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

Meeting Date: March 4th, 2022.

Start Time: 9:00 AM

End Time: 10:40 AM

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) Madhuri Koduru

Gave a demo on the security policies using the vscode Alfa plugin. Explanation on how attributes are defined, how the policies were written, how conditions are evaluated and how rules take precedence. She also identified a website named enforcer.identityserver.com to test the policies identified.

2) Sripadh (Working on Attributes and requirements document)

Could you please explain the point " G.A, where G is in the upward ancestor group path of A. This is not implemented in P2 to reduce complexity." in Object Attributes of updated ABAC Design & Implementation document?

Dr. Yue: Object is the asset that you store in the Block Chain. Resources is also defined as object that is stored in block chain and somebody would like to request asset and therefore everything which is stored in the blockchain is a subclass of object. Refer to the UML diagram for more information.

3) Ganesh (Working on CA and MSP)

Why the attributes and policy is defined separately?

Dr. Yue: It is a standard way to define the attributes and policy to be separate, so that whatever the attributes are there they can be used by the policy.

4) Sidhartha (Working on CA and MSP)

How the action attribute partial update will be evaluated?

Dr. Yue: When we call a Smart Contract, the parameter we pass is the asset action. Many assets could be sharing the same action. All the attributes update and partial update is conceptual. There are no clear rules on how we can differentiate the full update and partial update.

5) Farhana and Bhaavagni(Working on the Smart Contracts)

How are the attributes being passed into the Smart Contracts?

Dr. Yue: Make use of Fabric contract API that you use for passing the values to smart contracts. Make use of source file contract.go, contract_chaincode.go files. There will be a list of user-specified asset actions, those are input parameters. The input parameters have to be created by the invoker.

Dr. Yue's Summary: Explanation about the Change request policy. Understanding the context of the BCAsset document. The policy condition is that if you are the CISE from the lead organization of a project,

you can create a new change request document. However, CISE cannot set initial value of CR decisions.

Some attributes are stored in assets and among them some are subject and object attributes. We assume the object as the new BCAsset object to be created. When submitting a change request, We are creating a change request. It is an object to be stored in the block chain. New request is the new object that will be inserted into the block chain. The way we define the new object is an action.. When we change the action, we should also change the object. The action.newobject.assetType applies only to CR new object that will be inserted into blockchain. The action Id is passed by the invoker and the invoker is working on leader organization.

Explained about Update Change request. Who can make updates to CR is defined. Only CISE from lead organization can update the existing change request. However, CISE cannot change the values of CR. The CISE of a project cannot update a new CR for another project that he is not the CISE. Here the existing BCAsset object is updated. We should note that the actionID is also passed in by the invoker as a part. Here the actionId would be "U" i.e the full update. We update the decision that we already have with the new decision which we get. Although the CISE can update a change request, it cannot update any change request that is already done or same as the existing Change request decision. Also, a new policy is created.

Make CR is another policy that is explained. We are making the CR decision on the change request. The decisions are arrays. Here this policy will be permitting the addition of a CR decision into a change request object. For example, here the chairman from the control board of a project can change the decision. The CBM of a project cannot update the CRDecisions of a CR for another project that she is not the CBM. If the actionId is "p", i.e it means it is the partial update. Also, the ControlBoard maybe a virtual organization instead of a physical organization. Refer to Blockchain augmented organization. Need further research on how we can set this up. We also need to change the roles in attributes file, we may also need to differentiate between the manager and 'chair' of the control board in the future. The attribute update gives the lists of attributes that the attribute can update. The chair of the control board can only update change request decisions, but not other attributes. It is a partial update(P). Multiple Smart Contracts maybe using the same policy. The parameter which we pass to the smart contract is called as the asset action.

Items for next week:

1) Developing an external javascript application for invoking Smart Contracts.
2) Making improvements to the requirements identified from the BPMN Diagram.
3) Writing some example Alfa policies.
4) Accessing certificate attributes in smart contracts.
5) Adding attributes to the identities.