Mage: Mutual Attestation for a Group of Enclaves without Trusted Third Parties

Guoxing Chen, Shanghai Jiao Tong University; Yinqian Zhang, Southern University of Science and Technology

https://www.usenix.org/conference/usenixsecurity22/presentation/chen-guoxing
A Artifact Appendix

A.1 Abstract
This artifact is an implementation of the proposed mutual attestation mechanism, i.e., MAGE, for Intel SGX. It includes an SDK library libsgx_mage that facilitates developers to use mutual attestation.

A.2 Artifact check-list (meta-information)
- Run-time environment: Developed and tested under Ubuntu 18.04.6 LTS.
- Hardware: An Intel CPU that supports Software Guard eXtensions (SGX), e.g., Intel Core i5-6200U
- How much disk space required (approximately)?: 10 GB
- How much time is needed to prepare workflow (approximately)?: Couple of hours.
- How much time is needed to complete experiments (approximately)?: Couple of hours.
- Publicly available?: Yes, open-sourced on Github.
- Code licenses (if publicly available)?: BSD License

A.3 Description

A.3.1 How to access
libsgx_mage: https://github.com/donnod/linux-sgx-mage/tree/713fbd7479a37d1b768c6f3fd656c177d4d9601

A.3.2 Hardware dependencies
An Intel CPU that supports Software Guard eXtensions (SGX) is needed for the evaluation. Disk space requirement: 10 GB.

A.3.3 Software dependencies
This artifact is developed and tested under Ubuntu 18.04.6 LTS.

A.4 Installation
Installation instructions can be found in the README.md file.

A.5 Experiment workflow
- Install libsgx_mage following the instructions in the README.md file.
- Go to sub-folder: SampleCode/MutualAttestation, and run make in the terminal to build the application.
- Run the built binary.

A.6 Evaluation and expected results
Main claim. A group of enclaves could derive the other’s measurements without trusted third parties.
Steps. The example code builds three enclaves, each of which could derive the others’ measurements. Particularly, in the output of the executable, each enclave prints its own measurements and three derived measurements.
Key and expected results. Three enclaves output the same list of three derived measurements. Each of the derived measurement is the same as one of the enclaves’ own measurements.
The performance evaluation instructions and expected results are in the “Artifact Evaluation” section of the README.md file.