Dear Zilm & ETH Devs,

Apologies in advance if my post is deemed inappropriate forhttps://ethresear.ch the purpose of my post is to help find a solution for all ETH 2 nodes which may have had their validator or withdrawal keys breached.

It is pointless getting into the details of how it happened to me, what I think is important is trying to find a solution. I will make this attempt to share my thoughts in a manner which hopefully doesn't get me immediately banned.

The purpose of a system breach may not only be for financial purposes it may be to undermine the network and the Ethereum Foundation, so being extra prudent for when withdrawals are enabled is what I would like to discuss.

For a large number of nodes there will be two operators, the host (server side) who holds the validator key and the Staker (client side) who holds the withdrawal key. Below I will write a list of steps which would mean the two parties would need to work together to authorise each other to request a withdrawal, thus making it much harder for a hacker/bad-actor to use a compromised withdrawal key.

Note: This proposal is a little labor intensive and may not be for everyone, it could be optional

but for extra security and peace of mind it could be worth the effort and may be worth the client paying the host a fee for example $50-$100 for each withdrawal.

1. Maybe not popular, but with such large sums of money involved Host's should use KYC type security protocols.
2. Not everyone will want to withdraw funds when we reach phase 1.5 so could there be an option to "lock/unlock" the node withdrawal service, by default all nodes should be set to "locked" this way withdrawals will be impossible until the Staker chooses he/she/they is ready for a withdrawal.
3. Similar to a 3 way handshake a withdrawal could have multiple steps to protect the misuse of a key using the (server side) node key and the (client side) withdrawal key/request.
4. After a users ID has been fully verified by the host the Staker makes a request to the host for a withdrawal/skim.
5. Using the node validator Key the host (server side) would need to send a request to the network for a withdrawal/skim.
6. Each (server side) withdrawal request will trigger a unique forthcoming Epoch or Slot number to be sent to the node/host, for the purpose of this discussion we can think of an Epoch or Slot number as a type of PIN number similar to that used with a credit card (CC).
7. The PIN number could be sent to the client after full ID verification has taken place, the PIN could be sent using email, SMS, phone call or maybe even sent in the post similar to a CC PIN number?
8. The client now has their withdrawal key and a PIN, by rights the hacker only has the withdrawal key (we hope) rendering it useless without the PIN.
9. This PIN must be unique for each withdrawal request and can only be used once.
10. The client starts the withdrawal request using the PIN, withdrawal key, amount to withdraw and a wallet address to send the funds.
11. The withdrawal request will trigger an unlock request with the host (server side) and the host can confirm the withdrawal request was made by the client before unlocking the node.
12. Client verifies the wallet withdrawal address and confirms the withdrawal request was initiated by the client and the node is unlocked by the host.
13. The client will have only one chance with each request, should the PIN be input incorrectly the node would stay locked the host informed of a failed withdrawal request and if it was the client who made a mistake the withdrawal process would have to be started again. This with luck should make it very hard for a validator or withdrawal Key to be misused.
14. Client waits for Epoch or Slot number to be processed and with luck at this point in time a successful withdrawal/skim has taken place.
15. Node goes back to default state of being "locked".

It may seem laborious but by the time we get to phase 1.5 each node could have a value well in excess of $250,000 so in my view it is worth making the withdrawal process as secure as possible, which in effect renders the key useless without a PIN.

Of course this is just a rough idea and I am by no means an expert in blockchain, however I hope there are some steps that could be helpful to anyone like myself who sadly had an ETH 2 withdrawal key breached, a similar process could also be used for withdrawal key rotation, should a Staker wish to change the withdrawal key!

Thanks kindly for reading my post, I am ever so grateful for all your efforts and time.

Tobes