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

- App
- App
- App
- OS
- VMM
- Hardware
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

- **OS**
- **App Code**
- **App Data**
- **Enclave (.so)**

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

User Process

Enclave Code

Enclave Data

TCS (*n*)

SECS
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
- Enclave
  - SGX User Runtime
  - Page Tables

Privileged Environment
- SGX Module
- Instructions:
  - EGETKEY
  - EEXIT
  - EREPORT
  - EENTER
  - ERESUME
  - ECREATE
  - ETRACK
  - EADD
  - EWB
  - EEXTEND
  - ELD
  - EINIT
  - EPA
  - EBLOCK
  - EREMOVE

Exposed Hardware
- Platform
  - EPC
  - EPCM
Life Cycle of Enclave

Virtual Address Space

Physical Address Space
Life Cycle of Enclave

Virtual Address Space
- Enclave

Physical Address Space
- ECREATE
- System Memory
- EPC

EPCM
- Invalid
- Invalid
- Invalid
- Invalid
Life Cycle of Enclave

Virtual Address Space
- ECREATE
- Enclave

Physical Address Space
- System Memory
- EPC
- SECS
- Invalid
- Invalid
- Invalid

AESM

EPCM
- Invalid
- Invalid
- Invalid
- Invalid
Life Cycle of Enclave

Virtual Address Space
- Enclave

Physical Address Space
- ECREATE
- Code/Data
- System Memory
- EPC
- SECS
- AESM
- EPCM
  - Invalid
  - Invalid
  - Invalid
  - Valid, ID
Life Cycle of Enclave

Virtual Address Space

Physical Address Space

Enclave

Code/Data

System Memory

EPC

Code/Data

SECS

Invalid

Invalid

EPCM

Invalid

Valid, ID

ECREATE

AESM
Life Cycle of Enclave

Virtual Address Space

Enclave

Code/Data

ECREATE

EADD

Physical Address Space

Code/Data

System Memory

EPC

Code/Data

SECS

Invalid

EPCM

AESM

Invalid

Invalid

Valid, ID

Valid, ID
Life Cycle of Enclave

Virtual Address Space

- Enclave
- Code/Data
- Code/Data

Physical Address Space

- Code/Data
- System Memory
- EPC
- Code/Data
- SECS
- Invalid
- Invalid
- Invalid

- AESM
- EPCM
- Invalid
- Valid, ID
- Valid, ID
- Valid, ID
Life Cycle of Enclave

Virtual Address Space
- Enclave
  - Code/Data
  - Code/Data

Physical Address Space
- System Memory
  - EPC
  - Code/Data
  - Code/Data
  - SECS

EPCM
- AESM
- Invalid
- Valid, ID
- Valid, ID
- Valid, ID

ECREATE EADD
Life Cycle of Enclave

Virtual Address Space

Enclave
Code/Data
Code/Data

ECREATE
EADD
EEXTEND

Physical Address Space

System Memory
EPC
Code/Data
Code/Data
SECS

Valid, ID

AESM

EPCM
Invalid
Valid, ID
Valid, ID
Valid, ID
Life Cycle of Enclave

Virtual Address Space

- Enclave
- Code/Data

Physical Address Space

- System Memory
- EPC
- Code/Data
- SECS
- EPCM
- Invalid
- Valid, ID
- Valid, ID
- Valid, ID
Life Cycle of Enclave

Virtual Address Space
- Enclave
- Code/Data
- Code/Data
- Code/Data

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

- Enclave
- Code/Data
- Code/Data

Physical Address Space

- System Memory
- EPC
- Code/Data
- Code/Data
- SECS

EPCM

- Invalid
- Valid, ID
- Valid, ID
- Valid, ID

AESM
Life Cycle of Enclave

Virtual Address Space

ECREATE
EADD
EEXTEND
EINIT
EENTER
EEXIT

Enclave

Code/Data

Code/Data

Physical Address Space

System Memory

EPC

Code/Data

Code/Data

Valid, ID

SECS

Valid, ID

Valid, ID

AESM

EPCM

Invalid

Valid, ID

Valid, ID
Life Cycle of Enclave

Virtual Address Space
- ECREATE
- EADD
- EEXTEND
- EINIT
- ENTER
- EEXIT
- ERMOVE

Physical Address Space
- System Memory

Enclave

EPC

EPCM
- Invalid
- Invalid
- Invalid
- Invalid

AESM
Life Cycle of Enclave

Virtual Address Space
- ECREATE
- EADD
- EEXTEND
- EINIT
- EENTER
- EEXIT
- EREMOVE

Physical Address Space
- System Memory
- EPC

Discs
- AESM
- EPCM
- Invalid
- Invalid
- Invalid
- Invalid
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

**Intel SGX enabled CPU**
Intel SGX Call Gates

OS

Enclave (.so)

App Data

App Code

User Process

Ocalls

Ecalls
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]
In this corner, we have firewalls, encryption, antivirus software, etc. And in this corner, we have Dave!!
References

✓ A good read to understand SGX: http://theinvisiblethings.blogspot.com/2013/08/thoughts-on-intels-upcoming-software.html