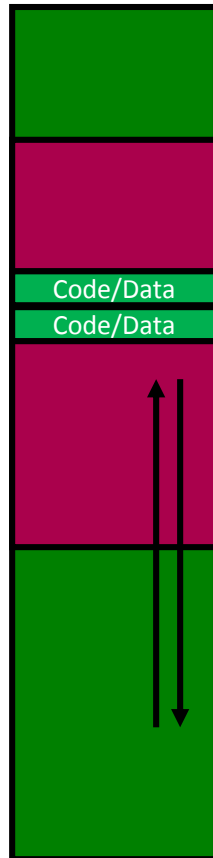
Build

MRENCLAVE



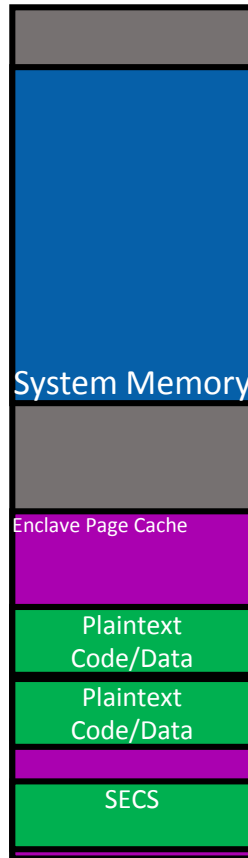
Life Cycle of An Enclave

Virtual Addr Space



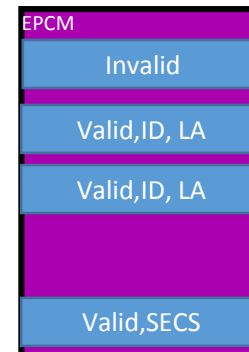
ECREATE (Range)
EADD (Copy Page)
EEXTEND
EINIT
EENTER
EEXIT

Physical Addr Space



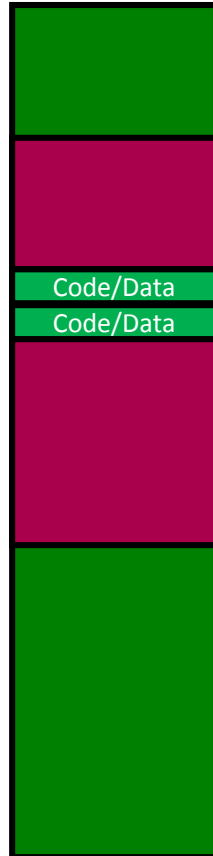
Build

MRENCLAVE



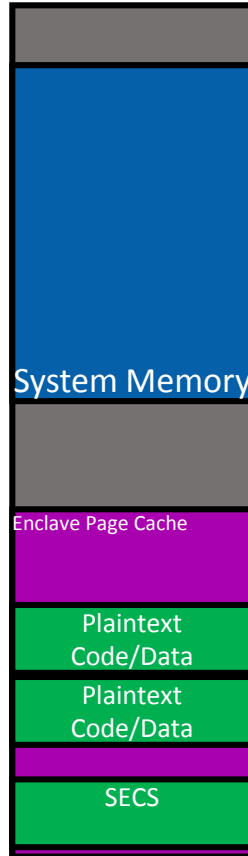
Life Cycle of An Enclave

Virtual Addr Space



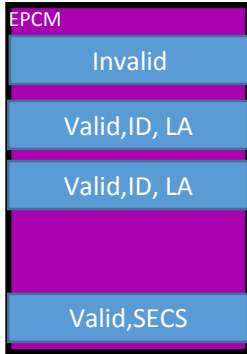
ECREATE (Range)
EADD (Copy Page)
EEXTEND
EINIT
EENTER
EEXIT

Physical Addr Space



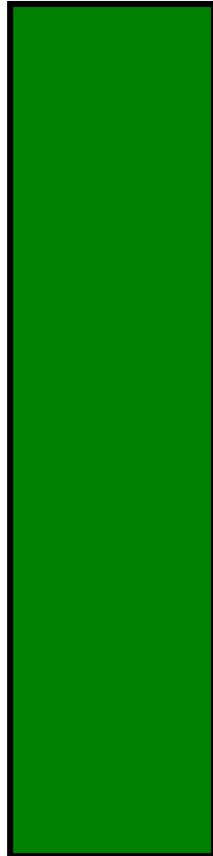
Build

MRENCLAVE



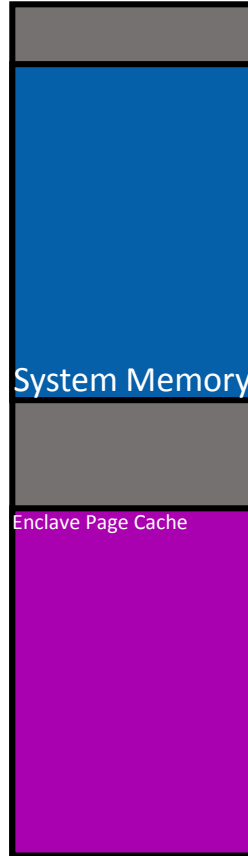
Life Cycle of An Enclave

Virtual Addr Space



ECREATE (Range)
EADD (Copy Page)
EEXTEND
EINIT
EENTER
EEXIT
EREMOVE

Physical Addr Space



Build

MRENCLAVE



SGX Paging Introduction

Requirement:

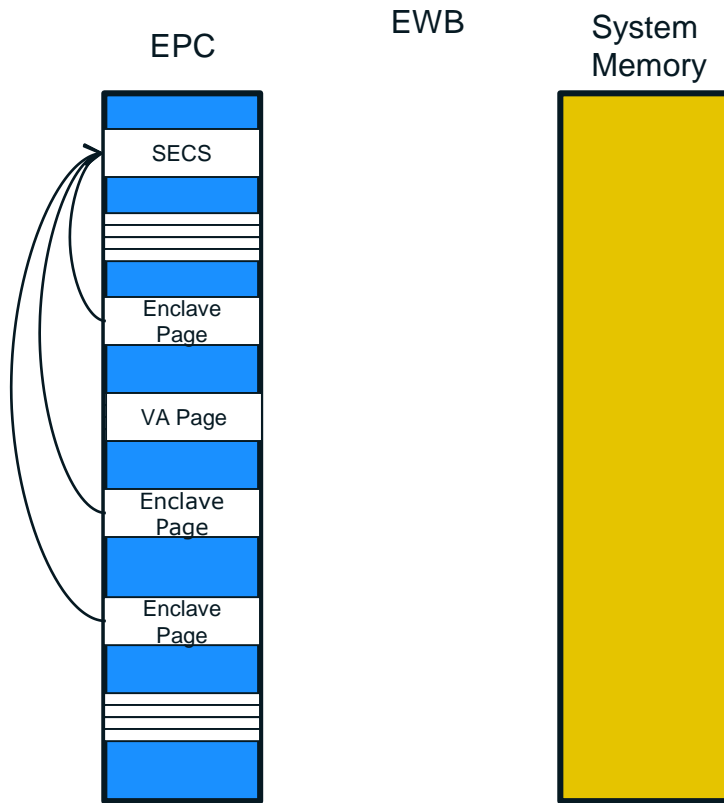
- Remove an EPC page and place into unprotected memory. Later restore it.
- Page must maintain same security properties (confidentiality, anti-replay, and integrity) when restored

New Instructions:

- EWB: Evict EPC page to main memory with cryptographic protections
- ELDB/ELDU: Load page from main memory to EPC with cryptographic protections
- EPA: Allocate an EPC page for holding versions
- EBLOCK: Declare an EPC page ready for eviction
- ETRACK: Ensure address translations have been cleared

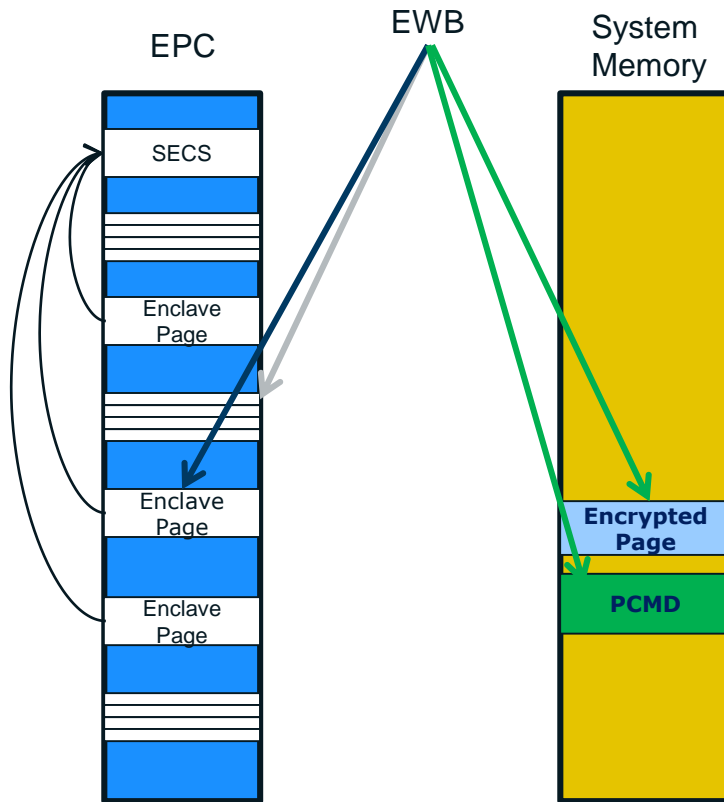
Page-out Example

BUILD



Page-out Example

BUILD

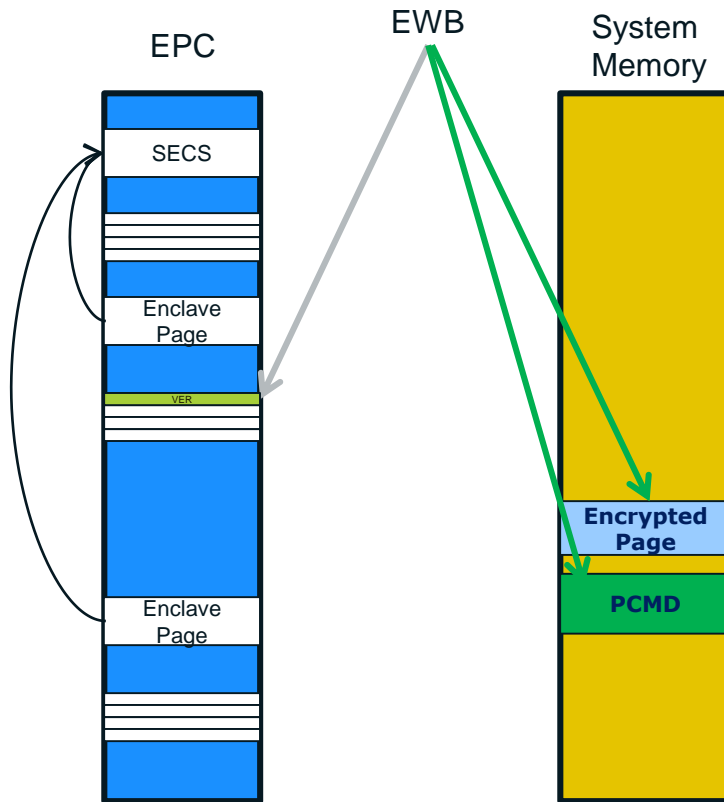


EWB Parameters:

- Pointer to EPC page that needs to be paged out
- Pointer to empty version slot
- Pointers outside EPC location

Page-out Example

BUILD



EWB Parameters:

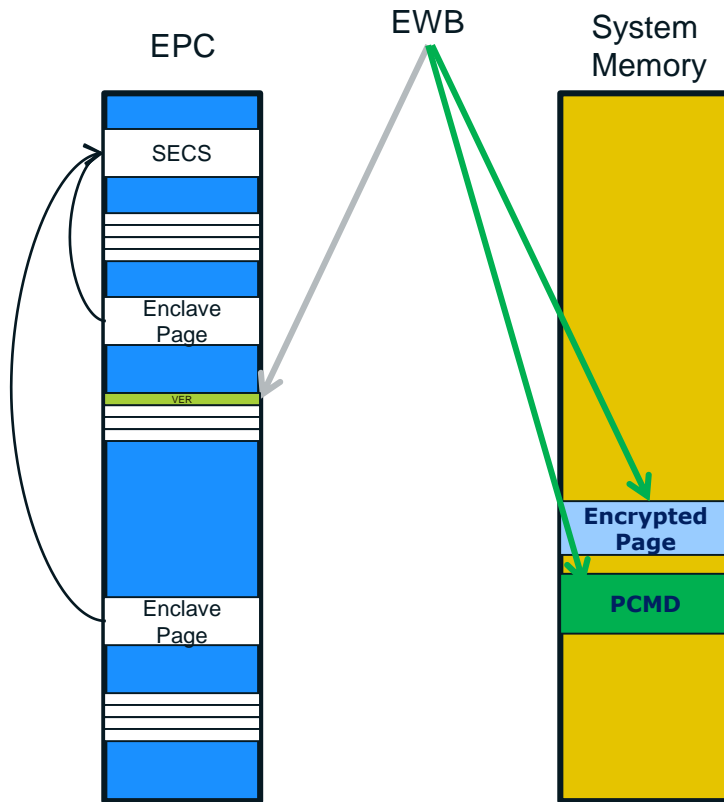
- Pointer to EPC page that needs to be paged out
- Pointer to empty version slot
- Pointers outside EPC location

EWB Operation

- Remove page from the EPC
- Populate version slot
- Write encrypted version to outside
- Write meta-data, PCMD

Page-out Example

BUILD



EWB Parameters:

- Pointer to EPC page that needs to be paged out
- Pointer to empty version slot
- Pointers outside EPC location

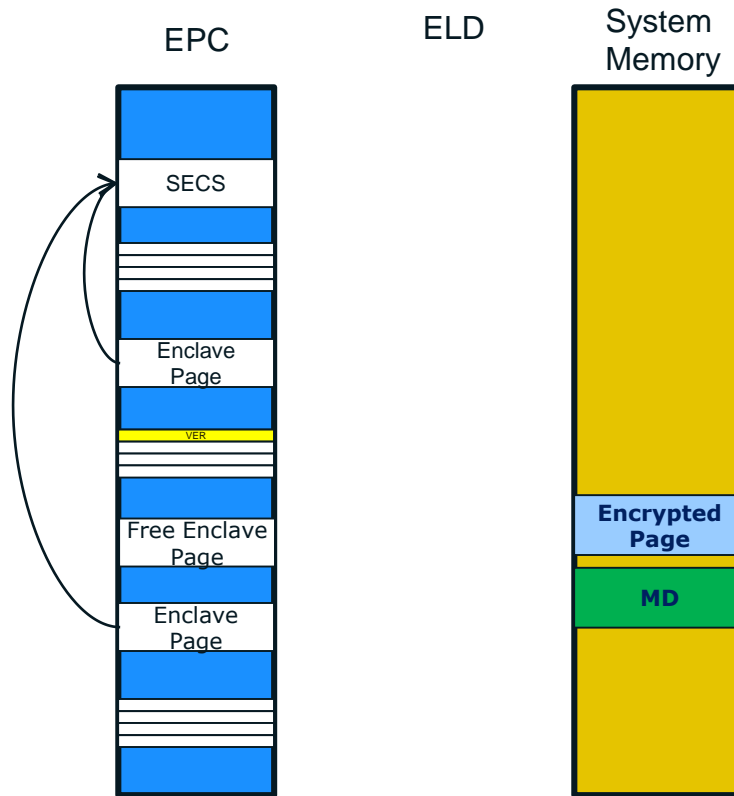
EWB Operation

- Remove page from the EPC
- Populate version slot
- Write encrypted version to outside
- Write meta-data, PCMD

All pages, including SECS and Version Array can be paged out

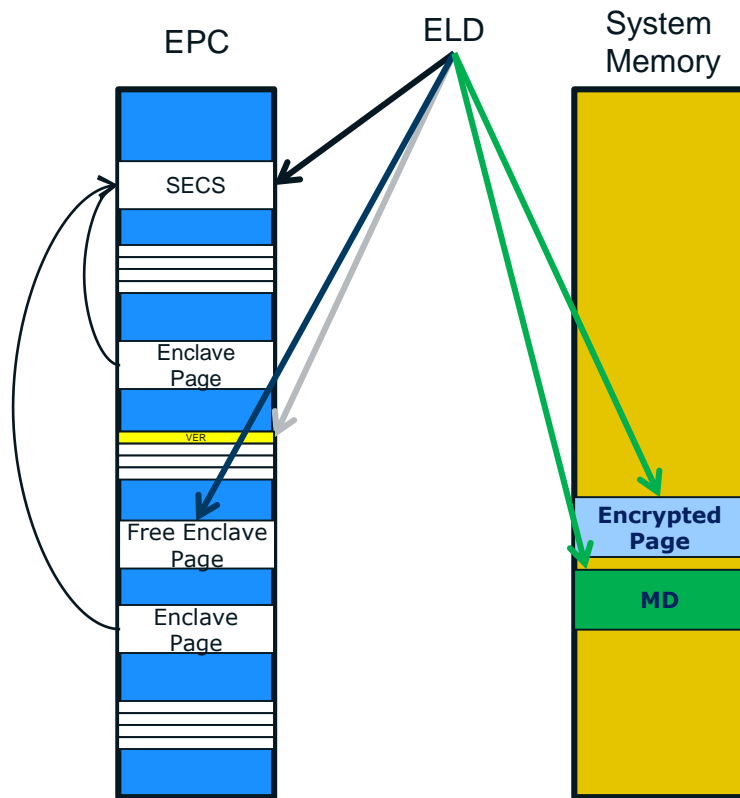
Page-in Example

BUILD



Page-in Example

BUILD

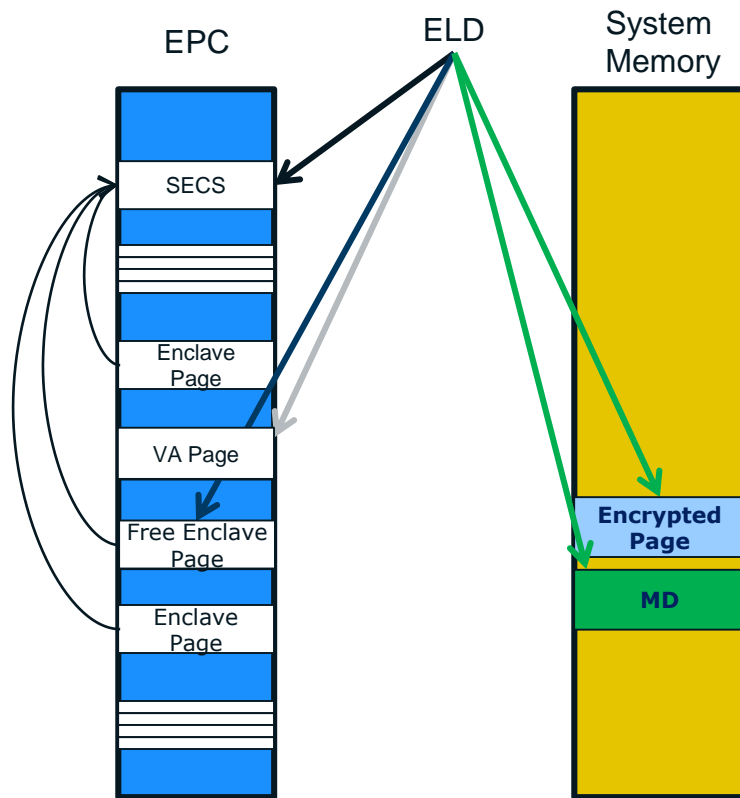


ELD Parameters:

- Encrypted page
- Free EPC page
- SECS (for an enclave page)
- Populated version slot

Page-in Example

BUILD



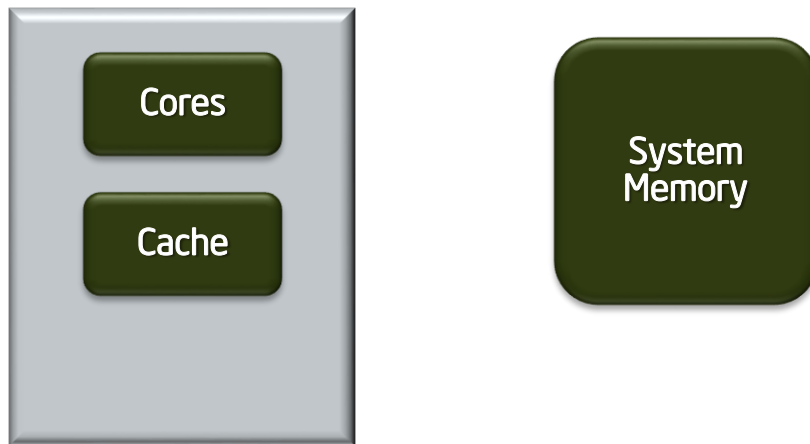
ELD Parameters:

- Encrypted page
- Free EPC page
- SECS (for an enclave page)
- Populated version slot

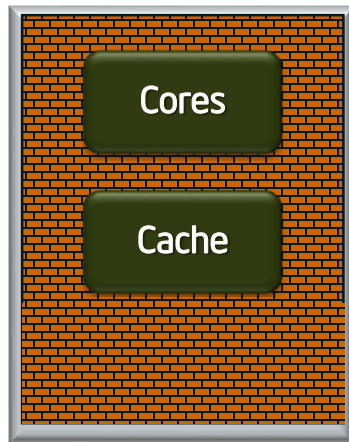
ELD Operation

- Verify and decrypt the page using version
- Populate the EPC slot
- Make back-pointer connection (if applicable)
- Free-up version slot

Protection vs. Memory Snooping Attacks

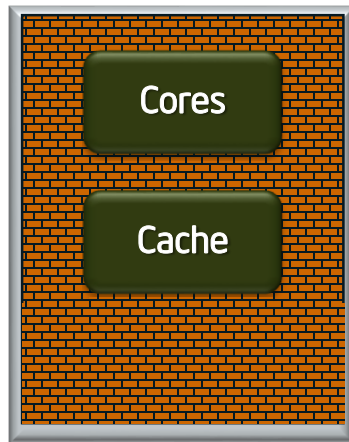


Protection vs. Memory Snooping Attacks



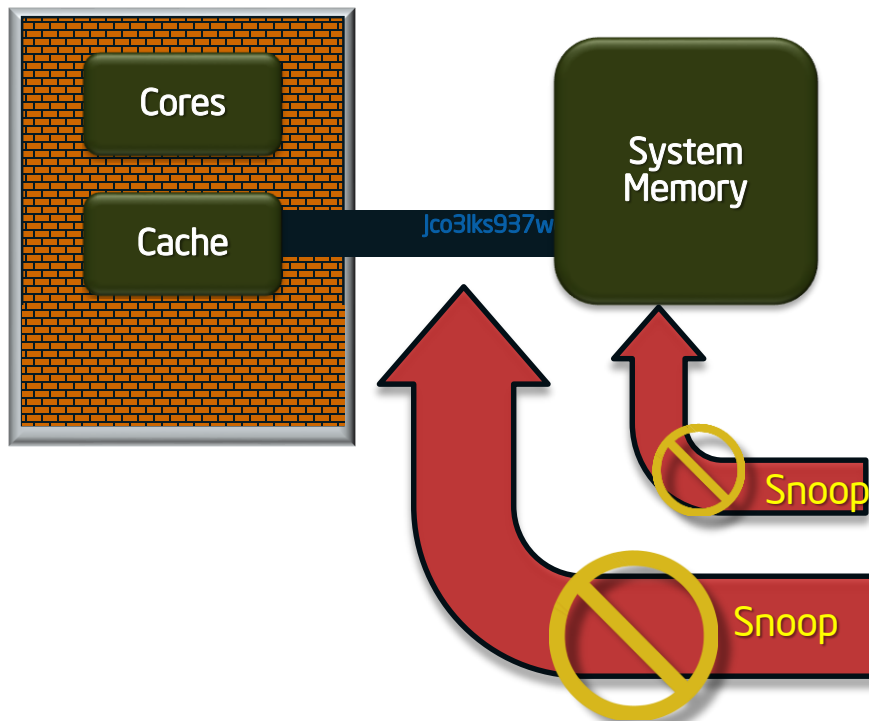
1. Security perimeter is the CPU package boundary

Protection vs. Memory Snooping Attacks



1. Security perimeter is the CPU package boundary
2. Data and code unencrypted inside CPU package

Protection vs. Memory Snooping Attacks



1. Security perimeter is the CPU package boundary
2. Data and code unencrypted inside CPU package
3. Data and code outside CPU package is encrypted and/or integrity checked
4. External memory reads and bus snoops see only encrypted data

SGX Technical Summary

- Provides any application the ability to keep a secret
 - Provide capability using new processor instructions
 - Application can support multiple enclaves
- Provides integrity and confidentiality
 - Resists hardware attacks
 - Prevent software access, including privileged software and SMM
- Applications run within OS environment
 - Low learning curve for application developers
 - Open to all developers
- Resources managed by SW
 - HW components are supported in a driver or OS



Thank You

