OpenID to SAML Gateway

Chris Hubing
cjh@psu.edu
Emerging Technologies
Information Technology Services
The Pennsylvania State University
Goals

1. Enable OpenID protocol without having to make changes to the Service Provider side

2. Ability for google/yahoo userids to appear as their email address
   - hubing@gmail.com rather than https://www.google.com/accounts/o8/id/id=AItOawl27F2M92ry4jTdjiVx06tuFNA

3. Make it secure
How it works

• Shibboleth IDP inside an OpenID relying party (mod_auth_openid for Apache)

  • Translates OpenID attributes into SAML and send them to SP

  • No changes on the SP side needed to consume these OpenID users (other than WAYF/DS)

  • Other services on campus (and outside) could use Shibboleth software and our OpenID IDP to "federate" their applications

• Only trusts email attribute sent by google or yahoo

• Rogue IDPs could send email attributes that don't match their OpenID scope

  • Additional code added for scope checking
**Example SP**

Federated WikiSpaces https://wikispaces.psu.edu/
- Confluence software
- >21,000 users
- >2,500 spaces
- spaces are self-provisioned
- Just an SP in InCommon Federation
- also has metadata for non InCommon IDPs (FPS, OpenID)

**Uses**

- Faculty Communities (180+ disciplines at Penn State)
- Biology 110 online textbook (1000+ students/semester)
- Center for Lignocellulose (DoE grant)
- CIC Auditor’s group
- Lots of Administrivia
Demo
What it’s Not

• It’s not account linking
• Users are not joined into a directory
• It’s not a registry

It’s just another proxy logon service
The Good: Allowing Access to Institutions not in InCommon

Chris

is not an InCommon schools but are part of our group. Their auditor has a gmail acct. Can you add it to the list so that he can test the access?

Gary

-----Original Message-----
From: Big Ten I/S Auditors [mailto:****@lists.psu.edu] On Behalf Of
Sent: Wednesday, November 10, 2010 3:28 PM
To: B10EDP-L@LISTS.PSU.EDU
The Bad: Inconsistent Attribute Release Policies

Ok, cool. Here's something to investigate when you have a moment....

I have a guy from [redacted] that I've given permissions to the [redacted] space on wikispaces. When he tries to log in using his [redacted] creds, he gets trapped in a redirect loop. I've fallen back to having him use an OpenID, but I'm curious as to what is happening to his login. When you get a chance, could you find out what happened to [redacted] when he tried to log in today between 11:16 and 11:40? I'm assuming it's not releasing the correct attribute(s) needed for wikispaces login.

Seriously, no rush. I've verified that he's in with his OpenID and can access the space.

Thanks!
J.
SHIB IDP ADMIN

Y U NO RELEASE EPPN
BY DEFAULT
Questions?

https://wikispaces.psu.edu/display/EmergingTechnologies/OpenID+Implementation+for+WikiSpaces

Chris Hubing
The Pennsylvania State University
cjh@psu.edu