Introduce of Intel SGX

한성대 김경호

https://youtu.be/33flxu-7jD8

HSU 한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

Contents

CryptoCraft LAB

1. What is Intel SGX | SE, TPM

- SE (Secure Elements)

  - 중요 데이터 저장 및 결제 같은 Secure App을 안전하게 실행할 수 있는 플랫폼
  - Malware Attack으로부터 데이터와 응용프로그램을 지켜주는 역할
  - 저장 용량 및 처리 속도가 제한적

- TPM (Trusted Platform Module)

  - 하드웨어 기반의 보안 관련한 기능만 제공하는 보안 암호화 프로세서
  - 다양한 변조 방지 메커니즘을 사용하여 안전한 암호화 연산 수행
  - 시스템 무결성 측정 및 키 생성 및 사용
  - 저장 용량이 제한적이고 암호화 기능만 수행함

1. What is Intel SGX | TEE

- TEE (Trusted Execution Environment)
  - 신뢰 할 수 있는 실행 환경
  - 메인 프로세서 내부의 보안 영역으로 격리된 환경에서 운영체제와 병렬 실행
  - 격리된 환경을 통한 응용프로그램의 무결성 및 기밀성 제공
  - H/W, S/W 모든 측면에서 보안성 극대화
  - Intel사의 SGX와 ARM사의 TrustZone

1. What is Intel SGX | Intel SGX

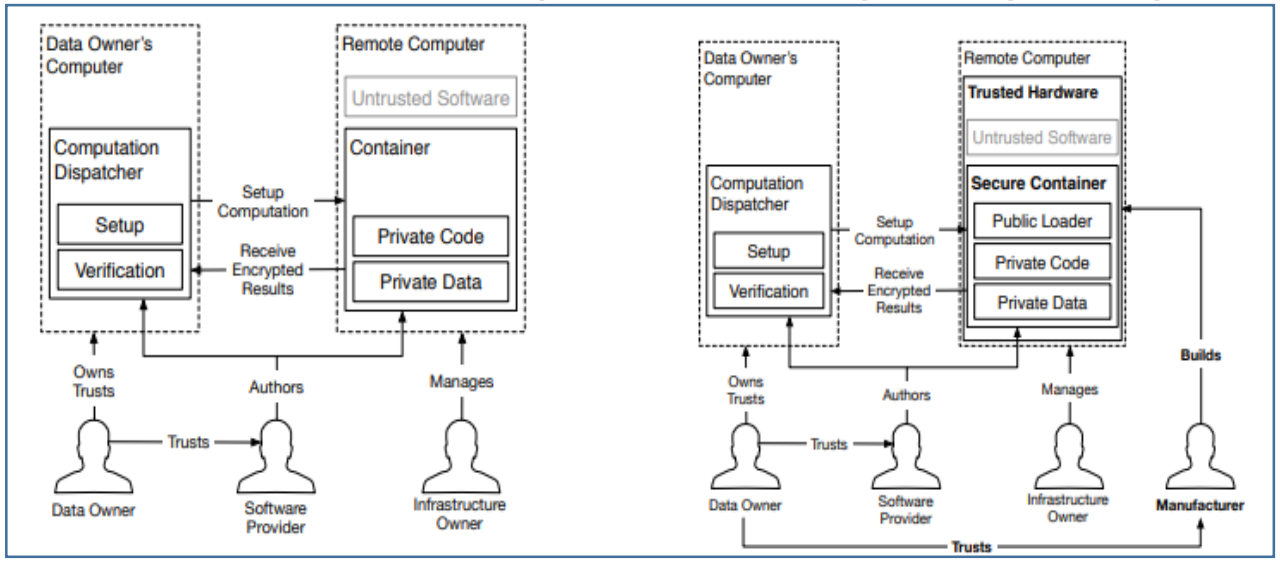
- Intel SGX

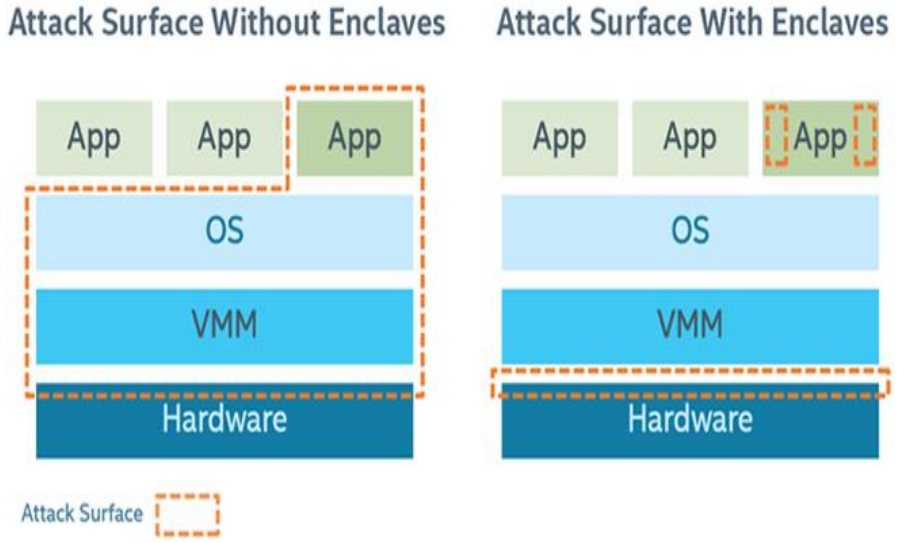
Intel에서 제공하는 CPU 명령어 코드

Enclave라고 하는 메모리에서 분리된 환경을 제공

운영체제, 하이퍼바이저 포함 어떤 수준의 권한으로도 접근이 불가능

Enclave를 사용함으로써 공격 범위를 효과적으로 경감





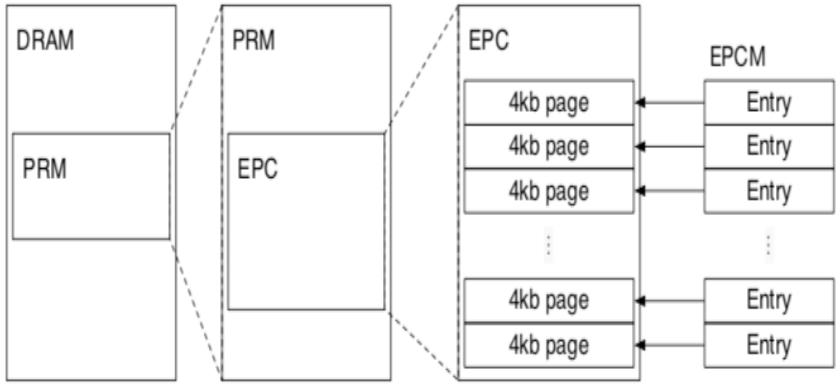
2. System Architecture | PRM, EPC

- PRM(Processor Reserved Memory)

  Enclave Code 및 Data 저장되는 DRAM에서 분리된 메모리
  다른 S/W는 접근 불가능 (운영체제, 하이퍼바이저 포함)

- EPC(Enclave Page Cache)

  Enclave Code, Data를 저장하는 4KB Pages로 구성된 PRM subset 메모리
  System Software의 주소 변환 체계를 그래도 사용하여 Page 관리
  Non-Enclave 소프트웨어는 접근이 불가능



2. System Architecture | EPCM

- EPCM(Enclave Page Cache Map)

  Enclave 할당은 기존 System Software의 주소 변환 체계를 그대로 사용
  System Software는 믿을 수 없는 S/W로 간주하여 확인을 위해 Map을 사용
  한 Page에 2개 이상의 Enclave를 할당했는지 확인
  Page의 의도된 용도를 Page Type으로 관리하여 어떤 명령어 쓸지 결정

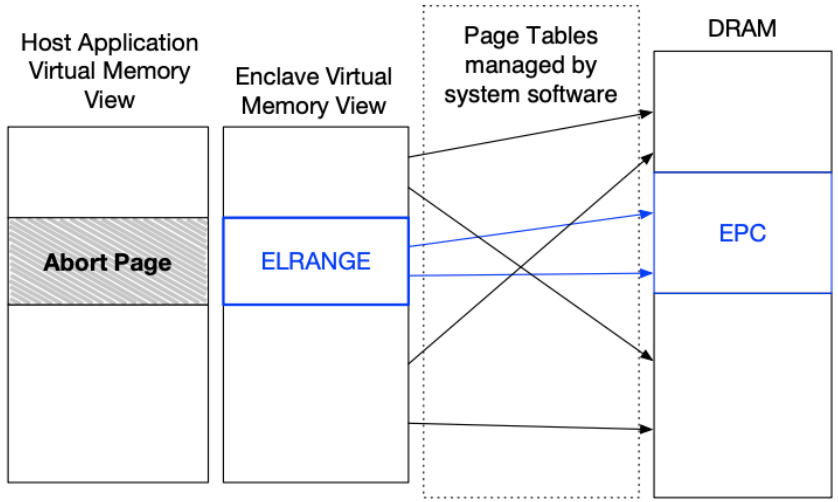
Page Type – PT_REG
PT_SECS

Field	Bits	Description
VALID	1	0 for un-allocated EPC pages
PT	8	page type
ENCLAVESECS		identifies the enclave owning the page

2. System Architecture | SECS

- SECS(The SGX Enclave Control Structure)
  - Enclave의 Metadata
  - EPCM의 Page type에 PT_SECS로 저장
  - Enclave를 할당할 때, 해제할 때 사용

- ELRANGE(The Enclave Linear Address Range)
  - EPC page를 Mapping한 Virtual Address Space
  - ELRANGE 내부의 데이터는 무결성 보장



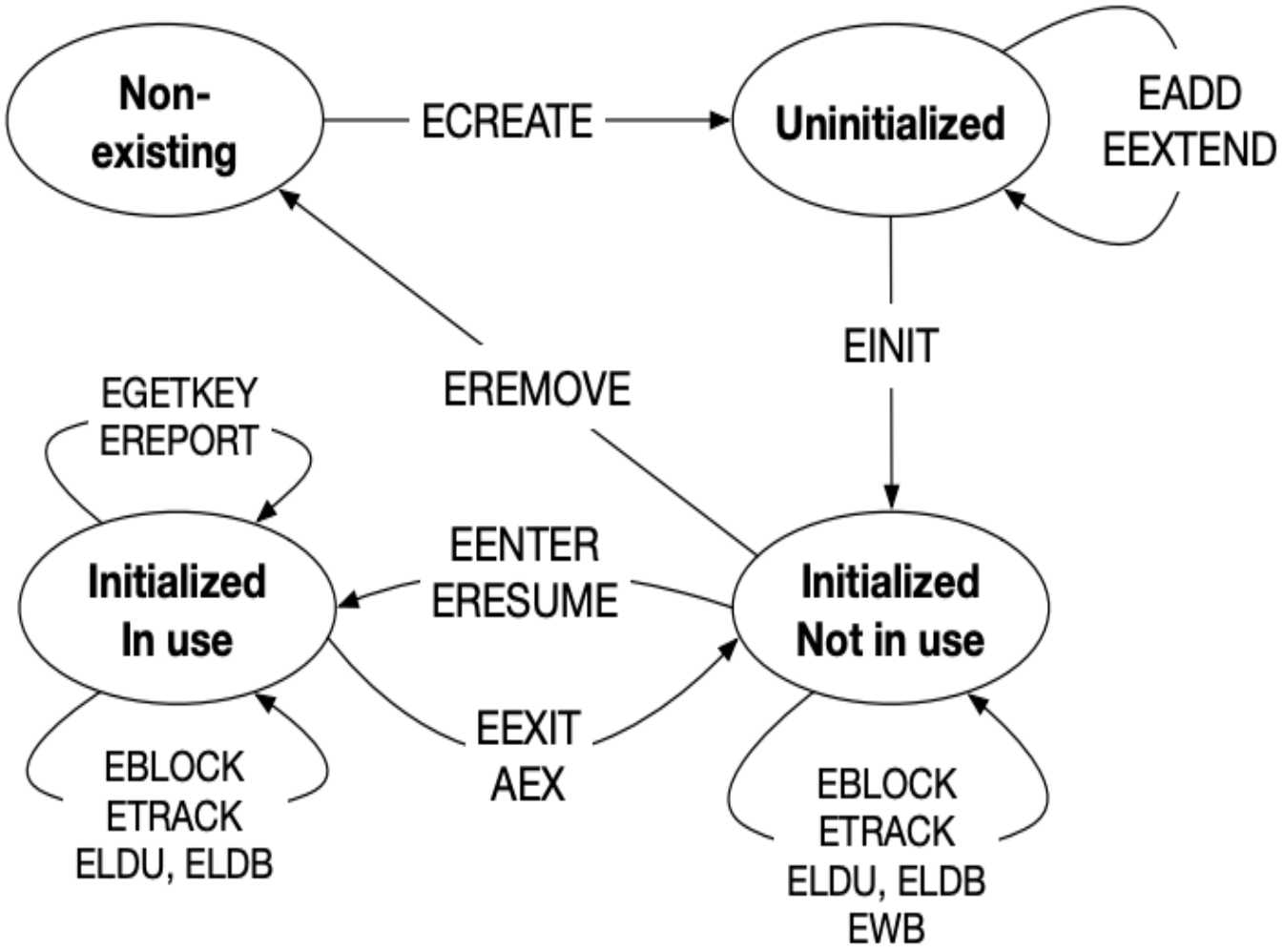
2. System Architecture | Address Translation

- Address Translation for SGX Enclaves

System Software의 주소 변환 방식 그대로 사용
Memory Mapping Attack – Specific Virtual Address
EPC page 할당 시 EPCM에 예상되는 가상 주소를 저장
주소 변환 결과 EPC page 가상 주소와 기록한 가상 주소가 일치하도록 보장
각 EPC 페이지의 액세스 권한이 인클레이브 작성자의 의도와 일치하도록 함으로써 Passive memory mapping attack, Fault Injection Attack을 보호

Field	Bits	Description
ADDRESS	48	the virtual address used to access this page
R	1	allow reads by enclave code
W	1	allow writes by enclave code
X	1	allow execution of code inside the page, inside enclave

2. System Architecture | The Life Cycle of an Enclave



SGX 명령어	기능
ECREATE	SECS영역에 enclave 기본정보 저장
EADD	enclave에 데이터 페이지를 로드
EEXTEND	measurement 업데이트
EINIT	enclave 초기화 완료
EENTER	enclave 코드 동작 시작
EEXIT	enclave 코드 동작 완료
EREMOVE	enclave clear

2. System Architecture | The Life Cycle of an Enclave

- Creation

  ECREATE 명령어 사용시 새로운 Enclave생성

  할당되지 않은 EPC page를 새로운 Enclave의 SECS로 바꿈

  (page의 BASEADDR 및 SIZE)

  ECREATE는 SECS에 초기화된 정보를 검증

  Enclave의 SECS의 INIT field를 False로 설정

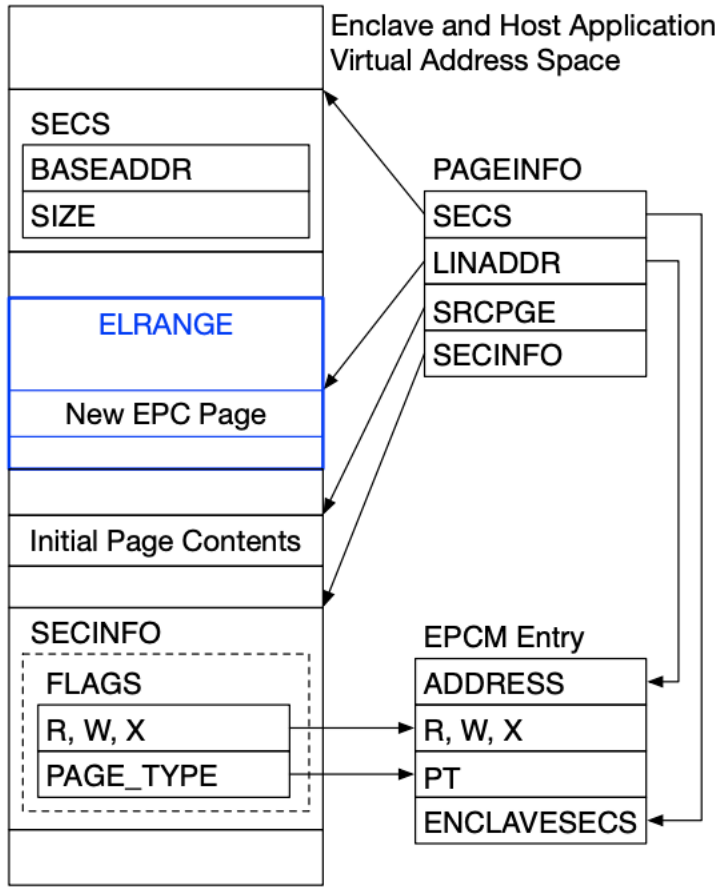
2. System Architecture | The Life Cycle of an Enclave

- Loading

  EADD 명령어로 Encalve Code & Data를 Load

  PAGEINFO 구조에서 Data를 읽어옴

  이미 SECS가 초기화된 상태에서 다시 EADD 명령어 사용시 General Protection Fault, 이미 할당된 EPC Page를 EADD 명령어 사용시 Page Fault



2. System Architecture | The Life Cycle of an Enclave

- Initialization

  Enclave Code & Data Loading 후 EINIT 명령어를 사용하여 초기화
  EINIT 명령어가 끝나면 INIT Field를 true로 설정 후 Enclave 실행 가능
  !! Launch Enclave(LE) -> Token !!

- Teardown

  EREMOVE 명령어를 사용하여 할당 해제
  EPCM -> VALID field를 0으로 설정하여 할당 해제

3. Measurement

- Measurement

  인텔 SGX는 Attestation, Sealing을 위해서 신원을 확인하는 절차가 필요
  신원 증명 시에 사용해야하는 값 -> Measurement
  Enclave를 식별하기 위해서 저장된 Measurement 값을 이용하여 비교
  특정 정보들을 SHA-2 알고리즘으로 Hash 결과값 저장
  Hash 값이기 때문에 조금의 변화로도 값이 변경

3. Measurement | MRENCLAVE, MRSIGNER

- MRENCLAVE

  Local Attestation 에서 사용하는 Measurement 값

  ECREATE, EADD, EEXTEND 과정에서 나오는 값들을 이용하여 Hash 값을 생성하고 EINIT에서 Measurement값을 최종화

- MRSIGNER

  Remote Attestation 에서 사용하는 Measurement 값

  RSA Key의 계수, 제품 ID, Security Version number 사용

Q & A