Security and Privacy Modeling and Implementation with XACML/ALFA and Fabric

Meeting Date: February 11, 2022.

Start Time: 2:30 PM

End Time: 3:40 PM

Attendees: Dr. Yue, Siddhartha Illa, Venkata Naga Bhaavagni Maddi, Farhana Shaik Begum, Sripada Vallabh Kaparthi, Ganesh Nyaupane, Preethi Vuchuru, Madhuri Koduru

Prepared By: Venkata Naga Bhaavagni Maddi

Items Discussed:

1) Siddhartha

Which team will be working on CA?

Dr. Yue.

a) Security team has to be working on the CA, and key focus should be on the security portion of the smart contracts. Work with RAs to understand Fabric network.

What are the tasks we should be working on?

Dr. Yue.

a) Try understanding the ALFA and eclipse plug-in, understand what a security policy is. Use the previous code as a reference. Read the Fabric sample, asset-transfer-abac.

How the smart contracts are authorized?

Dr. Yue

a) Authentication has to be done by CA and MSP, not by the smart contracts. ABAC helps us with this process. Rules are based on the attributes with the help of which we have control over who can access what.

2) Preethi

Which tool to be used for generating CA?

Dr. Yue.

a) You can use Cryptogen tool instead of the Fabric CA.

3) Ganesh

Shall we use minifab network or hyperledger fabric network in our project setup?

Dr. Yue.

a) Minifab is a simple tool for setting up the network, where as hyperledger fabric has a bit more complex script.

How internal CA works in the real-world scenario?

Dr. Yue.

a) Every organization will be having a CA, every CA has to be registered with Fabric. Root CA does the authentication process as we are using a testbed here.

4) Farhana

Are we using the static gateway or dynamic gateway in this project?

Dr. Yue.

a) We store data on every node. We donot need to make use of gateway in this project

5) Sripadh

How the front-end application can be linked with the block chain network?

Dr. Yue

a) No link was established in the earlier project, but make sure to test your security policy. So you would need a web client to test your security policy.

6) Bhaavagni

What kind of assets we would be working with?

Dr. Yue

The asset attribute may be stored in smart contract. We should be able to find out how to securely access those attributes. Make use of command line arguments and given inbuilt functions for creating assets.

To summarize, Dr. Yue explained about the Smart Contract algorithm that they are working on currently. Explained the role of API that is helpful for writing Smart Contracts, how we get the client id, what are the implicit asset actions. The invoker should be having the right privilege for a particular action (CRUPD), where P stands for partial update and how we execute an action.

Items for next week:

1) Understand ALFA policies.
2) Understanding how smart contracts can be invoked from JavaScript file.
3) Retrieval of attributes from Certificate Authority.
4) Understand BPMN diagram and UML diagrams.
5) Understanding ABAC.
6) Create a client application to test the smart contracts.