Project Progress Timeline: X.509 Certificate Transparency

Overview: This page outlines tasks and milestones in order to manage and achieve goals that are set for the "X.509 Certificate Transparency using Hyperledger Fabric Blockchain" project.

Project tasks and milestones

- [x] Week 1-3

- **Broader Goals for first Evaluation**
  - [x] Understanding CTB design (https://eprint.iacr.org/2018/1232)
  - [x] Running the existing proof-of-concept code for Hyperledger based CTB (HLCTB) network
  - [x] Building a proof-of-concept client/server application supporting HLCTB-assisted SSL/TLS connection

- **Work done**
  - May 27 - June 2
    - [x] Meeting with Prof. mahavir jhawar - Introduction and understanding the project
    - [x] Premier on using openssl for generating certificates and signing certificates by certificate authority.
    - [x] Read paper on CTB by mahavir jhawar: https://eprint.iacr.org/2018/1232.pdf
    - [x] Revisit Hyperledger key concepts: https://hyperledger-fabric.readthedocs.io/en/release-1.4/key_concepts.html
    - [x] Understand the structure of crypto-config folder where certificate for identity management are stored. (WIP)
    - [x] Run CTB network with two CA and browser organisations. Able to add certificate and query them.
    - [x] Reissue certificate while the previous one is active. I have gone through the go chaincode, *VerifyPKCS1v15* is at heart of reissuing certificate. But I am not able to understand what the signCert exactly is? Whether it is sign of newcertstring or newcertfile or sha256 of newcert using the current public key.
      - `openssl dgst -sha256 -sign currentCert.key -out sign.txt newCert.crt ,` `but this produces binary output and` *`VerifyPKCS1v15 is returning false.`*

  June 3 - June 9
    - [x] Create a github repository with POC of CTB network using hyperledger
    - [x] Reported issue related Wrong port number in build your first network
      ~~FAB-15602~~ - Wrong port number in build your first network CLOSED
    - [x] Understanding and running the basic-network, first-network and fabcar application of fabric-samples
    - [x] Write a blog on structure of crypto-config and how different keys are related

  June 10 - June 16
    - [x] Monday - Meeting with deva madala on progress till now and technical guidance
    - [x] Testing the HLCTB network POC written by deva madala (fabric 1.1) and understood how to connect to HLCTB network and executing the chaincode
    - [x] Modifying the HLCTB network by adding CA to each org and couchDB for each peers for fabric 1.4
    - [x] Besides the main goal, started with switching from direct container management to orchestration of containers using kubernetes
    - [x] Create the project timeline and meeting regarding the same
    - [x] Change in existing chaincode for proper revocation of certificates

  June 17 - June 23
    - [x] Using easybaas (VMware tool, https://labs.vmware.com/flings/blockchain-on-kubernetes) for creating the hyperledger related config for deploying on kubernetes and also modifying the same for incorporating the changes in fabric 1.4
      - https://hackernoon.com/how-to-deploy-hyperledger-fabric-on-kubernetes-1-a2ceb3ada078
      - https://labs.vmware.com/flings/blockchain-on-kubernetes
    - [x] Tuesday - meeting with Prof. mahavir jhawar regarding preparation for demo and current progress
    - [x] Create an application(SDK) for connecting to the network and executing chaincode functions
    - [x] Create a demo for server/client SSL PKI verification using HLCTB network
    - [x] Thursday - show the demo to deva madala

- [x] Write a readme on how to run demo server/client application for testing HLCTB network
  - https://github.com/harsh-98/ctb/tree/master/docs/run_demo.md
- [x] Friday- show the final step by step demo to Professor and deva madala and discussion of the second quarter plans

- [x] Week 4-6

- **Broader Goals for second Evaluation**
  - [x] Hosting the HLCTB over cloud
  - [x] FireFox Extension to support HLCTB-assisted https connections
  - [x] Development of an interface allowing registration of Certification Authorities to HLCTB network
- **Work Done**
  - June 24 - June 30

    - [x] Trying to add Yeasy/blockchain-explorer:0.1.0-preview to the hlf network.
    - [x] Added blockchain-explorer for fabric 1.4 on the HLF CTB network for easy monitoing of the transactions and the ledger.
    - [x] Created a script for automatic testing of network. Using this we can generate multiple ca, domains cerificates , push them to the network, renew the certs for domains and also revoke them. It uses the CA server as a proxy.
    - [x] Tested for serial processing of transactions for 100 domains and 5 times renewal of certificates and revoking them in the end. The network handled that, and blocks produced had one transaction each. Achieved a processing rate of 20-30 transactions per minute.
    - [x] Tested for parallel processing with the same settings as serial processing. Each blocks had upto 10 transactions and achieved a processing rate of 200 transactions per minute.
    - [x] Create a docker image of blockchain-explorer . It has two images , one for server and other for client.

  July 1 - July 7

    - [x] Raised issue on `Explorer not able to connect orderer from docker.` -
      ~~BE-676~~ - Explorer not able to connect orderer from docker. COMPLETE
    - [x] Attending mentors and mentees meet call.
    - [x] Adding caliper to network
    - [x] Testing using caliper for different number of transactions and tps while changing block size and batch timeout in configtx.yaml
    - [x] Adding swagger interface to ca server
    - [x] Adding authentication to ca server
    - [x] Deploying whole network on cloud with blockchain-explorer, ca server and caliper
    - [x] Making chrome extension

  July 7 - July 14

    - [x] Make firefox extension
    - [x] Add script for generating crypto-material and docker files for new CA organisation
    - [x] Adding new CA organisation to current HLCTB network(locally)
    - [x] Fixing queryCertificateHistory and adding creation of affiliation for orgs if not present
    - [x] Create pm2 process file for CA server, reports server and channel Config API.

- [x] Week 7-9

- **Broader Goals for third Evaluation**
  - [x] Scaling up of HLCTB: Simulation of https connections to sufficiently many HLCTB-registered domains
  - [x] Bench-marking HLCTB-assisted handshake overhead (on top of SSL/TLS handshake)
  - [x] Fine tuning of HLCTB operations for better efficiency and security

- **Work Done**
  - July 15 - July 21

    - [x] Monday meeting on caliper, firefox extension, CA server api and discussed further plan.
    - [x] Deploy network on cloud and joining new organisation to network present on different server(whole network contains of 2 server)

- [x] Patching TLS certificates of orderers and peers for including IP SANs and documenting the errors faced
- [x] Documenting how to add new CA organisation
- [x] Create transfer_asset script for transfer TLS certificate for CA server
- [x] Documenting how to connect CA server to CA organisation in HLCTB network

July 22 - July 28

- [x] Presentation on CTB and work done
- [x] Reading paper on scaling hyperledger handle order of 4 tps.
- [x] Adding demo for ctb-testing.ml using self-signed CA

July 29 - Aug 4

- [x] Meeting with mentor showing the work done and changes needed.
- [x] Adding demo for hfctb.ml using lets encrypt as CA

- [x] Week 10-12

- **Broader Goals for last Evaluation**
  - [x] Prepare report explaining completed tasks
  - [x] Certificate revocation
  - [x] Present your work done to hyperledger community
  - [x] Wrapping up and organising the codebase

- **Work Done**
  - Aug 5 - Aug 11

    - [x] Meeting with mentors on created presentation and suggested changes in it for better understanding
    - [x] Create more interactive presentation and also a demo video
    - [x] Looked into certificate revocation part and studied current methods CRL, OCSP, OCSP stapling and Must-Staple

    Aug 12 - Aug 18

    - [x] Attended Hyperledger internship presentation of other students
    - [x] Started working on report
    - [x] Setup a OCSP responder, webserver for handling OCSPERQUEST using ocsp npm package

    Aug 19 - Aug 25

    - [x] Meeting with mentors-- different ways of integrating currently available revocation models in HFCTB network
    - [x] Wrapping up and organizing the codebase