Xan

Intel Software Guard Extension

Top Level

- Intel designed a hardware trusted execution environment with the smallest possible attack surface: the CPU.
- Intel SGX has 17 new architecture instructions that can be used by applications to set aside private regions of code and data, and can prevent direct attacks on executing code or data stored in memory.

Compatibility

- Intel Skylake Processor
- Windows 7 - 10 or Ubuntu 14.04
- Intel Parallel Studio or Visual Studio
- C/C++ only

Objectives of SGX

- Protects sensitive data from modified rouge software running at a higher privilege level
- Protects sensitive code and data without using much resources
- Applications create a unique cert that is embedded in the processor to be ran with trusted privileges
- Developers can define secure regions of code

Why look at SGX?

- New Instructions
- Security focused
- Memory Encryption
- TPM replacement
- Most of all….CET

Use Cases

- Better Biometrics
- Better End-point solutions
- Protect EMR
- Key MGMT
- IoT Edge Devices
- Disk Protection

The Enclave

- Think of the enclave as the next TPM devices
- They hold cryptographic information while also running the application is a secure container
- The 17 new instructions for SGX are what make the enclave work correctly

Supervisor Instructions

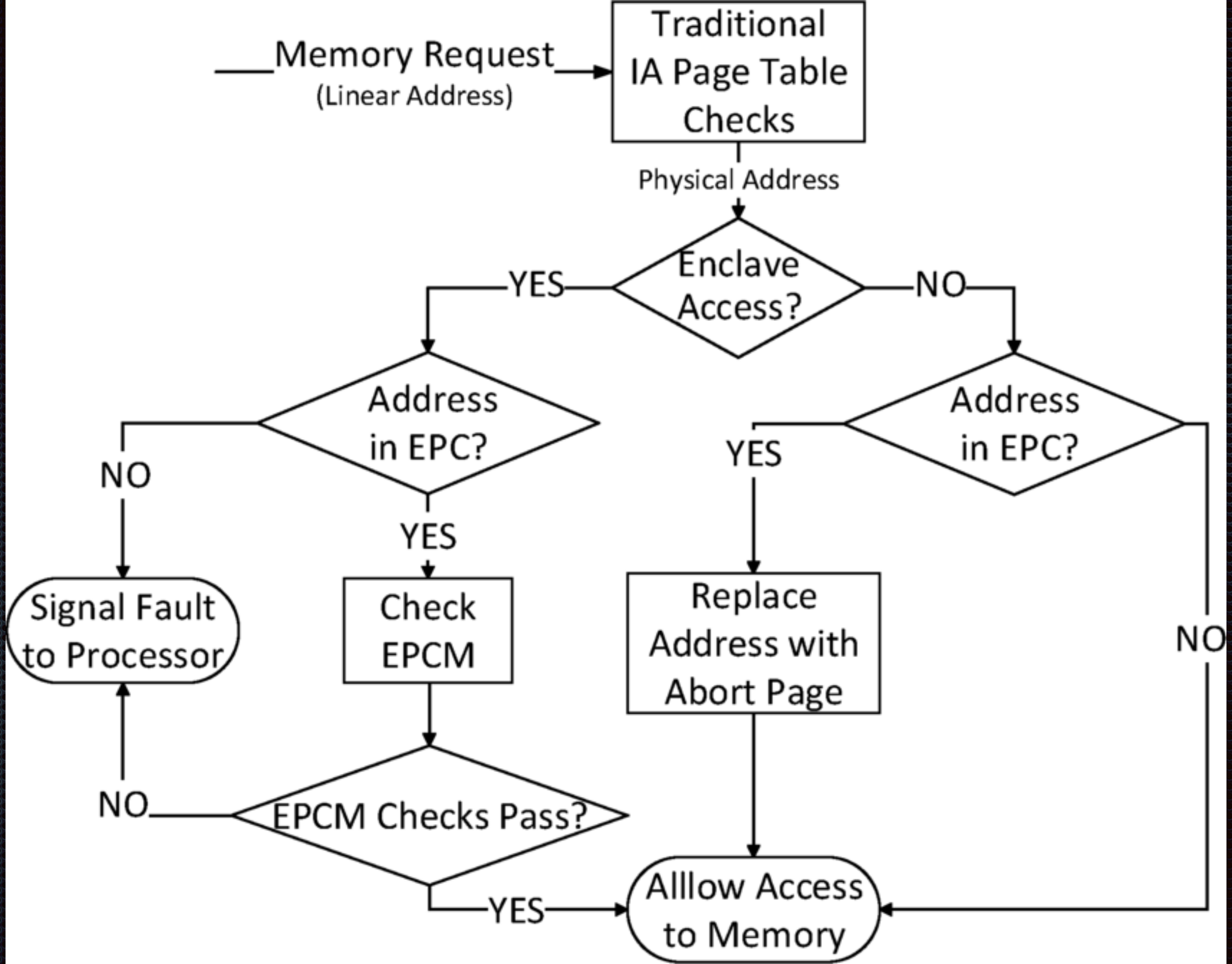
- ENCLS[EADD]: Add a page
- ENCLS[EBLOCK]: Block an EPC page
- ENCLS[EDBGRD]: Create an enclave
- ENCLS[EDBGWR]: Write data by debugger
- ENCLS[EEXTEND]: Extend EPC page measurement

Supervisor Instructions

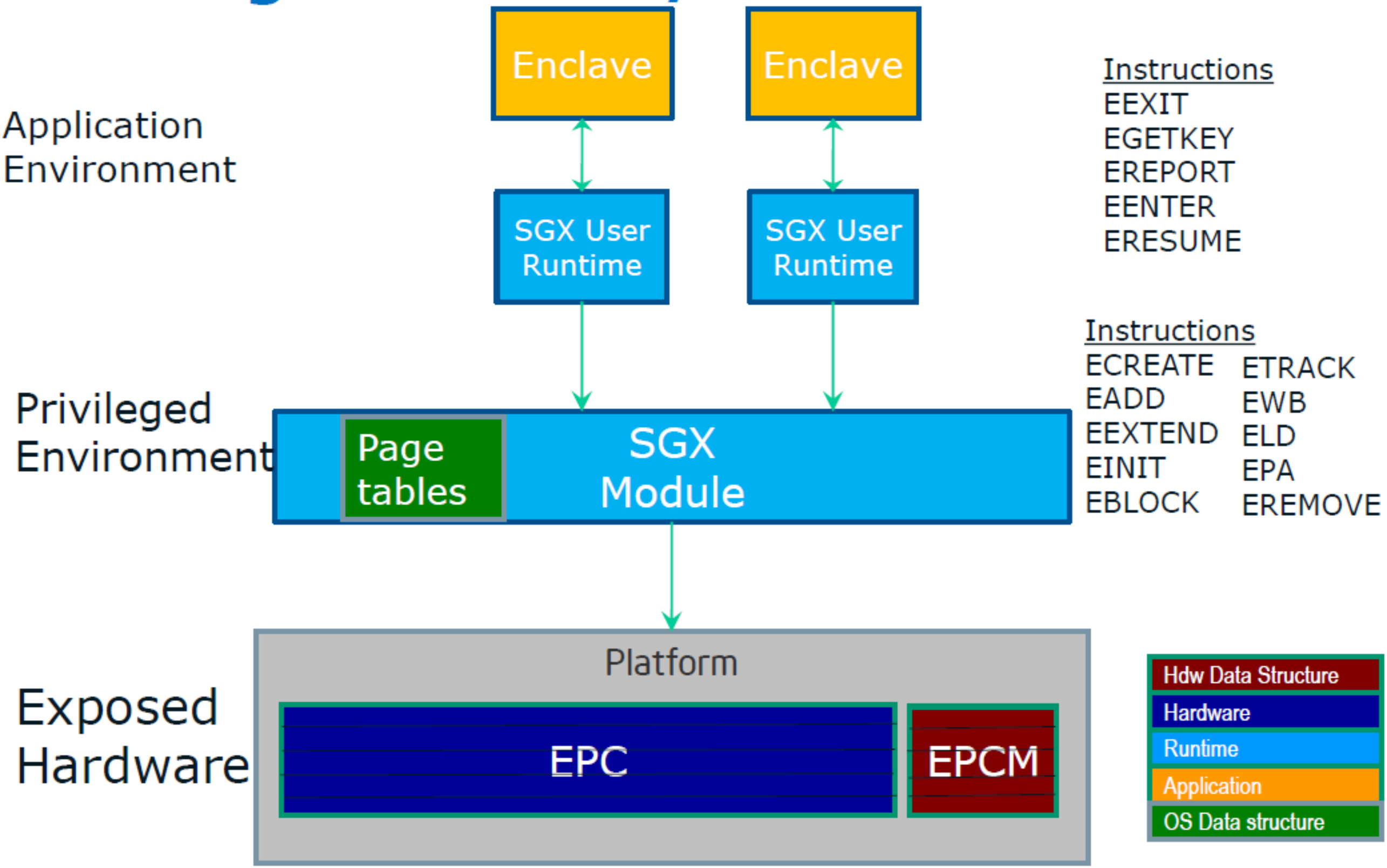
- ENCLS[EINIT] Initialize an enclave
- ENCLS[ELBD] Load an EPC page as blocked
- ENCLS[ELDU] Load an EPC page as unblocked
- ENCLS[EPA] Add version array
- ENCLS[EREMOVE] Remove a page from EPC
- ENCLS[ETRACK] Activate EBLOCK checks
- ENCLS[EWB] Write back/ invalidate an EPC page

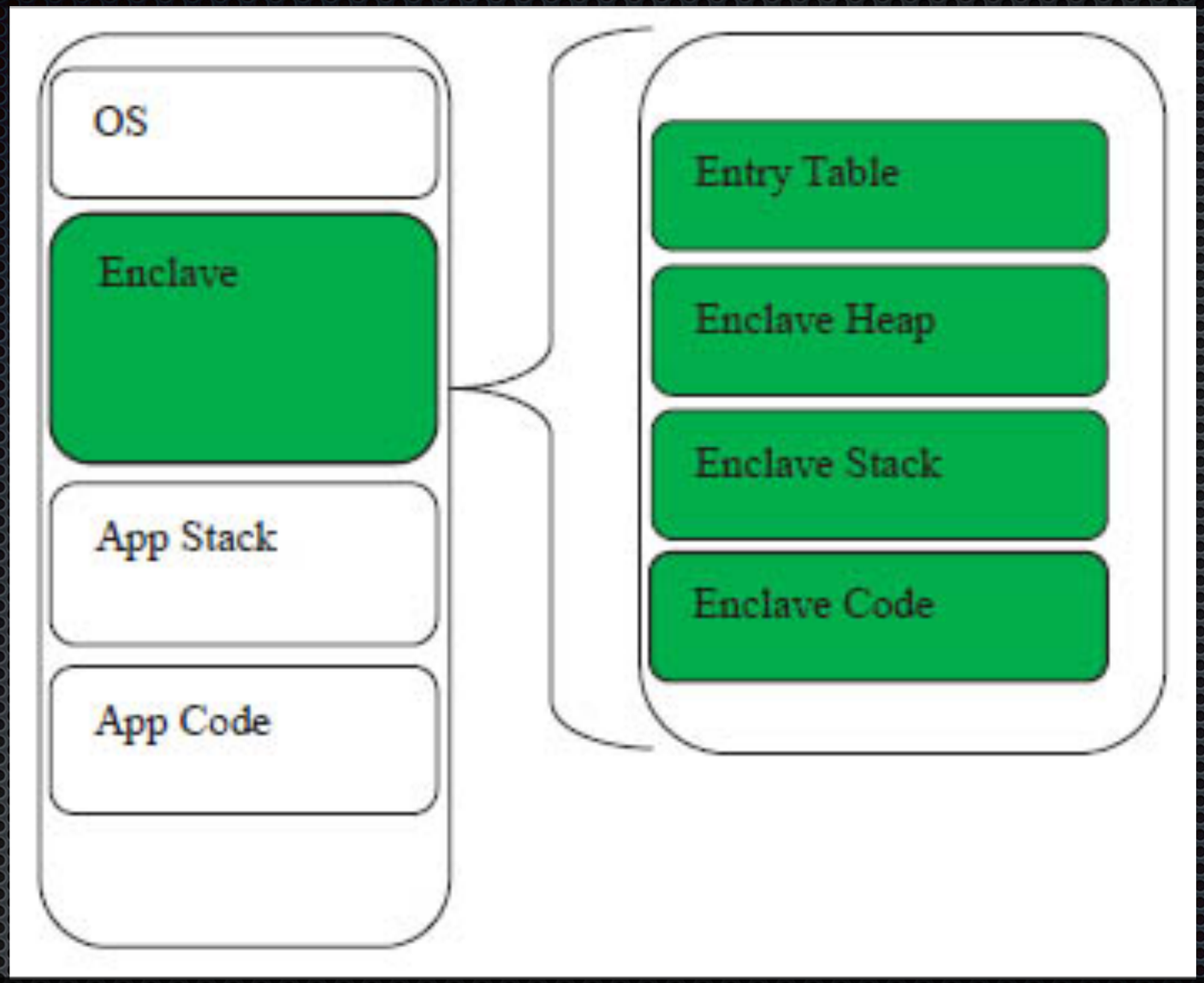
SGX User Instructions

- ENCLU[EENTER]: Enter an Enclave
- ENCLU[EEXIT]: Exit an Enclave
- ENCLU[EGETKEY]: Create a cryptographic key
- ENCLU[EREPORT]: Create a cryptographic report
- ENCLU[ERESUME]: Re-enter an Enclave


Memory Request
(Linear Address)
Traditional IA Page Table Checks
Physical Address
Enclave Access?
YES
NO
Address in EPC?
NO
YES
Signal Fault to Processor
Check EPCM
EPCM Checks Pass?
NO
YES
Address in EPC?
YES
NO
Replace Address with Abort Page
Alllow Access to Memory

SGX High-level HW/SW Picture





Shadow Stack

Attack Surface

- The attack surface of today is that you gain privilege at the App level and then pivot to the OS.
- The attack surface of SGX is that you gain privilege at the App level and then try to pivot to the hardware…..this is much harder to do.

The Good

- Improves security at the bare metal level
- Can have quick add-ons that improve SGX without the need for hardware changes
- Helps cloud providers in the long run
- RAM is encrypted spaces

The Bad

- You need a 6th gen Intel Processor or better
- Its still not entirely completed
- Intel cant market it
- AMD has a competitor with better reviews but not a better future

The Ugly

- You need to recompile code to get it working
- Intel uses an independent source to validate keys but doesn’t disclose who the source is.
- Intel doesn’t have a good roadmap for the future iterations
- For us hackers ROP is dead with CET which is apart of SGX

The Future

- Cloud Apps and Services
- Eventually this will be cheaper than adding TPMs
- Once App Devs get onboard this will be a easy win

To be continued…