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

Meeting Date: April 22, 2022.

Start Time: 2:00 PM

End Time: 3:40 PM

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

Prepared By: Venkata Naga Bhaavagni Maddi

Items Discussed:

1) Sidharth (Developing the Security Policy)

Clarified the details about the JSON Schema AssetAction and BCAssetSchema.

Dr. Yue

Your JSON Schema is newer version and the JSON file is older version. It is that the required fields are mandatory but you can also include other attributes if necessary. When the sample json is created the BCAsset is declared as string, is it the object or string? The BcAsset is not a string, it is representing the entire JSON Schema. We donot want to include external schema file for validation. But, the actual content of BCAsset should be a deifnition of all 10 different kinds of BCAssets. Using BCAsset schema, we have prepared a sample JSON file. You are supposed to create a JSON object in Golang. Your JSON structure is missing a JSON descriptor, Where the marshalling and demarshalling is done? As the key and struct names are same here, So we are not doing the marshalling and demarshalling. For any BCAsset, the struct is defined with the necessary fields, all that data is present in that object. For change request, the cr decision is empty, remaining are not empty. So based on Assettype we are supposed to store the required data and not store the other data? That's the null problem, you need to specify a way in which you can solve that. For example, in the MBSE model, you don't have a change request field. When we convert the struct to JSON, there are null values. If we are using static struct, try to resolve null problem, it is a common problem in NoSQL database. So you are required to try creating your own marshalizer and demarshalizer. Your teams static struct should demonstarte the marshalling and demarshalling, try to solve the null value problem.

Queries on Security policy

(a) Can you brief about the ReadCR policy in updaterequestpolicy. There is a condition like action.newobject.CRDecisions == object.CRDecisions, what does object object.CRDecisions mean in here?

Dr. Yue

CanupdateCR policy was used for creating ReadCR, that conditon is an error. Try to exclude it from the ReadCR policy.

(b) In the DocumentPackagePolicy of CreateDocumentPolicy, the DocumentPackageStatus is not included in the BCAsset.

Dr. Yue

JSON Schema might not be updated. All the ideas are usually converted to some kind of attributes. The

document package might be linked to the cr decision. All the attributes that are used in the document policy are present in the standard-attributes.alfa file.

Discussion on Smart Contract

Whenever the CreateCR is invoked, the JSON is passed a string to the smart contract. Later it is unmarshalled to an object. Then, the security policy CreateCR is called in which all the conditions are being checked and a boolean value is returned. If the return type is True, then the execution of Smart Contract continues else the invoker is not authorized to create a change request. Before storing it into the database, the data is marshalled. Gave an overview about CRDecisionStruct condition.

Dr. Yue

There are two main issues in here, your crdecision maynot have an empty field initially. The struct you are constructing is not having an empty value, it has all fields, every field with an empty value. You need to make sure to check properly the object field. Preethi suggested that there is a package that can help to deal with dynamic struct. The fabcar is not having this problem. The internal gaps package is also internally using the marshal and demarshal of JSON.

2) Ganesh and Sripadh

The program is making use of in memory wallet and postgres wallet. Any submissions that will happen are stored in postgres wallet. Also, there are import and export functions in postgres wallet to store it into the in memory wallet. A connection is present with the Fabric network client to invoke/submit the transactions. But, we are using the file system wallet in the test network. The authentication between the fabric consortium and the fabric MSP is under research. The identity is stored in the wallet and the postgres database as well. (Status Update)

Do we need to store the identities in CouchDB, File system or in memory wallet?

Dr. Yue

You need to configure your client in such a way that your client will have an in memory wallet. When you are using in memory wallet, you probably need to use few methods. So, use the in memory wallet.

3) Farhana and Bhaavagni (Implementing the Smart Contracts)

Can you brief us more about the marshalling and demarshalling of JSON object?

Dr. Yue

Shown an example of Sample BC Document, this sample file is only having 10 top level attributes. But your definition might include more than 40 attributes. The serial object has to be converted to a Golang object (deserialized). This serialization has to be done in such a way that you handle the null values. For example, in few cases, you are supposed to include the null values as well. After converting that might be a string, so you are supposed to deserialize it back to the object. This is an issue.

What is BCAsset type constraint property in BCAsset schema JSON file?

Dr. Yue

It is a technique for dealing with data integrity. In the MBSEVariant model, here the variant model is defined as a base model. Suppose your model is a gateway summary, this gateway summary is derived from the base model. It means, there can be many variants of the same asset. The constraints can be like a foreign key for any BCAsset Id etc. So, this BCAsset type is a way to specify the various types of constraints. For example, for the BCAsset type, the version cannot be a null value. You are not required to do anything with this, but the referential integrity is very crucial and has to be implemented. So, the BCAsset Id here can be considered as a primary key.

Items for next week:

1) Implementing the Security Policies.
2) Postgresql wallet and in memory wallet configuration.
3) Implementing Smart Contracts.