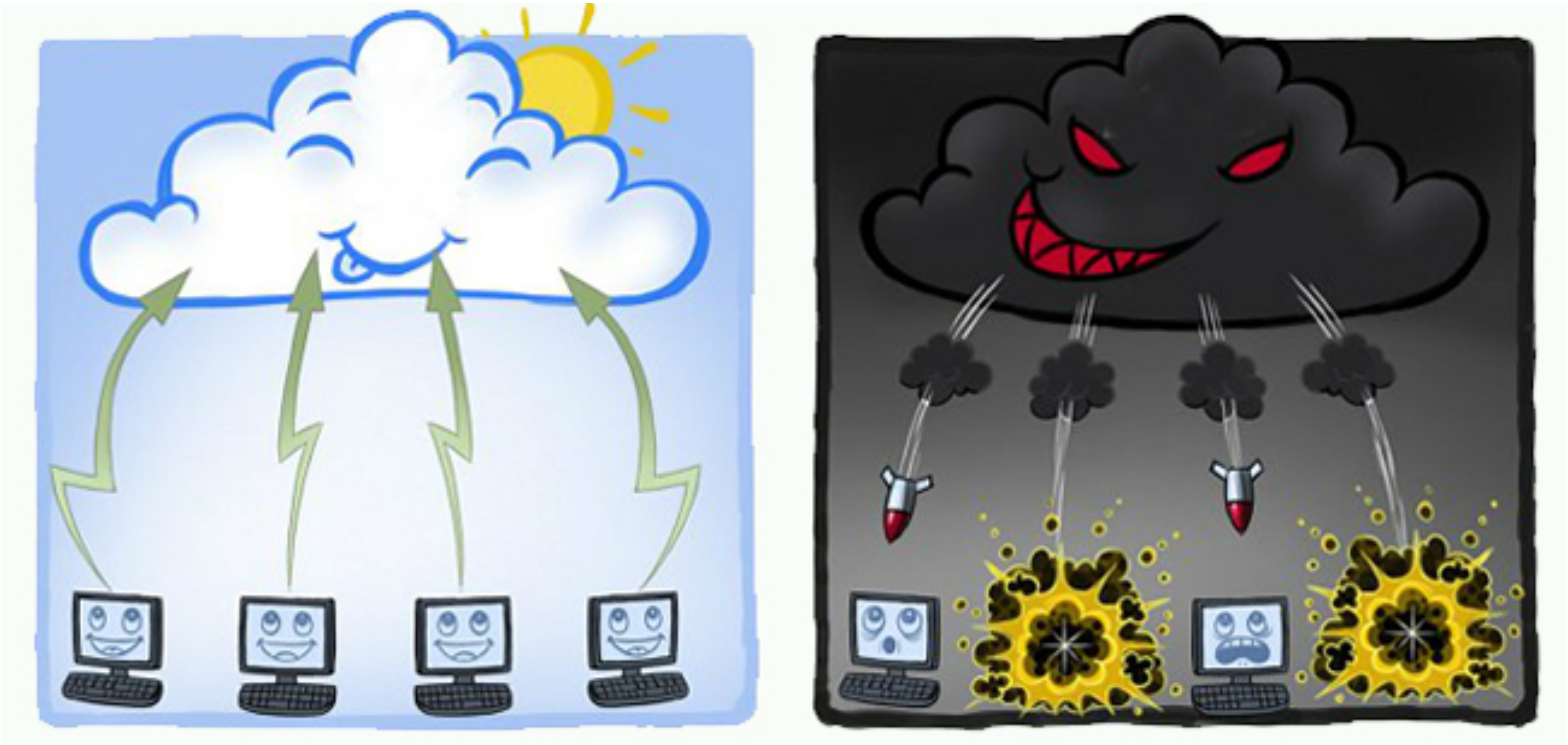
Intel Software Guard Extensions (SGX)

Prashant Pandey (ppandey@cs.stonybrook.edu)
Applied Algorithms Lab, Stony Brook University

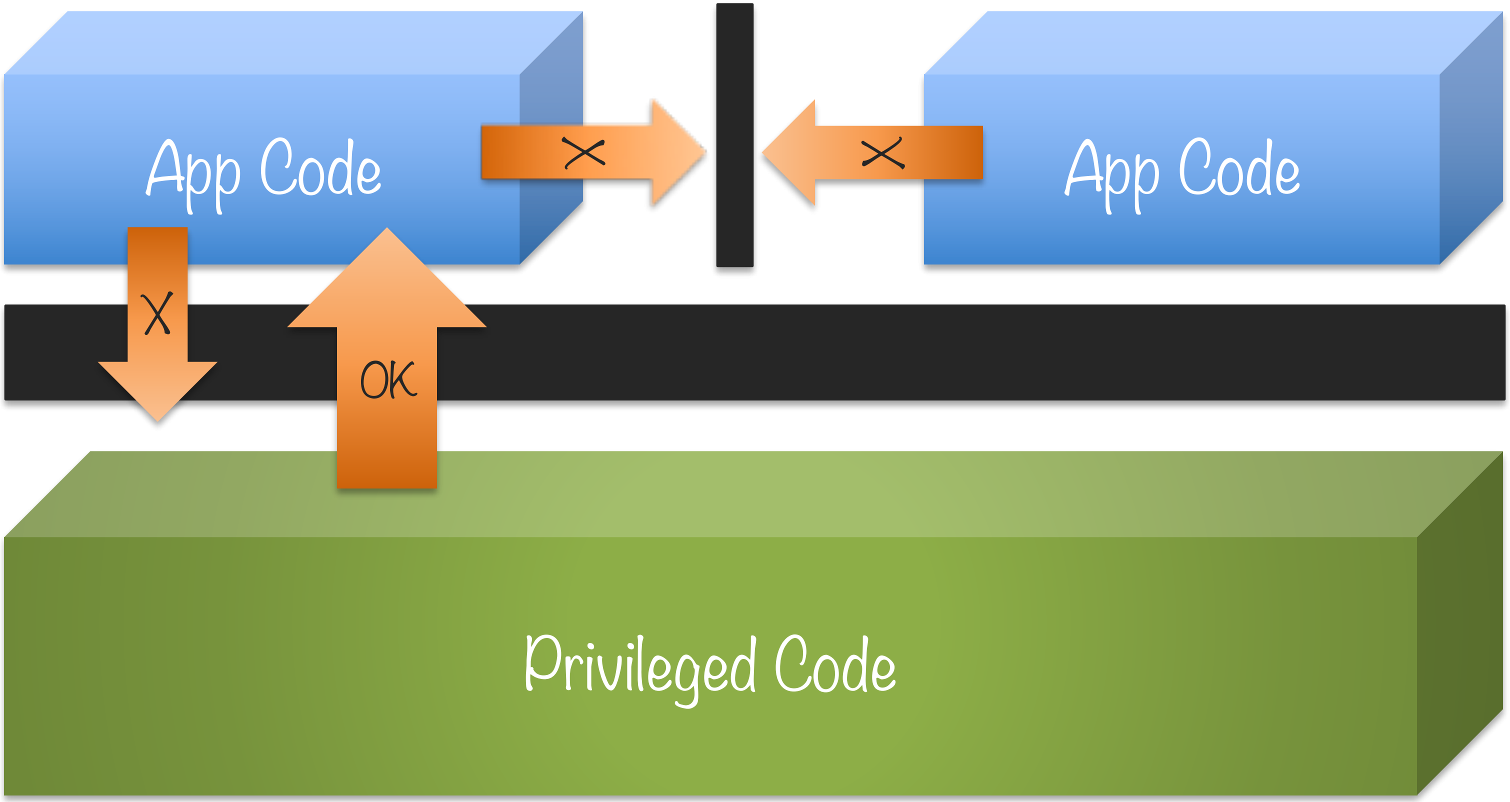
Story board

- ✓ Problem Statement
- ✓ Attack Surface and Overview
- ✓ Programming environment
- ✓ Enclave Life-Cycle
- ✓ Developing with SGX
- ✓ SGX usage models

Are compute devices trustworthy?

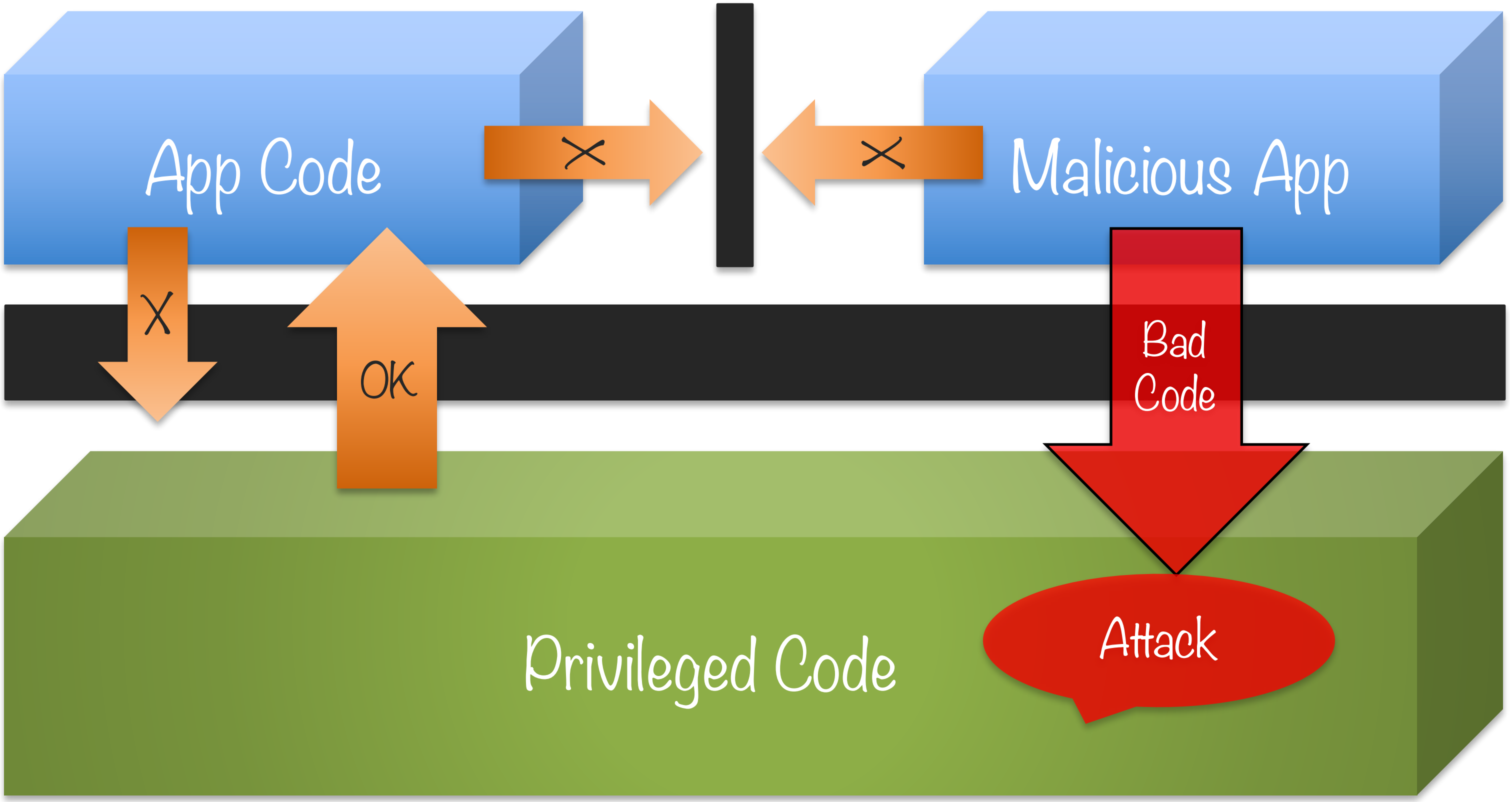


Basic Issue: Why aren't compute devices trustworthy ?



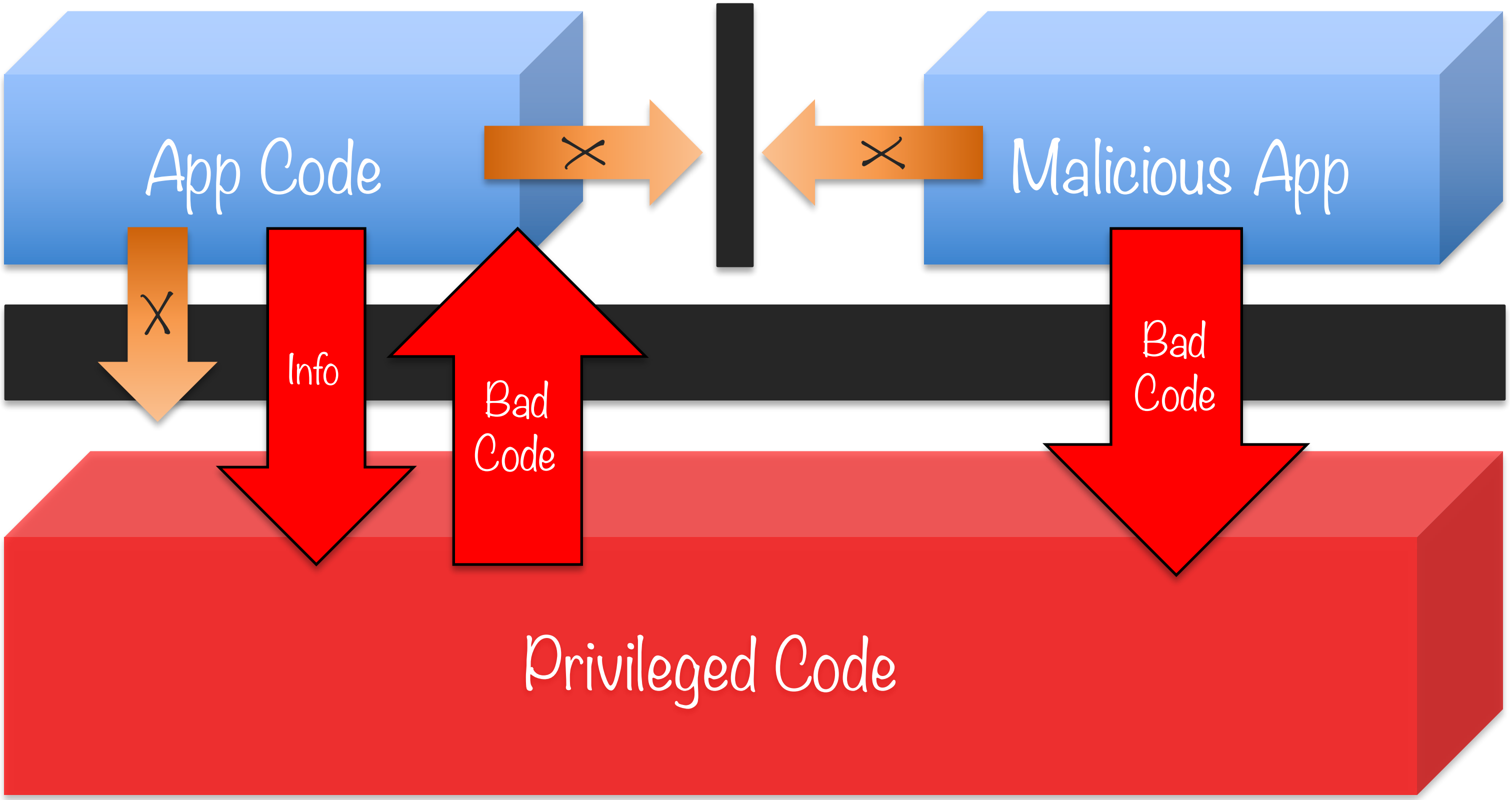
Protected Mode protects OS from app

Basic Issue: Why aren't compute devices trustworthy ?



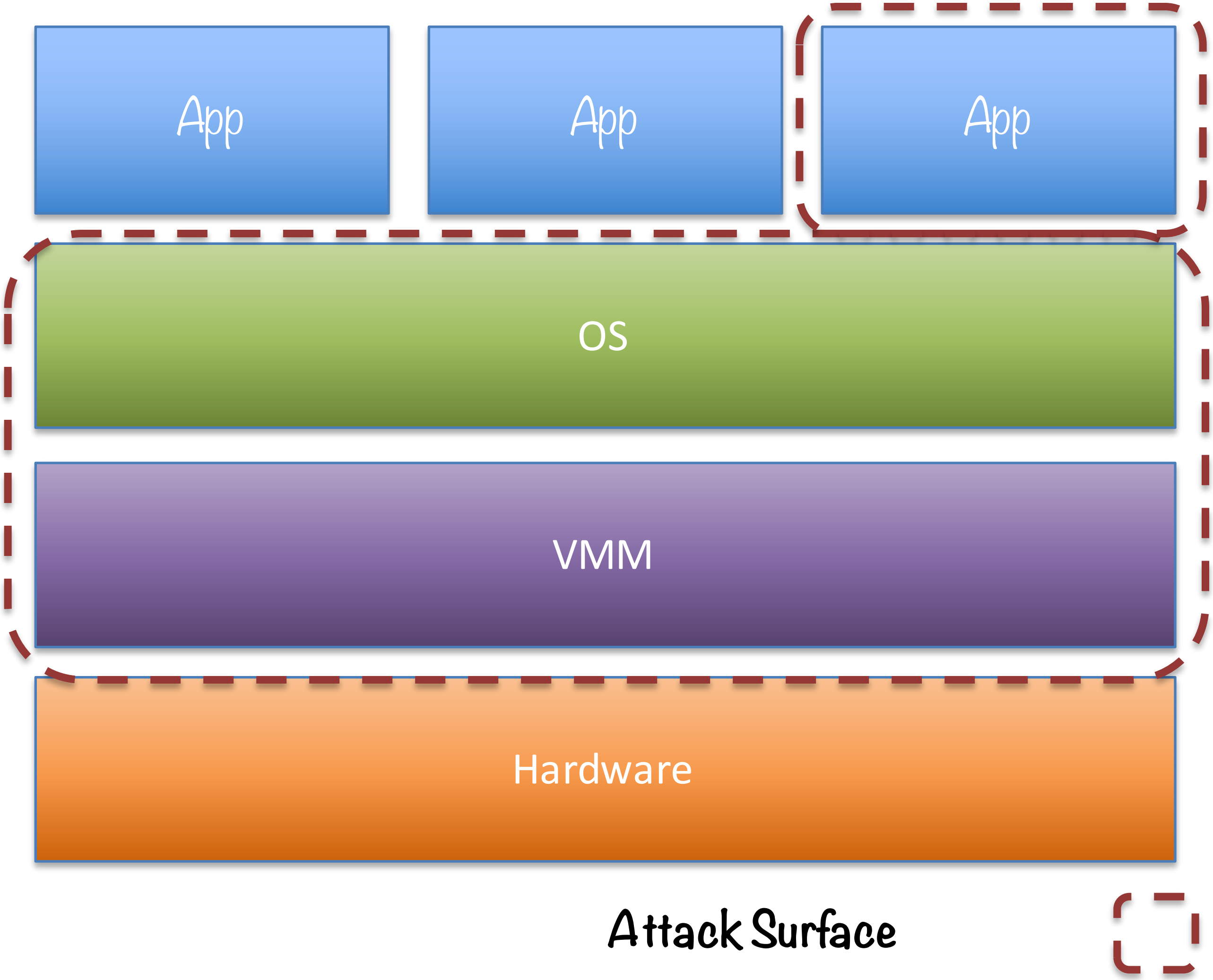
Apps not protected from privileged code attacks

Basic Issue: Why aren't compute devices trustworthy ?



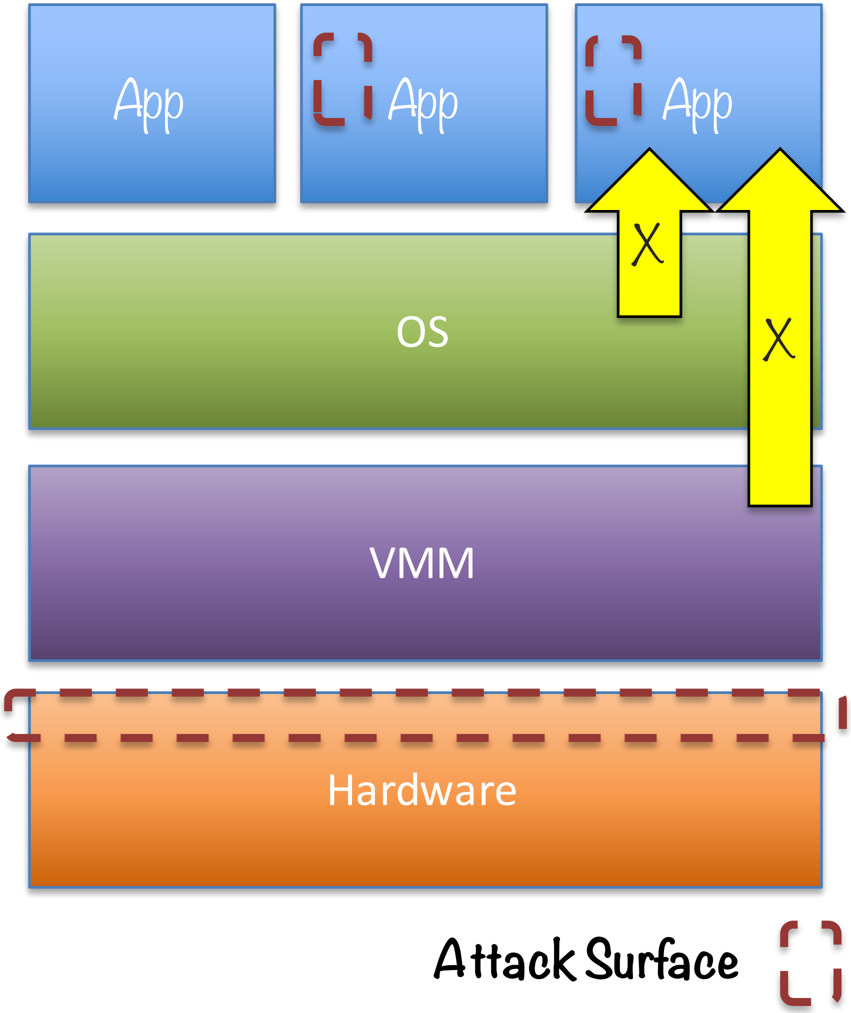
Apps not protected from privileged code attacks

Attack surface

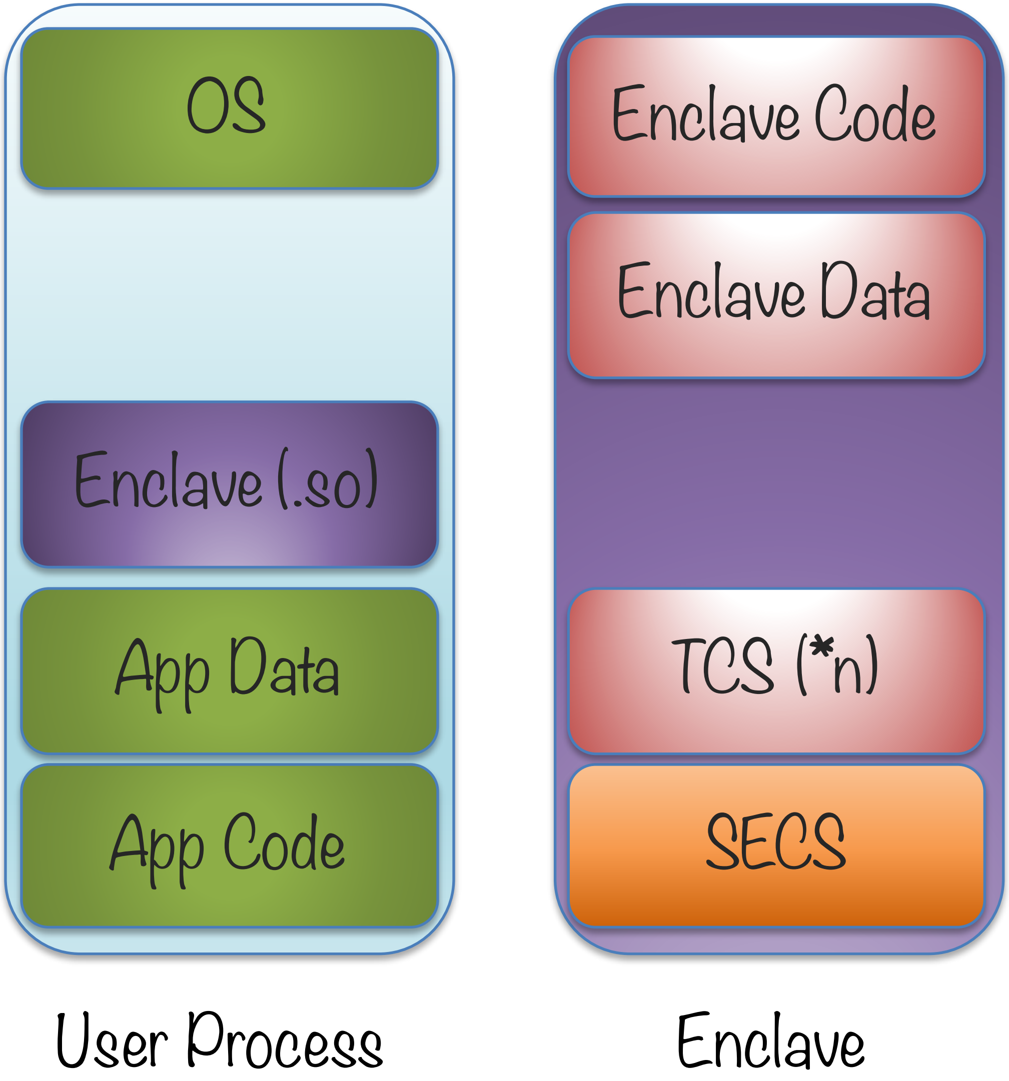


Reduced attack surface with SGX

- ✓ Application gains ability to defend its own secret
- ✓ Malware that subverts OS/VMM, BIOS, Drivers etc. cannot steal app secrets
- ✓ Single application environment



SGX Programming Environment



Enclave:

- ✓ Has its own code and data
- ✓ Provides Confidentiality
- ✓ Provides Integrity
- ✓ Has controlled entry points
- ✓ Supports multiple threads
- ✓ Has full access to app memory

Intel SGX Technology

- ✓ At its root, Intel SGX is a set of new CPU instructions that can be used by applications to set aside private regions of code and data

- ✓ Allows app developers to protect sensitive data by rogue software running at higher privilege levels

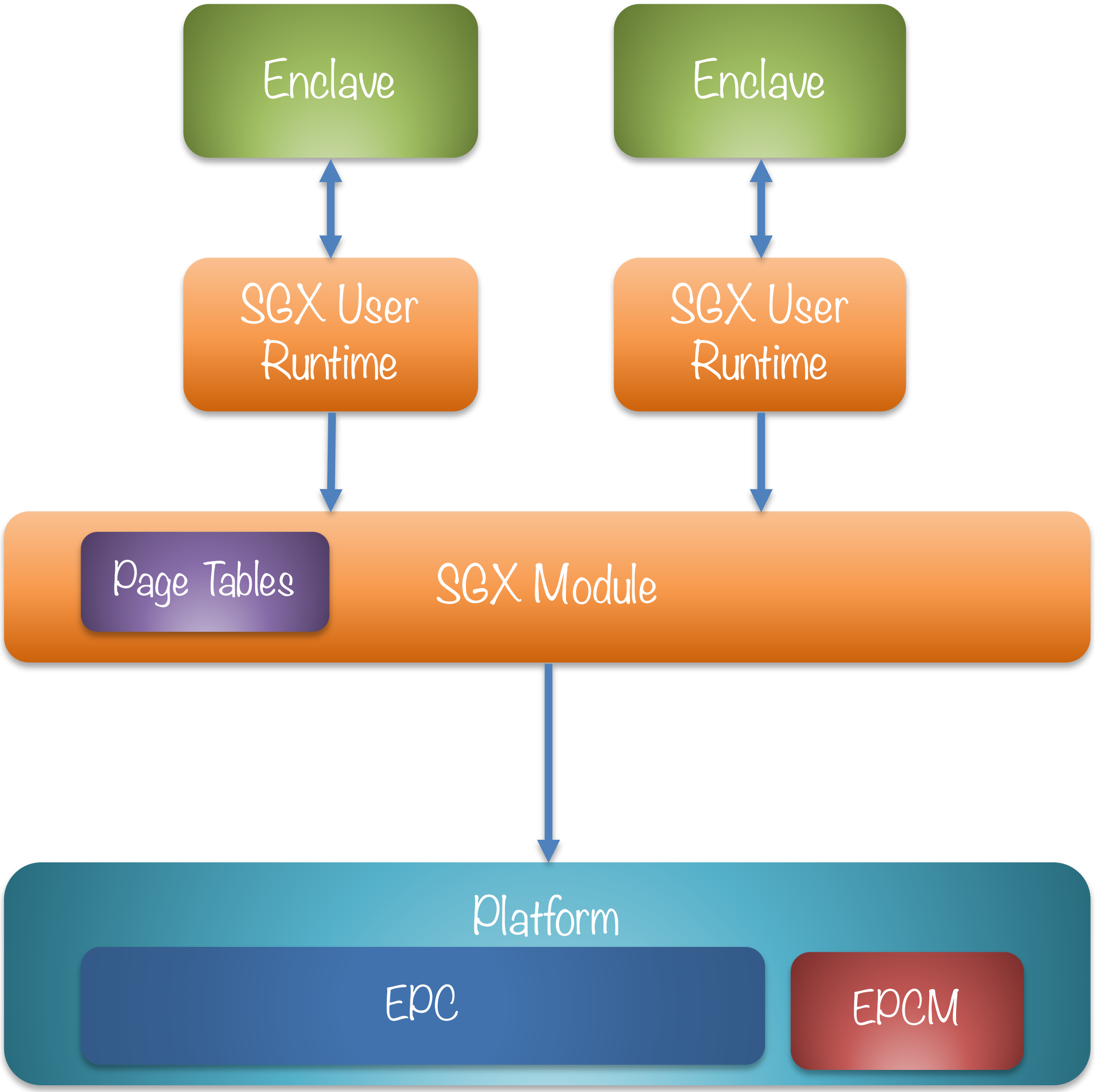
- ✓ Enable apps to preserve the confidentiality and integrity of sensitive code and data

SGX high-level HW/SW picture

Application Environment

Privileged Environment

Exposed Hardware



Instructions

EGETKEY
EEXIT
EREPORT
EENTER
ERESUME

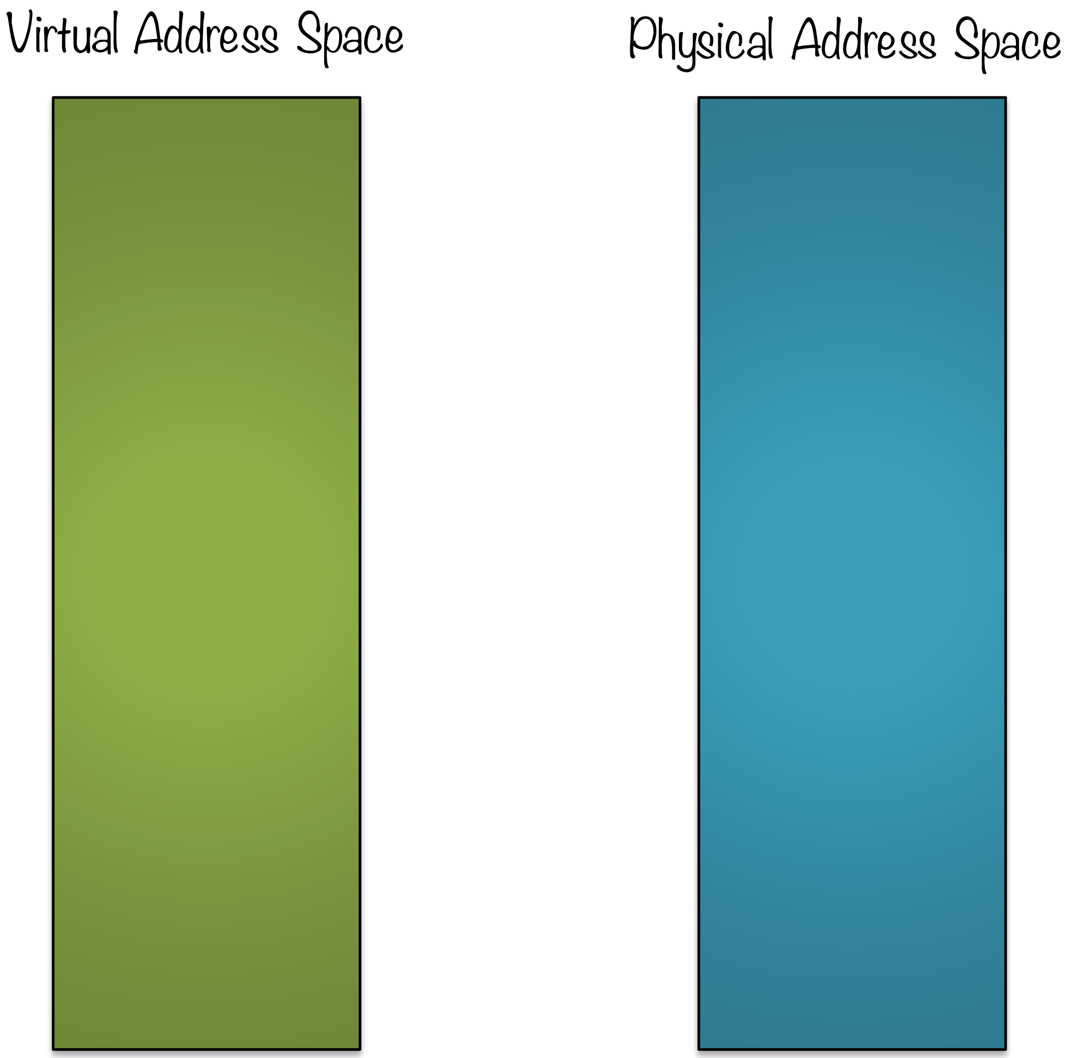
Instructions

ECREATE
EADD
EEXTEND
EINIT
EBLOCK

ETRACK
EWB
ELD
EPA
EREMOVE

Application
Runtime
OS Data Str
Hardware
HW Data Str

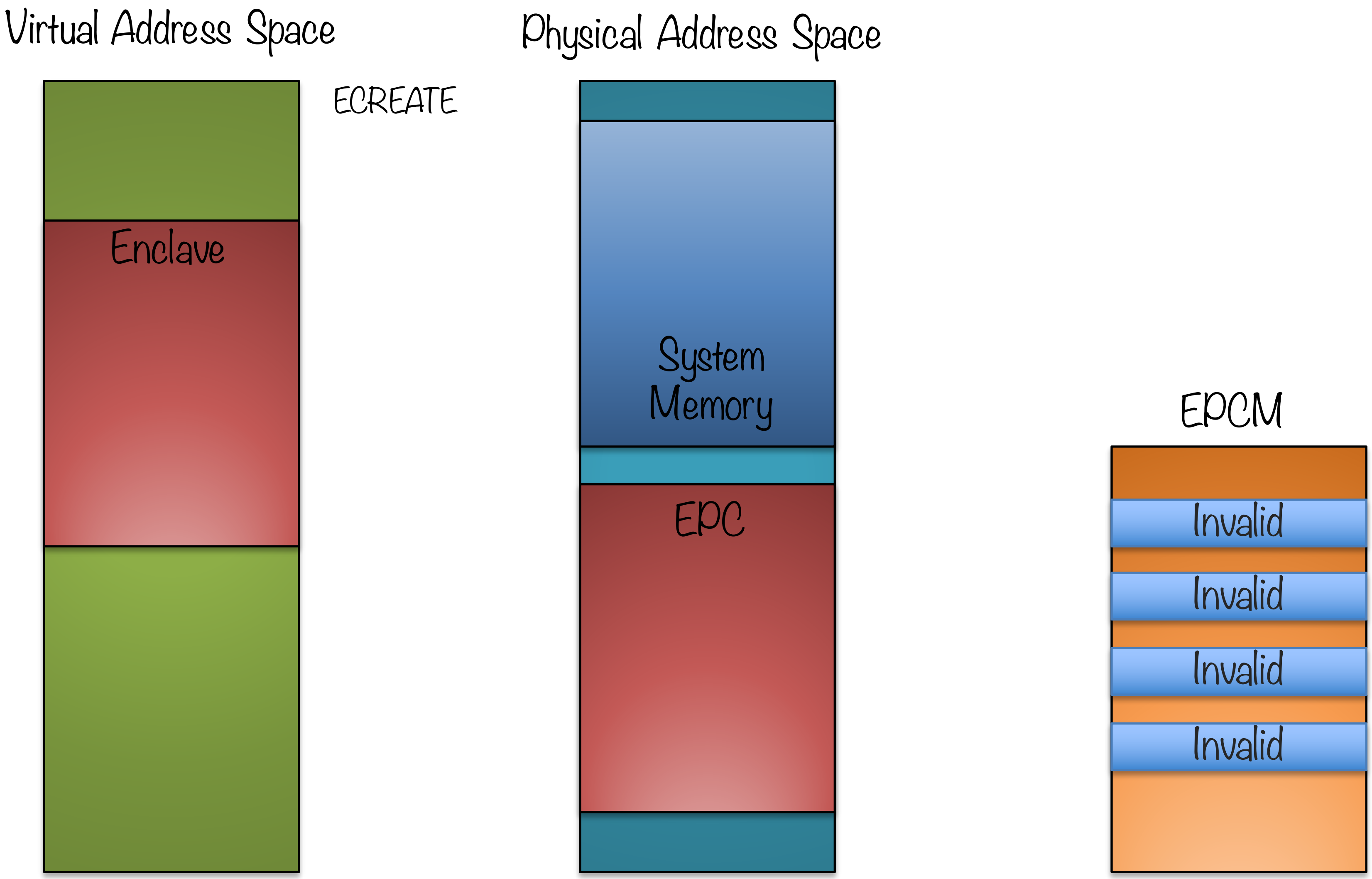
Life Cycle of Enclave



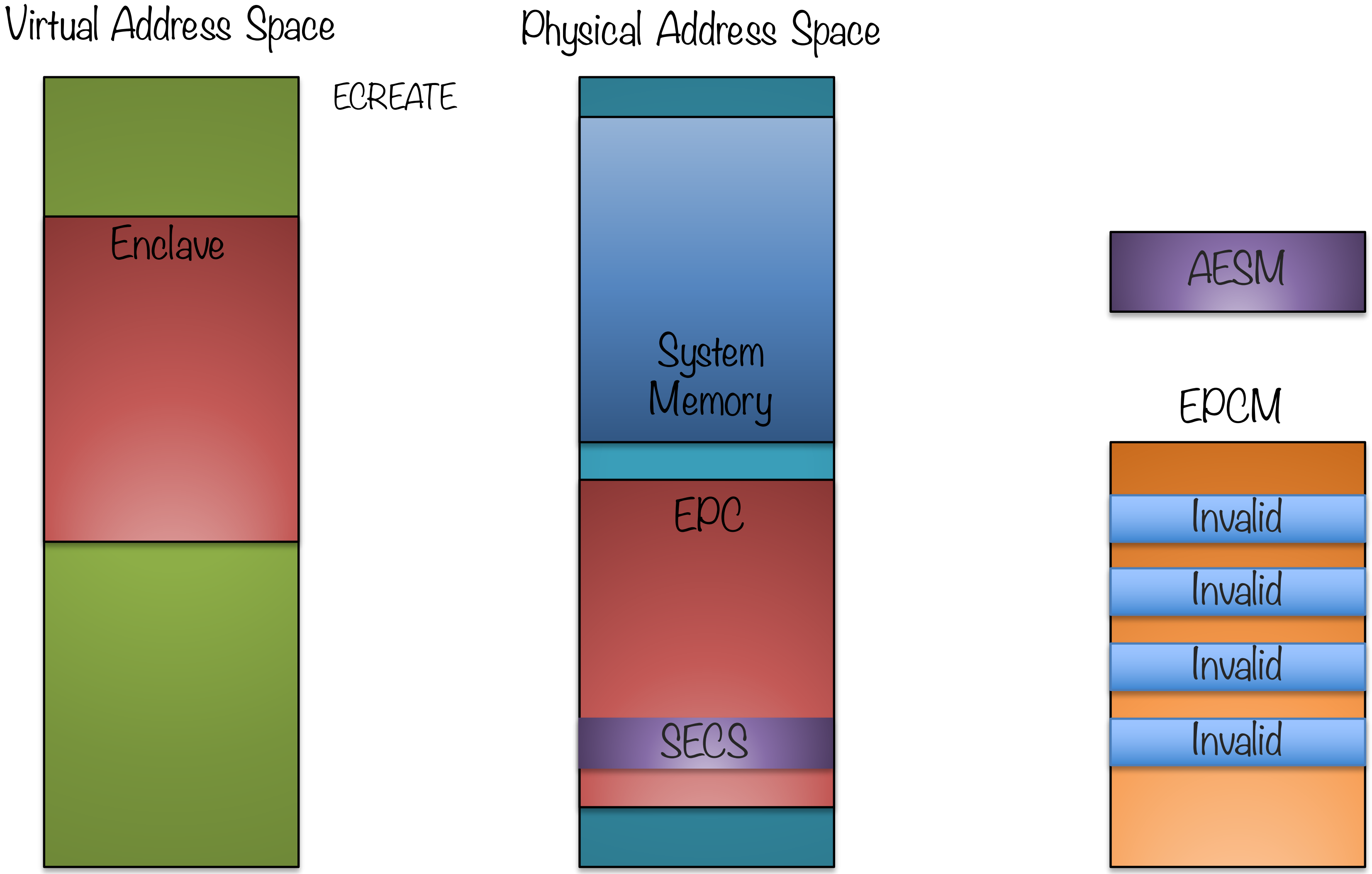
Virtual Address Space

Physical Address Space

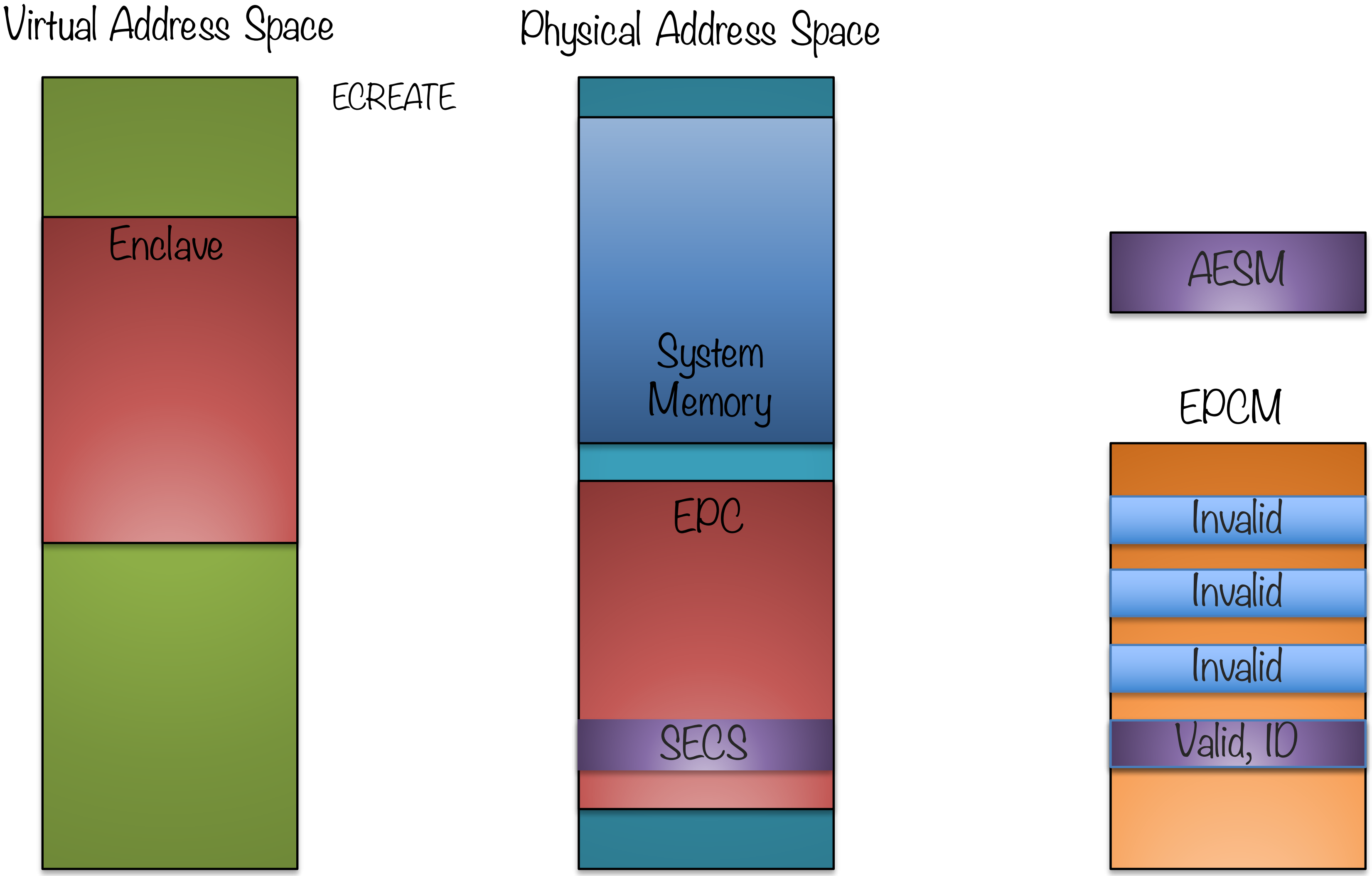
Life Cycle of Enclave



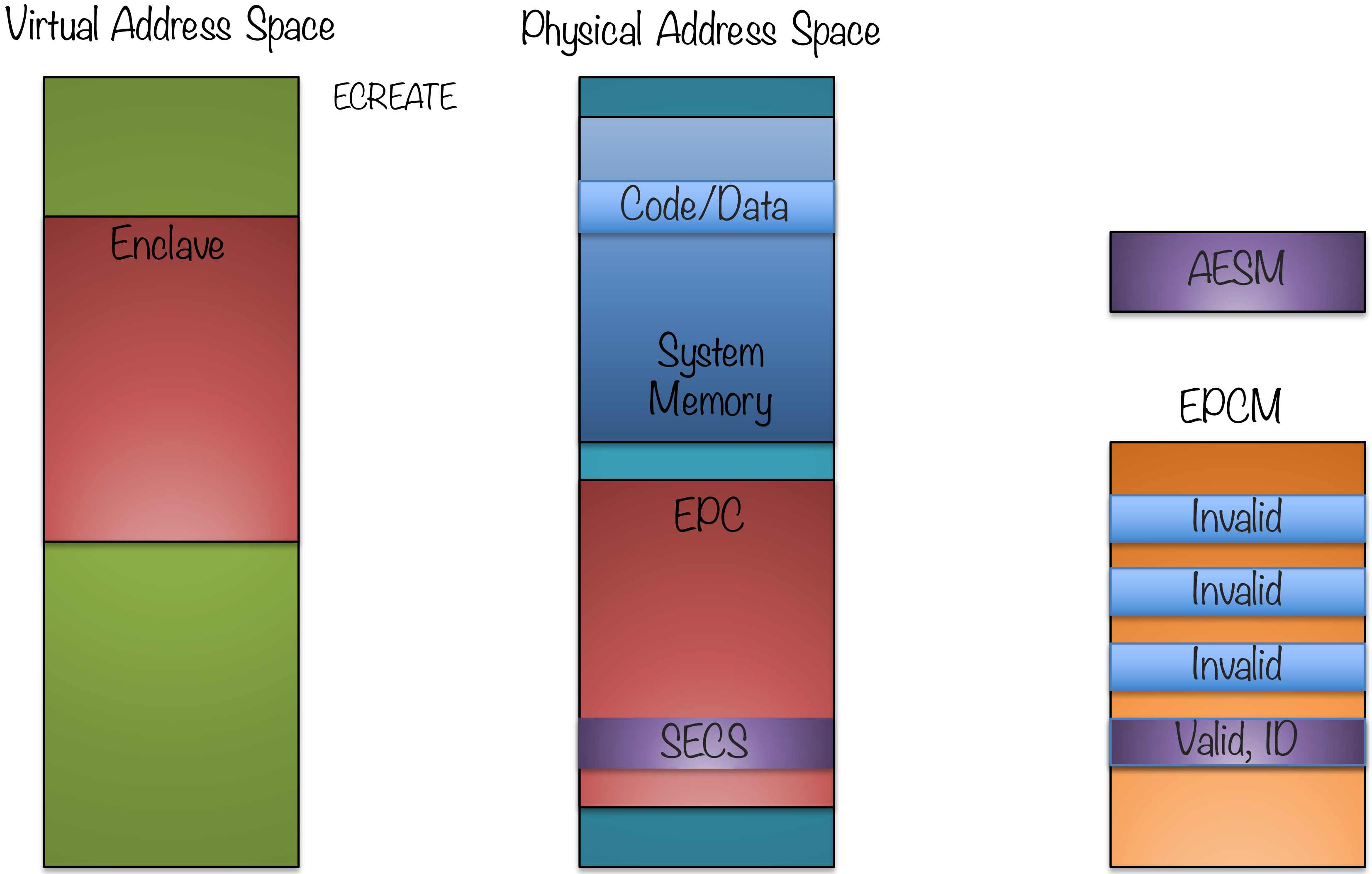
Life Cycle of Enclave



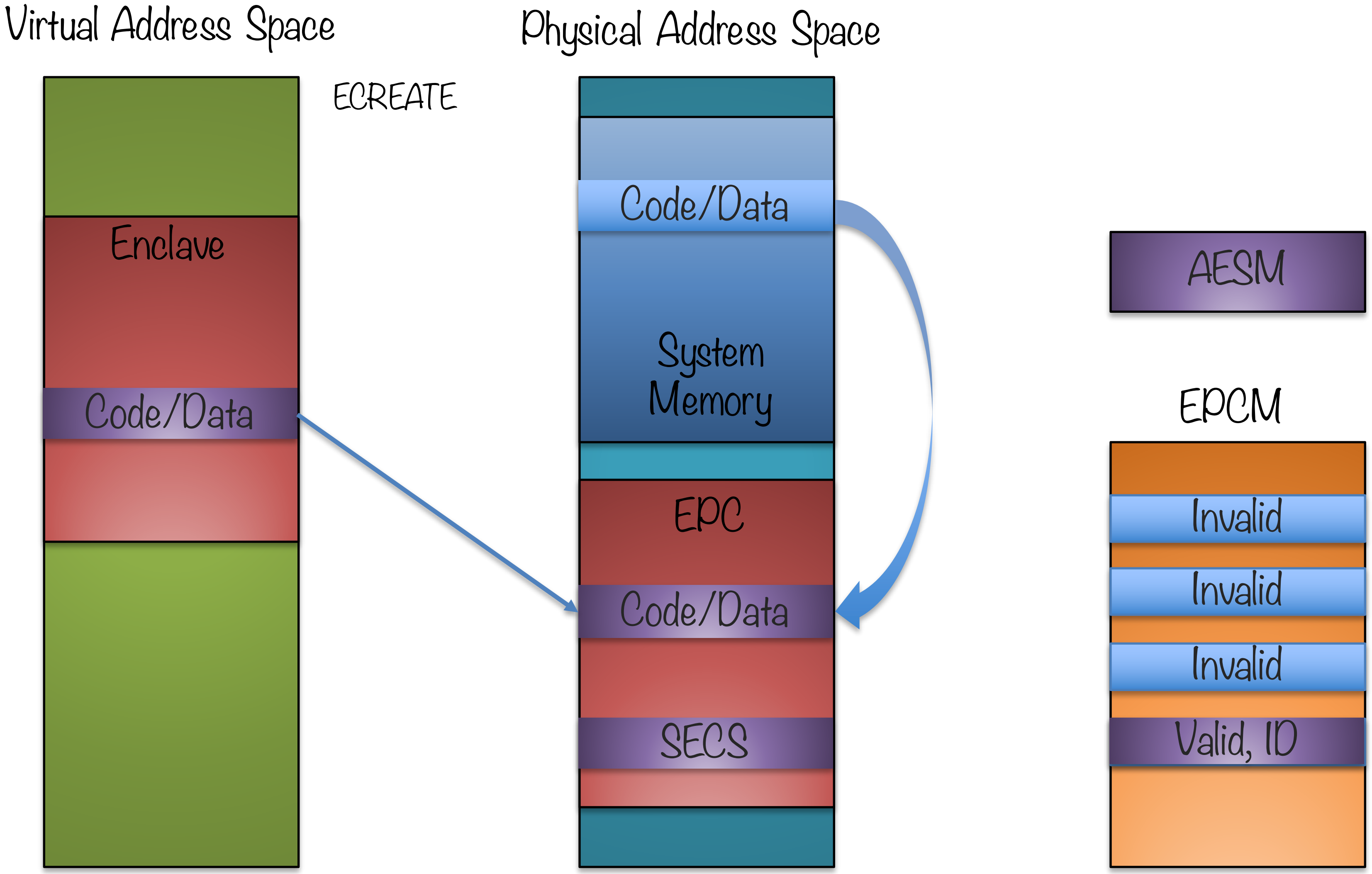
Life Cycle of Enclave



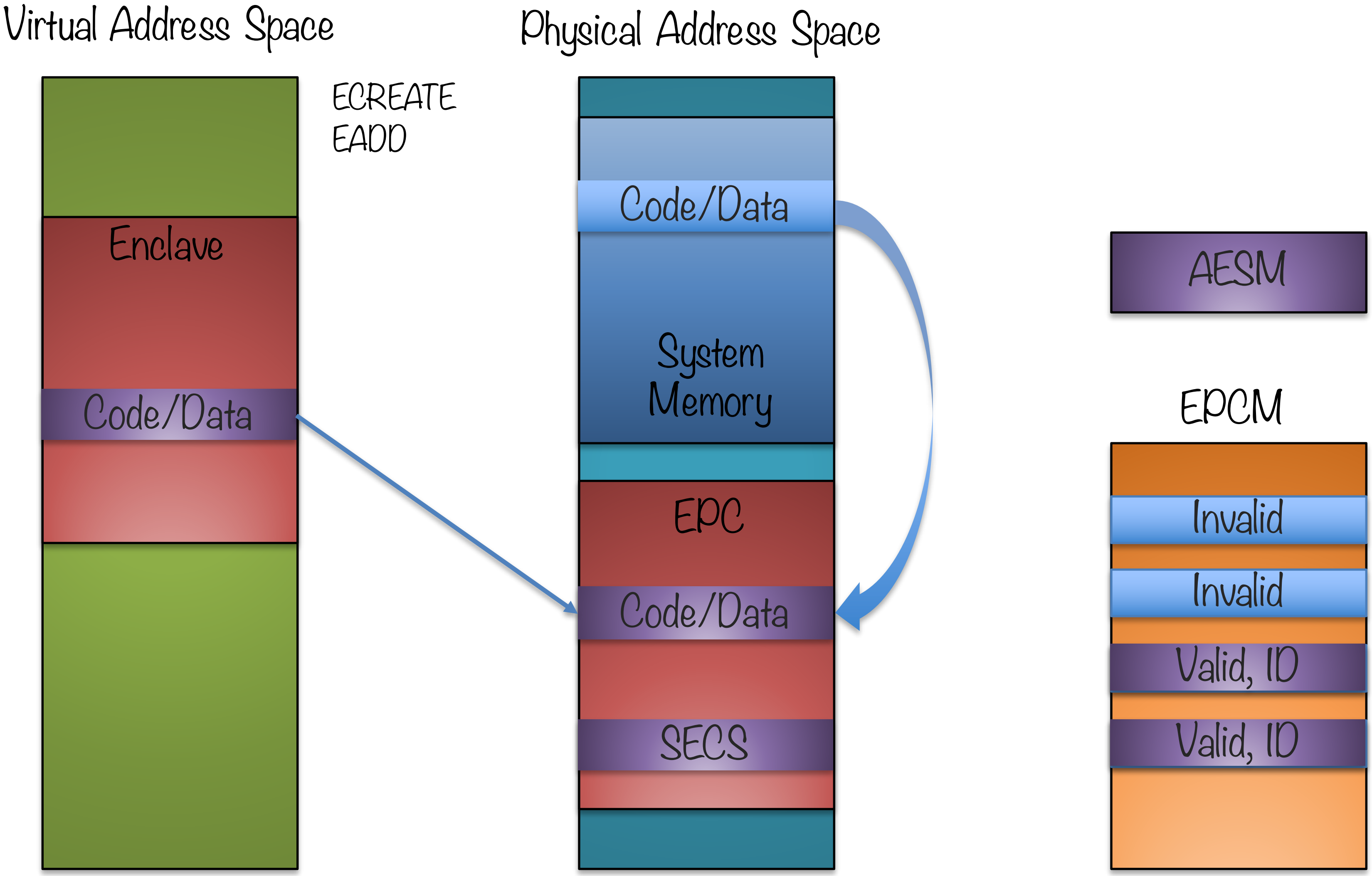
Life Cycle of Enclave



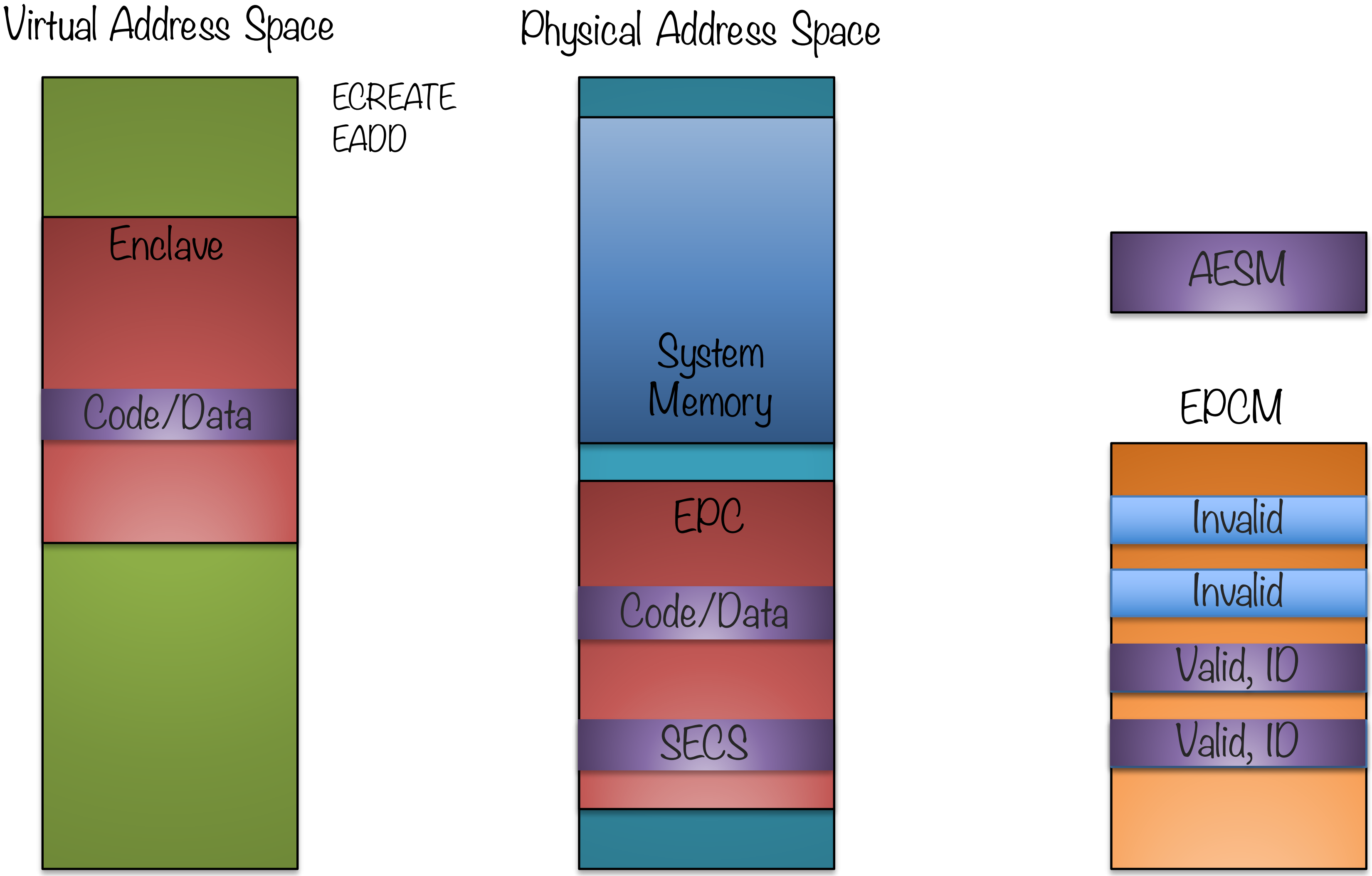
Life Cycle of Enclave



Life Cycle of Enclave



Life Cycle of Enclave



Virtual Address Space

Enclave

Code/Data

ECREATE
EADD

Physical Address Space

System Memory

EPC

Code/Data

SECS

AESM

EPCM

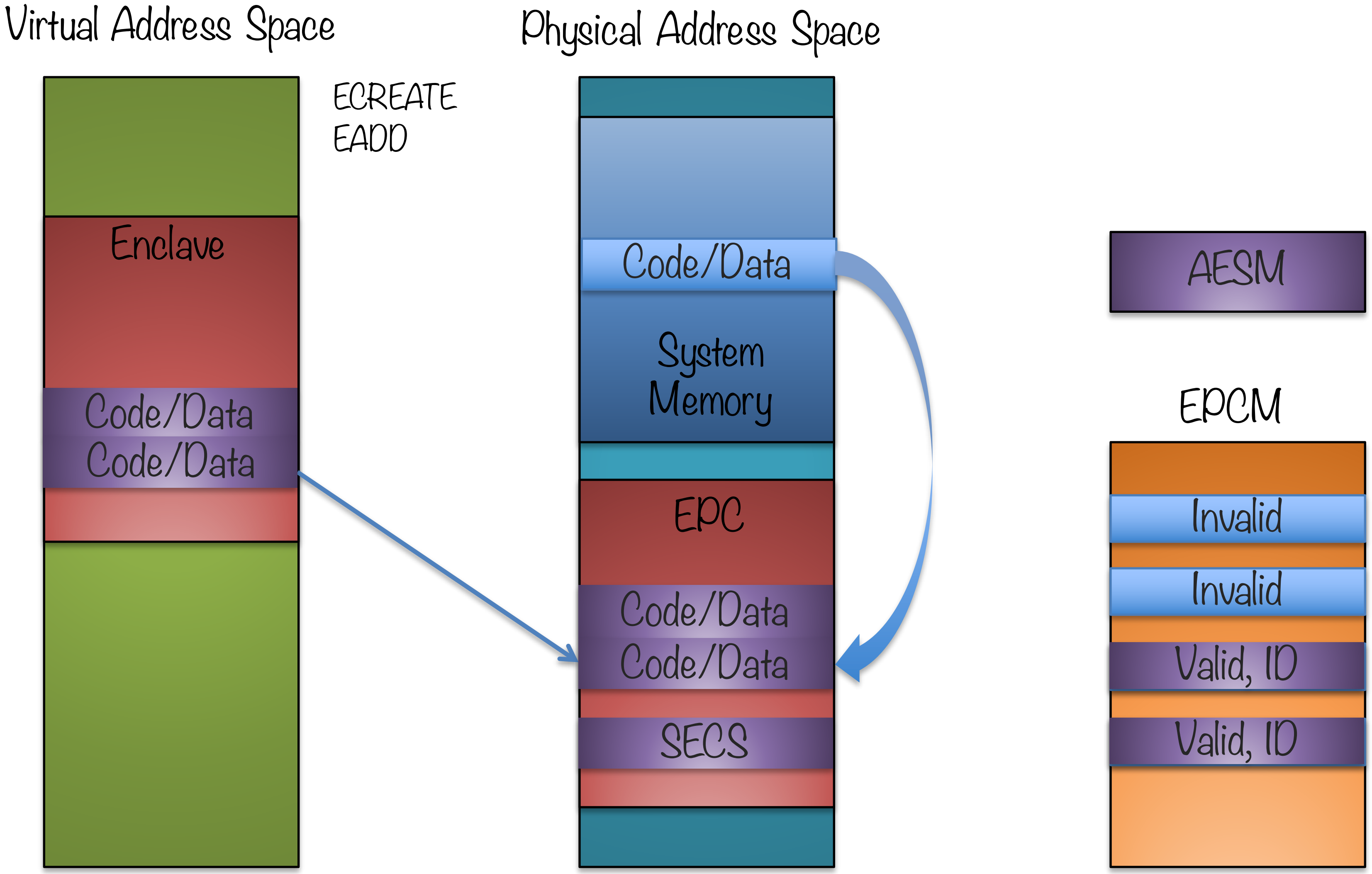
Invalid

Invalid

Valid, ID

Valid, ID

Life Cycle of Enclave

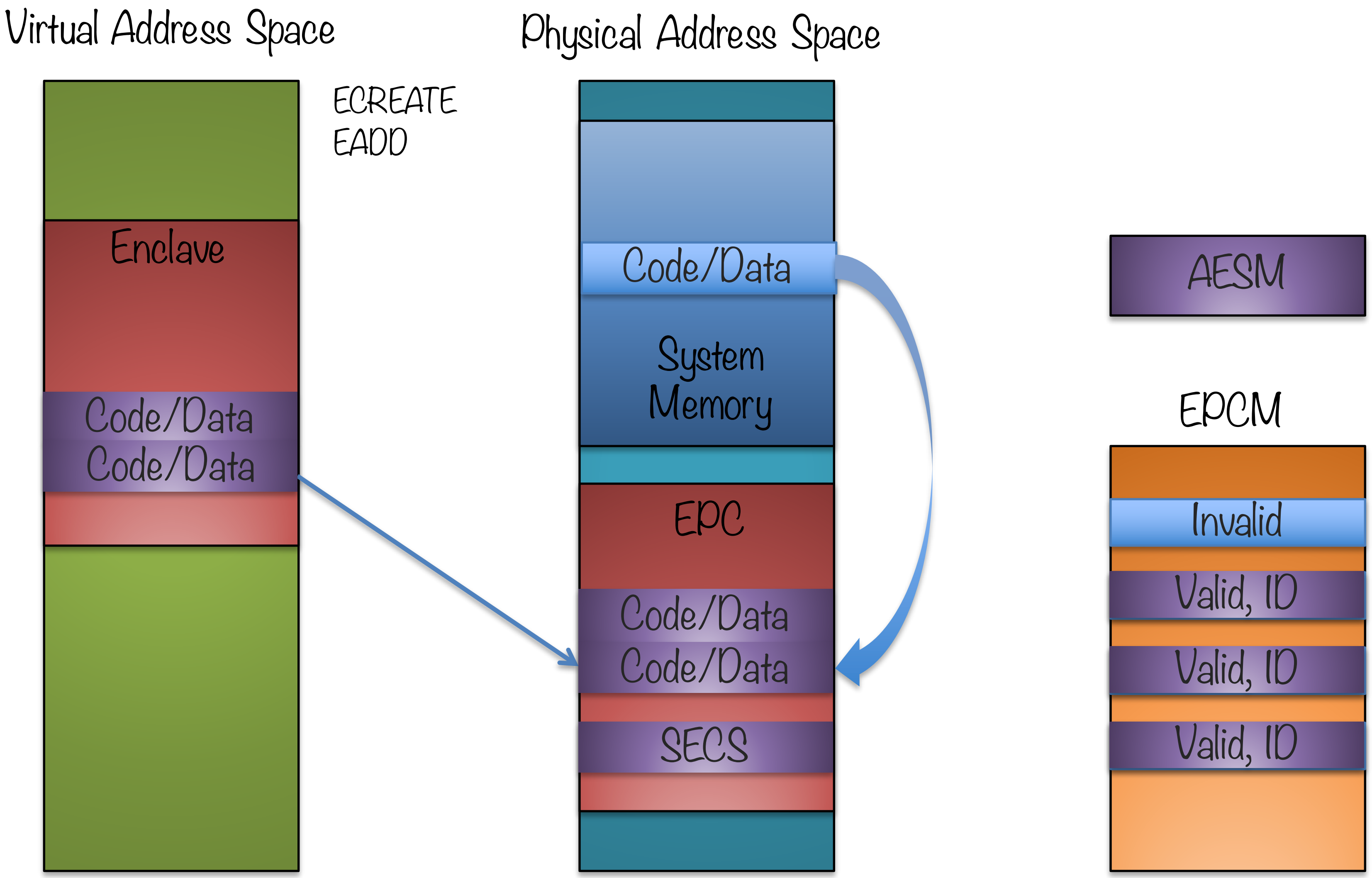


Virtual Address Space

ECREATE
EADD

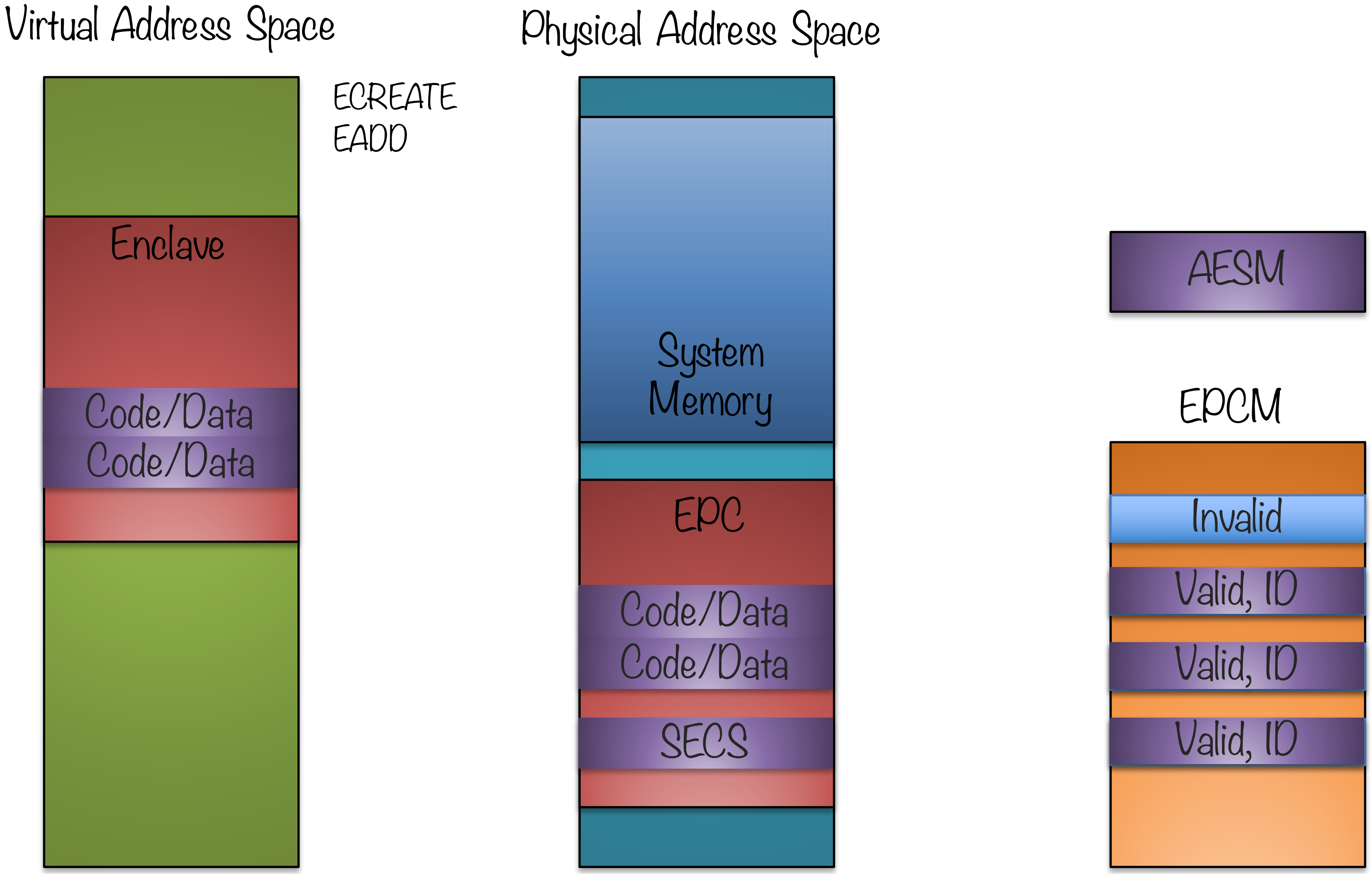
Physical Address Space

Life Cycle of Enclave

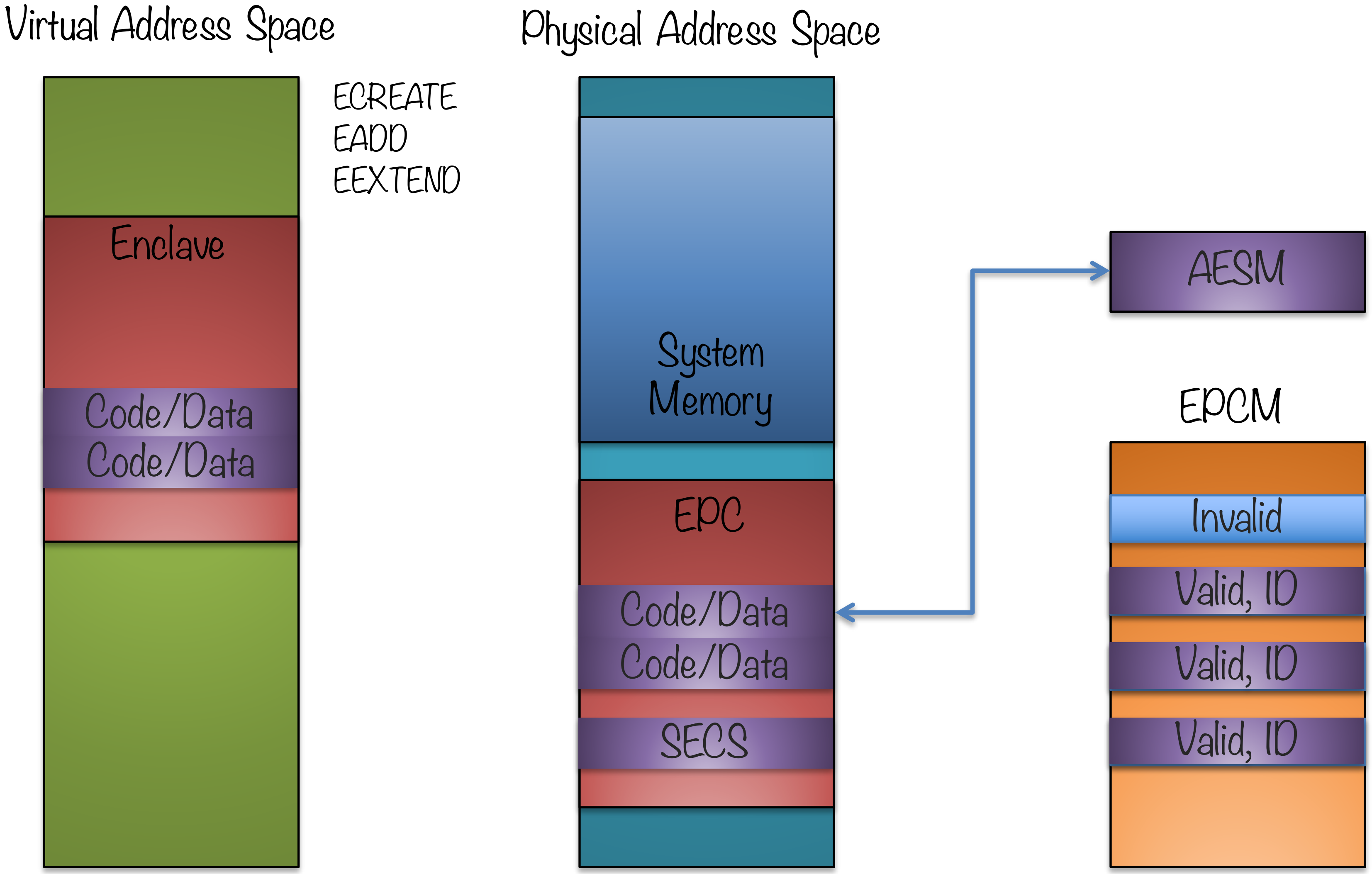


Life Cycle of Enclave

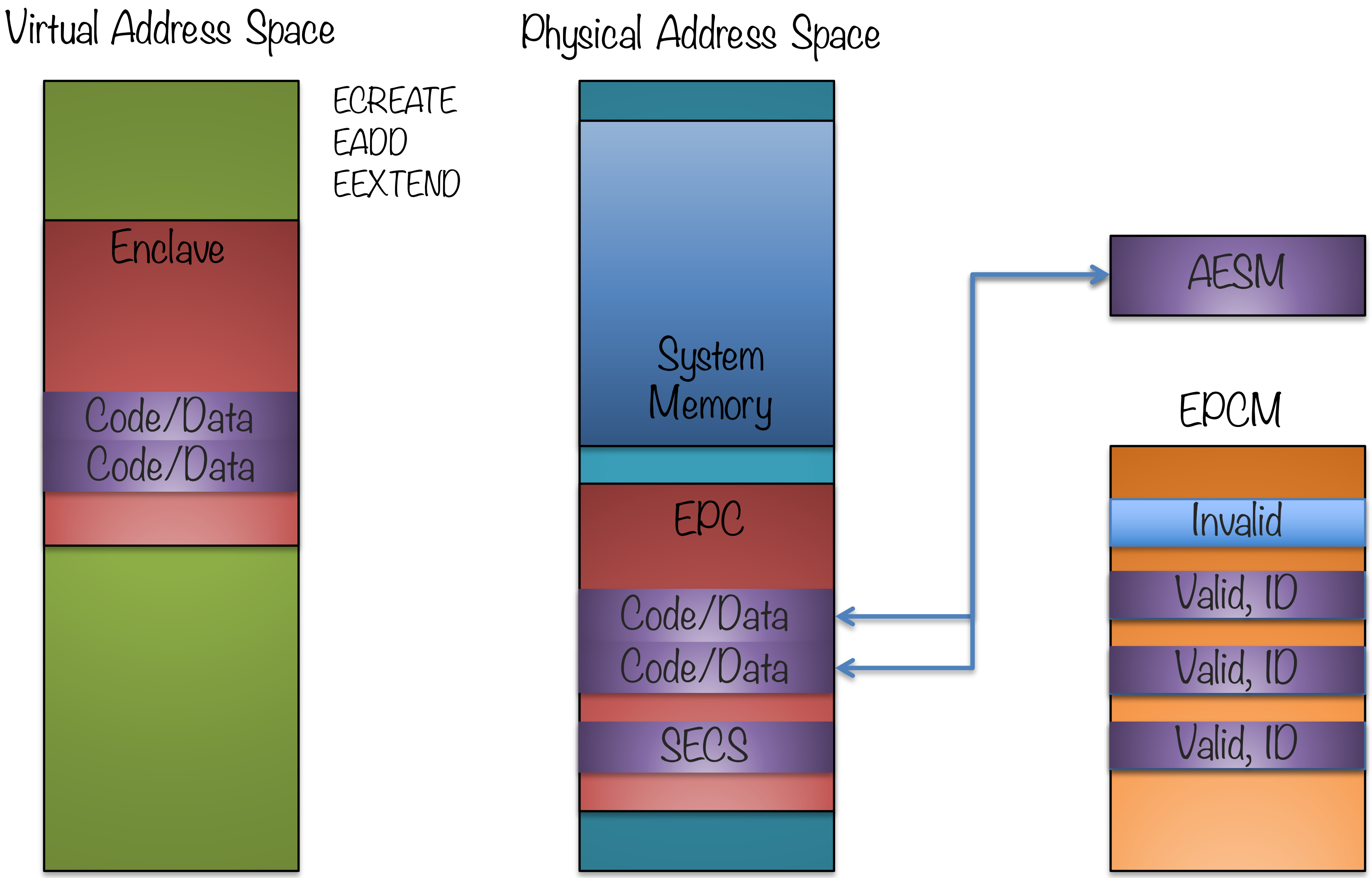
ECREATE
EADD



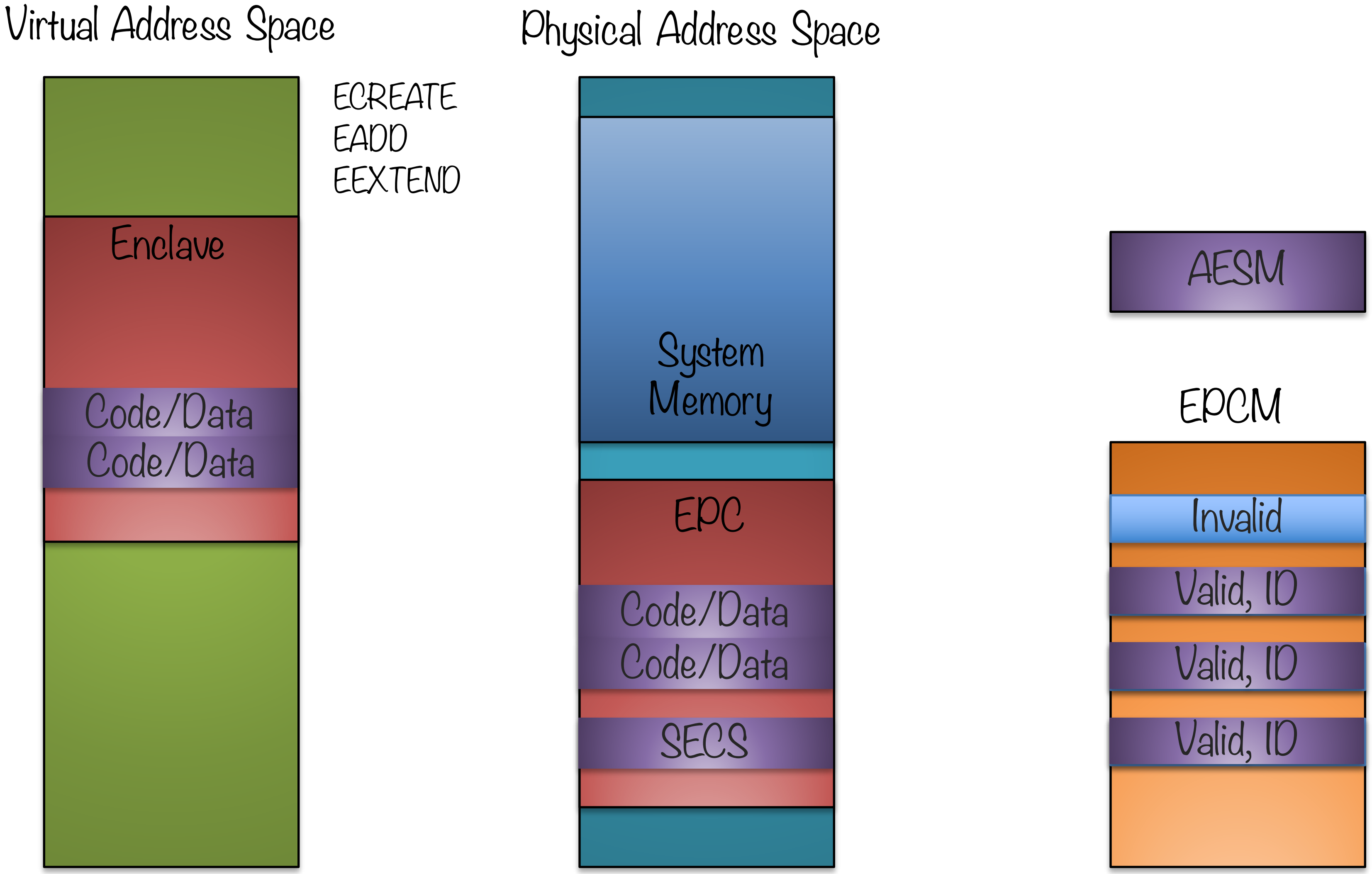
Life Cycle of Enclave



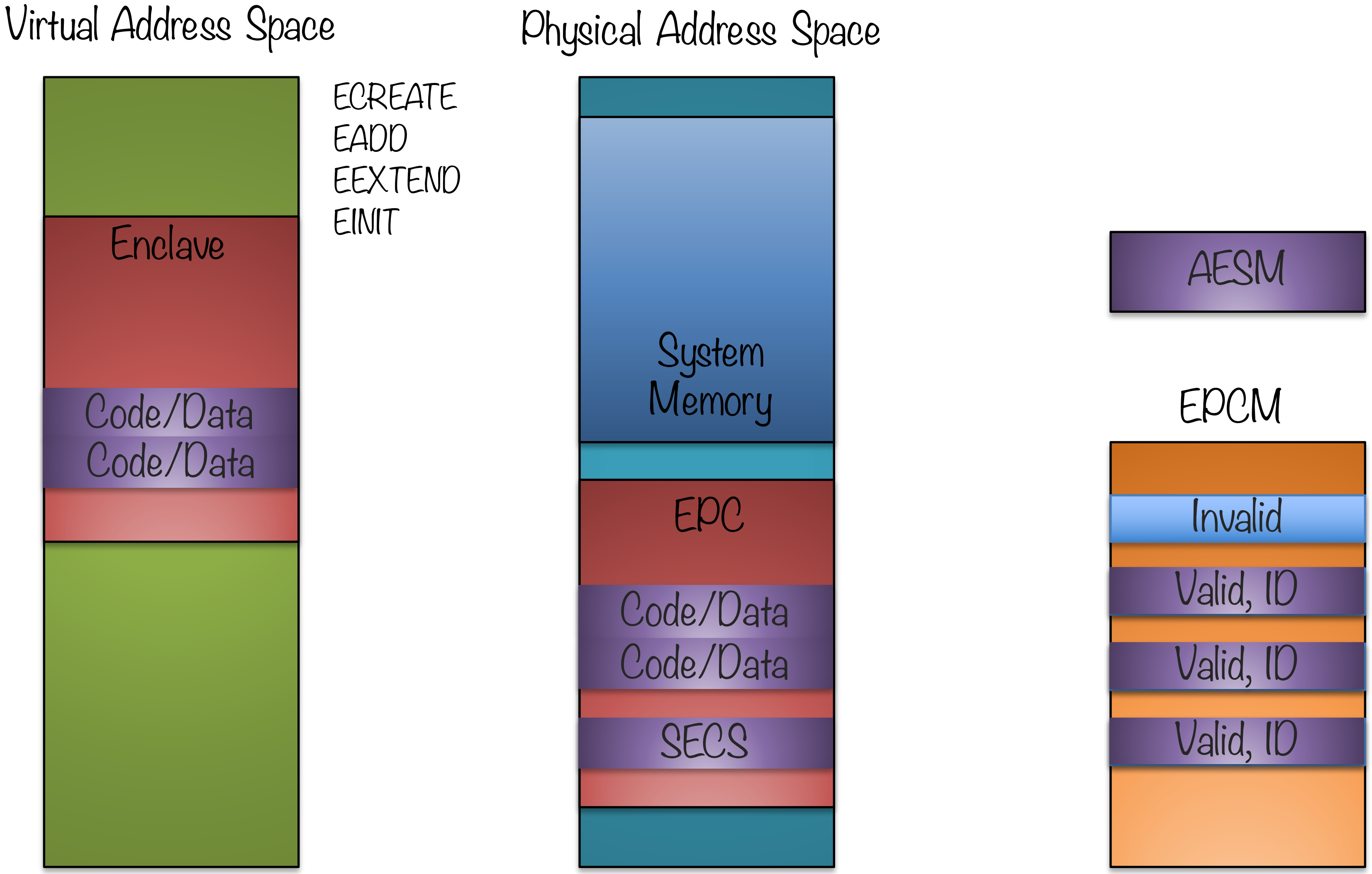
Life Cycle of Enclave



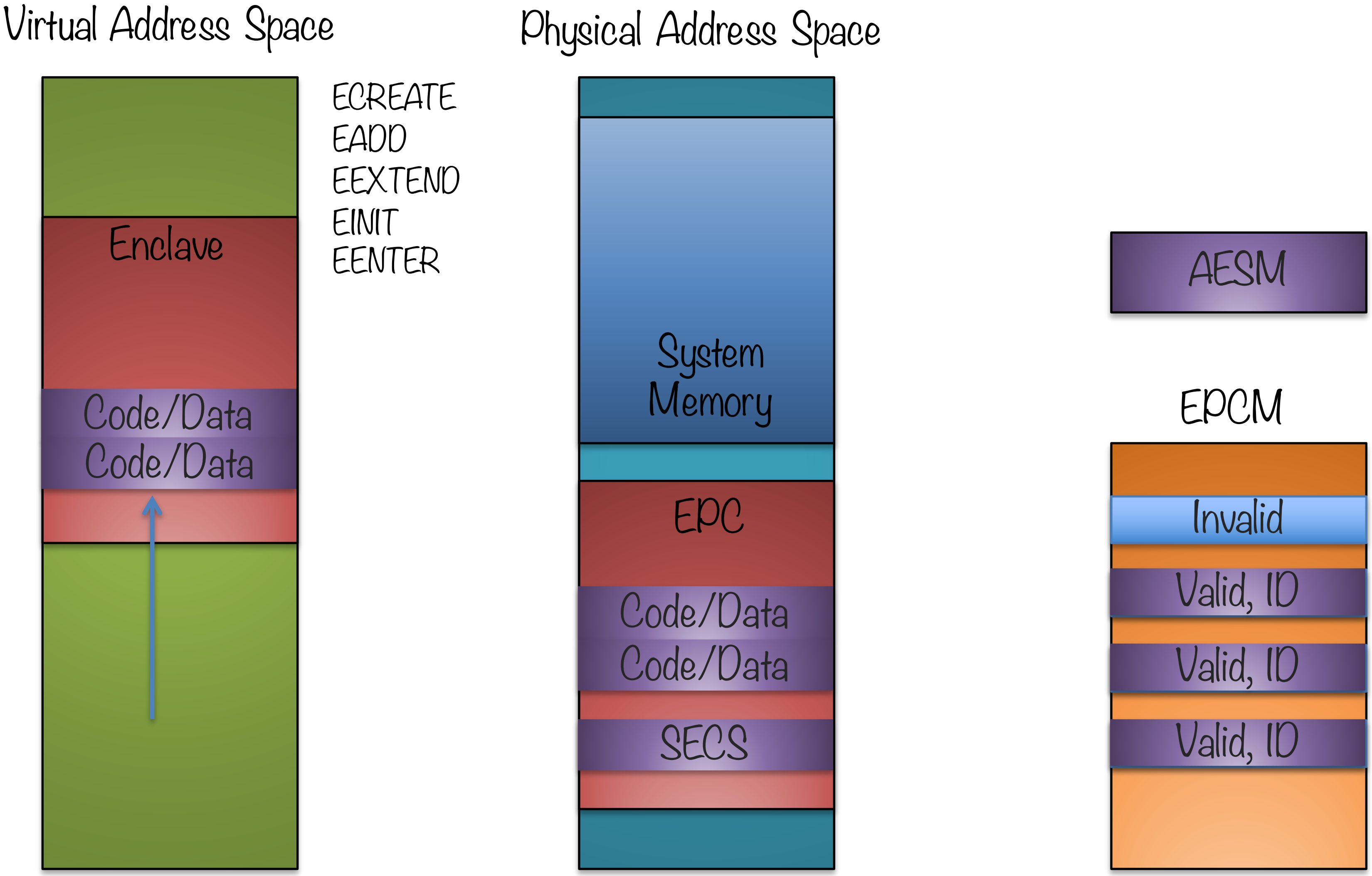
Life Cycle of Enclave



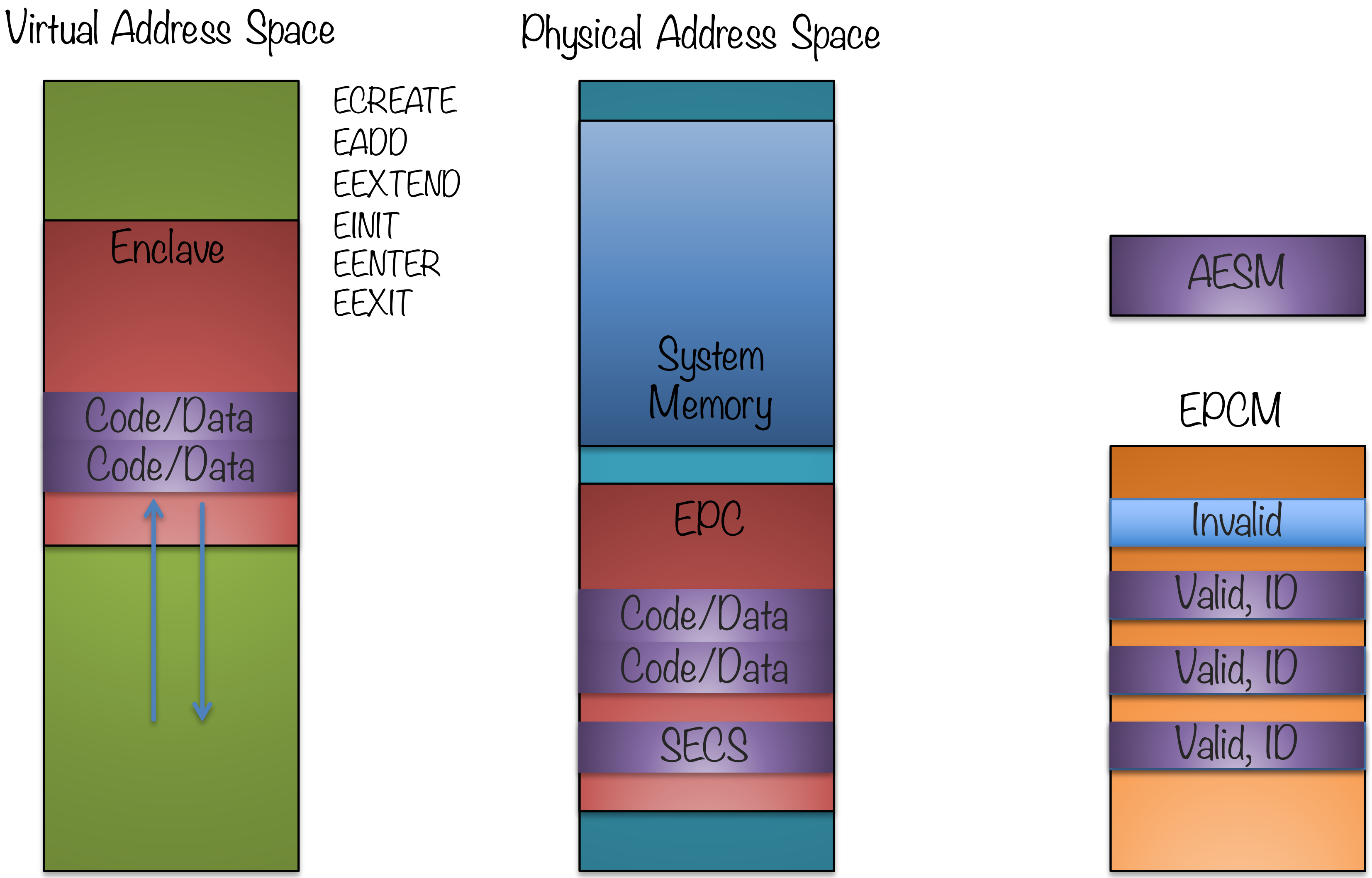
Life Cycle of Enclave



Life Cycle of Enclave



Life Cycle of Enclave



Virtual Address Space

Enclave

Code/Data

Code/Data

ECREATE
EADD
EEXTEND
EINIT
EENTER
EEXIT

Physical Address Space

System Memory

EPC

Code/Data

Code/Data

SECS

AESM

EPCM

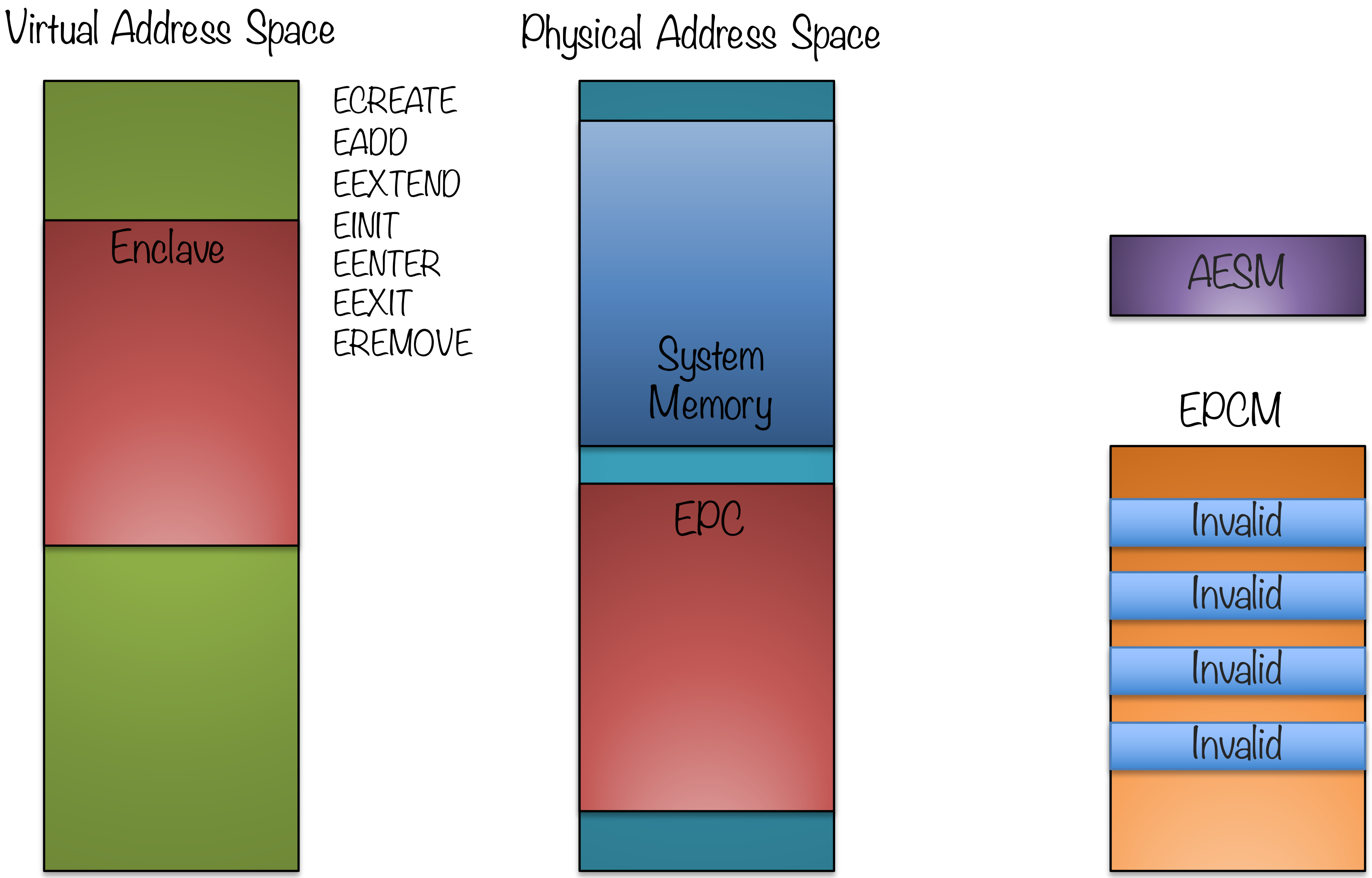
Invalid

Valid, ID

Valid, ID

Valid, ID

Life Cycle of Enclave

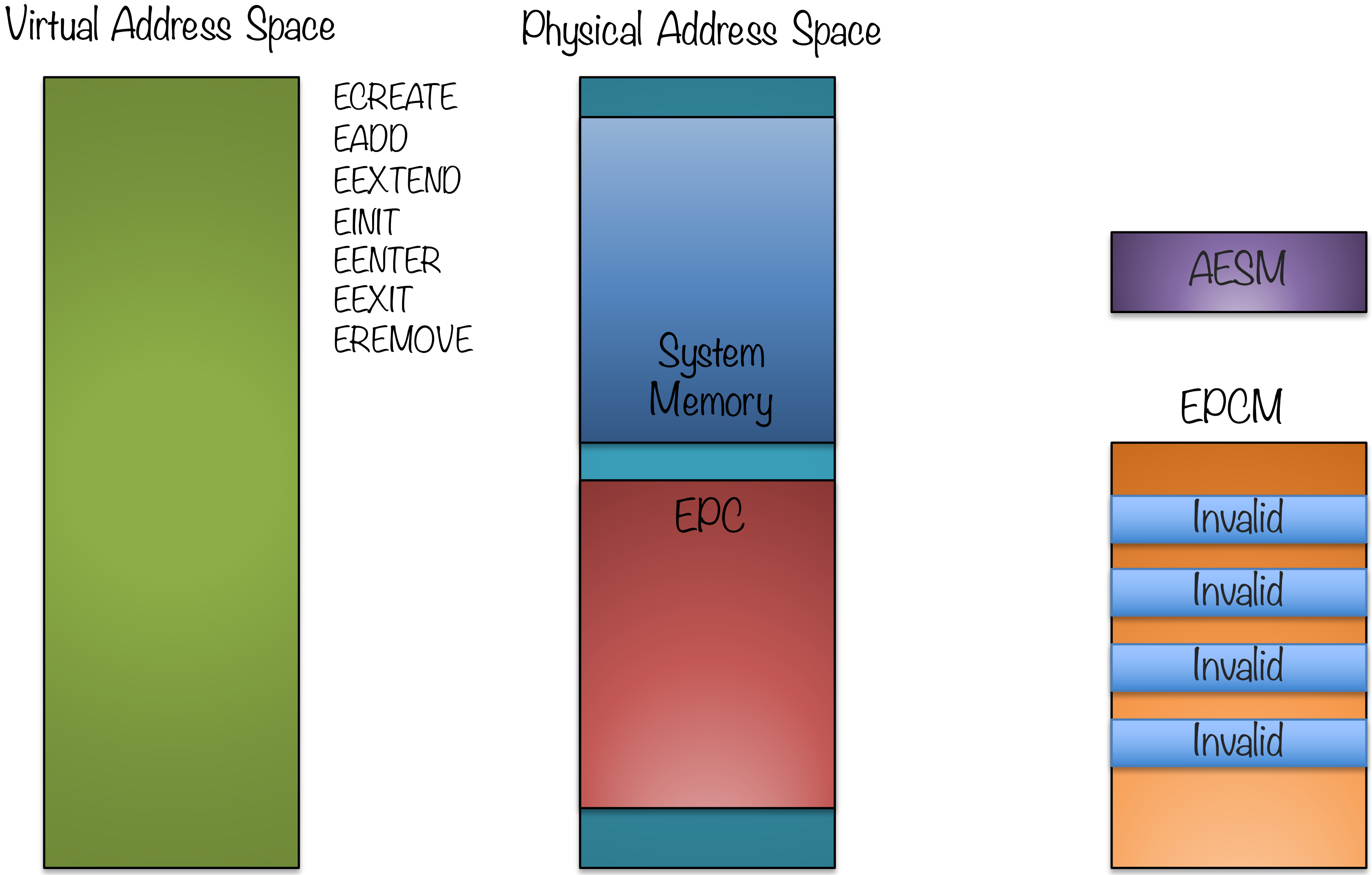


Virtual Address Space

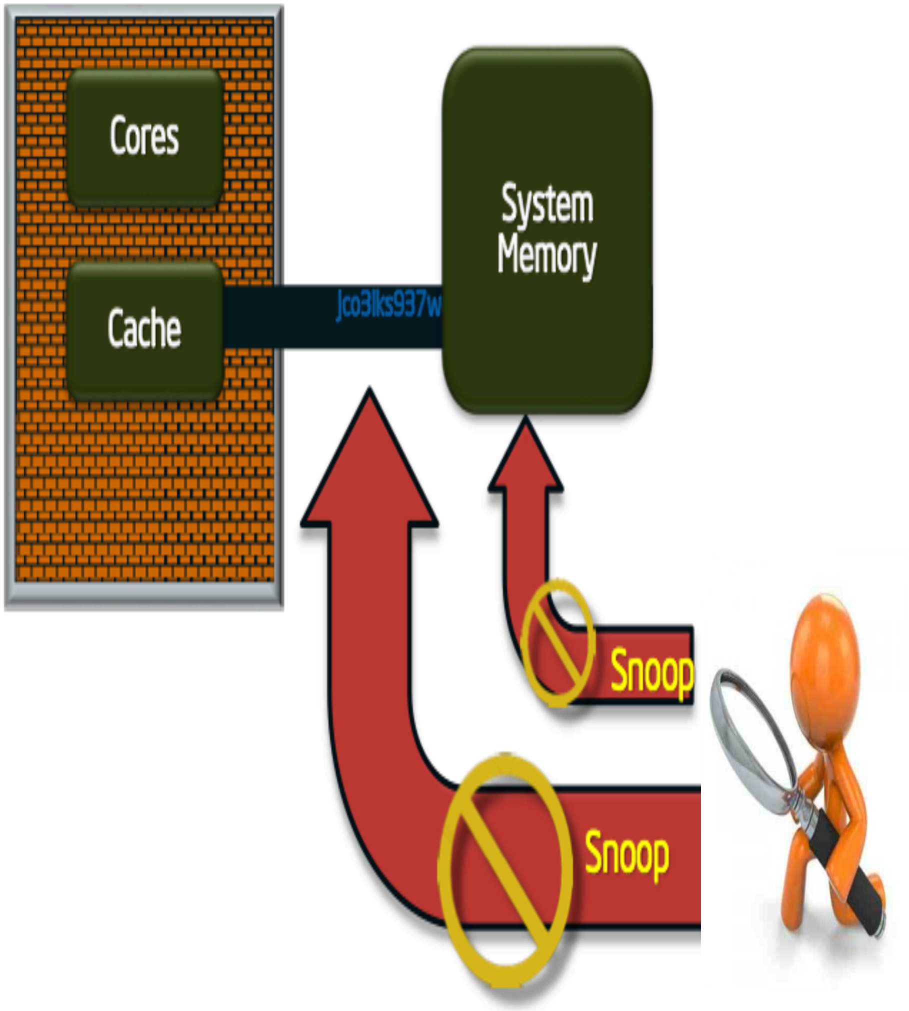
Physical Address Space

ECREATE
EADD
EEXTEND
EINIT
EENTER
EEXIT
EREMOVE

Life Cycle of Enclave



Protection vs. Memory Snooping



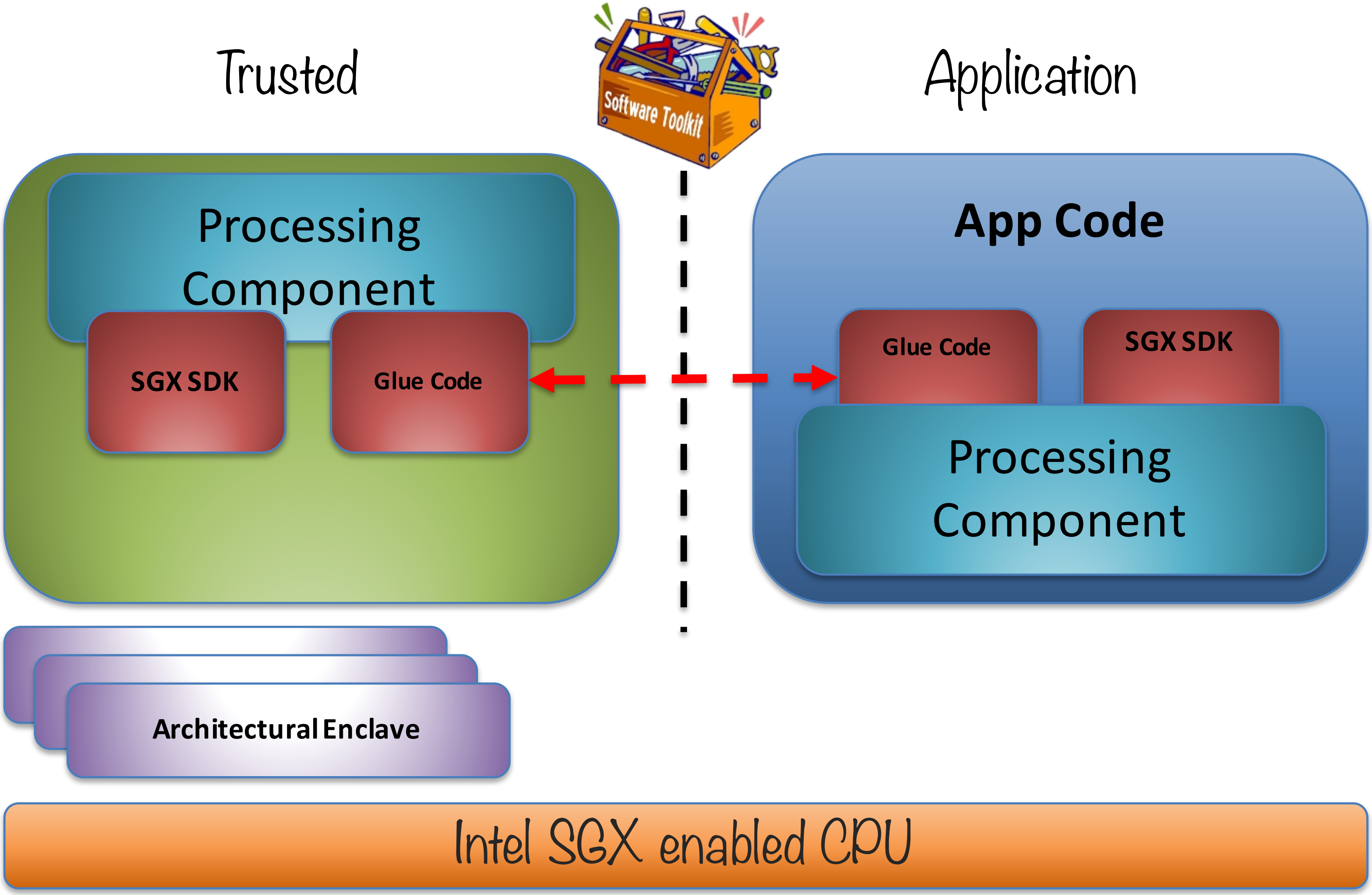
✓ Security perimeter is CPU package boundary

✓ Data and code unencrypted inside CPU package

✓ Data and code outside CPU package is encrypted and/or integrity checked

✓ External memory reads and bus snoops see only encrypted data

Developing with SGX



Trusted

Processing Component

SGX SDK

Glue Code

Application

App Code

Glue Code

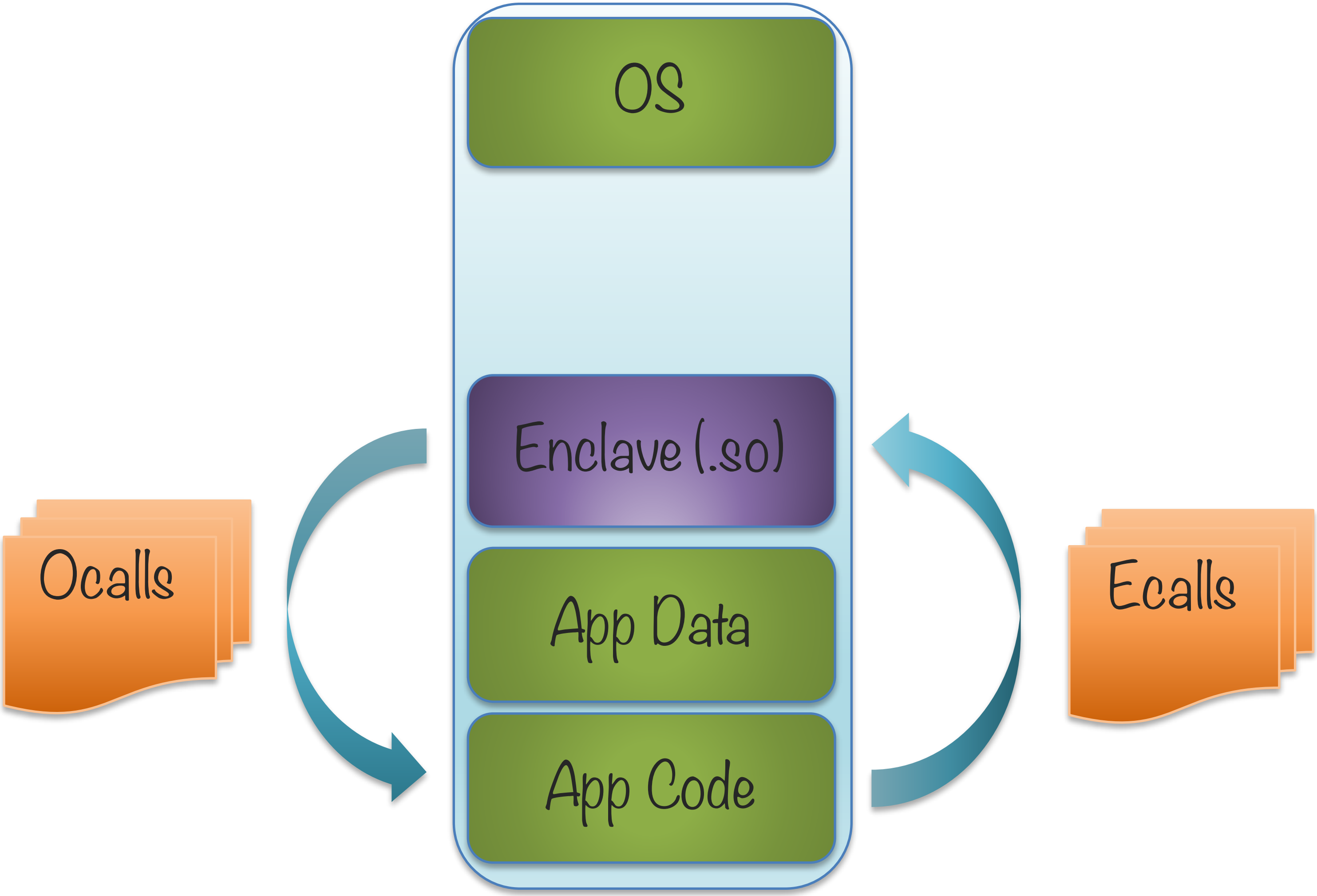
SGX SDK

Processing Component

Architectural Enclave

Intel SGX enabled CPU

Intel SGX Call Gates



User Process

Intel SGX advantages

- Intel SGX, provides an ability to create a secure *enclave* [a secure memory area] within a potentially compromised OS

- You can create an enclave with the desired code, then lock it down, measure the code there and if everything is fine, ask the processor to start executing the code

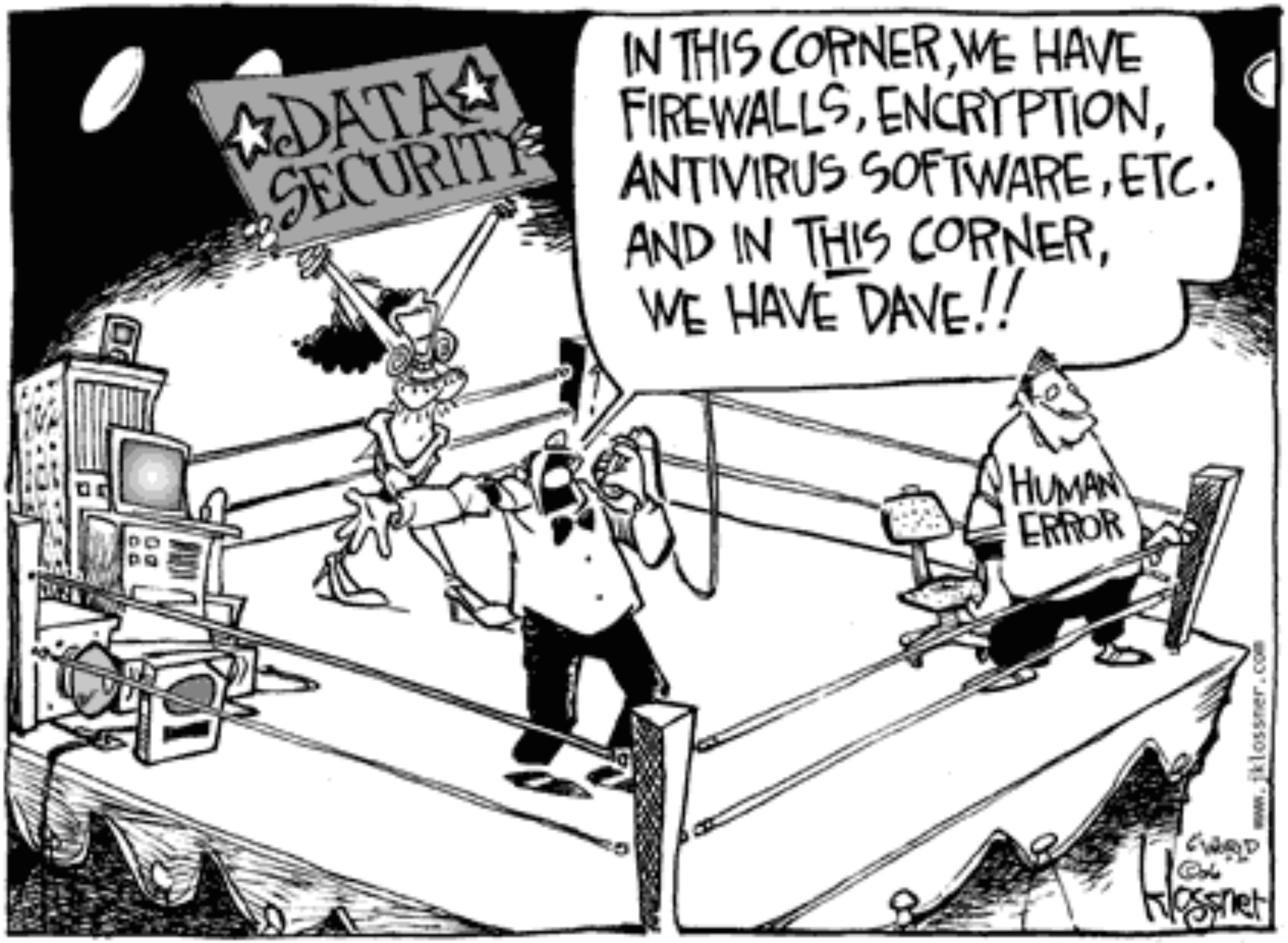
- A nice surprise is that SGX infrastructure no longer depends upon the TPM to perform the measurement

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
- ✓ Applications run within OS environment
  - ✓ Low learning curve for application developers
  - ✓ Open to all developers**
- ✓ Resources managed by system software

SGX usage models

- ✓ Running a LibOS inside an enclave
  - ✓ [https://www.usenix.org/system/files/conference/osdi14/osdi14-paper-baumann.pdf]
- ✓ Running hadoop map-reduce jobs inside enclave
  - ✓ [http://research.microsoft.com/apps/pubs/?id=210786]
- ✓ Building an encrypted file system using SGX to protect against cold boot attacks and DMA attacks
  - ✓ [Not published yet]
- ✓ Running privacy protected genomics workload inside enclave
  - ✓ [Not published yet]


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
CWORLD ©06
Klossner
www.jklossner.com

References

- ✓ http://software.intel.com/en-us/articles/innovative-instructions-and-software-model-for-isolated-execution
- ✓ http://software.intel.com/en-us/articles/innovative-technology-for-cpu-based-attestation-and-sealing
- ✓ http://software.intel.com/sites/default/files/article/413938/hasp-2013-innovative-instructions-for-trusted-solutions.pdf
- ✓ http://web.stanford.edu/class/ee380/Abstracts/150415-slides.pdf
- ✓ A good read to understand SGX: http://theinvisiblethings.blogspot.com/2013/08/thoughts-on-intels-upcoming-software.html