Making Federation Easier: Default Attribute Release and User Consent

IAM Online
February 8, 2017

Liam Hoekenga, University of Michigan

Mark Scheible, MCNC

Keith Wessel, University of Illinois at Urbana-Champaign

IAM Online is presented by InCommon, Internet2,
and the EDUCAUSE Higher Education Information Security Council

INFORMATION AND TECHNOLOGY SERVICES
UNIVERSITY OF MICHIGAN

Giving Users Control: U-M Attribute Release Policies

Liam Hoekenga (liamr@umich.edu)
ITS Identity and Access Management

History

- May 2009: Production Shibboleth IdP deployed
- January 2010: uApprove in production; Creation of default attribute bundle
- January 2012: U-M begins staged transition to Google Apps for Education
- March 2012: U-M deploys box.com
- March 2012: U-M starts wide-scale provisioning to GAE
- October 2015: U-M upgrades to IdP 3.x, migrating from uApprove to bundled consent engine

Attribute Bundle: Goals

- Allow users to access InCommon Service Providers without having to contact the IAM team and request additional attribute release.

Attribute Bundle: InCommon, REFEDS R&S

- eduPersonPrincipalName
- eduPerson(Scoped)Affiliation
- eduPersonEntitlement
- mail
- displayName
- givenName
- sn
- *eduPersonTargetedID*

Attribute Bundle: U-M

- eduPersonPrincipalName
- eduPerson(Scoped)Affiliation
- eduPersonEntitlement
- mail
- displayName
- givenName
- sn
- *eduPersonTargetedID*
- **uid**

Attribute: Policy

- Requests to release attributes not included in the bundle need to be approved by the appropriate data stewards.
- The release of attributes to contracted service providers requires the completion of a Data Protection Agreement, regardless of data sensitivity

Attribute: Policy

- If contract, release agreed-to attributes (in place of / in addition to default bundle)
- If local federation, release default bundle with consent*
- If InCommon, release default bundle with consent
- If R&S, release default bundle with consent

** We are reviewing our consent policy with the goal of clarifying the population of SPs that can request that consent be suppressed.*

Consent: Goals

- Notify users that information is being released
  - What information?
  - With whom?
- Allow users to authorize the release of information
- Satisfy FERPA compliance and local PPI policies

Consent: Deployment

- Original - prompt every user on every access
- Present - ask for consent annually for external services
- Configuration
  - Store attribute release consent in SQL database
  - Redisplay consent when…
    - The values of already approved attributes are updated
    - Additional attributes are added to the release filter
    - Anniversary of first access
- Localization
  - Branding

Consent: Use Cases

- **No confirmation needed.** Services provided by the university through an agreement with another provider -- such as M+Box and M+Google -- do not require user confirmation for attribute release.
- **User confirmation needed.** Before a person's attributes are released to an institution or provider for a non-university service, that person is asked to decide whether his or her identity information will be released. When a U-M user attempts to access the resource at the host SP, the user will be presented with a listing of the attributes that will be released. The user will be asked to confirm or deny the release of the information.

Consent: User Acceptance

- Not applicable

Consent: Process

- How are users provided information to help them make their consent decisions?
  - Documentation
  - Boilerplate on Consent screen

Consent: Revocation

- U-M does not currently provide a method to revoke consent

Consent: Policy

- Under what circumstances would we revisit our consent policies?
  - Passage of new state / federal privacy mandates
  - Expansion of services / managing UX
- Who would make the decisions?
  - Information and Infrastructure Assurance Domain

Consent: Feature requests?

- Data sanitization
- Ever-present release consent

What would we do differently?

- Bundles...
  - –FERPA / “private” users
  - –Release only required information
- Consent…
  - – TOS?

Questions?

Resources

- Data Stewardship at the University of Michigan
  http://safecomputing.umich.edu/protect-um-data/data-stewardship.php
- Governance: Information and Infrastructure Assurance
  http://cio.umich.edu/governance/assurance-domain.php
- U-M InCommon Attribute Release Policy and Procedure
  http://documentation.its.umich.edu/node/262/
- Securely Accessing External Institutional Resources Using Shibboleth
  http://documentation.its.umich.edu/node/260/

How UIUC Implemented User Consent in Six Months and Lived to Tell About It

Keith Wessel
Identity and Access Management

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Before Consent

- Liberal attribute release policy for InCommon and eduGAIN
  - R&S bundle to all SPs for non-FERPA-suppressed users
  - Not so great for FERPA-suppressed users
- Campus SPs requested attributes using our federation registry
- Other SPs configured manually

The spark that started the fire

- We worked with our registrar when deciding default attribute release to eduGAIN
- We let the IDP V3 user consent cat out of the bag
- Registrar's office saw this as a much better way to handle attribute release policy
- And so it began

Wessel's secret recipe: Step 1

- Get the right people on the same page
  - Registrar
  - User experience
  - Security/Privacy
- Demo user consent to all parties involved

Wessel's secret recipe: Step 2

- Break services into groups: InCommon/eduGAIN, R&S, local, etc.
- For each group, decide:
  - What to release
  - For which users
  - Is consent needed for some or all users?
- * Make educated guesses
- Present to your team in a digestible form

The digestible form

Federation	Category	Attributes requested?	Attributes released	Consent
InCommon & eduGAIN	Global R&S SPs	N/A	R&S bundle	FERPA-suppressed only
InCommon & eduGAIN	SPs with contracts	Yes	Requested attributes only	No
InCommon & eduGAIN	Other SPs	Yes	Requested attributes only	Yes
InCommon & eduGAIN	Other SPs	No	R&S bundle	Yes
University & non-federated	All SPs	Yes	Requested attributes only	No

Wessel's secret recipe: Step 3

- Design your consent screen
  - We specifically used the words "information sharing"
  - Friendly names for attributes are essential
  - Consent to everything and don't ask again can make security nervous unless worded carefully

ILLINOIS CONSENT TO SHARE INFORMATION

You are about to access Shibboleth.net Wiki. The service needs the following information:

Full name	Keith W Wessel
University affiliation	member
Service entitlement	urn:mace:dir:entitlement:common-lib-terms
NetID@illinois.edu	kwessel@illinois.edu
E-mail address	kwessel@illinois.edu

Learn more about sharing information with services.

Select how you would like to share your information, and how often you would like to be asked about this setting:

- ○ Share now, and ask me every time I log in.
- ◉ Share now, and ask again if the information I need to provide changes.
- ○ Always share with all services automatically, and do not ask again (this setting can be revoked at any time by using the checkbox on the login screen).

Proceed | Do Not Share

Wessel's secret recipe: Step 4

- Determine consent storage
  - Database means adding a dependency
  - Cookies means users must consent from each device
- We didn't want users to see the consent screen any more than necessary
- * So, we made as stable of a dependency as possible
- We also chose to have consent decisions remembered for one year

Wessel's secret recipe: Step 5

- Identify exceptions
  - We didn't want InCommon SPs with explicit contracts to prompt for consent
  - * We had a few locally configured SPs that needed consent
- Tip: Avoid IDP restarts by tagging entities in metadata for exception SPs

Wessel's secret recipe: Step 6

- Publicize: people get concerned about new pages in the login process
  - Give support staff and IT professionals a sneak peek
  - Communicate to users, or at least to those supporting them
  - Have a good knowledge base article explaining what this is about

How did we do?

- Our help desk has received no measureable amount of questions about user consent
- In the first five months
  - ~24,500 users have selected to have selection remembered
  - ~2,800 users have selected to not be asked again for any service
- So far, we're living happily ever after

Questions?

Keith Wessel
kwessel@illinois.edu

Summary

- An attribute release policy should be in place at every institution
  - Otherwise, it results in **frustration** for your users
  - and **makes more work** for you when users ask for SP-specific ARPs
- If your institution has **researchers or collaborators**, it is **most important** to adopt and release the R&S attribute bundle to R&S SPs (not the world)
- If you're already releasing attributes to R&S SPs, why not **release a default attribute bundle to any SP**, as long as your users consent to the release of their information
- **Implementing Consent** (through IdPv3) puts attribute release **in the hands of the user**, and should help with getting your data stewards to agree to a "well articulated" attribute release policy
- "**Consent**" is a globally hot topic
  - latest draft revision of NIST SP 800-63-3(C) Section 9.2 discusses user notification and consent
  - other consent work being done on several fronts (e.g. European meetings, KANTARA)
  - progress on Scalable Consent and CARMA (Consent-informed Attribute Release MAnager)
- *Please work with your data owners, develop default attribute release policies (including adopting R&S) and plan to implement Consent as soon as possible*

IAM Online Evaluation

Please complete a short evaluation of today's presentation

https://www.surveymonkey.com/r/IAM-Online-Feb-2017

Upcoming Events

Internet2 Global Summit - April 23-27, 2017

Washington, DC http://meetings.internet2.edu/2017-global-summit/

Shibboleth Installation Workshop – April 4-5, 2017

University of Michigan – Ann Arbor

Registration Opening Soon