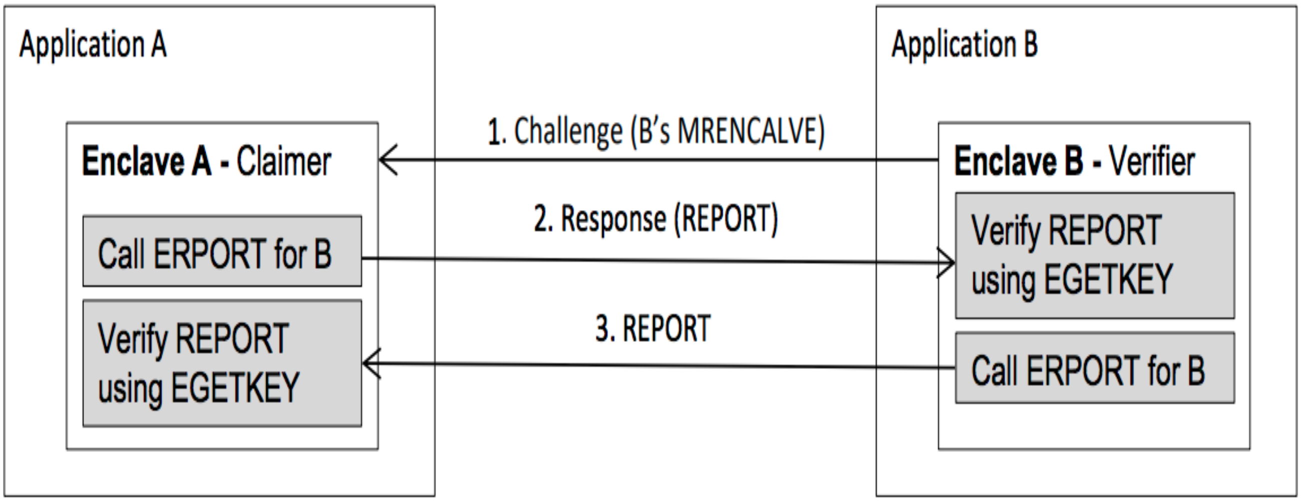
LOCAL ATTESTATION

Before multiple enclaves collaborate with each other on the same platform, one enclave will have to authenticate the other locally using Intel SGX Report mechanism to verify that the counterpart is running on the same TCB platform by applying the REPORT based Diffie-Hellman Key Exchange. This procedure is referred as local attestation by Intel. The successful result of local attestation will offer a protected channel between two local enclaves with guarantee of confidentiality, integrity and replay protection.

Local Attestation Abstract:



(http://www.sgx101.com/wp-content/uploads/2017/09/Screen-Shot-2018-07-01-at-7.55.51-PM.png)

1. There are two enclaves on the same platform, referred to as Enclave A and Enclave B. We assume they have established a communication path between each other, and the path doesn't need to be trusted. W.l.o.g we assume B is asking A to prove it's running on the same platform as B.
2. First, B retrieves its MRENCLAVE value and sends it to A via the untrusted channel.
3. A uses EREPORT instruction to produce a report for B using B's MRENCLAVE. Then A sends this report back to B. A can also include Diffie-Hellman Key Exchange

data in the REPORT as user data for trusted channel creation in the future.

4. After B receives the REPORT from A, B calls EGETKEY instruction to get REPORT KEY to verify the REPORT. If the REPORT can be verified with the REPORT KEY, then B assures that A is on the same platform as B because the REPORT KEY is specific to the platform.
5. Then B use the MRENCLAVE received from A's REPORT to create another REPORT for A and sends the REPORT to A.
6. A then also can do the same as step 4 to verity B is on the same platform as A.
7. By utilizing the user data field of the REPORT, A and B can create a secure channel using Diffie-Hellman Key Exchange. Information exchange can be encrypted by the shared symmetric key.

References:

1. https://www.idc.ac.il/en/schools/cs/research/Documents/jackson-msc-thesis.pdf (https://www.idc.ac.il/en/schools/cs/research/Documents/jackson-msc-thesis.pdf)
2. https://software.intel.com/en-us/articles/innovative-technology-for-cpu-based-attestation-and-sealing (https://software.intel.com/en-us/articles/innovative-technology-for-cpu-based-attestation-and-sealing)
3. https://software.intel.com/en-us/node/702983 (https://software.intel.com/en-us/node/702983)

NEXT PROJECT > (HTTP://WWW.SGX101.COM/PORTFOLIO/REMOTE_ATTESTATION/)

< PREV PROJECT (HTTP://WWW.SGX101.COM/PORTFOLIO/ATTESTATION_PRIMITIVES/)

TWITTER FACEBOOK