AWS Nitro Enclaves

Overview

Nitro Enclave is a technology introduced by AWS that allows users to create secure computing environments within AWS EC2 instances, also called parent instances. A Nitro Enclave is an isolated, hardened, and highly constrained virtual machine with its own kernel, memory, and CPUs; the enclave has no persistent storage or external networking and does now allow interactive access. The hardware resources of the enclave are protected and isolated by the Nitro Hypervisor which ensures that users, applications, and libraries running on the parent instance are not allowed to access the CPU and memory of the enclave.

The only means of communication with an enclave is via a vsock (short for "virtual socket"), a local communication channel between the enclave and its parent instance. All data moves in and out of the enclave via this vsock connection.

One important advantage of Nitro Enclaves is their flexibility: they are not processor-dependent and can run on EC2 instances powered by different CPU vendors, and they are also compatible with any programming language.

Attestation

Cryptographic attestation is used by Nitro Enclaves to prove their legitimacy and the legitimacy of the code they are running in order to gain the trust of an external party. The attestation process is performed with the help of the Nitro Hypervisor which generates a signed attestation document used by an enclave to prove its identity. An attestation document can only be requested from inside the enclave and contains information about the enclave, including unique measurements of the enclave, a cryptographic nonce, and additional information specified by the external party.

Enclave Measurements

The measurements of an enclave include a series of hashes and platform configuration registers (PRCs) that are unique to each enclave. Currently, an enclave has six measurements:

- PCR0: the hash of the enclave image;
- PCR1: the hash of the Linux kernel and bootstrap;
- PCR2: the hash of the application;
- PCR3: the hash of the AWS IAM (Identity and Access Management) role assigned to the parent instance;
- PCR4: the hash of the instance ID of the parent instance;
- PCR8: the hash of the enclave image file signing certificate.
-

PCR0, PCR1, and PCR2 are automatically generated when the enclave image is built and are related to the enclave and the application running on the enclave. PCR3 and PCR4 are associated with the parent instance, while PCR8 ensures that attestation succeeds when the enclave is booted from an image signed by a specific certificate.

References

1. AWS Nitro Enclaveshttps://aws.amazon.com/ec2/nitro/nitro-enclaves/
2. AWS Nitro Enclaves Cryptographic Attestationhttps://docs.aws.amazon.com/enclaves/latest/user/set-up-attestation.html
3.

Previous Intel SGX Next Miscellaneous Last updated6 months ago On this page *Overview * Attestation * Enclave Measurements * References