May 2022

Trusted Holochain Networks

Niranjan M M

Trusted Holochain Networks

AUTHOR:
Niranjan M M

ABSTRACT

Holochain combines hashing, digital signatures, and Distributed Hash Tables (DHTs) to form a tamper-proof distributed ledger. Holochain uses digital signatures for authenticity and ownership of the data, which uses dual-key (public key-private key pair) cryptography. Each hash-chain entry is cryptographically signed and in multi-party interactions, like transactions, it is mutually counter-signed by both the parties. Currently Holochain systems uses Distributed Public Key Infrastructure (DPKI) to generate keys of various types i.e., revocation, identity, encryption, signing. But there are no existing techniques which consider using TPM (for hardware) or vTPM (for software/virtual) to generate private key and public key pair required for authentication and encryption, also existing techniques does not use attestation information to provide trust in the Holochain based systems. The techniques presented herein propose method to use TPM/vTPM and attestation information for Holochain based system to provide authentication and encryption along with trust. This method simplify some of the Key management aspects of DPKI. As per this method, use TPM (for hardware) and vTPM (for virtual) certificate for device identity and authenticate the peer device using private and public keys populated by the TPM/vTPM. Private and Public Key pair is used to generate symmetric keys for encryption. Along with generating keypairs using TPM/vTPM, this method incorporate attestation method to provide proof of integrity, freshness of proof of integrity and known good values.

DETAILED DESCRIPTION

Holochain combines hashing, digital signatures, and Distributed Hash Tables (DHTs) to form a tamper-proof distributed ledger. Hashing technique is used to generate fingerprint for the data (includes transaction details etc.,), digital signatures are created using dual-key cryptography and, DHTs are distributed database that can store and retrieve information associated with a key in a network of peer nodes that can join and leave the network at any time.

Holochain uses digital signatures for authenticity and ownership of the data, which uses dual-key (public key-private key pair) cryptography (aka Public Key Cryptography). Each hash-chain entry is cryptographically signed and in multi-party interactions, like transactions, it is mutually counter-signed by both the parties. For encrypting data between nodes (Happs), symmetric and asymmetric encryption methods are used where-in encryption keys are derived using public key cryptography.

Currently Holochain systems uses Distributed Public Key Infrastructure (DPKI) to generate keys of various types (revocation, identity, encryption, signing) from seeds generated from the Primary Seed (i.e., Primary Seed is nothing but "secret" used in the context of DPKI). DPKI uses hierarchical deterministic key generation system, based on a Primary Seed, from which additional seeds can be generated which then are in-turn used to actually generate many key-pairs. By-convention, uses first seed generated by the Primary Seed as the seed for revocation keys and subsequent seeds as seeds for generating keys to separate Holochain devices (nodes/Happs). This concept is implemented in DeepKey application as reference. But none of the existing techniques consider using TPM (for hardware) or vTPM (for software/virtual) to generate private key and public key pair required for authentication and encryption, also none of the existing methods use attestation information to provide trust in the Holochain based systems.

The techniques presented herein propose method to use TPM/vTPM and attestation information for Holochain based system to provide authentication and encryption along with trust. This method simplify some of the Key management aspects of DPKI. As per this method, use TPM (for hardware) and vTPM (for software/virtual) certificate for device identity and authenticate the peer device using private and public keys populated by the TPM/vTPM. Private and Public Key pair is used to generate symmetric keys for encryption. Along with generating keypairs using TPM/vTPM, this method incorporate attestation method to provide proof of integrity, freshness of proof of integrity and known good values.

A. In TPM consideration (for hardware):

As we know TPM is used to secure the network devices by protecting device identity (and hence resistant to physical attacks). TPM can also be used to generate cryptographic keys for providing authentication and encryption functionality at the software/application level. In other words, TPM provides hardware fingerprint which can be used as device identity.

In TPM based Holochain system, every Holochain device (node) need to have Public and Private Key (PK, SK) pair. The certified Public and Private key (PK, SK) pair is provided by the TPM available on the microchip of the device (node). Generally TPM does not expose security keys to the applications, but provides option to migrate the keys, so that applications can use them for the authentication and encryption methods.

B. In vTPM consideration (for software/virtual):

Virtual Trusted Platform Modules (vTPMs) have been widely used in commercial cloud platforms to provide virtual root-of-trust for virtual machines. In vTPMs, instead of using physical NVRAM, it uses a file, denoted as a NVRAM file, to hold secret keys. Similar to a physical TPM chip, a vTPM stores credentials for trust & identity, crypto operations and integrity measurement in this file.

There are couple of methods to protect a vTPM.

- TPM-based protection: It uses a physical TPM to seal the NVRAM file of a vTPM to bind the vTPM to the physical TPM and provision static protection for TPM's secret data.
- Tailored lightweight VM to support virtual TPM functions. This method relies on VM isolation to provide security separation.
- SMM-based protection: It places the vTPM into CPU System Management Mode (SMM) to achieve strong isolation.

This vTPM is used to generate private key and public key pair for the applications to use for the authentication and encryption functionality.

C. Trustworthiness using attestation method:

The technique presented herein applies attestation method to all the signed transactions published by the node to the Holochain DHT. This method adds attestation information to the signed transactions as an extension that embeds:

- A hardware finger print (derived from TPM/vTPM/SUDI or similar)
- PCR values, Counters, time-ticks etc.,
- Software - OS, BIOS, kernel, version, application binaries/libraries etc.,
- Known Good Values (KGV) - The KGV is gathered by the manufacturing as part of software build and regression process. The signed KGV will be published and maintained by the manufacture in a well-known location. This is used against the measurement information received by the node.

The receiver node who validates the transaction will use this attestation information to verify whether the source node is trustworthy and make policy decision to accept/reject the transactions received.

The technique presented herein is explained in detail as below:

- Holochain based devices (nodes/Happs) generates pair of keys, Private Key SK and Public Key PK. These certified keys are provided by the TPM available on the microchip of the device for the hardware based systems.
- vTPM is used to provide certified keys for the software (virtual) based systems.
- The generated Private Key is used for digital signature to provide authenticity and ownership of the data.
- The generated Public Key and Private Key pair is used to generate symmetric keys for encrypting data (transaction) between Holochain devices (nodes/Happs)
- With the Private Key and Public Keys being generated using TPM/vTPM, trust between Holochain nodes (Happs) is achieved implicitly.
- The attestation information would be carried as part of signed transaction and available in the Holochain DHT.
- The node who validates the signed transaction, would validate against the attestation information also before proceeding with further action (i.e., accept/reject the received transaction).

The figure-1 below depicts use of TPM/vTPM to generate Public and Private Key pairs used for authentication and encryption in Holochain based networks. Here, Holochain network with 10 nodes (N1...N10) where N1 is Source Node and N10 is Received Node uses their TPM/vTPM to generate (PK, SK) pair.

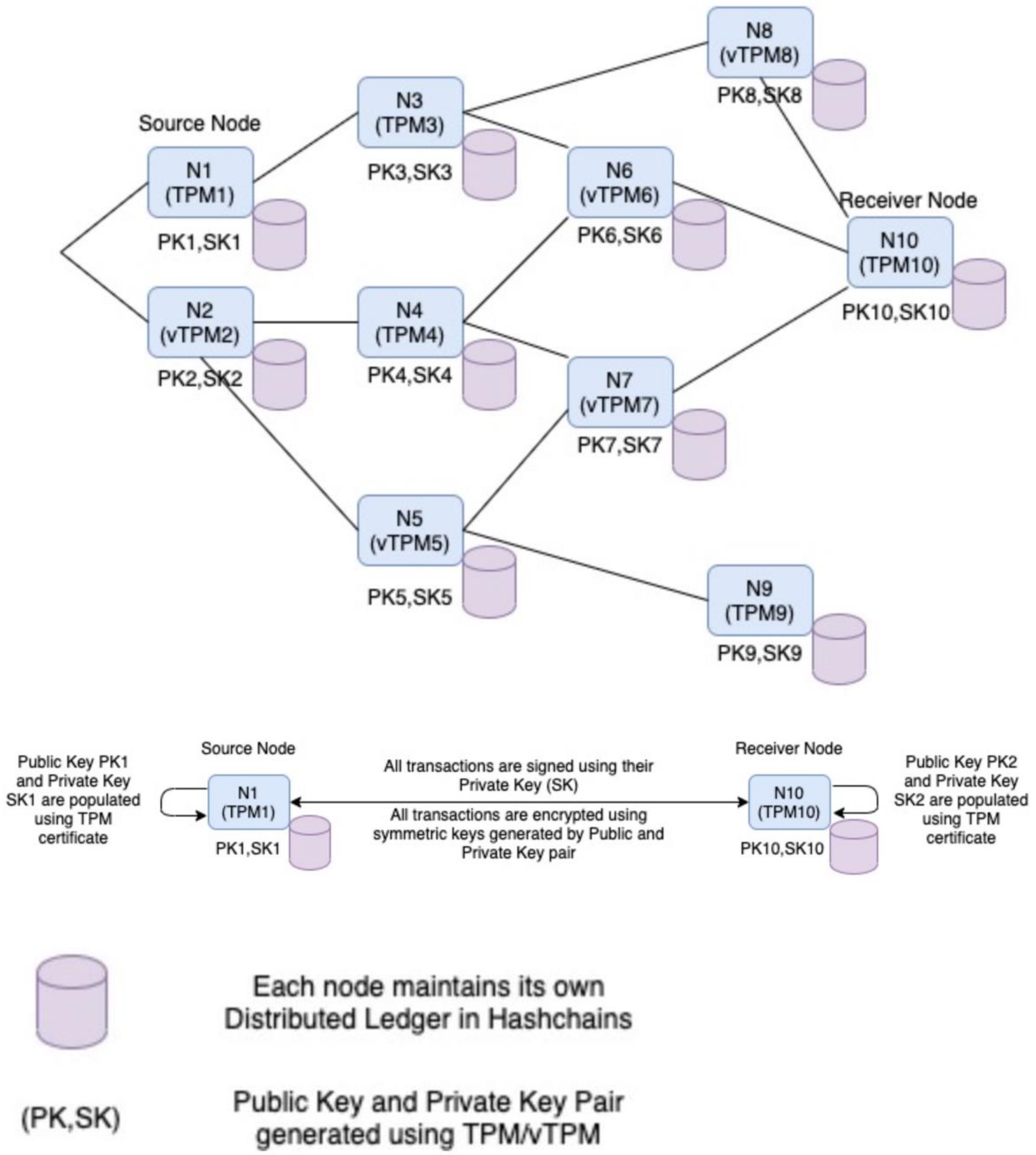
Source Node
N1 (TPM1)
PK1,SK1
N2 (vTPM2)
PK2,SK2
N3 (TPM3)
PK3,SK3
N4 (TPM4)
PK4,SK4
N5 (vTPM5)
PK5,SK5
N6 (vTPM6)
PK6,SK6
N7 (vTPM7)
PK7,SK7
N8 (vTPM8)
PK8,SK8
N9 (TPM9)
PK9,SK9
Receiver Node
N10 (TPM10)
PK10,SK10
Public Key PK1 and Private Key SK1 are populated using TPM certificate
Source Node
N1 (TPM1)
PK1,SK1
All transactions are signed using their Private Key (SK)
All transactions are encrypted using symmetric keys generated by Public and Private Key pair
Receiver Node
N10 (TPM10)
PK10,SK10
Public Key PK2 and Private Key SK2 are populated using TPM certificate
Each node maintains its own Distributed Ledger in Hashchains
(PK,SK)
Public Key and Private Key Pair generated using TPM/vTPM

Figure-1

In summary, the technique presented herein propose method to use TPM on the microchip (tamper proof) of Holochain nodes or vTPM on virtual nodes, to generate certified Public and Private Key pair. This method does not require complex Key Management system (DPKI). (i.e., Existing DPKI provides method to create new keys for nodes. In the technique presented herein, TPM/vTPM available on each node is used to generate its own keys. Existing DPKI provides method to revoke compromised keys and re-issue keys for the nodes. As in the proposal method, with the use of TPM/vTPM reduces compromised key threat and even TPM provides method to generate new key pairs. And, existing DPKI provides method to securely manage the private keys. With the proposed method to use TPM/vTPM, which implicitly secure the private keys). Moreover, this method provides trustworthiness among Holochain nodes using attestation method. Additionally, this method can be used to implement trusted Happs for cryptocurrency, to provide trust to the supply chain management system and, in general, this method can be used in Holochain based networks to enhance authentication and encryption along with trust.