X.509 Certificate Transparency using Hyperledger Fabric Blockchain

Title	X.509 Certificate Transparency using Hyperledger Fabric Blockchain
Status	PROJECT COMPLETED
Difficulty	MEDIUM

Description

The security of web communication via the SSL/TLS protocols relies on safe distributions of public keys associated with web domains in the form of X.509 certificates. Certificate authorities (CAs) are trusted third parties that issue these X.509 certificates. However, the CA ecosystem is fragile and prone to compromises. Starting with Google's Certificate Transparency project, a number of research works have recently looked at adding transparency for better CA accountability.

Leveraging recent advances in blockchain development, we recently proposed a novel system, called CTB (Certificate Transparency using Blockchain), that makes it impossible for a CA to issue a certificate for a domain without obtaining consent from the domain owner (See https://eprint.iacr.org/2018/1232 for a copy of the paper). A proof of concept implementation of CTB is developed using Hyperledger Fabric. CTB works on top of the current certificate validation mechanism present in X.509-assisted SSL/TLS system.

CTB proposes a Hyperledger Fabric (HF) network among the member certification authorities by requiring each certificate authorities to play the role of endorsing peers and they belongs to different organisations (orgs in HF vocabulary). An organisation, representing internet browsers, is also created.

The aim of this project is to scale up the existing proof-of-concept implementation through several stages:

1. Development of client application for Certificate Authority organisation and Browser organisation facilitating access to the underlying fabric blockchain network.
2. Setting up the CTB over cloud.
3. Chrome extension for browser client application.
4. Benchmarking CTB-assisted SSL/TLS handshake duration

Additional Information

- The Chaincode, written in Go, for proof-of-concept CTB is available at https://www.dropbox.com/sh/vne21wpusk6yaq1/AABy8pB4jd14tIXdo1WFyO8Ra?dl=0&preview=ca-blockchain.go
- The CTB paper (https://eprint.iacr.org/2018/1232) has fair details on X.509-assisted SSL/TLS connections.

Learning Objectives

- CTB is a non-trivial use case developed using Fabric. The intern will be introduced fully to the background details on CTB that includes discussions X.509 certificates, SSL/TLS, openssl and Hyperledger Fabric architecture
- Expertise in writing chaincode
- Expertise in Hyperledger Fabric Client SDK
- Developing one fully functional non-trivial distributed application (CTB) on Fabric

Expected Outcome

Setting up and managing CTB Hyperledger Fabric Network on Amazon Web Services

Relation to Hyperledger

Hyperledger Fabric, Composer

Education Level

Graduate/Undergraduate student

Skills

-
- Previous Hyperledger Fabric experience (desired, but not required)
- Experience in Hyperledger Fabric Client SDK (desired, but not required)
- Experience in RESTful API
- Experience building a browser extension
- Amazon Web Services (AWS)

Preferred Hours and Length of Internship

Full-time (40 hours a week for 12 weeks during the summer)

Mentor(s) Names and Contact Info

Mahavir Jhawar, mahavir.jhawar@ashoka.edu.in, mahavir.jhawar@gmail.com

Deva Surya Vivek Madala, vivek.madala@ashoka.edu.in

Mentee Names and Contact Info

Harsh Jain, harshjniitr@gmail.com harsh-98

Summary Report