UserSelectAttributeReleaseUseCase

A Proposal for a User-Select Attribute Release Management Mechanism

Status: Early Draft (from Albert Wu)

Update: There has been discussions in Shib-dev about incorporating this capability into Shib 2.2. Stay tuned.

Overview

A recurring problem in deploying Shibboleth is answering the question:

Which attributes should this new SP see?

So far, most have tackled this question from an institutional data release policy angle, i.e., the SP submits a request to the proper data stewards, wait a few days to a few weeks, get answer back. Get data for a not so precise population of people with exceptions here and there.

Things get worse in a federated scenario (think Dreamspark). This attribute release negotiation become a discussion measured in months, even years.

A better way to address this problem may be to shift the decision of data release (at least personal data such "who I am" and "what roles I play") to the individual signing onto the resource.

Proposal

We propose placing a filter on an Shibboleth IdP such that:

Upon successful login, the filter checks to see if the user has an existing attribute release policy for the SP. If not, it presents the user with a somewhat intelligent page describing what it knows about the SP and offers the user a set of data release choices specific to the SP. Optionally, it remembers the user's preference for future sessions.

Telling the user what we know about the SP

In order to help the user make an informed decision, the IdP should disclose security and trust information relevant to the SP such as:

- What is the purpose of this SP?
- Who operates this SP?
- How secure is the SP's environment?

For the first 2 items, we are proposing within UCLA a trust level scale:

Registered: A "registered" SP is any SP that has presented valid meta-data to our IdP either via a bilateral or federated relationship.

Trusted: A "trusted" SP is a registered SP whom we have vetted. It is operated by a trust-worthy entity.

Endosed: An "endorsed" SP is a trusted SP performing official university business functions.

Separate to the trust level, we are proposing to disclose whether an SP has been subjected (and passed) to the latest campus security scans (UCLA's Security Office offers an application security scanning service).

Seeking attribute release acknowledgment from the user

In order for this mechanism to work, we believe that the user interface has to be designed in such a way that a user can comprehend and make release decisions in just a few seconds. Therefore, the UI should group attributes into logical groups and presents the choices at first in high level chunks, while offering options to drill down for more fine grained release choices.

An example of the top list of choices may be:

- Tell the SP who I am.
- Share my email address (click here to release additional contact information)
- Describe to the SP how I am affiliated to the university.

Issues

- How will the user "reset" or "change" her attribute release preference?
- How will the institution be able to override the individual's choice?
- What kind of helpdesk overhead are we anticipating?
- Should the user be able to set "global" preference?