Network level

Noting all network design specific attack vectors. The design of a privacy focused computation network is not without its compromises. Some of these compromises dont have direct impact on the contract level but are attack vectors on the network design itself. The most notable of these attack vectors are listed in this thread. Please be aware that many of these attacks are research avenues in cryptography in general or specifically by SCRT labs. Secret puts TEE usage at a new frontier and will continue to innovate to remove potential attack vectors by creating new and novel designs not done anywhere else.

Upgrade transparency - MRSIGNER

Recall thatnodes in our network share secrets in their enclaves. This happens when a new nodes registers their enclave/node in the network, and their enclave in turn is provisioned with the network's secret keys.

Secure enclaves have no persisted memory, so instead, SGX has an API (called sealing) for persisting data from the enclave. This essentially encrypts the data inside of the enclave (using an encryption key that is hard-wired to the specific machine's TEE), and persists it on disk. The enclave (and only the enclave) can then 'unseal' the data, which is essentially loading it from disk into the enclave's memory and decrypting the information.

Sealing API provides two types of sealing policies: MRENCLAVE and MRSIGNER:

1. MRENCLAVE: Only allows the same 'enclave' (i.e., the same code binary) to unseal previously sealed data, even from the same machine.
2. MRSIGNER: Allows the entity who signed the enclave's code binary to unseal the data.
3.

Secret currently leverages MRSIGNER as explained in the network bootstrap section of this documentation. This comes with several different tradeoffs dubbed Upgrade transparancy. Meaning that with using MRSIGNER the original signer of the network binary code (SCRT Labs) can deduct the network consensus seed and private key by actions not controllable or visible on-chain.

Find a deep dive in the long term roadmap for this attack vector in the below forum post.

Tradeoffs Discussion: Upgrade Transparency Secret Network

Storage access - Access pattern hiding

This section describes an attack on all host computed privacy platforms like HME, MPC and TEE systems where the information about what items are retrieved from storage is not obfuscated. Monitoring these access patternes reveals information about potential senders and receivers of information and has mostly impact on transactional privacy usescases on Secret Network like the SNIP-20 tokens.

As from thepaper revealing this:"All of these blockchains inherit a key-value storage programming model for their existing smart contract languages. This is backed by encrypted data stored locally on the node performing the execution. In the example of a private token, each account balance may be stored as a separate record. None of the systems whose codebases we evaluate hides access pattern, and so an untrusted host OS can potentially learn private information (such as recipient addresses in the private token ex- ample) by monitoring accesses to the key-value storage. This is the most pronounced in Secret and Oasis, which leak the exact key that is being accessed. Obscuro uses a TEE-based database library called EdgelessDB, which reads and writes to the filesystem using 4KB blocks. Phala uses an entirely in-memory data structure for contract state, thus it would leak to the untrusted OS page fault handler which memory page is being accesed. To address this issue, it is crucial to employ effective obfuscation techniques such as the use of oblivious RAM/data structures or encrypted databases"

More information on the tradeoffs in this discussion can be found on the forum

Tradeoffs Discussion: Access pattern hiding / Spicy Printfs Secret Network

Compartmentalization - Permmissionless Nodes

This speaks to the definied access to the network private key which in Secret is completelly permissionless only requesting a genuine enclave. This means there is a bigger attack surface to attack the SGX enclaves as any full-node or validator obtains the network private key. Other TEE focused networks take more permissioned approaches, a discussion about where Secret should focus in the long term is available on the forum.

Tradeoffs Discussion: Compartmentalization Secret Network

Last updated7 months ago On this page *Upgrade transparency - MRSIGNER* Storage access - Access pattern hiding * Compartmentalization - Permmissionless Nodes

Was this helpful? Edit on GitHub Export as PDF