Intel SGX를 이용한 병원 정보 시스템 제안

한성대학교 IT융합공학부

김경호 김현준 최승주 서화정

HSU 한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

Contents

1. Hospital Information System (HIS)

2. HIS의 정보 보호 이슈

3. Trusted Execution Environment (TEE)

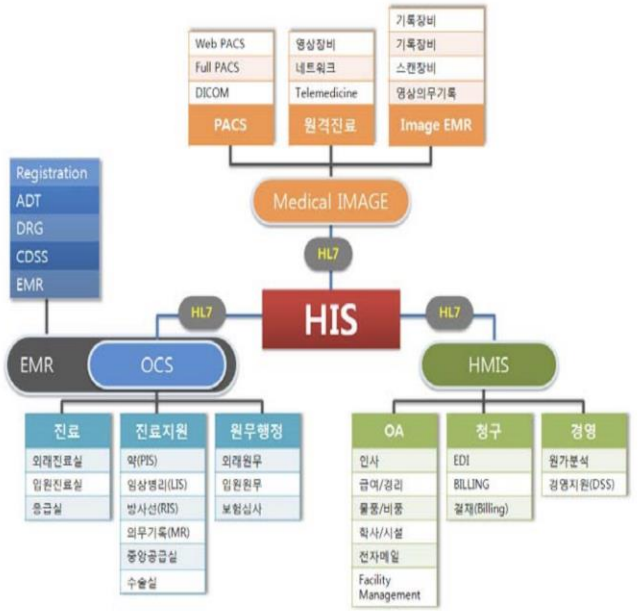
4. Intel SGX

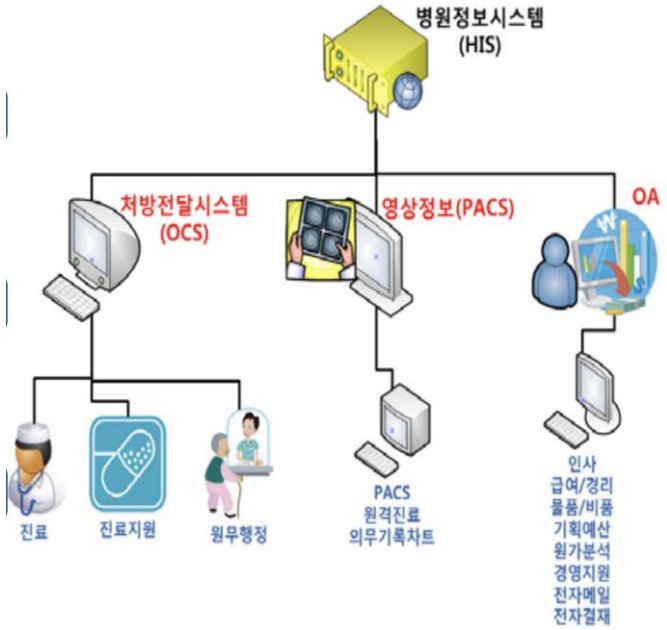
5. Intel SGX를 활용한 HIS 제안

CryptoCraft LAB

1. Hospital Information System

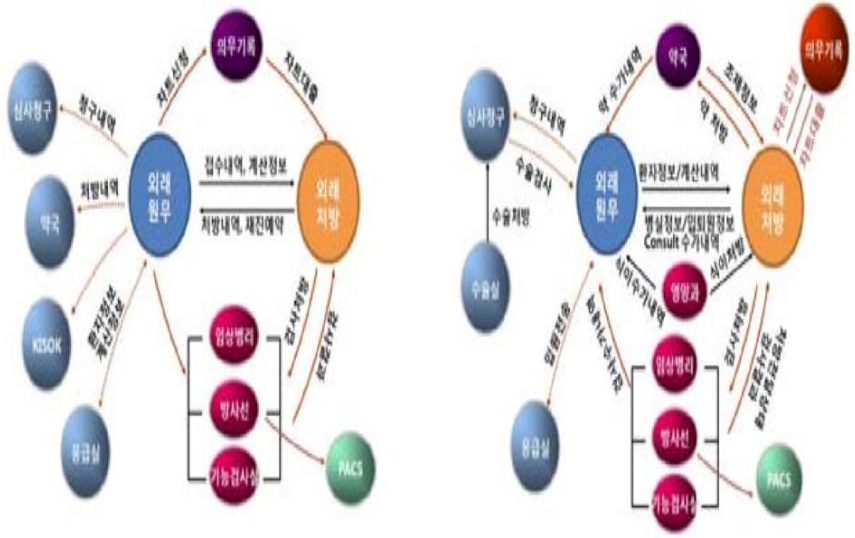
- Hospital Information System (병원 정보 시스템)
  - 의료 기관의 진료, 진료지원, 영상정보, 접수, 수납에 이르는 관리 업무를 전산화한 시스템
  - OSC, PASC, OA 로 구성

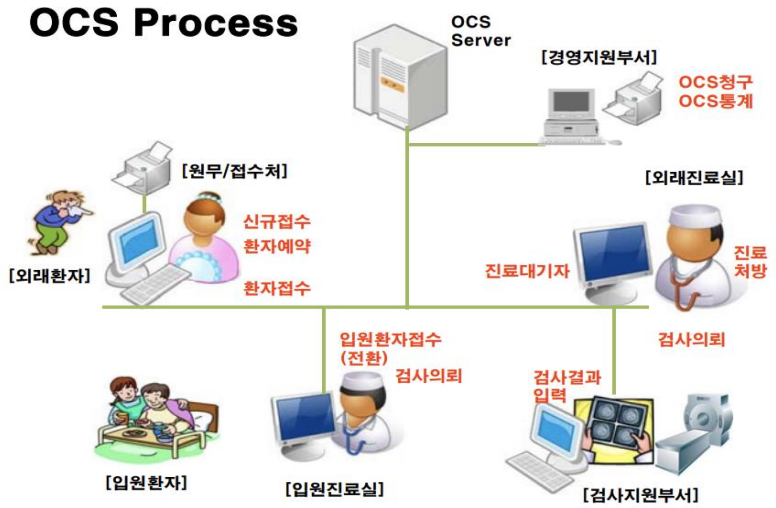




1. Hospital Information System | 처방 전달 시스템(OCS)

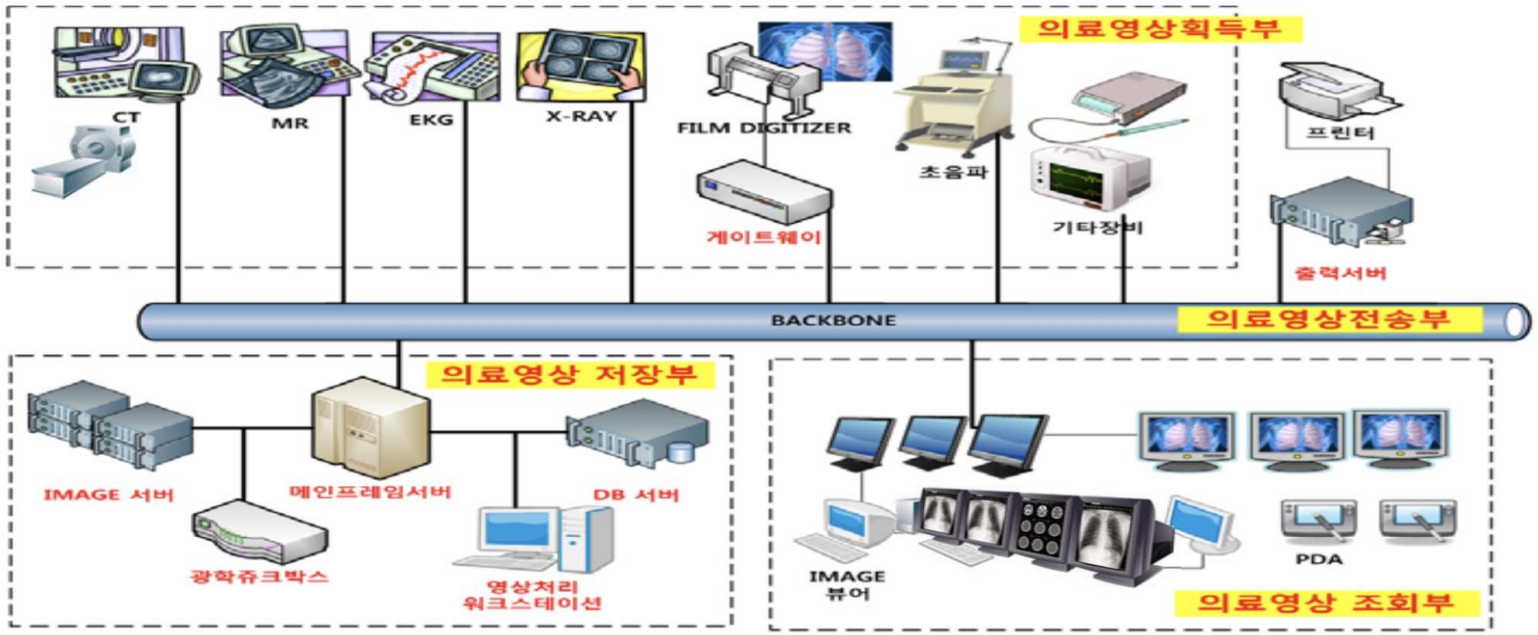
- 처방 전달 시스템 (Order Communicating System)
  - 의사의 처방과 환자의 개인 정보를 인력이나 기계적인 방법에 의존하지 않고 컴퓨터 시스템을 이용하여 신속, 정확하게 각 필요 부서로 전달하는 시스템





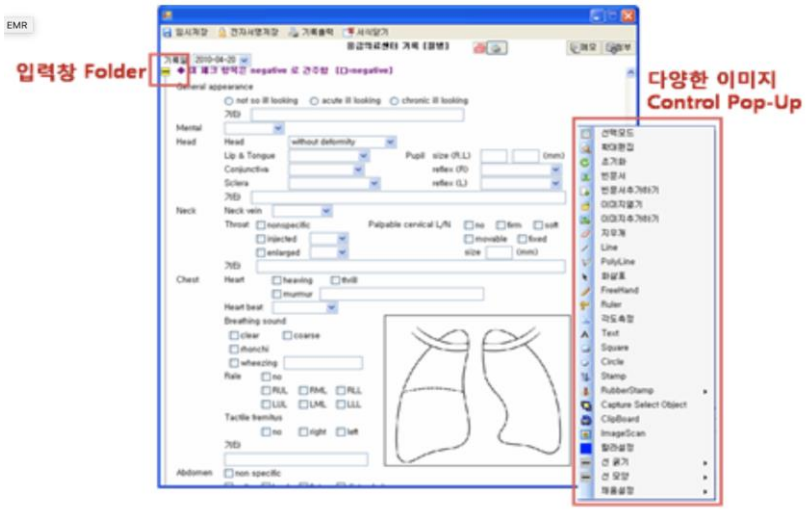
1. Hospital Information System | 의료영상 저장 전송 시스템(PACS)

- 의료영상 저장 전송 시스템 (Picture archiving communication system)
  - 영상 획득 장치를 이용하여 의학 영상을 디지털 데이터로 변환하여 DB 서버에 저장하고 네트워크로 연결된 다양한 단말기로 조회하는 시스템



1. Hospital Information System | 의무 기록 전산화(EMR)

- 의무 기록 전산화 (Electronic Medical Record)
  - 기존에 종이 차트로 사용하던 인적사항, 병력, 건강상태, 진찰, 입퇴원 기록 등의 환자의 모든 정보를 전산화 하여 입력, 관리, 저장하는 형태
  - 기술의 발전으로 개개인에 맞는 맞춤형 의료서비스를 제공하기 위해 필요한 환자 정보



2. HIS의 정보보호 이슈

- 의료 정보는 희소성과 활용성이 높아서 해커들의 표적이 되기 쉬움
  (메일 주소를 이용하여 성형 수술 내역 유포 협박)

정보	가격 (1건당)
의료정보	60달러
주민등록번호	15달러
신용카드정보	3달러

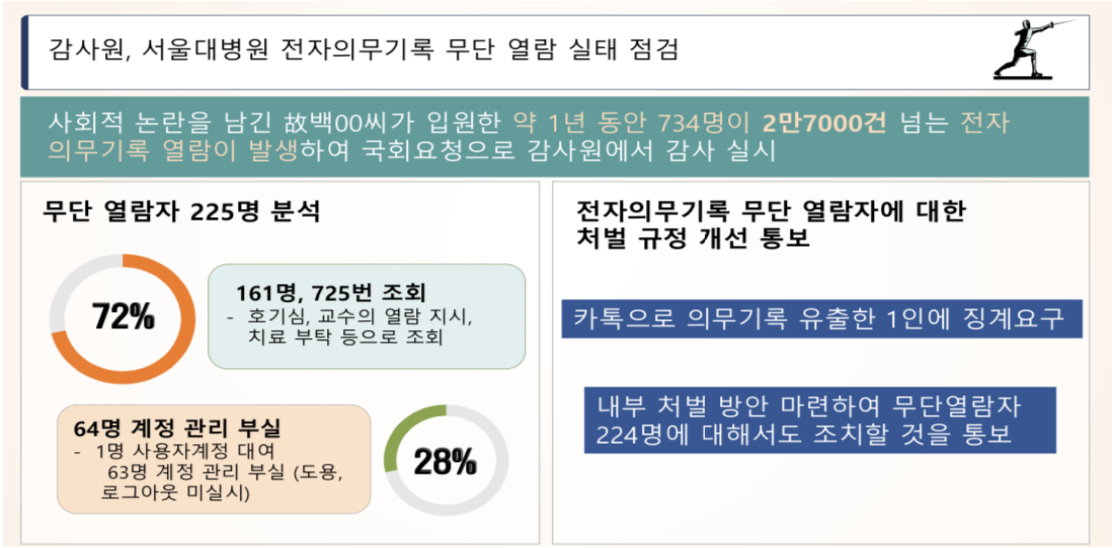
암시장에서 개인정보 거래 가격

- 최근에도 의료 기관 해킹은 꾸준히 발생

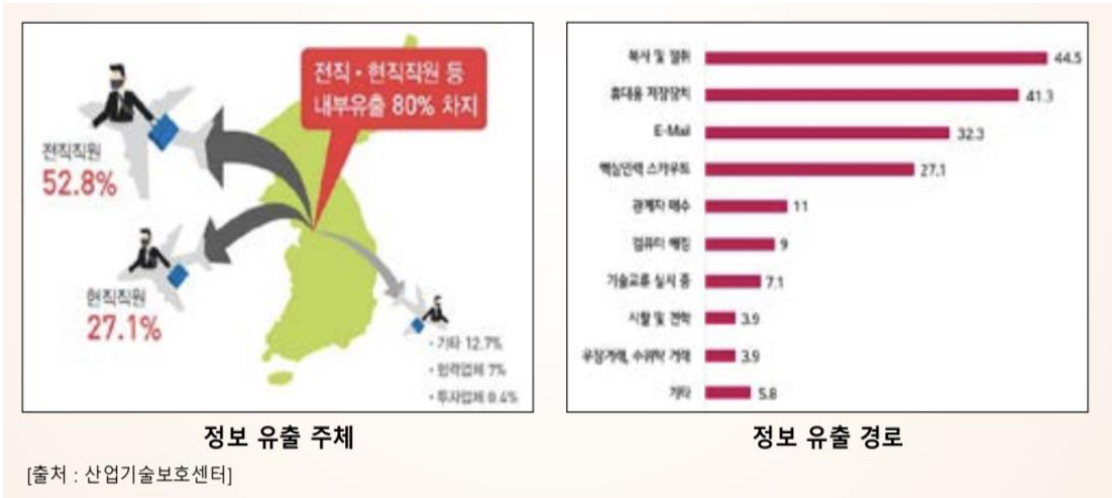
일시	내용
2013.12	약사들이 사용하는 약국경영관리 소프트웨어를 통해 **7억 4000만건에 달하는 처방정보를 IMS헬스업체에 판매**
2015.1	병원 의료정보 소프트웨어 **개발업체가 소프트웨어 업데이트 과정을 이용**하여 파일을 수집할 수 있는 모듈을 삽입, **환자정보 7억건 유출**
2015.8	백신 취약점을 이용하여 대형 대학병원의 **중앙서버 및 관리자 PC가 북한발 해킹에 점령**, 해당 병원은 **해킹 당한 사실도 모르고 8개월째 방치**
2016.8	병원 홈페이지 관리자 페이지가 단순 비밀번호를 사용하는 취약점을 이용해 해킹, **홈페이지 기술적 보호조치를 소홀히 한 병원장 등 8명 불구속**

2. HIS의 정보보호 이슈

- 사회적 논란을 가진 환자에 대한 개인 정보(EMR) 무단 열람 사례



- 대부분 환자 개인 정보 유출은 의료 기관 내의 의료 관리자들에 의해서 발생
  (카톡, 메일, USB)



정보 유출 주체 정보 유출 경로

[출처 : 산업기술보호센터]

3. Trusted Execution Environment (TEE)

- SE, TPM, TXT의 단점을 보완한 보안 플랫폼
- Secure World와 Non-Secure World로 실행 환경 분리
- 격리된 환경을 통한 응용프로그램의 무결성 및 기밀성 제공
  - Intel SGX(Software Guard eXtensions)
  - ARM TrustZone
  - AMD PSP(Platform Security Processor)

4. Intel SGX

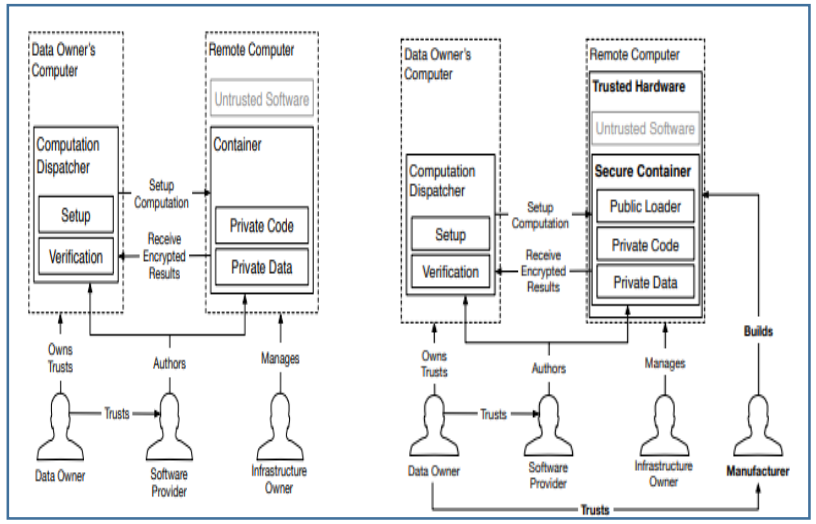
- Intel SGX

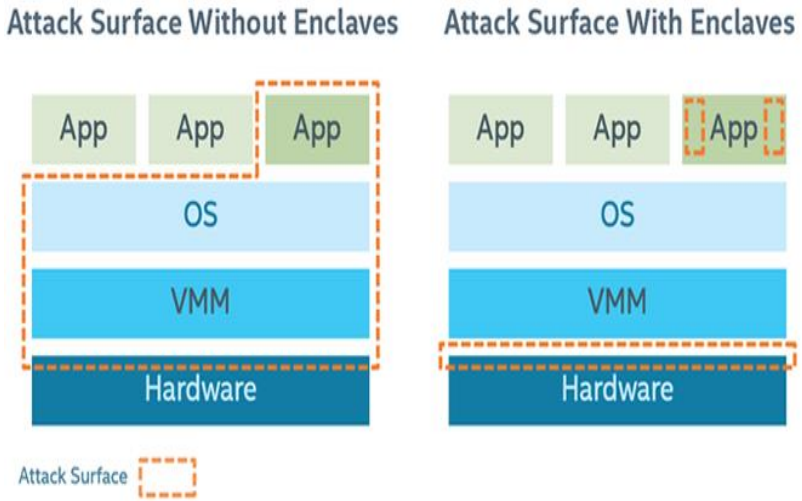
Intel에서 제공하는 CPU 명령어 코드

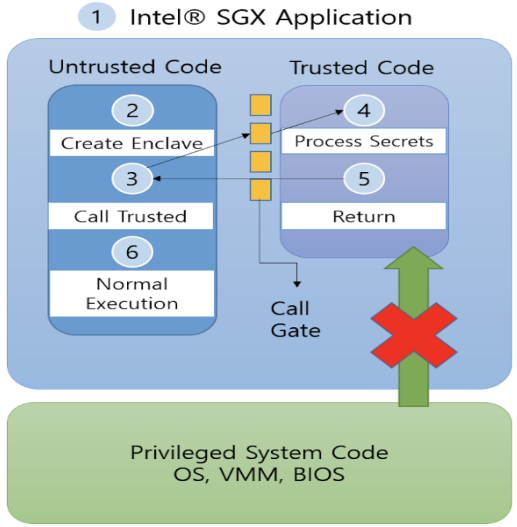
Enclave라는 Secure Container 제공

운영체제, 하이퍼바이저 포함 어떤 수준의 권한으로도 접근이 불가능

Enclave를 사용함으로써 공격 범위를 효과적으로 경감







4. Intel SGX | Security

- MEE(Memory Encryption Engine) 을 이용하여 메모리 암호화
  (물리적 메모리 공격 보호)
- Enclave 실행 후 Disk 저장 파일 암호화 (Sealing)
  (디스크에 저장된 중요 데이터 보호)
- 다양한 종류의 암호화 키 제공
- BIOS, VMM, OS 등의 높은 권한의 System S/W도 접근 불가능
  (System S/W 해킹시에도 저장된 데이터 무결성 및 기밀성 보장)
- jump, function call 등의 분기문으로 Enclave 메모리 접근 불가
  (StackOverflow 같은 비정상적 분기를 이용한 메모리 접근 방어)

4. Intel SGX | Attestation

- Attestation

  Enclave가 정보를 주고 받기 위해 자신을 입증하는 과정

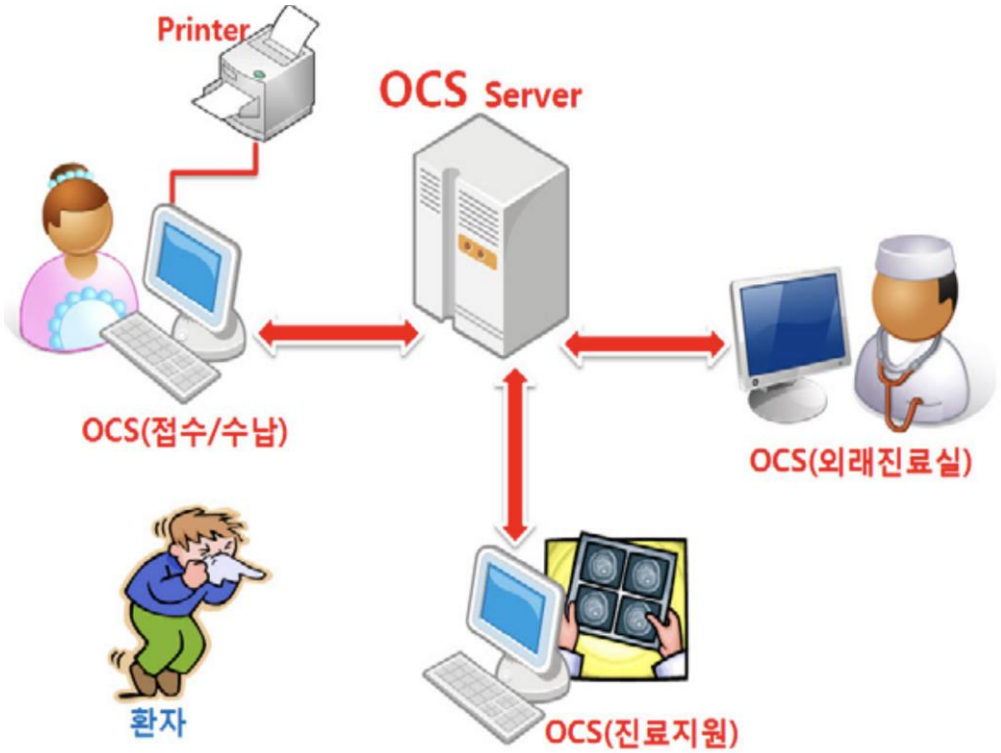
  같은 SGX 지원 CPU에서 호스팅 되는 다른 Enclave와 신뢰 관계 구축

  Local Attestation

  Enclave가 원거리의 다른 제 3자와 서비스 하기 위해 신뢰 관계 구축

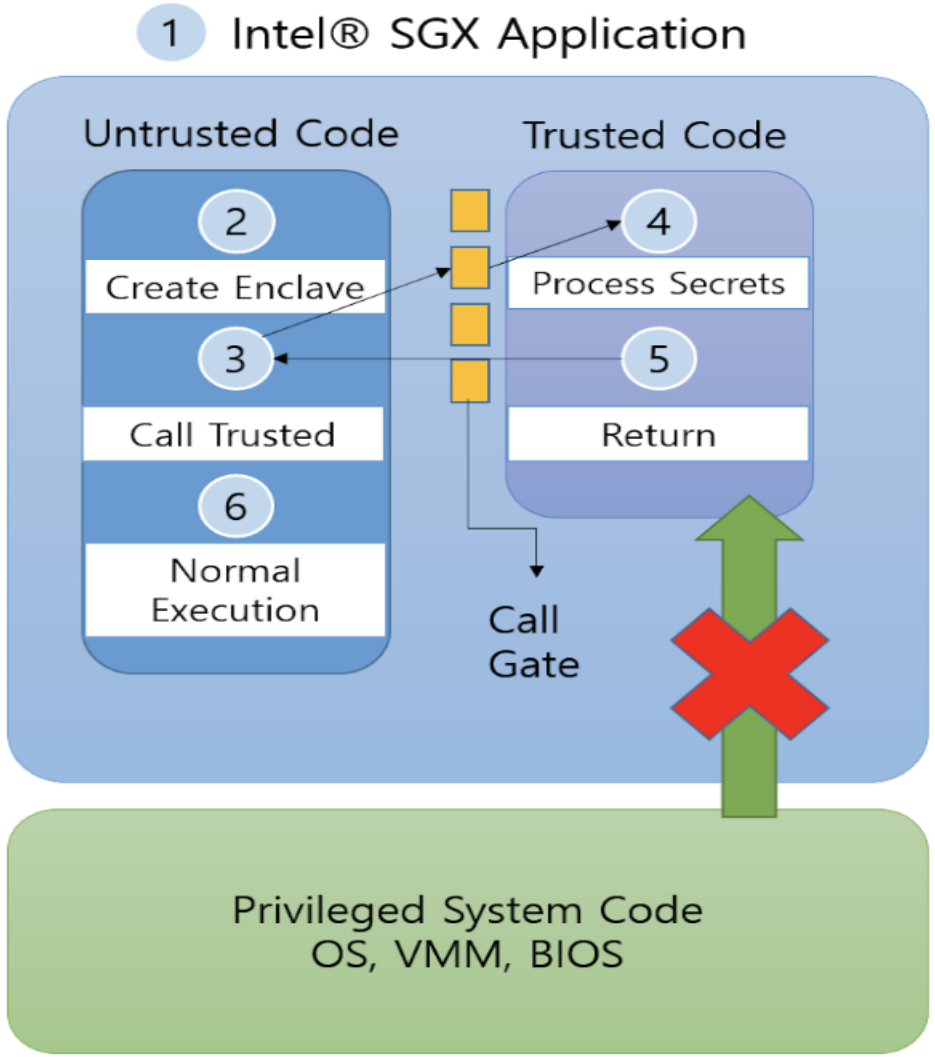
  Remote Attestation

5. Intel SGX를 활용한 HIS 제안



- 환자의 의료 정보가 담긴 파일을 처리 할 때 해커의 공격에 안전한 환경 제공
- HIS에서 사용하는 서버와 각 클라이언트 PC 사이에서 Intel SGX의 Attestation 과정을 추가하여 안전한 정보 전달
- HIS에서 처리 후 환자의 개인 정보 및 의료 정보가 담긴 파일을 Sealing 기능을 이용하여 암호화 후 저장

5. Intel SGX를 활용한 HIS 제안 | 안전한 실행 환경 제공

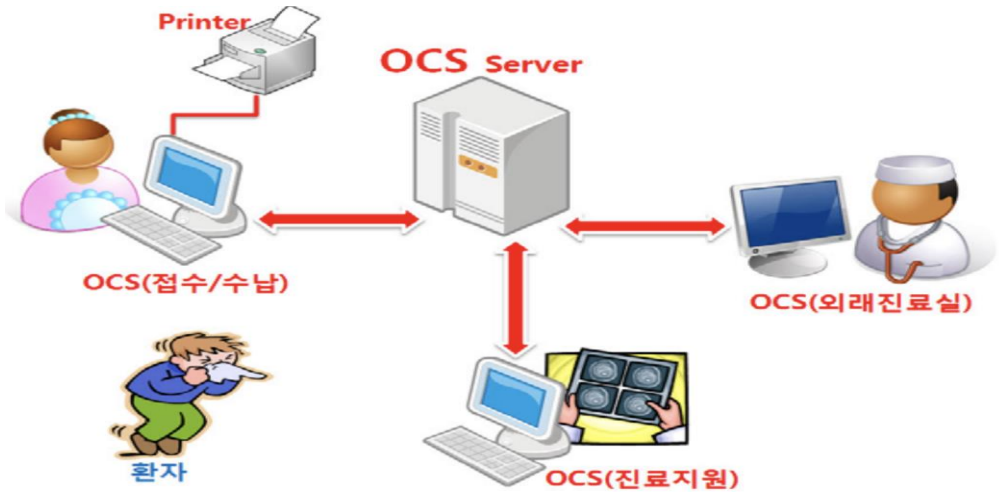


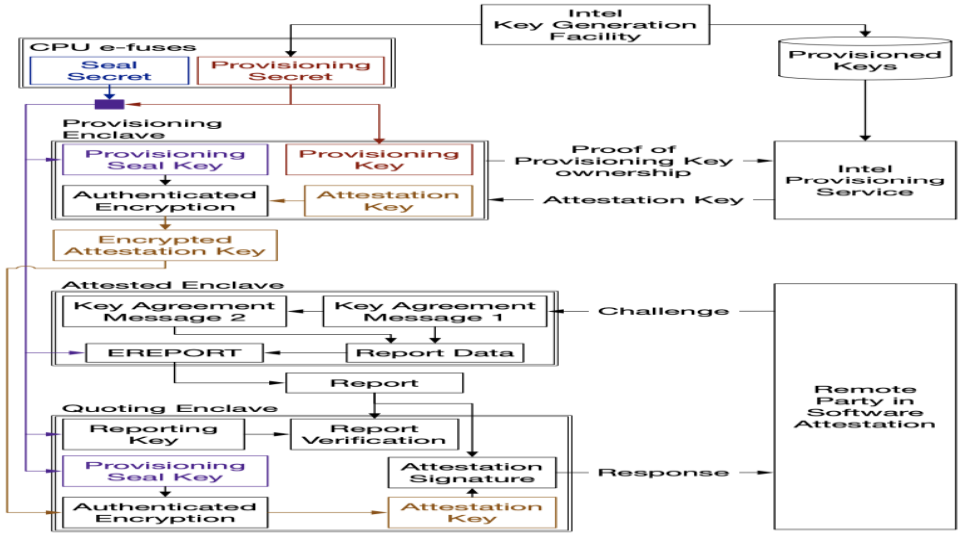
1. 환자의 정보를 출력하거나 값을 업데이트 해야하는 액세스 상황이 발생

2. 환자의 정보를 처리하는 프로세스를 Enclave에서 실행

3. 정보 처리 후 결과물을 Return

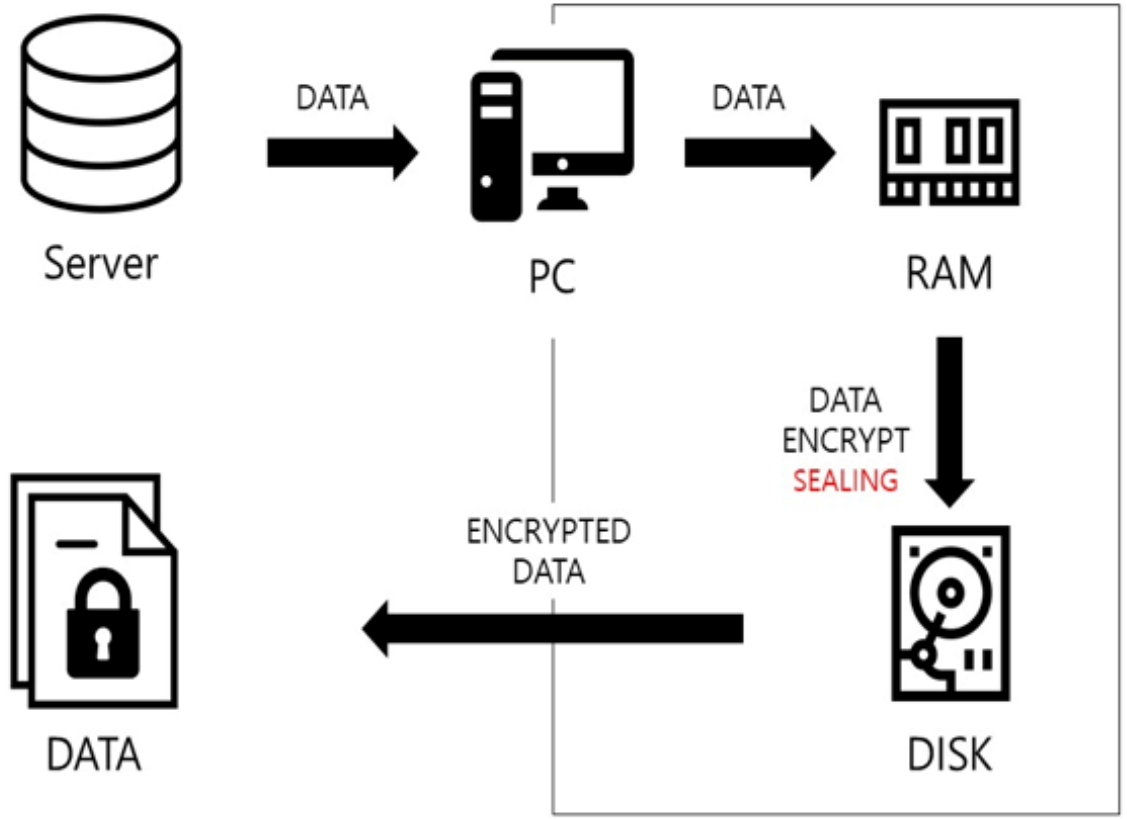
5. Intel SGX를 활용한 HIS 제안 | Attestation





- 병원에서 사용하는 중앙 서버와 각 클라이언트 PC가 통신을 해야하는 상황 발생 (환자 정보 검색, 의료 정보 업데이트)
- Remote Attestation을 이용한 서버와 안전한 통신 채널 구축
- 같은 클라이언트 PC에서 환자 정보를 처리할 때 다른 Enclave가 서로 통신을 해야하는 상황이 발생할 경우 Local Attestation을 통한 안전한 통신 채널 구축

5. Intel SGX를 활용한 HIS 제안 | Sealing



1. 서버에서 환자의 개인 정보를 PC로 받아옴 (Remote Attestation)
2. Enclave를 이용하여 메모리에서 데이터 처리
3. Sealing을 이용하여 Disk에 암호화된 데이터 저장
4. 저장된 데이터가 메신저, 메일, USB로 유출된다 하더라도 무결성과 기밀성을 유지할 수 있음

5. Intel SGX를 활용한 HIS 제안 | 개선 사항

- 기존 병원 정보 시스템에 대한 정확한 이해
- SGX를 사용한 오버헤드 발생
- 최대 256MB Enclave 사용 용량 제한

Q & A