SGX-SPS Security & Reliabillity

Why SGX?

Intel SGX is one of the most used and widely available implementations of Trusted Execution Environments (TEEs). Secret Network has selected this technology for the initial version of the Secret Network for two main reasons: Usability & Security.

Usability

SGX is more performant and more flexible than other solutions for privacy-preserving computation. The Secret Network is building a platform for decentralized, general-purpose private computation. This requires a privacy solution that can enable a wide range of use cases. It also requires computations to be on par, performance-wise, with non-privacy preserving computation, so that speed does not limit application usability.

Security

SGX is one of the most widely adopted technologies for TEEs, it is also battle-hardened. Attacks are often theoretical, executed in laboratory settings, and are rapidly addressed by Intel. Many high-value targets exist that have not been compromised. No privacy solution is 100% secure, but we believe the security guarantees provided by Intel SGX are adequate for a wide range of use cases.

Secret Network only allows for Intel SGX chips, AMD-SEV or other TEE technologies are not usable for running nodes on the network.

SGX-ME And SGX-SPS

SGX comes in 2 forms; SGX-ME and SGX-SPS. SGX-ME (management engine) uses small extra chips to manage functions related to the enclave such as memory and energy management. SGX-SPS (Server Platform Services) allows the bypassing of the ME chip. To further reduce the number of possible attack vectors on the network, Secret Network has opted to only use SGX-SPS. Hence, all attack vectors of the ME chip do not apply to Secret Network.

Furthermore, each full node on Secret Network creates an attestation report that proves that their CPU is using the latest firmware/microcode (processor firmware) upgrades before it registers. The entire network verifies the attestation report of the new node on-chain, to ensure that node operators cannot decrypt anything. Once the new node gets the shared key of the consensus they become part of the consensus and are able to process computations and transactions in parallel to the network.

Last updated1 year ago On this page *Why SGX? * Usability * Security * SGX-ME And SGX-SPS

Was this helpful? Edit on GitHub Export as PDF