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

29 June 2018

Revision: 2.2 Open Source (version: 2.2.100.45311)

Contents:

1 Introduction

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

This document provides system requirements, installation instructions, limitations and legal information.

Product Contents

Intel® Software Guard Extensions SDK package includes:

- An 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 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 2.2:

- Support for Switchless Calls - It is a new mode of operation to perform calls from/to SGX enclaves
- Bug fixes

Changes in Previous Releases

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
- Support for Intel® SGX Protected Code Loader (Intel® SGX PCL) - It is intended to protect Intellectual Property (IP) within the code for Intel® SGX enclave applications
- Bug fixes

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:

- Security updates to Intel® SGX SDK
- New `sgx_register_wl_cert_chain` API for Intel® SGX application to register an enclave
- Support for CentOS* 7.4
- Support for SUSE* Linux Enterprise Server 12
- Bug fixes

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

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

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

- Added C++11 support

  To improve support for C++11 in Linux, 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 the next release.
- Support for 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
- Bug fixes

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

- Support for the TCMalloc library
- Support for new Linux* distributions. See Software Requirements for details
- Bug fixes

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

- Cryptography for Intel® Integrated Performance Primitives (Intel® IPP) library is updated to version 9.0 Update 4
- Bug fixes

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

- New `setjmp/longjmp` APIs in the trusted C library
- Bug fixes

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

- Support for profiling Intel SGX applications using Intel® VTune™ Amplifier. To profile Intel SGX applications, use VTune™ Amplifier 2016 Update 2, the "Intel SGX Hotspots" analysis type.
- Intel® SGX Eclipse* plug-in to create Intel SGX enclave projects
- Support for implicit Thread Local Storage (TLS)
- Support for nested HW exception in a trusted environment

3 System Requirements

Software Requirements

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

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 it is lower than 7.9.1.

5 Disclaimer and Legal Information

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest forecast, schedule, specifications and roadmaps.

The products and services described may contain defects or errors known as errata which may cause deviations from published specifications. Current characterized errata are available on request.

Intel technologies features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at Intel.com, or from the OEM or retailer.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel, the Intel logo, Xeon, and Xeon Phi are trademarks of Intel Corporation in the U.S. and/or other countries.

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