Return to Advance CAMP wiki

Advance CAMP Thurs, Oct. 19, 2017

10:20pm-11:10pm

Pacific C Room

CAR (consent-informed attribute release) Demo and feedback

CONVENER: Rob Carter

MAIN SCRIBE: Marwan Shaher

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: 23

DISCUSSION:

CAR: Consent Informed Attribute release.
Having the user/institutions be in control of what attributes they are consenting to releasing and what is done with those attributes.
Demo with Logging to CILogon

- After login, you are presented with an intercept page for consent to release attributes
    - Email Address, Legal First and Last name, Display Name, Scoped NetID
    - Ability to proceed with permitting/denying all or to edit every attribute in the list

Question: Ability to select one attribute value for multi-valued attributes (e.g: email address, group memberships, etc..)?
Answer: Yes, CAR supports per value consent, not just per attribute consent.
Part of the informed consent information, consume the privacy policy URL, Relying Party Logo and Description (in the future there will be trust marks for the relying party to provide the user with further information about the trustworthiness of the service they are trying to access).

Workflow: The user logs in against the Idp, the Idp sends a signed JWT with the attributes that the SP requested to the CAR system, the CAR system unpacks the JWT message and presents the consent page for the user to make an informed decision.
The user once the decision is made about the attributes has the option to save the decisions about the relying party and future relying parties, just for this one time, and not to save the changes at all.
Question: If the user choses to save his/her settings, is there a way to change these settings at any point in the future?
Answer: Yes. There is a self service interface whereby users can view and edit all their saved consent decisions. Information about the relying party name, URL, last update date, and a link to manage/change the policy for that particular relying party.
Selecting to manage/change the policy for a particular RP presents another screen with the attributes names, the value(s), the current choice of the user, and the institutional recommended release policy for that particular attribute.
The choices available for user policy on attribute (all values) or attribute (specific values) are:

- Permit
- Deny
- Ask Me
- Follow Institutional Advice (which is subject to change)

There are two other settings that the user is presented with in the self service interface:

- All Other Information: What to do with attributes that are not listed but that the relying party maybe asking for
- While I'm Away : What to do when user is not in web flow and not present to ask (out of band/offline requests from resource holder)

Question/Comment: two relying parties, one internal and another external. The external could be relying on the first's. Is the user presented with two consent screens even though they may not know about the "proxy" service.
Answer: it can be configured to either present or to hide the consent for the "proxied" service. This could be an institutional consent policy.
Revocation is essentially a change of consent policy. In the policy database, every version of the policy update is kept, so previous versions can be reviewed and audited.
Question: should this be called "policy manager" or "consent manager"?
Answer: the interface is fully skinnable, so it can be customized according to the organizations' likings. There is also support for multi-language support
Question/Comment? Interested in the cost of running the service,

Answer: The service is horizontally scalable. Each component depends on the database, which ideally should be running in HA. The service could run on the same server as the database if desired.
Question: Have you done work to integrate with CAS or other non-shib auth services?
Answer: Not yet as far as doing the work goes, but this is not just a shib-only solution. It should work with any authentication service.
Question: How many people would be interested in buying into a multi-tenant solution for this?
Answer/comment: There has been discussions in the SAAS world about this. If you're going to have multi-tenancy that is shared, it is better to do multi-instance solution

ACTIVITIES GOING FORWARD / NEXT STEPS:

- Replacing UI for intercept and self-service
- Building out admin interfaces (policy admin and config admin)
- Code available Jan 2018

=====

Note: please be sure to link to or attach any key resources from this breakout session