

Attributes and Providers

RL "Bob" Morgan
University of Washington / Internet2 / InCommon

The Tao of Attributes
NIH
September 2009

A Good IdP

- Andrew Nash of Paypal talks about the importance of being a good IdP (courtesy Asimov):
 - IdP shall not harm its users through action or inaction
 - IdP must do what its users ask, except in violation of above rule
 - IdP must protect itself, except in violation of above rules
- a good *consumer* IdP, perhaps?

Consumer vs enterprise IdPs

- enterprise runs identity infra to support biz purposes
 - relationship with SP, including attribute usage, primarily biz-driven; user is less involved
- consumer service runs IdP as feature to appeal to users (to get more traffic)
 - relationship with SP is driven by user interest; IdP is only facilitator
- those big gray areas
 - enterprise IdPs used for personal purposes
 - consumer IdPs supporting biz apps

Attribute channels: stone age

- enterprise engages outsourced provider
 - sends big batch file, on regular schedule (eg nightly), with info about all possible users of service
 - often modeled on access internal apps have to enterprise person data
 - way too many, since orgs don't know very well who actually should or will use a service
 - way too much, since data tends to come from apps/biz people

Attribute channels: atomic age

- fix stone age problems by
 - only doing account setup for users who show interest in outsourced service by trying to use it, by sending attrs at signon
 - only sending data required for use/access by that app, perhaps with user consent, under IdP control
- new problems
 - no attribute update if user doesn't sign on
 - no user info in app until user signs on
 - consent may filter out needed attrs

Attribute channels: brave new world

- accounts at SP based on user interest is good
 - but supplement with account setup for others on request, by policy
 - need not be at signon time, in fact
- account setup at SP also creates on-demand channel for SP->IdP for that user, to selected information, under policy+user control
- "federated provisioning"
 - also has much appeal in consumer cases
 - too much burden for SPs?

What access is OK?

- "no LDAP through the firewall" ... everyone says
- push more acceptable than pull?
- attribute access at signon time better than "whenever"?
- some kinds of queries OK, others not?
 - SAML attribute queries OK for backchannel?
 - OAuth?

Access control distribution of work

- managing access takes work
 - setting policy, translating policy to bits, user assignments, exceptions, etc
 - finer-grained, higher-risk increases work, increases information needed for decisions
 - work distributed among biz, IdM, apps, compliance
 - and among mechanisms: groups, roles, privs, workflow/approval, audit
 - having many tools is good ... but scalability needs some kinds of consistency
 - eg eduPersonEntitlement ...