Getting Started with OpenEnclave

Introduction

This document provides a step-by-step tutorial to begin using the OpenEnclave SDK. It explains how to obtain, build, and install the SDK. It also describes how to develop and build a few simple enclave applications.

Licenses

Microsoft plans to release the OpenEnclave SDK under the MIT license, included here in the source distribution.

https://github.com/Microsoft/openenclave/blob/master/LICENSE

OpenEnclave builds on various third-party packages. It modifies and redistributes libunwind and in addition downloads other third-party packages on-the-fly during the build process. Licensing details for all third-party packages shown in the table below.

Package	License
dlmalloc	https://github.com/Microsoft/openenclave/blob/master/3rdparty/dlmalloc/LICENSE
libcxx	https://github.com/Microsoft/openenclave/blob/master/3rdparty/libcxx/LICENSE
libcxxrt	https://github.com/Microsoft/openenclave/blob/master/3rdparty/libcxxrt/LICENSE
libunwind	https://github.com/Microsoft/openenclave/blob/master/3rdparty/libunwind/LICENSE
mbedtls	https://github.com/Microsoft/openenclave/blob/master/3rdparty/mbedtls/mbedtls/LICENSE
musl libc	https://github.com/Microsoft/openenclave/blob/master/3rdparty/musl/COPYRIGHT

Obtaining the source distribution

OpenEnclave is available from GitHub. Use the following command to download the source distribution.

```
# git clone https://github.com/Microsoft/openenclave
```

This creates a source tree under the directory called openenclave.

Quick Start

If you wish to skip ahead to the section on developing a simple enclave, you can follow the instructions below to set up a working environment. If you want more details on prerequisites, building or installing, refer to the subsequent sections that discussing each topic individually.

Prerequisites

Execute the following commands from the root of the source tree to install the prerequisites (required packages, the SGX driver, and the SGX AESM service).

```
$ sudo ./scripts/install-prereqs
$ sudo make -C prereqs
$ sudo make -C prereqs install
```

The second and third commands are only necessary if you wish to install the Intel(R) SGX driver and the Intel(R) AESM service. OpenEnclave can be used in simulation mode without these components.

Building

Build is generally out-of-tree (in-tree is possible, though not recommended). To build, pick a directory to build under ("*build/*" below). Then use cmake to configure the build and generate the out-of-tree make files and build.

```
$ mkdir build/
$ cd build/
build$ cmake ..
build$ make
```

Installing

As of now, there is no real need to install the SDK system-wide, so you might use a tree in your home directory:

```
build$ cmake -DCMAKE_INSTALL_PREFIX:PATH=~/openenclave ..
build$ make install
```

Prerequisites

The following are prerequisites for building and running OpenEnclave.

- Intel® X86-64bit architecture with SGX1 or SGX2
- Ubuntu Desktop-16.04-LTS 64bits
- Various packages: build-essential, ocaml, automake, autoconf, libtool, wget, python, libssl-dev, libcurl4-openssl-dev, protobuf-compiler, libprotobuf-dev, build-essential, python, libssl-dev, libcurl4-openssl-dev, libprotobuf-dev, uuid-dev, libxml2-dev, cmake, pkg-config
- Intel® SGX Driver (/dev/isgx)
- Intel® SGX AESM Service (from the Intel® SGX SDK)

Once Linux and the various packages are installed, it is necessary to install the SGX driver and the SGX AESM service. These can be obtained from the following GitHub repositories.

- https://github.com/01org/linux-sgx-driver
- https://github.com/01org/linux-sgx

Both contain detailed instructions about building and installing these pieces. As a convenience, OpenEnclave provides a script for downloading, building and installing both the driver and the AESM service. From the root of the OpenEnclave source tree, type the following command:

```
$ sudo make -C prereqs
$ sudo make -C prereqs install
```

After this completes, verify that the AESM service is running as follows.

```
$ service aesmd status
```

Look for the string “active (running)”, usually highlighted in green.

Building

Build is generally out-of-tree (in-tree is possible, though not recommended). To build, pick a directory to build under ("*build/*" below).

```
$ mkdir build/
```

```
$ cd build/
```

Configure with

```
build$ cmake ..
```

In addition to the standard CMake variables, the following CMake variables control the behavior of the Linux make generator for OpenEnclave:

Variable	Description
CMAKE_BUILD_TYPE	Build configuration (*Debug*, *Release*, *RelWithDebInfo*). Default is *Debug*.
ENABLE_LIBC_TESTS	Enable Libc tests. Default is enabled, disable with setting to "Off", "No", "0", ...
ENABLE_LIBCXX_TESTS	Enable Libc++ tests. Default is disabled, enable with setting to "On", "1", ...
ENABLE_REFMAN	Enable building of reference manual. Requires Doxygen to be installed. Default is enabled, disable with setting to "Off", "No", "0", ...

E.g., to generate an optimized release-build with debug info, use

```
build$ cmake .. -DCMAKE_BUILD_TYPE=relwithdebinfo
```

Multiple variables can be defined at the call with multiple "-D*Var*=*Value*" arguments.

Once configured, build with

```
build$ make
```

This builds the entire OpenEnclave SDK, creating the following files.

Filename	Description
output/bin/oegen	Utility for generating ECALL and OCALL stubs from IDL
output/bin/oesign	Utility for signing enclaves
output/lib/enclave/liboeenclave.a	Core library for building enclave applications
output/lib/enclave/liboelibc.a	C runtime library for enclave
output/lib/enclave/liboelibcxx.a	C++ runtime library for enclave
output/lib/host/liboehost.a	Library for building host applications
output/share/doc/openenclave/	HTML API reference for OpenEnclave

If things break, set the **VERBOSE** make variable to print all invoked commands.

```
build$ make VERBOSE=1
```

Building from within a subtree of the build-tree builds all dependencies for that directory as well. "**make clean**" is handy before a spot-rebuild in verbose mode.

A successful build only outputs the HTML API reference into the build-tree. To update the refman *.md-files in the source-tree, use

```
build$ make refman-source
```

Testing

After everything has been built, execute the tests via **ctest** (see "**man ctest**" for details).

```
build$ ctest
```

To run the tests in simulation mode, use

```
build$ OE_SIMULATION=1 ctest
```

If things fail, "**ctest -V**" provides test details. Executing ctest from a sub-dir executes the tests underneath.

libcxx tests are omitted by default due to their huge cost on building (30mins+). Enable by setting the cmake variable **ENABLE_LIBCXX_TESTS** before building.

```
build$ cmake -DENABLE_LIBCXX_TESTS=ON ..
build$ make
```

If you are in a hurry and just need a quick confirmation, disable the libc tests with the **ENABLE_LIBC_TESTS** cmake variable like so:

```
build$ cmake -DENABLE_LIBC_TESTS=OFF ..
[...]
```

To run valgrind-tests, add "**-D ExperimentalMemCheck**" to the ctest call. Enclave tests all seem to fail today, though this succeeds:

```
build$ ctest -D ExperimentalMemCheck -R oeelf
```

Installing

This chapter describes how to locally install the SDK from the compiled OpenEnclave tree. To create a redistributable binary package (such as a .deb package), see the next chapter.

Specify the install-prefix to the cmake call. As of now, there is no real need to install the SDK system-wide, so you might use a tree in your home directory:

```
build$ cmake -DCMAKE_INSTALL_PREFIX:PATH=~/openenclave ..
build$ make install
```

If you want the SDK tools to be available to all users and headers/libs available from a system default location, you may opt to install system-wide. This naturally requires root privileges. Note that there is no uninstall script (we target an rpm/deb-based SDK install in the future), hence we recommend overwriting the default (/usr/local/) with a singular tree.

```
build$ cmake -DCMAKE_INSTALL_PREFIX:PATH=/opt/openenclave ..
build$ sudo make install
```

On Linux, there is also the **DESTDIR** mechanism, prepending the install prefix with the given path:

```
build$ make install DESTDIR=foo
```

The following table shows where key components are installed.

Path	Description
<install_prefix>/bin	Programs
<install_prefix>/include/openenclave	Includes
<install_prefix>/lib/openenclave/enclave	Enclave libraries
<install_prefix>/lib/openenclave/host	Host libraries

<install_prefix>/lib/openenclave/debugger	Debugger libraries
<install_prefix>/share/doc/openenclave	Documentation
<install_prefix>/share/openenclave	Samples and make/cmake-includes

For *Makefile* based projects, you may use the make-include in **<install_prefix>/share/openenclave/config.mak** in your own project for sourcing variables containing version info and SDK install paths.

For *CMake* based projets, you may use the cmake-include in **<install_prefix>/share/openenclave/openenclave.cmake** in your own project. It provides the following taregets (e.g., for inclusion in **target_link_libraries**) to set the required compiler flags, include dirs, and libraries.

Target	Description
oeenclave	Enclave code: OpenEnclave intrinsic functions. Must be present in all enclave code.
oelibc	Enclave code: OpenEnclave C library. Includes oeenclave.
oelibcxx	Enclave code: OpenEnclave C++ library. Includes oelibc.
oeidl	Enclave code: Misc helpers required with IDL-compiled code. Includes oelibc.
oehost	Host code: OpenEnclave intrinsic functions.
oehostapp	Host code: Must be present with host binary for proper linker flags.
oesign	Build: shorthand for the signing tool executable.
oegen	Build: shorthand for the IDL compiler executable.

Create Redistributable SDK pacakge

To create a redistributable package (deb, rpm, ...), use **cpack**. Specify the final installation prefix to cmake using the CMAKE_INSTALL_PREFIX variable as above. E.g., to create a debian package that will install the SDK to /opt/openenclave, use:

```
build$ cmake -DCMAKE_INSTALL_PREFIX:PATH=/opt/openenclave ..
build$ cpack -G DEB
```

Samples

Find the samples under **share/openenclave/samples/** of the installation.

Change to the new samples directory and build and run the samples.

```
$ cd ~/openenclave/share/openenclave/samples
$ sh test-samples.sh
```

If these samples run without an error, then OpenEnclave is installed and working correctly.

Developing a simple enclave (echo)

This chapter shows how to develop a simple enclave called echo. The next chapter explains how to use this enclave in a host application. This example is included in the installed samples directory (see <install_prefix>/openenclave/share/openenclave/samples/cmake/hello/).

The ECALL

The echo enclave implements a single ECALL named EnclaveEcho(), which is called by the host (in the next chapter). This function has the following signature.

```
OE_ECALL void EnclaveEcho(void* args);
```

The args parameter can be whatever the host and the enclave agree on. In this case args is a pointer to a zero-terminated string in host memory. The OE_ECALL macro exports the function and injects it into a special section (.ecall) in the ELF image. When the host loads the enclave, it builds a table of all ECALLs exported by the enclave.

The Echo enclave Listing

Here's the full listing for the echo enclave (enc/enc.c):

```
#include <openenclave/enclave.h>

OE_ECALL void EnclaveEcho(void* args)
{
    OE_CallHost("HostEcho", args);
}
```

Notice EnclaveEcho() performs an OCALL, calling the host's HostEcho() function with the same arguments.

Enclave build collateral

The samples provides cmake helper includes under samples/cmake/cmake/ simplifying OpenEnclave application writing. **add_enclave_executable.cmake** provides the **add_enclave_executable()** function. It extends CMake's **add_executable()** by adding the intrinsic target (oeenclave) and also signing the enclave. For the echo sample, this ***CMakeLists.txt*** suffices:

```
include(add_enclave_executable)
add_enclave_executable(samples-echoenc echo.conf private.pem
    enc.c
    )
```

The **echo.conf** argument is the name of a configuration file that defines enclave settings, such as stack size, heap size, and the maximum number of threads (TCSs). Here is the echo sample:

```
# echo.conf
Debug=1
NumHeapPages=1024
NumStackPages=1024
NumTCS=2
```

The **private.pem** argument is a private RSA key used to sign the enclave, here included with the sample. To generate a self-signed private key yourself, use OpenSSL as follows.

```
# openssl genrsa -out private.pem -3 3072
```

Then the public key can be generated from this key as follows.

```
# openssl rsa -in private.pem -pubout -out public.pem
```

Developing a simple host (echohost)

Next, we develop a host to run the echoenc.signed.so enclave that we developed in the previous chapter. The listing from samples/cmake/echo/host follows.

```
#include <openenclave/host.h>
#include <stdio.h>

OE_OCALL void HostEcho(void* args)
{
```

```
    if (args)
    {
        const char* str = (const char*)args;
        printf("%s\n", str);
    }
}

int main(int argc, const char* argv[])
{
    OE_Result result;
    OE_Enclave* enclave = NULL;

    if (argc != 2)
    {
        fprintf(stderr, "Usage: %s ENCLAVE_PATH\n", argv[0]);
        return 1;
    }

    result = OE_CreateEnclave(argv[1], OE_FLAG_DEBUG, &enclave);
    if (result != OE_OK)
    {
        fprintf(stderr, "%s: OE_CreateEnclave(): %u\n", argv[0], result);
        return 1;
    }

    result = OE_CallEnclave(enclave, "EnclaveEcho", "Hello");
    if (result != OE_OK)
    {
        fprintf(stderr, "%s: OE_CallEnclave(): %u\n", argv[0], result);
        return 1;
    }

    OE_TerminateEnclave(enclave);

    return 0;
}
```

This host performs the following tasks:

- Defines an OCALL: HostEcho()
- Instantiates an enclave: OE_CreateEnclave()
- Calls into the enclave: OE_CallEnclave()
- Terminates the enclave: OE_TerminateEnclave()

Host build collateral

The ***CMakeLists.txt*** is rather straight-forward, though note the **oehostapp** link target in the add_executable() call:

```
add_executable(samples-echohost host.c)
target_link_libraries(samples-echohost oehostapp)
```

The additional target instructs CMake to provide the open enclave includes and host libraries (via oehost), as well as the proper linker flags for the host OCall targets to be resolved.

Completing the echo sample

In the project file **samples/cmake/CMakeLists.txt**, note the line:

```
include(${OE_PREFIX}/share/openenclave/openenclave.cmake)
```

This sources the CMake include providing the OpenEnclave targets.

Build the samples, e.g. in a subdirectory under samples/cmake:

```
samples/cmake$ mkdir build && cd build
samples/cmake/build$ cmake .. -DOE_PREFIX=../../../.. && make
```

After building, we are ready to run the samples:

```
samples/cmake/build$ ctest
```

Other build systems

If you are not using CMake for your project, the Makefile samples under ***samples/make/*** provide guidance on the necessary includes, libraries, and flag definitions.

Specifically, the OpenEnclave includes for the intrinsics are located under /include/openenclave (or via the **OE_INCLUDEDIR** make variable when using the make include installed under /share/openenclave/config.mak).

Necessary gcc compiler flags for enclave code are:

```
CFLAGS=-nostdinc -fPIC
```

Necessary gcc linker flags for an enclave are:

```
LDFLAGS=\
    -nostdlib \
    -nodefaultlibs \
    -nostartfiles \
    -Wl,--no-undefined \
    -Wl,-Bstatic \
    -Wl,-Bsymbolic \
    -Wl,--export-dynamic \
    -Wl,-pie \
    -Wl,-eOE_Main
```

The -eOE_Main option requires some explanation (see the ld man page about other options). This option specifies the name of the entry point for the enclave. The linker stores the virtual address of the OE_Main() function in the ELF header (Elf64_Ehdr.e_entry) of the resulting binary. When the enclave is instantiated by the host, this entry point is copied to each TCS (Thread Control Structure) in the image. When the host invokes the SGX EENTER instruction on a TCS, the hardware fetches the entry point from the TCS and jumps to that address and the OE_Main() function begins to execute.

The necessary enclave library contains the enclave intrinsics, including the OE_Main() entry point. Note that the echo sample uses neither a C nor C++ runtime library. Other samples will show how these are used.

```
LIBRARIES = -L${OE_LIBDIR}/openenclave/enclave -loeenclave
```

To sign the enclave, use the **oesign** tool. This tool takes the following parameters.

```
$ oesign

Usage: oesign ENCLAVE CONFFILE KEYFILE
```

The CONFFILE argument is the name of a configuration file that defines enclave settings, and the KEYFILE argument is a private RSA key used to sign the enclave. See the CMake section for details on these files.

Debugging the enclave

We can't use GDB directly to debug enclave application since it doesn't understand enclave yet. OpenEnclave includes a GDB plugin to help developers to debug enclaves that is developed using this SDK.

Note: the enclave must be created with debug opt-in flag, otherwise debugger can't work since it can't read the enclave memory. The default sample enclave is created with debug flag, refer to:

```
result = OE_CreateEnclave(argv[1], OE_FLAG_DEBUG, &enclave);
```

This flag (OE_FLAG_DEBUG) should only be set in development phase. It must be clear out for production enclave.

The debugger is installed at <install_prefix>/bin/oe-gdb. The usage is same with GDB, for example: the following command will launch the simple enclave application under debugger:

```
# /opt/openenclave/bin/oe-gdb -arg ./host/echohost ./enc/echoenc.signed.so
```

After the enclave application is loaded, you can use b to set breakpoint, bt to check stack etc.