Authorization Techniques and Strategies

> ⚠️ *draft and subject to change as it is reviewed*

Link to top level of Access Management Recipe

Preamble

Any (useful) application written has some form of authorization about what it will do on behalf of the user. This is an attempt to capture some of the different approaches and contrast their benefits and drawbacks.

To frame the conversation, we must:

- start with the assumption that an identity presented to the application is a bona fide one.
- there may or may not be additional information in the payload about the identity (name value pairs, x509 attributes in the payload wrapper)
- the context of the authentication mechanism may be useful to know
- the context of how the data is asserted to the application may be useful.

Common techniques are catalogued below:

Authorization Techniques	Centralization Friendly?	Decentralization Friendly	Observations	Benefits	Drawbacks	Scaling Technique (s)
Attribute based Approach (What you are.)	Can be	Yes		Applications manage everything so are flexible to choose what to observe	Applications manage everything so are flexible – fragments consistent behaviour across apps	
Claims based Approach (What someone says about you)	Y	Yes, but conditionally				
Group/Role based Approach (What you belong to.)	Can be	yes, but conditionally				
Rule based Approach (What the application computes about you)	Can be	Can be				

Rule Based Approach

- happens today, but consistent application across applications hard as it will be encoded in each implementation in the code (PHP/Java/Ruby /Grails/perl/etc)
- Is a mashup of the Attribute, Claims, and Group/Role based approach together with logic operators (AND/OR/NOT)
    - e.g. allow person is authorized to click submit button IF their AcademicCareer=BSc AND if their AcademicLevel=2 AND IF they are in group=MATH201-1-Fall AND if their Claim=Student and NOT instructor
- allows for maximum flexibility, but architecting an approach across the application space drives necessity to:
    - have some datamodel to point to that transcends applications
        - e.g. insure student means student...and answer these style of questions: Is this true?--> group(student) == Claim(student) ?
        - How about: Person is member in group(Stats200-1-Fall) imply (==) academicCareerLevel=2? Uhg!
    - find a consistent way to capture rules, preferably in a re-usable format (XACML sounds right, but heavy)

On this last point, there is a possibility to centralize the decision process into the the Shib Identity Provider and trigger a rule being evaluated via a scriptlet to populate a value (for example:'IdPSuccessfullyAuthorized=true) upon proper conclusion of the rule evaluated in the scriptlet.

- This is a simplistic example of a yes/no answer for wholesale access, but more elegant rules can be written with any number of conditions
- In the Shib world, begs the question of whether or not these rules can be housed in the resolver as a central repository of logic for authorization & policy enforcement point: https://wiki.shibboleth.net/confluence/display/SHIB2/ResolverScriptAttributeDefinition and the results passed on downstream to the application via simple attribute population. (an authorization protocol within a protocol if you will – yes provocative, but why add more machinery when you can do it today?)

Groups & Roles vs Entitlement (Privileges)

<pending>

Centralized vs distributed models

<pending>

- Classic model is distributed & most everyone's reality today --> everyone decides for themselves what works and what they will use to authorize on.
    - rife with all the problems of don't know what depends on what, who is responsible for what and when
- A controlled distributed model is one which has some structure and intent on decentralization

Mix and Match or Hybrid Approach

<pending>

Calculating Costs

<pending>

Access Management Work in the Community Identity Framework for Research and Education (CIFER)

CIFER is a cross-consortial collaboration between Kuali, Internet2 and Jasig to develop and support a comprehensive open source solution for IAM for higher education and research. One of the core work areas is Access Management. There are and will continue to be close ties between Paccman and CIFER teams. Links to CIFER work include the following (Note that some of the materials are still under the pre-CIFER acronym, OSIdM4HE):

- http://ciferproject.org
- https://spaces.at.internet2.edu/display/OSIdM4HEteam/OSIdM4HE+Team
- https://spaces.at.internet2.edu/display/OSIdM4HEteam/Access+Management+Team