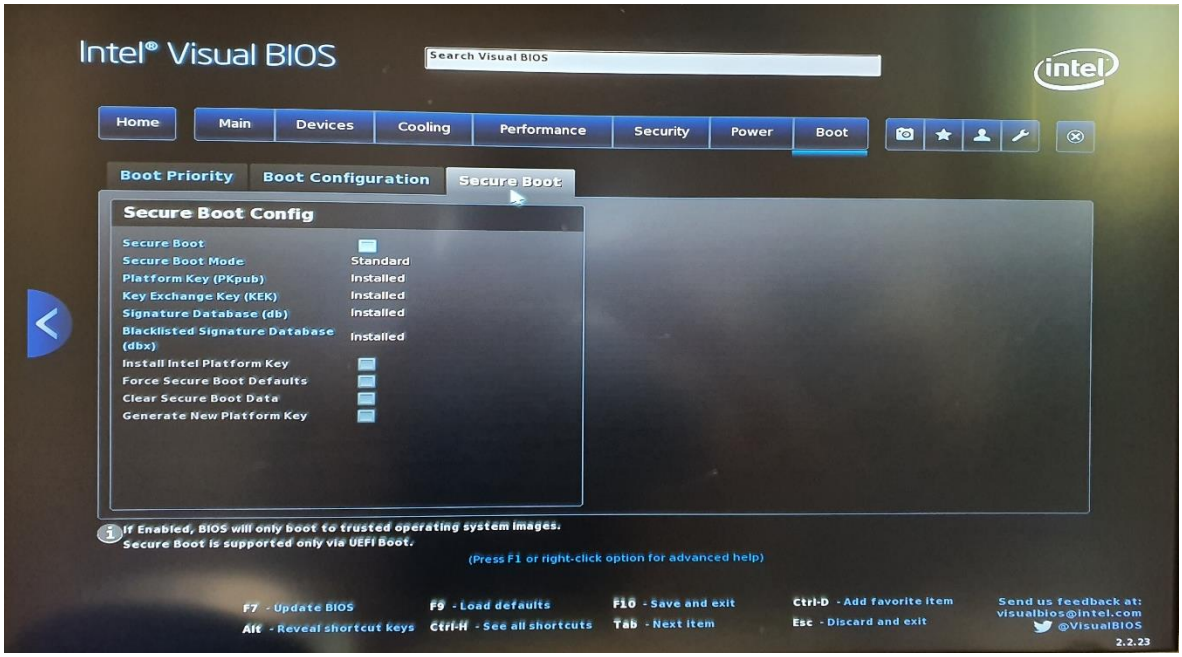
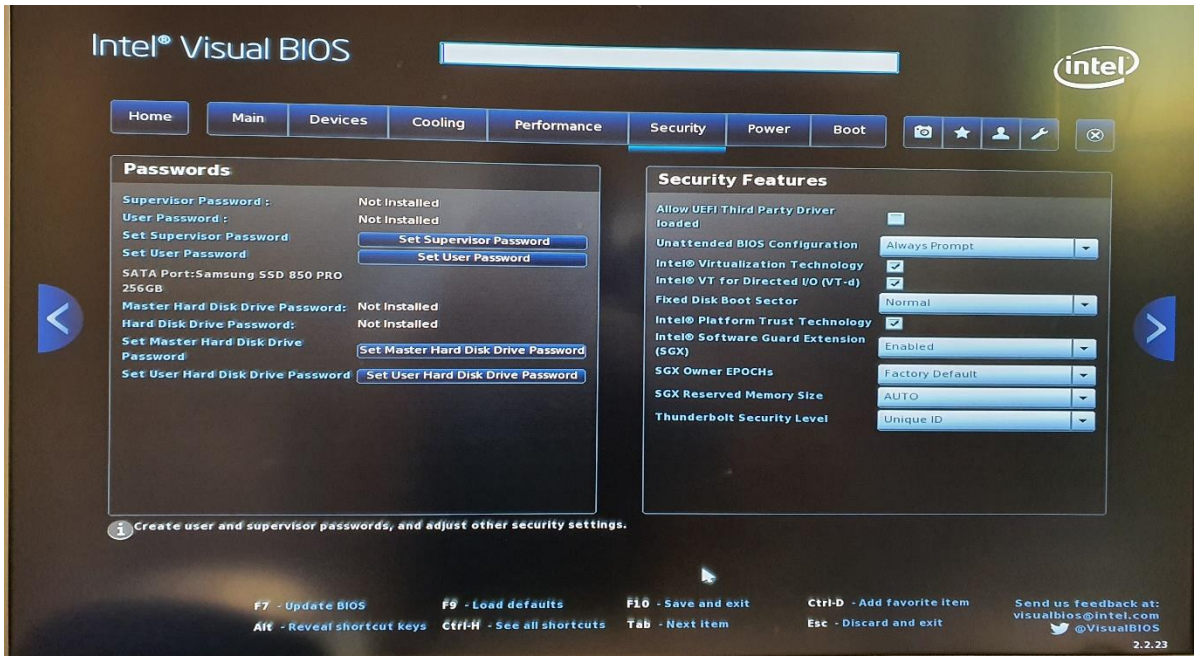
Intel SGX 설치 방법

1. SGX를 설치하기 전에 바이오스 세팅이 선행되어야 한다.

먼저 secure boot를 해제한다.



그리고 SGX를 Enabled로 변경한다.



2. 디렉토리 경로에는 영어만 포함되어야 한다.

3. 디렉토리 설치 순서를 꼭 맞춰서 진행해야 하며, 각 디렉토리의 루트(root) 디렉토리를 지정한대로 따라야한다. 루트 디렉토리가 달라질 경우 에러가 발생할 수 있다.

4. 설치는 우분투 16.04 버전을 기준으로 한다.

5. 인텔에서 깃허브에 올린 코드를 사용할 것이기 때문에 '$ sudo apt-get install git' 을 선행한다.

6. 대략적인 설치 순서는 다음과 같다: linux-sgx-driver -> linux-sgx(SGX SDK) -> dynamic-application-loader-host-interface -> SGX PSW

7. 사용자가 원하는 루트 디렉토리를 지정한다. 본 문서에서는 루트 디렉토리를 홈(home)으로 칭한다. 드라이브 설치를 위해 인텔에서 제공하는 linux-sgx-driver 깃허브 페이지에 접속하면 설치 과정이 나와있다.

```
(home) $ git clone https://github.com/intel/linux-sgx-driver
(home) $ cd linux-sgx-driver
```

8. 설치 된 커널의 헤더 버전과 활성화 된 커널의 버전이 일치해야 한다. 따라서 다음 명령어를 통해 헤더 버전을 맞춰준 다음 코드를 빌드한다.

```
(linux-sgx-driver) $ dpkg-query -s linux-headers-$(uname -r)
(linux-sgx-driver) $ sudo apt-get install linux-headers-$(uname -r)
(linux-sgx-driver) $ sudo apt-get install libelf-dev
(linux-sgx-driver) $ make
```

9. 다음 명령어를 통해 SGX Driver를 설치한다.

```
(linux-sgx-driver) $ sudo mkdir -p "/lib/modules/"`uname -r`"/kernel/drivers/intel/sgx"
(linux-sgx-driver) $ sudo cp isgx.ko "/lib/modules/"`uname -r`"/kernel/drivers/intel/sgx"
(linux-sgx-driver) $ sudo sh -c "cat /etc/modules | grep -Fxq isgx || echo isgx >> /etc/modules"
(linux-sgx-driver) $ sudo /sbin/depmod
(linux-sgx-driver) $ sudo /sbin/modprobe isgx
```

10. SGX Driver의 설치가 완료 되었다면 SGX Driver와 SGX(SDK, PSW)의 상위 디렉토리를 맞춰주기 위해 SGX Driver의 상위 디렉토리인 홈으로 이동한다.

(linux-sgx-driver) $ cd ..

(home) $ git clone https://github.com/intel/linux-sgx

(home) $ cd linux-sgx

11. SDK 설치 요구 도구들을 빌드한다.

(linux-sgx) $ sudo apt-get install build-essential ocaml automake autoconf libtool wget python libssl-dev

12. PSW 설치 요구 도구들을 빌드한다.

(linux-sgx) $ sudo apt-get install libssl-dev libcurl4-openssl-dev protobuf-compiler libprotobuf-dev debhelper

13. 소스코드 패키지를 다운 받는다.

(linux-sgx) $ ./download_prebuilt.sh

14. SDK, PSW 빌드한다.

(linux-sgx) $ apt-get install cmake

(linux-sgx) $ make

15. SDK Installer 빌드한다.

(linux-sgx) $ make sdk_install_pkg

16. PSW Installer 빌드한다.

(linux-sgx) $ make deb_sgx_enclave_common_pkg

17. linux/installerdeb/libsgx_enclave-common에 바이너리 코드가 생성된 것을 확인한다. 확인이 되었다면 SDK, PSW의 빌드가 끝났으며, 설치를 해야한다.

(linux-sgx) $ sudo apt-get install build-essential python

(linux-sgx) $ cd linux/installer/bin

(bin) $ ./sgx_linux_x64_sdk_${version}.bin

18. source를 통해 환경변수 추가한다.

(bin) $ source ${sgx-sdk-install-path}/environment

19. PSW 설치한다. 필요 라이브러리를 가져온다.

(linux-sgx) $ sudo apt-get install libssl-dev libcurl4-openssl-dev libprotobuf-dev

20. PSW를 정상적으로 작동하기 위해선 'iclsClient'라는 파일이 필요하다. 기존에는 다운로드가 가능하였지만 현재는 불가능하다. 따라서 해당 파일을 연구실 github에서 다운로드 가능하다.
https://github.com/solowal/DEVELOP/blob/master/SGX/iclsClient-1.45.449.12-1.x86_64.rpm

21. 아래 명령어를 통해 iclsClient를 설치한다.

(linux-sgx) $ sudo apt-get install alien

(linux-sgx) $ sudo alien --scripts iclsClient-1.45.449.12-1.x86_64.rpm

(linux-sgx) $ sudo dpkg -i iclsclient_1.45.449.12-2_amd64.deb

22. dynamic-apllication-loader-host-interface를 깃허브에서 클론한다.

(linux-sgx) $ git clone https://github.com/intel/dynamic-application-loader-host-interface

23. 아래 명령어를 통해 JHI를 설치한다.

(linux-sgx) $ cd dynamic-application-loader-host-interface

(dynamic-application-loader-host-interface) $ sudo apt-get install uuid-dev libxml2-dev cmake pkg-config

(dynamic-application-loader-host-interface) $ sudo apt-get install libsystemd-dev

(dynamic-application-loader-host-interface) $ cmake .;make;sudo make install;sudo systemctl enable jhi

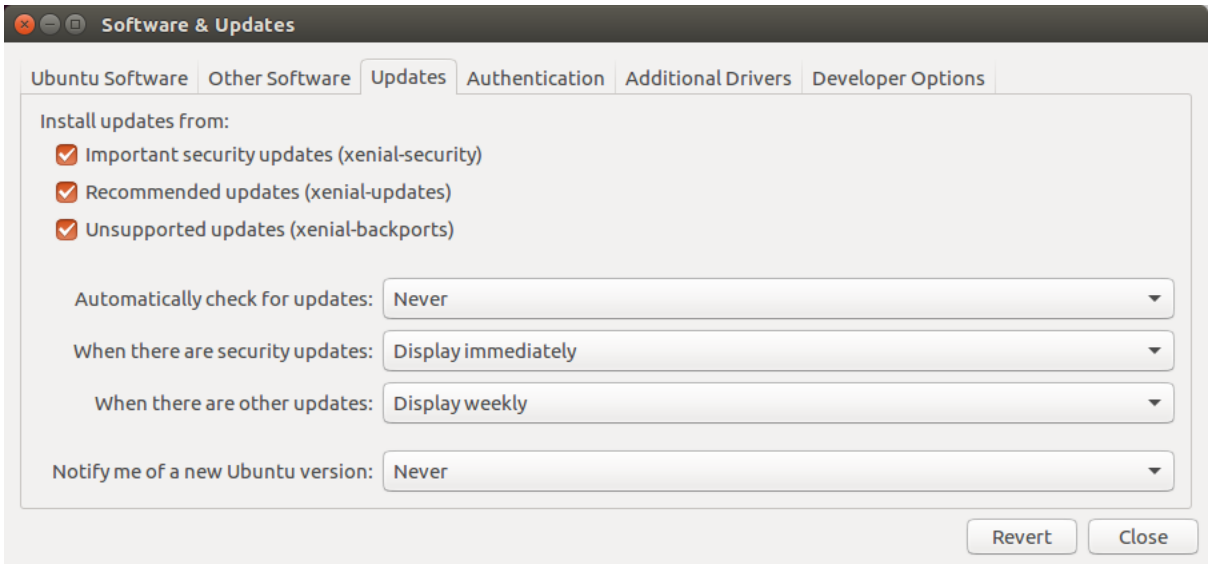
(dynamic-application-loader-host-interface) $ cd ..

24. PSW 설치하기.

(linux-sgx) $ cd linux/installer/deb/libsgx-enclave-common

(libsgx-enclave-common) $ sudo dpkg -i ./libsgx-enclave-common_${version}-${revision}_amd64.deb

25. 자동 소프트웨어 업데이트 중단 시키기.



26. 예제 코드 실행하기.

(linux-sgx) $ cd linux/installer/bin/sgxsdk/SampleCode/LocalAttestation/

27. 인텔 제공하는 샘플코드에서 SGX 하드웨어를 사용하여 컴파일 및 실행한다.

(LocalAttestation) $ make

(LocalAttestation) $ ./app