Enclave Memory Measurement Tool for Intel® Software Guard Extensions (Intel® SGX) Enclaves

Scope

This paper describes how to use the Enclave Memory Measurement Tool (EMTT) to help tune the memory footprint of Intel® Software Guard Extensions (Intel® SGX) enclaves. Both Microsoft* Windows* and the Linux* operating systems are covered. The paper assumes an understanding of Intel SGX. General information on Intel SGX can be found on the Intel SGX portal at: https://software.intel.com/sgx.

Enclave Memory Measurement Tool (EMMT)

The Intel SGX SDK provides the EMMT tool to help tune the memory footprint of enclaves. Developers can use the tool to measure peak stack and heap usage for a given enclave, then adjust those memory sizes on subsequent builds for more efficient enclave memory use.

For Intel SGX enabled applications targeting Microsoft Windows, an Intel SGX application's enclave memory is limited in size. During system boot-up, a total of 128 MB is typically reserved for Intel SGX, and 96 MB of that is allocated to the Enclave Page Cache (EPC). The EPC is shared among all running enclaves on the system.

Since Linux supports paging, for Intel SGX enabled applications targeting Linux, the application's enclave memory size is not limited to 128 MB, although it's still a good idea (for performance reasons) that your enclave fit into the 128MB EPC.

> **Note:** The more EPC space your enclave uses, the less space there is for other enclaves. Enclaves should follow a "good neighbor" policy of always using the least amount of EPC space possible.

For enclaves, the maximum enclave stack and heap sizes are allocated at application load time based on values specified when the application is built. These sizes are specified in an XML source file called the Enclave Configuration File (ECF). Actual enclave memory-utilization levels, however, can differ from defaults/expectations based on the implementation and functionality of a given enclave.

If the heap and stack sizes allocated at build time are more than actually used at run time, use of EPC memory is inefficient. To improve the efficiency of enclave memory use, developers can use the EMMT to see actual peak stack and heap usage information for their enclaves. Then they can update their enclave's ECF to specify a smaller maximum stack and/or maximum heap size. Figure 1 shows the format of the default ECF, with the stack and heap size parameters highlighted in red.

```
<EnclaveConfiguration>
      <ProdID>100</ProdID>
      <ISVSVN>1</ISVSVN>
      <StackMaxSize>0x50000</StackMaxSize>
      <HeapMaxSize>0x100000</HeapMaxSize>
      <TCSNum>1</TCSNum>
      <TCSPolicy>1</TCSPolicy>
     <DisableDebug>0</DisableDebug>
     <MiscSelect>0</MiscSelect>
     <MiscMask>0xFFFFFFFF</MiscMask>
</EnclaveConfiguration>
```

Figure 1. Example ECF highlighting maximum stack size and heap size definitions

EMMT usage

The CLI program name for the EMMT is **sgx_emmt**, for both Microsoft Windows and Linux. **sgx_emmt** measures only the peak stack usage and peak heap usage for an enclave, as these are the only memory areas that can be tuned. (Code, global data, number of trusted threads, etc., are fixed.)

To measure the memory usage of an enclave, use the **sgx_emmt** tool to launch the target Intel SGX application. Syntax for **sgx_emmt** is as follows:

```
sgx_emmt [--enclave=<enclave list>] application_name <application args>
```

Table 1 lists arguments for **sgx_emmt** and indicates which are mandatory or optional.

Table 1. Command arguments for the Intel® SGX sgx_emmt tool

Argument	Argument Type	Description
`--enclave=<enclave list>`	Optional	Specifies the enclave(s) to be measured. Use comma separators with enclave lists.
`application_name`	Mandatory	Name of the Intel® SGX application that contains the enclave(s) to be measured.
`<application args>`	Optional	Intel SGX application arguments, if they exist and are needed. Use spaces as separators when more than one argument is provided.

For example, an **sgx_emmt** command might look as follows:

```
sgx_emmt --enclave=Enclave1.signed.dll, Enclave2.signed.dll myApp.exe
app_arg1 app_arg2
```

The command line above specifies two enclaves, the application, and two application arguments.

Notes

- **sgx_emmt** requires debugging information of a signed enclave to perform its measurements. So the target enclave specified in **sgx_emmt** must be built in Debug mode (or Simulation mode). For details on supported modes, see this paper: https://software.intel.com/sites/default/files/managed/e5/d8/intel-sgx-build-configuration.pdf.
- If an Intel SGX application contains more than one enclave and the heap or stack of a specific enclave needs to be measured, then the target enclave name must be specified in the command-line argument; otherwise, explicit specification of enclave names in the command-line is unnecessary.
- The Intel SGX application must call `sgx_destroy_enclave` for **sgx_emmt** to work.
- For Linux, **sgx_emmt** requires that the SGX application have the symbol `g_peak_heap_used` in the global section of the enclave linker script.

Enclave Measurement in Linux*

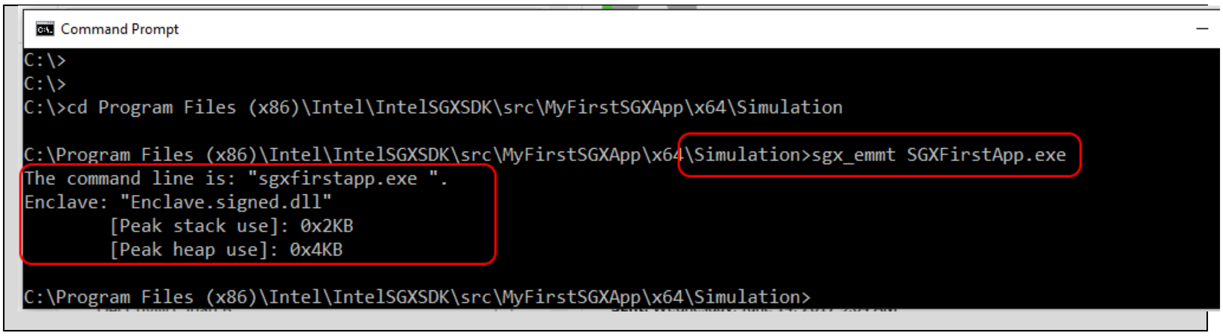
sgx_emmt also measure peak stack/heap memory usage for applications written for Linux. However, usage of the measurement tool in Linux environments differs from Windows environments. Follow these steps for Linux:

1. Make sure that the SGX application has the symbol `g_peak_heap_used` in the global section of the enclave linker script when you build it.
2. After loading the application into **sgx-gdb**, execute the `enable sgx_emmt` command.
3. Run **sgx-gdb**.

Note: To disable **sgx_emmt**, enter `disable sgx_emmt` at the **sgx-gdb** command prompt.

EMMT output

Figure 2 shows an EMMT invocation (Windows Command Prompt) and output for an application named `SGXFirstApp.exe`. Since no enclave is specified in the command line, EMMT uses the enclave in the same folder as the application. Since the application was built in Simulation mode, the application and enclave file are in the `Simulation` folder.



```
C:\>
C:\>
C:\>cd Program Files (x86)\Intel\IntelSGXSDK\src\MyFirstSGXApp\x64\Simulation

C:\Program Files (x86)\Intel\IntelSGXSDK\src\MyFirstSGXApp\x64\Simulation>sgx_emmt SGXFirstApp.exe
The command line is: "sgxfirstapp.exe ".
Enclave: "Enclave.signed.dll"
        [Peak stack use]: 0x2KB
        [Peak heap use]: 0x4KB

C:\Program Files (x86)\Intel\IntelSGXSDK\src\MyFirstSGXApp\x64\Simulation>
```

Figure 3. Intel® SGX sgx_emmt tool output

EMMT displays the command line parameters and enclave filename being measured, then launches the application. When the application exits, EMMT displays the **Peak stack use** and **Peak heap use** values. Developers can compare these values with the max values in their enclave's ECF to refine their stack and heap maximum memory usage on subsequent builds.

Summary

Total memory used by all Intel SGX enclaves residing on a single Windows computer is restricted to less than 128 MB. (Paging in Linux can increase the total amount available for enclaves.) Because of this restriction, it is beneficial to measure the exact values for both stack and heap peak usage for an enclave to understand actual EPC memory use.

To measure this enclave memory usage, run EMMT to measure actual peak usage of enclaves' stacks and heaps. Then use these measurements to adjust enclaves' memory usage as needed on subsequent builds to ensure efficient memory usage.

References

1. Intel Software Guard Extensions SDK for Windows. https://software.intel.com/sgx-sdk/download.
2. Intel SGX SDK Developer Guide for Windows OS — 2017 Intel Corporation. https://software.intel.com/sgx-sdk/documentation.
3. Intel SGX SDK Developer Reference for Windows OS — 2017 Intel Corporation. https://software.intel.com/sgx-sdk/documentation.
4. Intel SGX SDK Developer Guide for Linux OS — 2017 Intel Corporation. https://software.intel.com/sgx-sdk/documentation.
5. Intel Software Guard Extensions SDK Developer Reference for Linux OS — 2017 Intel Corporation. https://software.intel.com/sgx-sdk/documentation.
6. Intel SGX Support Forums: https://software.intel.com/forums/intel-software-guard-extensions-intel-sgx — Intel.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL® ASSUMES NO LIABILITY WHATSOEVER AND INTEL® DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL® PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL® AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL® OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL® PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

No computer system can provide absolute security under all conditions. Built-in security features available on select Intel® processors may require additional software, hardware, services and/or an Internet connection. Results may vary depending upon configuration. Consult your system manufacturer for more details.

Intel®, the Intel® Logo, Intel® Inside, Intel® Core™, Intel® Atom™, and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and/or other countries. Other names and brands may be claimed as the property of others.

* Other names and brands may be claimed as properties of others.