Open Enclave SDK Project Review 2024

As a project of the Confidential Computing Consortium (CCC) in the Incubation stage, the Open Enclave SDK has published a growth plan for reaching the Graduation stage in accordance with CCC Technical Advisory Council mentorship. This report summarizes updates of the project information since its annual report a year ago.

1. Updated and additional information for the project submission template since the last annual report:

- List of project official communication channels – No updates
    - The Open Enclave SDK conducts its public communication through the oesdk@lists.confidentialcomputing.io mailing list.
- List of 3rd party dependencies – No new dependencies
- Release methodology – No updates
    - Same as before - APT repo, nuget.org as well as on Github.
- Project mentor – Alec Fernandez

2. In terms of the progress against the growth plan:

- The OE SDK has settled into a 6month release cadence, currently on v0.19.4
    - Releases are also made when there are CVEs fixed in dependent libraries.
- Continues to be actively maintained, averaging ~2.3 commits weekly(~3.3 at this time last year). CVEs are mitigated in a timely manner.
- The cumulative number of contributors is at 166 (164 last year), the project has been starred 991 times (884 times in the last annual report) and forked 347 times (334 times in the last annual report).
- The community that supports OP-TEE in Open Enclave SDK has shrunk and the OP-TEE specific code is not actively maintained. We have not made progress on attracting developers to maintain the OP-TEE specific code.
- The committers is making progress towards the completion of Inclusive Open Source Community Orientation. This is currently tracked by an issue on the repo.
- Over the last year, the committers have added support for
    - OpenSSL3.1 inside enclaves
    - TDX attestation verification

    - Tests for WS2022
    - Release development containers with the latest Intel PSW and also test against the latest PSW

- At this point, the OE SDK is not ready to request a vote from the TAC to move to the Graduation stage, and will continue to iterate on its growth plan to address the remaining requirements as follows:
    - Our CGC has shrunk as two members retired and one member stepped down to prioritize other opportunities. We will invite contributors from other organizations to become maintainers and members of CGC.
    - OE SDK has not yet published a public list of adopters (i.e. ADOPTERS.md) or advertised their logos as recommended in the project progression policy.
    - The community can add support for additional TEEs

3. For budgeting purposes
    - The Zoom account used for public meetings is funded by CCC.
    - The OE SDK DL oesdk@lists.confidentialcomputing.io is hosted via CCC's "groups.io" site.
    - There was a basic LF license scan done.
    - No new requests.
4. Results of license scan: The scan results for the first 3 are issues in the OP-TEE related directories and since that community has shrunk, we have not been able to mitigate *all* these findings. Please see Appendix 1

    Some notes:

    a. We are considering removing the OP-TEE code to address Findings 1-3
    b. We have updated our OpenSSL support to include OpenSSL 3.1. We continue to carry OpenSSL 1.1.1 in our repo since some users have not yet migrated to use OpenSSL 3.1. This addresses the last finding below
5. OE SDK does not display the OpenSSF best practices badge as yet and will look into it

Appendix 1

Finding #1
Files:
Openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/emu/vexpress-qemu_armv8a/rootfs.cpio.gz/rootfs.cpio/bin/busybox
Priority: Very High
This appears to be a compiled binary / object code file that contains GPL-2.0 content without corresponding sources. This file should be removed from the repo.
Mitigation: Pull devkit out of the repo and place it on a blob store. Pull it during extension's build process and provide documentation pointing directly to public sources for creating the devkit binary (buildroot/OP-TEE test framework).
Alternative: Remove OP-TEE support

Finding #2
Files:
openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/emu/vexpress-qemu_armv8a/rootfs.cpio.gz/rootfs.cpio/usr/bin/strace-log-merge
Priority: High
This file contains content under LGPL-2.1, a weak copyleft license. This file should likely be removed from the repo.
Mitigation: Pull devkit out of the repo and place it on a blob store. Pull it during extension's build process and provide documentation pointing directly to public sources for creating the devkit binary (buildroot/OP-TEE test framework).
Alternative: Remove OP-TEE support

Finding #3
Files:
openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/emu/vexpress-qemu_armv8a/qemu-system-aarch64
openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/emu/vexpress-qemu_armv8a/rootfs.cpio.gz/rootfs.cpio/lib/libpthread-2.28.so
openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/emu/vexpress-qemu_armv8a/rootfs.cpio.gz/rootfs.cpio/usr/bin/strace
openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/sdk/optee/ls-ls1012grapeboard/lib/openenclave/enclave/liboelibc.a/iconv.c.o
openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/sdk/optee/vexpress-qemu_armv8a/lib/openenclave/enclave/liboelibc.a/iconv.c.o
Priority: High
This appears to be a compiled binary / object code file. We do not recommend including binary files in the source code repo. These files should likely be removed.
Mitigation: Pull devkit out of the repo and place it on a blob store. Pull it during extension's build process and provide documentation pointing directly to public sources for creating the devkit binary (buildroot/OP-TEE test framework).
Alternative: Remove OP-TEE support

Finding #4:
Files:
openenclave/3rdparty/openssl/include/bn_conf.h
openenclave/3rdparty/openssl/include/dso_conf.h
openenclave/3rdparty/openssl/include/opensslconf.h
openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/emu/vexpress-qemu_armv8a/rootfs.cpio.gz/rootfs.cpio/etc/ssl/misc/tsget.pl
openenclave/docs/GettingStartedDocs/Contributors/SignUsingEngines.md
Priority: Medium
This file contains content under the old (pre-3.0.0) OpenSSL license. The old OpenSSL license used to require certain statements to be included in advertising materials and redistributions. Is it possible to omit these files from the repo, or to upgrade them to versions from OpenSSL 3.0.0 or later (which are under Apache-2.0)?
5 files (show files)

Mitigation: We have updated our OpenSSL support to include OpenSSL 3.1. We continue to carry OpenSSL 1.1.1 in our repo since some users have not yet migrated to use OpenSSL 3.1. This addresses the last finding below