Lifestyles of the Attribute Rich and Privacy Preserved

IAM Online – June 11, 2014

Ken Klingenstein, Sr. Director, Middleware and Security, Internet2
Thank you to InCommon Affiliates for helping to make IAM Online possible

Brought to you by Internet2’s InCommon in cooperation with the Higher Education Information Security Council

2 – 6/11/14, © 2014 Internet2
Lifestyles of the Attribute Rich and Privacy Preserved

IAM Online – June 11, 2014

Ken Klingenstein, Sr. Director, Middleware and Security, Internet2
Who owns your attributes?

Who governs:
- Privacy?
- Production?
- Release?
- Transmission?

Who is:
- Responsible?
- Accountable?
- Liable?
- Enabled?

Attribute impedance = Bad user experience
R&E federations world-wide
R&E Europe
Federated identity: what’s working

- The basic model
  - Deployable
  - Scales in number, in diversity, in metadata
  - International, standards-based (technology)
- The ability to adapt and extend easily
  - The network externality effect for MFA
  - Metadata is key
  - R&E continues to drive much of the forward progress
- Its use in other verticals
  - Law Enforcement, Real Estate, Medical, Securities, etc.
- Its influence
  - NSTIC, European identity efforts, social identity providers
- ***Creating a broad new layer of the Internet that serves the needs of the R&E community well ***
The work in deploying federated identity

The First ten years

- Federated infrastructure: 80
- End user experience: 10

The Next Five Years

- Federated infrastructure: 30
- End user experience: 100

6/11/14
Federated identity: what’s not working

• Populating, releasing and using attributes
  – Attribute retentive institutions
  – International complexities
• The social identity providers rules of engagement
  – Rules about identifiers and their characteristics and their use, attributes and their release, downstream use of information, etc. are elusive and shifting
• The economics of higher LOA – benefit to SP; cost to IdP
• Federated incident handling
Webinar agenda

- NSTIC Scalable Privacy and the Original Vision
  - Lifestyles of the Attribute Rich and Privacy Preserved activity
- The big policy issues
- Activity: Assessing our own campus policy space
- PrivacyLens, a privacy manager that extends uApprove
- Attribute-rich access control for accessibility, veterans support, etc..
- Activity: Assessing campus technology needs for user-managed privacy, accessibility, etc..
- How to Stay Engaged
Scalable Privacy

- 2+ year grant to Internet2/InCommon
- Development partners include CMU, Brown, Wisconsin, Ohio State and others
- Several focal points
  - Promotion of multi-factor authentication
  - Citizen-centric attributes and schema
  - Development and deployment of privacy managers
  - Examination of anonymous credentials
- https://spaces.internet2.edu/display/scalepriv

Work described in this presentation is supported by the National Strategy for Trusted Identities in Cyberspace (NSTIC) National Program Office and the National Institute of Standards and Technology (NIST). The views in this presentation do not necessarily reflect the official policies of the NIST or NSTIC, nor does mention by trade names, commercial practices, or organizations imply endorsement by the U.S. Government.
Fulfilling the original federated identity vision

• The original vision was for
  – Rich attributes
  – Active end user privacy management options for those attributes on a meaningful level
• Along the way, we created SAML, SSO, Shibboleth, InCommon, etc..
• We are now returning to that vision with a set of powerful capabilities (schema and identifiers) and new end user privacy tools
• Identity management isn’t about identity. Its about attributes. Some of which may be identifiers that can connect to a specific identity and blah blah blah
• Lifestyles of the Attribute Rich and Privacy Preserved (LARPP), an NSTIC supported activity
Not Live Action Role Playing
Lifestyles of the 
Attribute Rich and Privacy Preserved

• A set of avatar institutions that are actively working to complete the original federated identity vision.
• Sponsored by the Scalable Privacy NSTIC grant
• Key topics include:
  – Attribute release and end-user consent tools
    • Informed revocable, off-line, etc.
    • Respectful of international issues
  – Attribute-based Accessibility
  – Attribute-based veterans services
  – Review of anonymous credentials
• https://wiki.larpp.internet2.edu/confluence/display/LARPP/LARPP+Home
The big policy issues

- User-consent and attribute release
- Institutional use of trust marks (end-entity categories) to shape attribute release
- Being a full citizen of the federation
  - Users are now expecting it
- International federation
  - The Swiss federation now requires deploying consent tools for any IdP that wants to act internationally; others have similar approaches
- International campuses
- Avoiding the pain of too-intrusive consent
  - Defaults
  - Out of band options
  - Predictive
• Much of it is organizationally contractual, and so the IdP decides a universal release policy to enable the proper execution of the contracted service
• Most services are non-contractual, so some RP are now tagged to enable IdP decisions to release proper attributes
• For all that is non contractual and not RP-tagged, there is a world of pain
  – And that includes users of many national cyber infrastructure resources, science domain gateways, departmental wikis, virtual organization services, Google apps, international resources and collaborations, individual use of cloud services, national associations, and a whole lot more.
• (And, btw, the RP has no clue what attributes to ask for.)
The release of attributes from the IdP to the RP

- The single biggest challenge today in federated identity
  - Attribute retentive institutions versus promiscuous self-asserted attributes from a gmail account
- A complex space
  - International dimensions, vagaries of PII interpretations, role of an organization, roles within organizations, business models, “know the customer” directives, lack of national policy and plethora of state policies, etc.
- Several factors affect which policy umbrella to use, including location of IdP and RP, business vs. social purpose, etc.
- “Minimal release for constrained purpose” is our base line
Consent and the law

• Globally, the driving force is EU policy directives
  – The US and Asian countries tend to lack national level laws
  – EU policy directives tend to be EU centric, e.g. EU to EU policies and EU to the rest of the world policies
  – Article 7 of the EU Privacy Directive requires user consent or alternative justification
  – [https://www.terena.org/mail-archives/refeds/pdfRxzCwYW7Sr.pdf](https://www.terena.org/mail-archives/refeds/pdfRxzCwYW7Sr.pdf)
• Consent now comes with requirements, including informed, accessible, revocable, etc.
• Conventional wisdom is that consent is hard to do and so use some other justification for an institutional decision.
  – Standard exceptions (medical emergency, law enforcement, etc.)
  – Contractual basis (e.g. outsourced service supplied to employees)
  – “Legitimate interests” of the RP (hmmmm)
• Hide/inform/consent the release to the user
Who decides on privacy and consent

- For faculty? For students? For staff?
- Does the approach need to be consistent across communities?
  - All the overlaps...
- Are there institutional values that bear on the approaches
- A poll
Google and consent
Privacy manager background and future

- Based, in plumbing, on the original Swiss uApprove and the Japanese enhancements
- Discussions with CMU privacy research community and a resulting centerpiece in the NSTIC grant proposal
- Research, human subject testing, and development work over the past 18 months
- Visibility of this effort due to NSTIC and the cred of InCommon
- Will have more capabilities to tap into in IdP v3
- Open source community, lots of work ahead
PrivacyLens

- Open source privacy manager funded by NSTIC
- v 0.5 now available on github
  - https://github.com/cmu-cylab-privacylens/Privacy-Lens
- Well-researched and clear UI
- Informed consent enabled
- Defaults to minimal release
- Histories and logs
- Easily configurable privacy
- Designed for the spectrum of users
CMU's Calendar is asking CMU for your:

- **name:** Lujo Bauer
- **Andrew ID:** lujo
- **CMU affiliation:** faculty
- **credentials to access CMU services**

Use the toggle switches to select the items that will be sent to CMU's Calendar. Items marked with * are required to access and personalize the calendar and cannot be unselected.

Continue to CMU's Calendar?

[Yes] [No] [Settings & History] [Explain]
Logged in to CMU's Calendar on 2014-05-05 23:10

Items sent:
- Andrew ID: 'iujo'
- CMU affiliation: 'Faculty'

Next time you access CMU's Calendar, CMU should:
- Ask whether and what items to send to CMU's Calendar.
- Send the following items automatically, but remind you that they are being sent.

Save  Back

Provided by CMU Cylab Privacy Lens team
Logged in to CMU's Calendar on 2014-05-05 23:10

Items sent:
- Andrew ID: "lujo"
- CMU affiliation: "faculty"

Next time you access CMU's Calendar, CMU should:
- Send the following items automatically, but remind you that they are being sent.
  - Andrew ID (lujo)*
  - credentials-to-access-CMU-services
  - full name (Lujo Bauer)
  - surname (Bauer)
  - CMU affiliation (faculty)

CMU will remind you what items are being sent...
Every 2 times you log into CMU's Calendar.

Provided by CMU Cylab Privacy Lens team
Serving the Spectrum of Users

• Privacy fundamentalists
  – Fine grain attribute release management
  – Variety of informed consent mechanisms
    • Displays trust marks, reputation systems, etc.
  – Ability to review each transaction
  – Intelligent design

• Pragmatics
  – First use is minimal release setting
  – In recurring use, comes up in last used setting
  – Intelligent design

• Unconcerned
  – First use is minimal release setting
  – In recurring use, comes up in last used setting
  – Can be set to only reappear after change/time triggers
Next steps for PrivacyLens

- Move to v 1.0 version
- Share internationally
- Develop informed consent mechanisms
- Add bundles, cope with names
- Add UMA backend capability (permitting off-line and direct RP use of individual attribute release policies)
- Port to OpenId Connect and OAuth
- Study effectiveness
- Create predictive assists for users
Being attribute-rich

• Turning on your users eduperson attributes
  – Most are calculated on the fly using standard LDAP values
• Exploring new accessibility opportunities
  – Accessibility everywhere
  – Accessibility with privacy
• Exploring new veterans support
• Thinking of ORCID, rethinking identifiers
The purpose of the Global Public Inclusive Infrastructure (GPII) is to ensure that everyone who faces accessibility barriers due to **disability, literacy, digital literacy, or aging**, regardless of **economic resources**, can access and use the Internet and all its information, communities, and services for education, employment, daily living, civic participation, health, and safety.

- Automatic personalization of user interfaces and user context adaptation based on user preferences, across platforms.
- Schema standard is AccessForAll (ISO/IEC JTC1 24751).
- [http://gpii.net](http://gpii.net)
- Pilot applications, proofs of concept beginning with:
  - User preferences stored and accessed securely in an online repository.
  - Those preferences drive presentation features that provide accessibility accommodations when user visits online resources.
  - All leveraging UMA profiles of Oauth 2.0 aligned with emerging GPII security and privacy architectures.
Veterans Support

- DoD Form 214 (aka discharge notice) provides a rich schema
- Applications include student loans, special discounts, veterans ombudsmen services, specialized medical alerts, etc..
- As with accessibility, delivering personal information but with privacy
- As with the broad shift from authentication to use of attributes for access control, the trick is to bundle and manage the complexity (the high tax of being attribute rich).
Activity – Interest and readiness

• What is the institutional capability to support end-user consent tools?
  – Federation is hard enough already
  – We’d rather count on the help desk
  – Let them suffer
  – We needed this yesterday

• Do you think there is institutional interest in some of the enabling accessibility opportunities? Would the technology community know where to reach out to the relevant user communities to engage?
How to stay engaged

• Follow the LARPP discussions
• Think about MFA
  – Leveraging federation and MFA is huge
• Build awareness on campus
  – Privacy, Research Officers, Security, Accessibility
• https://wiki.larpp.internet2.edu/confluence/display/LARPP/LARPP+Home
Evaluation

Please complete the evaluation of today’s webinar

https://www.surveymonkey.com/s/IAM_Online_June_2014
Identity Week 2014 will take place at the Technology Exchange

Advance CAMP, CAMP, Trust and Identity

October 26-30, 2014 - Indianapolis, Indiana

http://events.internet2.edu/2014/technology-exchange/
InCommon Shibboleth Installation Workshops

Single Sign-on and Federating Software

July 24-25 – Indiana University – Indianapolis, IN

September 29-30 – New Jersey Institute of Technology – Newark NJ

November 10-11 – University of Utah – Salt Lake City

Details and registration at www.incommon.org/shibtraining
Cloud Services Cookbook

Federating with cloud services has become a popular trend. Cloud services can benefit your organization, but to make a service deployment successful, it’s essential to follow best practices. The CIC’s Identity Management Task Force has been working on a cloud services cookbook to provide recipes for successful cloud service deployment.
Thank you to InCommon Affiliates for helping to make IAM Online possible

Brought to you by Internet2’s InCommon in cooperation with the Higher Education Information Security Council