Chia Reserve Custody System

21st March 2018

OVERVIEW

CHIA Networks' Strategic Chia Reserve (SCR) will be a primary asset for the company and due to the expected value of the SCR an alluring target for theft. This document proposes a technical and procedural custody system designed to mitigate the risk of both loss and theft of the SCR. The goal of the custody system is to be resilient against loss from passive threats, such as hardware failures and natural disasters, while also protecting against dedicated attackers inside and outside the company trying to steal from the SCR.

Threat Categories

The proposed custody system was designed to mitigate risks from a number of different types of threats. Identified threats to CHIA's SCR can be broken down into two categories, Active threats and Passive Threats.

Passive Threats

The passive threats category covers all threats to the system that occur without a human taking a deliberate act against the system.

Natural Disasters

Any custody system will face numerous potential disaster style threats. The custody system will have to mitigate the risk of a natural disaster destroying a site responsible for the storage of critical infrastructure. In addition, the custody system will need to account for how a natural disaster or transportation accident could lead to the death of multiple key-holders at the same time.

Hardware Failures

Trusted and/or tamper resistant hardware is a common component in cryptocurrency custody systems, however the custody system will need to account for the possibility of unexpected failure of any piece of critical hardware. An added complication is hardware failures are often

linked to manufacturing batches, so any hardware purchased at the same time may have similar failure rates / times. In addition, many of the commercial hardware wallets on the market today have only been produced for a short time, so it is difficult to accurately predict the mean time between failures.

Human Failures

People's memory is inherently fallible, if the custody system requires trusted team members to memorize arbitrary secrets then the custody system must account for people forgetting these secrets.

Active Threats

Active Threats covers any attack where a person or persons takes deliberate action to violate the security of the custody system. These attacks could have the goal of theft from or simply the destruction of the SCR. These attacks may or may not involve trusted insiders.

Technical Attacks

Any cryptocurrency custody system will need to have technical components in order to generate legitimate transactions, these components must be expected to come under attack. In component with an active connection to the internet must be considered to be at high risk of an attack. However, physically isolated devices are still likely to come under limited technical attacks and the custody system should account for these risks.

Physical Attacks

The custody system for the SCR will need to provide protection from multiple types of physical attacks. A primary goal of the system should be to deter an adversary from targeting individual key-holders or their families as a means of stealing from the SCR. In addition, the custody system should be resilient against adversaries attack any secure site used to store critical infrastructure.

Overview of Custody System

Signature Scheme

The proposed signature scheme is designed to mitigate multiple active and passive threats while not imposing extreme separation requirements on CHIA employees. The scheme is based around the concept of having an inside team and outside team where both teams have specific signature requirements. As an example for the purposes of this document Team A will be the insider team and consist of the CHIA CEO, COO, CFO, and GC as well as a designated survivor. Again for the purposes of an example Team B will be the outsider team and consist of at least four independent members of the CHIA board of directors (this team does not have to be

connected to the board of directors, but it makes for a good example.) Under the proposed signature scheme all transactions from the SCR would require the following signatures

- Three members of Team A (corporate officers) and one signature from Team B (outsiders)

OR

- Three member of Team B (outsiders) and one signature from Team A (corporate officers)

Due to the fact that all of Team A will frequently be located at CHIA headquarters at the same time the custody system needs to account for the possibility of both and attack at CHIA headquarters or the possibility of a natural disaster. In order to deter an attack against CHIA headquarters, a gathering of corporate officers should not be sufficient to approve transactions from the SCR. In addition, any planned meetings between members of Team A and Team B should be conducted in such a way as to not gather a sufficient number of people to approve SCR transactions at the same location. Secondly, in order to mitigate the natural disaster risk, the Designated Survivor (DS) is an additional member of Team A. The DS is a highly trusted person, preferably with no obvious connection to the company, whose purpose is to allow Team B to approve SCR transactions in the event of a worst case scenario. If Team B does consist of members of the board of directors, or otherwise has group meetings, Team B will have to designate someone to serve as the designated survivor for each meeting. In addition, since Team A will almost certainly spend a majority of time in the San Francisco area, Team B should live and meet outside of Silicon Valley area, and preferably outside of California.

Technical Components

Hardware Wallet

A hardware wallet will be necessary for each key-holder and will be their primary means to approve any SCR transaction. While there are multiple hardware wallets on the market, none currently support BLS signatures so something custom will be required. This market is currently dominated by Trezor and Ledger, and while both have some unique security features, the fact that only Ledger uses a separate secure element to protect the key from physical attacks makes it a clear winner. Another important feature of current Ledger products, is that it displays a summary of the transaction being approved. Without this feature the computer interacting with the wallet must be a trusted system, or an attacker could present the user with a transaction different from what is being sent to the wallet for approval. While the current Ledger products offer significant security, there are additions that could be made to the product that would significantly increase the security of the custody system. First, introducing the concept of a duress code, a pin that appears to be valid and signs the requested transaction, but in reality it wipes the key from storage and signs the transaction with a random value. This limits the effectiveness of any plan to attack key-holders and force them to sign a transaction. While

key-holders may fail to use their duress code, an attacker now has to plan to deal with this risk. In order to reduce the attack surface of the hardware wallet, the USB interface can be replaced with a simple serial interface. Trezor's hardware wallets have a unique pin input mechanism where the wallet displays a randomized number pad layout, and the pin is entered via an attached computer on a blank number pad. While this limits what an attacker with access to the computer can learn about the pin, it does reveal if the pin contains duplicate digits. An obvious next step would be to randomize the pin pad after each digit. This document only covers high-level requirements of hardware wallets for CHIA SCR custody, additional documentation is available if CHIA would like to pursue custom development.

Transaction Computer

The Transaction Computer (TC) will be stored at A-sites and will be used by the key-holders to generate transaction information to be signed by the hardware wallet. While the use of a secure hardware wallet reduces the risk of using a compromised computer for generating transactions, the transaction computer will be protected from outside compromise in order to add additional layers of security. The TC should be purchased from a local store from the supply on hand to mitigate supply chain attacks against the system. In addition the configuration should be witnessed by a key-holder. The TC should have all wireless networking components removed before it is used. Once the TC is configured it should be stored at an A-site, while stored it will be kept inside a tamper evident bag, and all external ports will be covered with tamper evident seals. Before use, the serial numbers for all tamper seals will be verified. Once the transaction has been signed, the key-holders will write down the resulting BLS signature, and the TC will be sealed with new tamper seals.

Secure Container

Given the requirement for key recovery material to protect against both hardware failure and human memory failure, the secure storage of this material is critical as it is clearly the best vector for theft from the SCR. No safe is unbreakable, however, provided that the recovery material is widely dispersed, the SCR can be protected by detecting attacks against recovery material and quickly performing a key revocation. As long as CHIA can reliably detect an attack against the recovery material, an adversary will need to attack a majority of the recovery material almost simultaneously. A mechanism to achieve this goal can be developed with commercially available products and two custom software applications. IPS safes are safes designed to secure computer systems while they are operating, providing a path for power to enter the safe, and providing airflow to cool the system. These safes can be procured with multiple types of sensors (latch, light, infrared, sound, environmental), and in multiple form-factors, including disguised in office furniture. However, there is not currently a product that does a sufficient job of monitoring the state of these sensors and reporting the status back in a secure fashion. However, it is feasible to develop a custom application that monitors the state of the sensors and sends a

routine state of the system message as well as an immediate alert if a sensor is tripped. In order to minimize the ability of an attacker to gain access to the safe without CHIA being alerted, each safe will have a unique key and will sign and encrypt each message, will send a message on a randomized interval between one and ten minutes, these messages will be sent via multiple channels (e.g. Slack and Keybase.) If a safe fails to send a regularly scheduled message, it will be treated as compromised. Depending on the exact security requirements, and cost sensitivity the security of these containers can be increased by isolating the monitoring computer inside an RF enclosure, further isolating it from the outside world.

Key-Holder Communications

In order to detect an ongoing attack against key-holders routine communication for all the key-holders will be necessary. Each key-holder should have a secondary phone, the sole purpose of this phone will be for securely communicating with other key-holders and CHIA security management. Only the identified secure messaging app should be installed on the phone, and only that app should be used for communications.

Site Requirements

As part of the proposed custody procedures CHIA will have requirements for at least two types of secure spaces. A-sites will be used for the storage of trusted hardware for generating transactions as well as being the meeting location for conducting transactions. B-sites will be used for the storage of recovery material. Due to the risk of compromise of recovery material, the security requirements for B-sites will be more strict. The use/lease of all secure sites should be arranged through an intermediary to obfuscate the link between the sites and CHIA. The locations of the sites should be treated as sensitive information, and CHIA should take steps to minimize the number of people who know the location of multiple sites.

A-Site Requirements

In order to deter an attack against an A-site while a transaction is being conducted, CHIA should maintain multiple geographically disparate A-sites, so that the personnel at single site are not sufficient to approve a transaction. In addition having at least three A-sites allows key-holders to randomly choose which sites to use, and forces an adversary to attack all A-sites simultaneously, even if they know the time and date when a transaction will be generated.

B-Site Requirements

Since B-Sites are only used for the storage of recovery material, these sites have minimal physical space requirements. B-Sites will only need enough space for the secure container (as outlined in the Technical Components section), and be able to provide power for the secure container. Due to the risk of compromise of recovery material, B-Sites should have additional physical security beyond what is provided by the secure container, at a minimum this should

include real locks, and a alarm system with twenty-four hour monitoring and contractually enforced response times. For example, B-sites could be a dedicated cage in a datacenter, as most have significant physical security, or even hidden in office furniture in a large law firm office. There should be a seperate B-site for each key-holder as any compromise (real or suspected) of a B-site will require an immediate key revocation\replacement procedure. Reducing and/or co-locating B-sites dramatically increases the risk that an attacker could compromise enough recovery material to approve their own transaction before the keys could be replaced. Preferably the location of a B-site would only be known by the individual key-holder and no individual or computer network would no the location of all B-sites.

Personnel Security Requirements

In order to detect and mitigate attacks against the SCR there will be security requirements for all key-holders. Key-holders will be required to maintain positive communication with the CHIA security team. An example policy could specify that Team A members (Corporate insiders) will either communicate in person at CHIA headquarters or via the identified secure messaging system with the identified member of the CHIA security team by Noon PST every weekday, Team B members will check-in via identified secure messaging system every 24-hours. All key-holders will be provided with a duress phrase or indicator allowing CHIA to identify that they are communicating under duress.

Procedures

Transactions

When a transaction from the SCR is necessary, all key-holders will be notified via secure messaging app. Team A will identify the number of key-holders from Team B that are required as well as the time that the transaction will be generated. Each team will determine which members of the team will conduct the transaction, and key-holders will randomly choose which site they will travel to. Identified members will buy refundable tickets to at least two A-site locations scheduled to arrive at approximately the same time. Twelve hours before departure the key-holders will cancel the extra tickets. Once all members are at their appropriate site, the transaction computer will be removed from storage and all tamper seals will be verified against photos taken on previous use. The transaction will be generated on the TC and the hash of the transaction will be verified by key-holders by generating the same transaction on a personal device. Once the transaction hash has been verified each key-holder will connect their hardware wallet, verify the the transaction hash on the wallet is the same as what was previously verified, and then enter their pin to approve the transaction. Once the transaction has been signed the resulting BLS signature will be copied by hand to paper and verified by each key-holder. The verified signature will be sent via secure messaging app to all key-holders. Team A will be responsible for consolidating all partial BLS signatures into a unified signature and transmitting

the transaction to the CHIA blockchain. Once the signature has been communicated, the key-holders secure the TC with new tamper seals and all tamper seal serial numbers will be recorded via picture, and the pictures will be sent to all key-holders.

Key Revocation / Replacement

Key replacement procedures will be similar to standard transaction procedures, with a few modifications. All key-holders will be required to travel to an A-site. All key-holders will receive a new hardware wallet and generate a new private key. Key-holders will broadcast their new public key to all key-holders, so that all key-holders can validate the resulting transaction hash.

Next Steps

- Hardware wallet development
- Secure physical storage development
- Further define A-site and B-site requirements, identify potential A-sites
- Further define communications requirements and procedures
- Further define transaction procedures, specifically for exceptional circumstances, worst-case scenario recovery procedures