Hi Secret Community,

I am writing to start an open conversation about several tough tradeoffs in Secret Network's security and privacy design.

The goal of these posts is to stimulate a community discussion, and to encourage actionable next steps for the community to take. Ideally, through these discussions the community could come up with ideas (and eventually - solutions) to certain difficult questions. Many of these don't have a clear answer, so it's important to gauge where community sentiment lies.

For this post I'll just focus on the first issue:

Software upgrade transparency.

Right now, the master consensus seed is sealed using the "MRSIGNER" rule. There was a forum post about this, and more information can be found here: The Initialization Of Secret Network - Secret Network, but that discussion thread ended without a clear resolution. I have also written a blog post about this (here). The current version of Secret does

use MRSIGNER, and so it does

exhibit this backdoor risk. Essentially MRSIGNER means that any enclave signed by the developers can access a sealed file containing the consensus seed. This means the developers could, if they chose to, run an enclave that decrypts the consensus seed, by code signing a malicious enclave that prints the key in plaintext and running this malicious enclave on one of their own nodes. Especially in a world where we know 3rd parties will exert pressure on developers, this is unwanted. Because this is an entirely offline attack, there would be no trace of it, and there is no way for developers to prove this hasn't happened.

Even though Secret Network applies a voting process to approve software upgrades, these process is not enforced

by the enclaves themselves. An alternative approach, which is already implemented in other privacy focused networks such as Phala and Oasis, and is being planned by Obscuro, is called "upgrade transparency," and basically means that old enclaves will validate the on-chain voting process (as well as the developer signing key) before transfering the consensus seed to new enclaves.

The tradeoff is that this mechanism complicates the enclave, and not only is not trivial to implement, but also increases the risk of an implementation error "bricking" the network into an unrecoverable state. It's thus a tough tradeoff between the risk of privacy breach and the risk of total shutdown.