Intel® Software Guard Extensions SDK for Linux* OS Release Notes

1 February 2019

Revision: 2.4 Open Source (version: 2.4.100.48163)

Contents:

Introduction
What's New
System Requirements
Known Issues and Limitations
Disclaimer and Legal Information

1 Introduction

Intel provides the Intel® Software Guard Extensions Software Development Kit (Intel® SGX SDK), a software isolation technology, to help you protect your applications.

This document provides system requirements, installation instructions, limitations, and legal information for the Intel SGX SDK.

Product Contents

Intel® Software Guard Extensions SDK package includes:

- Intel® Software Guard Extensions SDK installer for Linux* OS. It includes binaries to develop enclave applications. The main components include:
    - Trusted libraries including standard C library, C++ runtime Added support, C++ STL, and others.
    - Development tools including edger8r, signing tool, and others.
    - Sample projects.

2 What's New

Intel® Software Guard Extensions SDK includes the following changes in version 2.4:

- Added support for the Key Separation and Sharing (KSS) feature.

- Provided a set of new encryption and decryption functions such as sgx_hmac256_*.
- Provided a new untrusted API: `sgx_get_target_info`.
- Provided a new untrusted API: `sgx_create_enclave_from_buffer_ex`.
- Updated the cryptography library to the Intel® Integrated Performance Primitives Cryptography 2019 Update 1.
- Fixed bugs.

Changes in Previous Releases

Intel® Software Guard Extensions SDK includes the following changes in version 2.3:

- Added support for the Ubuntu* 18.04 LTS 64-bit Desktop and Server version.
- Provided a new set of the Intel SGX common loader APIs in sgx_enclave_common.h.
- Provided a sample code for the Switchless Call.
- Provided a new API in tcrypto: `sgx_ecc256_calculate_pub_from_priv`.
- Changed the `sgx_create_enclave` API: the function ignores the parameter of a launch token and does not update it after the function succeeds.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.2:

- Added support for Switchless, a new mode of operation to perform calls from or to Intel SGX enclaves.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.1.3:

- Updated the cryptography library to Intel® Integrated Performance Primitives Cryptography 2018 Update 2.1. Mitigated security vulnerability CVE-2018-3617 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3617). For more details, refer to Security Advisory INTEL-SA-00106 (https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA00106&languageid=en-fr) and INTEL-SA-00135 (https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA00135&languageid=en-fr).
- Provided enhancements to the Intel® SGX Cryptographic library.

- Added support for the Intel® SGX Protected Code Loader (Intel® SGX PCL). It is intended to protect Intellectual Property (IP) within the code for Intel® SGX enclave applications.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.1.2:

- Mitigated security vulnerability CVE-2018-3626 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3626). For more details, refer to Security Advisory INTEL-SA-00117 (https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00117&languageid=en-fr).

Intel® Software Guard Extensions SDK includes the following changes in version 2.1.1:

- Updated security to the Intel® SGX SDK.
- Added the new `sgx_register_wl_cert_chain` API that allows the Intel® SGX application to register an enclave.
- Added support for the CentOS* 7.4.
- Added support for the SUSE* Linux Enterprise Server 12.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.0:

- Added support for the Intel® SGX Enclave Dynamic Memory Management (Intel® SGX EDMM) to dynamically manage enclave memory: dynamic heap expansion, dynamic stack expansion, dynamic thread creation, and page attribute modification.
- Added support for the Red Hat* Enterprise Linux* Server 7.4.
- Added support for Safe String APIs of the C library in an enclave.
- Added an option to build the Intel® SGX SDK using the Intel® SGX SSL crypto library instead of the Intel® Integrated Performance Primitives Cryptography open source version.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 1.9.100.39124:

- Added C++11 Added support

  To improve support for C++11 on the Linux* OS, the Linux* SDK 1.9 includes a new trusted C++ library based on libc++ (see http://llvm.org/svn/llvm-project/libcxx/trunk). Note that the Standard C++ Library based on STLPort (sgx_tstdcxx) will be deprecated in future releases.

- Added support for the Protected File System – a basic subset of the regular 'C' file API for Intel® SGX enclaves that provides files with both confidentiality and integrity protection.

- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 1.8.100.37689:

- Added support for the TCMalloc library.

- Added support for new Linux* distributions. See Software Requirements for details.

- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 1.7.100.36470:

- Updated the cryptography for the Intel® Integrated Performance Primitives (Intel® IPP) library to version 9.0 Update 4.

- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 1.6.100.34478:

- Added new `setjmp/longjmp` APIs in the trusted C library.

- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes before version 1.5.100.32783:

- Added support for profiling Intel® SGX applications using the Intel® VTune™ Amplifier. To profile Intel® SGX applications, use the VTune™ Amplifier 2016 Update 2, the "Intel SGX Hotspots" analysis type.

- Added the Intel® SGX Eclipse* plug-in to create Intel® SGX enclave projects.

- Added support for the implicit Thread Local Storage (TLS).
- Added support for a nested HW exception in a trusted environment.

3 System Requirements

Software Requirements

- Supported Linux* OS distributions:
    - Ubuntu* 16.04 LTS 64-bit Desktop and Server version
    - Ubuntu* 18.04 LTS 64-bit Desktop and Server version
    - Red Hat* Enterprise Linux* Server 7.4 (for x86_64)
    - CentOS* 7.5 (for x86_64)
    - SUSE* Enterprise Server 12 (for x86_64)
    - Fedora* 27 Server version

NOTE: It is highly recommended to use the listed Linux* OS distributions. Other distributions have not been tested.

4 Known Issues and Limitations

- Intel® SGX for Linux* OS does not support setting a different charset in GNU* Project Debugger (GDB*).
- Building the Intel® SGX SDK sample project “RemoteAttestation” is possible only within the Intel® SGX SDK installation folder.
- Intel® SGX does not support the “long long” type in C++ templates.
- `sgx-gdb` depends on GDB* 7.9.1 or later versions. Please upgrade GDB* if its version is lower than 7.9.1.
- If Intel® SGX EDMM feature is used, you should use the version 2.2 or higher of both Intel® SGX PSW and Intel SGX SDK 2.2.
- `sgx-gdb` does not support watching Thread Local Storage variables in the enclave.
- The addresses of all stack variables are randomized. The randomization comes at the expense of increased stack usage. Enclaves built with the Linux 2.4 SDK should increase their stack size setting by 4 KB.
- Intel® SGX PCL interaction with KSS: In Intel® SGX SDK 2.4, if the Intel® SGX PCL sealing enclave is configured to support KSS (Enclave configuration XML includes entry EnableKSS with value 1) then when sealing the Intel® SGX PCL decryption key, the

Intel® SGX PCL sealing enclave cannot use sgx_seal_data. Instead, the Intel® SGX PCL sealing enclave must use sgx_seal_data_ex and assign key_policy such that SGX_KEYPOLICY_MRSIGNER bit is set to 1 and KSS bits (SGX_KEYPOLICY_CONFIGID, SGX_KEYPOLICY_ISVFAMILYID and SGX_KEYPOLICY_ISVEXTPRODID) are set to 0.

- When user application meets Intel® SGX remote attestation failure and receives Platform Information Blob (PIB) from Intel® Attestation Server, user application can't call sgx_report_attestation_status() interface in libsgx_uae_service.so to process PIB blob. User can visit Intel® SGX open source project in GitHub and build Intel® SGX PSW installer to fix this issue.

5 Disclaimer and Legal Information

disclose or transmit this software or the related documents without Intel's prior written permission.

This software and the related documents are provided as is, with no express or implied warranties, other than those that are expressly stated in the License.

Optimization Notice
Intel's compilers may or may not optimize to the same degree for non-Intel microprocessors for optimizations that are not unique to Intel microprocessors. These optimizations include SSE2, SSE3, and SSSE3 instruction sets and other optimizations. Intel does not guarantee the availability, functionality, or effectiveness of any optimization on microprocessors not manufactured by Intel. Microprocessor-dependent optimizations in this product are intended for use with Intel microprocessors. Certain optimizations not specific to Intel microarchitecture are reserved for Intel microprocessors. Please refer to the applicable product User and Reference Guides for more information regarding the specific instruction sets covered by this notice. Notice revision #20110804

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