TrustDer - Key Maker

Requirements Document Draft

Authors

Project Manager	Pramod Illuri <pilluri@andrew.cmu.edu>
Technical Team	Keshava Srinivas <keshavas@andrew.cmu.edu> Nithin Ram Gomatam Vasudevan <ngomatam@andrew.cmu.edu> Noora Alfayez <nalfayez@andrew.cmu.edu> Prerit Pathak <preritp@andrew.cmu.edu> Vaanya Gupta <vaanyag@andrew.cmu.edu>

Revision History

Version	Date	Change	Name
0	Sep 13, 2022	First draft of requirements	Keshava Srinivas Nithin Ram Gomatam Vasudevan Noora Alfayez Prerit Pathak Pramod Illuri Vaanya Gupta

Table of Contents

Introduction

Summary

The goal of this project is to develop a software-based information theoretic approach that allows device identity to be verified by network participants. This approach aims to be decentralized to prevent a single point of failure and be as effective as imprinting an identity in silicon.
Currently, the Keymaker protocol has been proposed which is a set of smart contracts, protocols and functions that create multiple shards, distribute shards to adjacent nodes and verify the identity of a device. The protocol has been proposed in theory but hasn't been deployed in a distributed system. This project would act as a Proof of Concept of the practicality of the protocol.

Scope

The scope of this project is to implement the keymaker protocol in its entirety on a distributed blockchain network as a smart contract. This is to be done by integrating and testing the entire workflow on 5 Raspberry Pi devices which will act as a proxy for a variety of DER devices.

Motivation

Currently, the method used to store identities of devices is imprinting a secret/identity information in a silicon chip such as an EEPROM or SRAM. These identities are verified using hardware cryptographic operations like digital signatures and encryptions. The disadvantage in this method is that the manufacturing cost of imprinting secrets in these types of silicon is high. Moreover, The hardware required to implement Secure Hash Algorithms for digital signatures is expensive. This method also requires an additional protection mechanism, to prevent invasive attacks, which would consume a lot of power.
The advantage a software based approach provides is that the identity of devices can be verified while preserving privacy, meaning it does not need an additional protection mechanism. In doing so, the cost and power consumption of the devices are also reduced.

Functional Requirements

FR-1	The system should successfully verify the identity of a device entering the network.
FR-2	The system should adopt a social verification mechanism using a suitable blockchain network to verify the identity of a device
FR-3	The Social Verification of a device identity should be implemented using the keymaker protocol involving Shamir secret sharing. The verification should abide by the following constraints: 1. Only k shards are required to perform the verification of the secret key. k<n where n is the total number of shards distributed 2. Any shard must not be a subset of the key 3. All shards combined must not reveal the key.
FR-4	The verification should utilize authenticated encryption along with the Shamir secret sharing (SSS) in order to retrieve the device key in case it is lost.
FR-5	The proof of concept should be thoroughly reliable for a blockchain network involving 5 raspberry pi devices.

Non–Functional Requirements

Note : Since the project is an early proof of concept for a research idea, NFRs doesn't have much relevance at this stage of the project. However, highlighting a few key ones to be kept in mind

NFR-1	The social verification algorithm must respond with consensus within <n> seconds *(YTBD)*
NFR-2	The developed proof of concept (POC) must be scalable to a large network of devices in the blockchain *(<number> YTBD)*
NFT-3	The performance of the verification system must be as effective as imprinting device credentials in silicon
NFT-4	The blockchain network should be reliable and not susceptible to attacks. The smart contract should be executed securely in all devices.

Constraints

1. Technical Constraints

1. Domain knowledge : Lack of adequate experience in blockchain technology
2. Choice of blockchain : Limited time to validate different blockchains to select the one that suits the requirements of the project
3. Choice of programming language: Dependency on the choice of blockchain used, availability of packages, and developer support

2. Business Constraints

1. Availability and cost of physical resources: The project requires purchase of at least 5 raspberry pi devices which incur a certain cost to the project
2. Initial cost of adding a block to the blockchain

References

1. M. Malik, “Digital Identity Management,” *YouTube*, 16-Sep-2021. [Online]. Available: https://www.youtube.com/watch?v=9XgmZtdlSBQ. [Accessed: 13-Sep-2022].
2. A. Shamir, “How to share a secret,” *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.