Remote Attestation

Remote attestation, an advanced feature of Intel SGX, is the process of proving an enclave is established in a secure hardware environment. A remote party should be able to verify that the right application is running inside an enclave on an Intel SGX enabled platform.

Remote attestation provides verification for three things:

- The application's identity
- Its intactness (that it has not been tampered with)
- That it's running securely within an enclave on an Intel SGX enabled platform
-

Attestation is necessary in order to make remote access secure because an enclave's contents may have to be accessed remotely, not from the same platform [1]

Steps to make a valid proof

The attestation process consists of seven stages, encompassing several actors, namely the service provider (referred to as a challenger) on one platform; and the application, the application's enclave, the Intel-provided Quoting Enclave (QE), and Provisioning Enclave (PvE) on another platform. A separate entity in the attestation process is Intel Attestation Service (IAS), which carries out the verification of the enclave [1][2][3].

In short, the seven stages of remote attestation comprise of making a remote attestation request (stage 1), performing a local attestation (stages 2-3), converting the local attestation to a remote attestation (stages 4-5), returning the remote attestation to the challenger (stage 6), and verifying the remote attestation (stage 7) [1][3].

Secure communication channel

Intel Remote Attestation also includes the establishment of a secure communication session between the service provider and the application. This is analogous to how the familiar TLS handshake includes both authentication and session establishment.

Last updated1 year ago On this page *Steps to make a valid proof * Secure communication channel

Was this helpful? Edit on GitHub Export as PDF