Return to Advance CAMP wiki

Advance CAMP Monday, Oct. 5, 2015

11:20am-12:10pm

Room 22

Attribute Release and User Consent

CONVENER: Ken et al.

MAIN SCRIBE:
Chris Phillips
Ni

ADDITIONAL CONTRIBUTORS:
Gabor Eszes (Old Dominion)
Jeremy Rosenberg
Mike Grady
trscavo

# of ATTENDEES: ~30

DISCUSSION:

IdPs have turned out to be “attribute retentive”
Did we make some mistakes in eduPerson that actually make this space more difficult? Let’s see.
  mistakes such as all group memberships in same attribute

R&S was a reaction to that difficulty in getting institutions to release attributes

SWITCH invented/created uApprove

SWITCH also maintains attribute release profiles centrally. These get pushed out to IdPs that choose to implement the profile (or not).

https://www.switch.ch/aai/support/tools/uapprove/

- They do the hard work of interacting with relying parties
- Which attribs are required? Which optional?

eduGAIN is a game changer.

Selective release of multivalued attributes

What do we do about proxies and gateways, where there might be two different layers of attribute release -- additional attribute authorities being consulted at proxy layer (or SP etc.)?

NSTIC grant: Scalable Privacy
Citizen-centric schema
Attribute release and consent

In the EU, consent is neither necessary nor sufficient (hmm, so what good is it?)
Is there a different situation in the US? Let's see

Consent options:

- client specific
- Shibboleth IdP V3:
    - client-side consent enabled by default
    - a server-side version is being worked on
- infrastructure (e.g., UMA)
- federation metadata for carrying user-focused info on attributes being requested and why?

ORCID consent is built on the OAuth2 model

Do users understand the consent options they're presented? Do we have an existence proof that consent actually works? Yes, there is some since other federations have been dabbling in consent for years.

See LARPP wiki for more info on this, a few links to research and surveys:
https://wiki.larpp.internet2.edu/confluence/display/LARPP/LARPP+Home
in particular: https://wiki.larpp.internet2.edu/confluence/x/aoAw
https://tnc15.terena.org/core/session/34

Consent gets IT (and the lawyers) out of the loop, which is itself a Big Win

Consent characteristics:

- informed
- fine-grained
- revocable
- human palatable
- suppressible
- required vs. optional
- offline vs. inline (in-band vs. out-of-band)
- consistent user experience

Discussion about user primacy versus institutional primacy in release decisions, about faculty asking students to use arbitrary service X (no institutional contract), usefulness of anonymized (opaque, non-correlatable other than by institution) identifier, etc. About EU directives that it isn't consent if user needs to access service to do their job, courses, whatever

Shib IdP v3 -- Consent built-in, based on uApprove, tradeoffs in consent storage choices, option to turn on per attribute consent

ORCID -- fine-grained control on what is or isn't released, dialog to release to a given service, Oauth2 underneath, opt-out, human palatable language

Info about PrivacyLens (see LARPP website above), CMU research on informed consent user interface, planned work, provide API

show the values of the attributes or not?

ACTIVITIES GOING FORWARD / NEXT STEPS:

If slides are used in the session, please ask presenters to convert their slides to PDF and email them to acamp-info@incommon.org