Shibboleth and Federation: The Second Decade

Scott Cantor
The Ohio State University / Internet2
cantor.2@osu.edu

Milestones

- 1999 – Shibboleth Project Inception
- 2001 – SAML 1.1
- 2004 – Shibboleth 1.3
- 2005 – SAML 2.0, OpenID
- 2007 – OAuth 1.0
- 2008 – Shibboleth 2.0
- 2010 – Shibboleth 1.3 End of Life
- 2011? – Shibboleth 3.0 (IdP)

State of the Technology

- Federated web authentication well covered (and re-covered) by multiple standards and specifications
- Federated attribute exchange well covered but implementations less mature
- Notions of “assurance” (well?-)defined for authentication, undefined for attribute exchange
- Federation of non-web protocols lacks consensus on solution parameters, usability criteria

State of the Deployments

- Many mature federations spread throughout national RE sectors
- Federating applications still “hard”, asks developers to grok a lot; strong need for a “bible” on development practices
- Effective for large-scale business relationships with contractual sharing of data
- Ineffective for small-scale collaborations

Federation Futures

- Consent-based Federation
- Non-Web Applications
- Delegation
- Interfederation

Consent-Based Federation

- Move policy, and sometimes trust, decisions to the user
- Acceptance likely to vary by regulatory regime, organization/culture
- Absolute necessity for scaling of federation
- Resources asymmetric in value between user (high) and organization (low)
- Lots of usability unknowns

Non-Web Federation

- Too many ideas, all of them with drawbacks, none with consensus
  - Launch and coordinate with browser (SASL, OAuth)
  - “Pure” SAML via SASL/GSS
  - Moonshot (http://www.project-moonshot.org/)
  - PAM w/ a OTP
  - Just use a certificate
  - Screw it, here’s my password

Delegation

- Beta-level Shibboleth code available to address multi-tier HTTP applications
  - https://spaces.internet2.edu/x/n4Sg
- Federated version of CAS proxy tickets
- Significant simplification expected for developers in subsequent releases

Interfederation

- Scale federations beyond national/geographic boundaries
- Relieve SPs of need to join and contract with a dozen or more federations
- A lot of technical progress, but a lot of non-technical issues

Clouds

- SaaS (you authenticate to get to your data)
- Federated Service (you authenticate to get to somebody else's data)
- Difference in risks and implications of faulty organizational vetting
- Industry embracing OAuth, leaving a lot of details undefined

Shibboleth Consortium

- Extensive dependence on Shibboleth code base by multiple national federations
- Internet2 alone insufficient in resourcing, governance to ensure long term viability
- Consortium initially bootstrapped by Internet2, SWITCH, JISC