Hi all

,

SCRT Labs is seeking feedback on a proposed a new design for the consensus seed sealing mechanism on Secret Network. This design would move away from using MRSIGNER for sealing the consensus seed to using MRENCLAVE. The goal of this change is to further decentralize Secret Network.

Background

MRENCLAVE

The MRENCLAVE (Measurement of Enclave) in SGX is calculated using a SHA-256 hash of the enclave unsigned

binary. The enclave unsigned binary is the compiled code of the enclave, which is the trusted part of an SGX application.

To calculate MRENCLAVE, the enclave binary is first divided into 4096-byte chunks. Each chunk is then hashed using SHA-256. The hashes of all the chunks are then concatenated to form the final MRENCLAVE.

The MRENCLAVE is a unique identifier for the enclave binary. It can be used to seal confidential data that can be unsealed only by an enclave with the same MRENCLAVE.

MRSIGNER

The MRSIGNER (Measurement of the Signing Key) in SGX is calculated using a SHA-256 hash of the enclave's developer public key.

To calculate MRSIGNER, the enclave's developer public key is first converted to a byte string. The byte string is then hashed using SHA-256. The hash is the final MRSIGNER.

The MRSIGNER is a unique identifier for the enclave's developer public key. It can be used to seal confidential data that can be unsealed only by an enclave with the same MRSIGNER.

Secret Network

In 2020, SCRT Labs decided to use MRSIGNER to seal the consensus seed. This means that for every version of Secret Network, SCRT Labs has signed the enclave with its private key.

The main reason for choosing MRSIGNER is that it made upgrading the chain easy. If SCRT Labs had opted to use MRENCLAVE, we would have also needed to implement a handover mechanism to send the consensus seed from the old enclave to the new enclave every time the chain is upgraded.

EDIT: To emphasize, sealing with MRENCLAVE was significantly more difficult to implement and would have introduced potential risks that could have been fatal for the network without also implementing proper mitigations (which will be discussed later in this post). All of this would have delayed the mainnet release of Secret Network by at least 6 months, possibly a year.

The main challenge with using MRENCLAVE is the need for a proof system inside the enclave. This is to ensure that the new enclave is approved by the network and that the old enclave is not sending the consensus seed to a malicious enclave.

As of October 2023 (including v1.12), SCRT Labs has not yet implemented that proof system inside the enclave. Any solution that uses MRENCLAVE for consensus seed sealing would also require that proof system to be implemented inside the enclave first.

Proposed Design

1. There will be a proof system inside the enclave, that can verify the chain's state using merkle proofs.
2. There will be two new on-chain params: current_mrenclave

& next_mrenclave

.

1. We'll modify the upgrade proposal to also include a new next_mrenclave

param and change it if the proposal passes.

1. The upgrade handler would update next_mrenclave

and then trigger a “migrate consensus seed workflow” inside the old enclave.

1. The old enclave would read current_mrenclave

& next_mrenclave

from the chain and verify both with merkle proofs, secured by the enclave’s light client (I.e., signed by >2/3 of validators).

1. The old enclave would check that current_mrenclave

matches its own identity.

1. The old enclave would perform a local attestation for the new enclave binary and check that the next_mrenclave

parameter matches the new enclave’s identity.

1. The old enclave would use a local communication scheme (TBD, can be local socket, HTTPS, etc.) to send the seed from the old enclave to the new enclave. This can be done using the same encryption protocol that is currently used for sending the seed to new nodes.
2. The new enclave would seal the seed with MRENCLAVE.
3. The new enclave would update the on-chain parameter current_mrenclave = next_mrenclave

.

1. The chain would resume producing blocks with the new enclave.

We will require at least two upgrades to reach the final state. The first upgrade will introduce the code that allows the old enclave to verify the new enclave and send the consensus seed. The second upgrade will allow the new enclave to receive the consensus seed and enable MRENCLAVE sealing.

Seed Recovery and Safety Mechanisms

In case of a bug in the handover mechanism, the chain could reach a limbo state where the old enclave cannot verify the new enclave or send the consensus seed. To address this issue, we will add a way to allow a specific MRENCLAVE to read the consensus seed by introducing a special transaction type that is signed by SCRT Labs in addition to all or most of the validators.

EDIT: This mechanism isn’t fully fleshed out yet, but the goal is to add a way to send the consensus seed to a new enclave without going through governance, in case the chain is halted.

Additionally, to prevent a governance attack or bug, we are considering adding the requirement that SCRT Labs vote yes on an upgrade proposal in order for it to pass. At least for the first few upgrades, until everyone is more comfortable with the new process.

Pros & Cons

Pros:

- SCRT Labs will no longer be able to decrypt the entire state at will (not that we ever did).
- Given a reproducible build setup, anyone will be able to compile and run their own binaries on mainnet. Currently, only SCRT Labs can compile the SGX enclave because it requires our developer key for MRSIGNER sealing to work on mainnet.

Cons:

- Upgrades will become more dangerous, because if there is a bug in the consensus seed handover mechanism implementation, no one will be able to compile a version that fixes it. To mitigate this risk, the proposed design will gradually migrate from MRSIGNER to MRENCLAVE over multiple chain upgrades to ensure that the mechanism and implementation are sound.

Feedback

SCRT Labs would like to receive community feedback on this proposed design. We welcome any questions, notes, insights regarding the proposed design, pros, cons, seed recovery, safety mechanisms, or anything else.

We are very excited about this proposal and see it as a huge leap forward for Secret Network in terms of maturity and decentralization.