The Art of Attributes

Ken Klingenstein

Internet2

Topics

- Goal: to help a community of interest to use attributes well

- Of identifiers and attributes
- Avoiding some deep water about attributes
- Intrinsic issues in sharing attributes
- Where the Art is Being Practiced
- Access Control Uses and Normative Bundles
- Competencies, attributes and verifiable credentials
- A few observations and actionable items

Of identifiers and attributes

- Identifiers
  - 1-1 correspondence to a subject
  - Key characteristics - vetted or not; reassignable or not; uniqueness
  - {Anonymous, pseudonymous, displayname, pair-wise distinct, etc}
  - Identifiers used by other parts of the stack (e.g. sessionids, web fingerprints)
- Attributes
  - Access control at scale
    - Fine-grain and coarse-grain
  - Personalization
  - Compliance and regulation
  - Skills and competencies and certifications

Avoiding some deep waters about attributes

- LOA (levels of assurance about the value of the attribute), shelf life, other metadata concerns
  - Best handled out of band
- Re-identification from attribute aggregation
  - Bucket size of identities having this attribute
  - A threat to privacy
- Syntax

Intrinsic Issues in Sharing and Moving Attributes

- Shared meaning, including metadata
- Permissions to move attributes
- The transport protocol
  - LDAP
  - SAML and Oauth tokens
  - Verifiable credentials
- Security (and privacy) of the transport
- Trust in the received value
  - Is it meaningful and untampered?
  - Issuer authorization to assert

Where the Art is being Practiced

- On campuses daily – for both on-prem and SaaS apps
- Institutional and inter-institutional
- NISO-Seamless Access Contract Language
- Refeds Schema Discussions
- IMS Badging Work
- Big Research Collaborations with Complex Access Control Needs

INTERNET 2

Permissions to move attributes

- Integrated User and Institutional Control of Attribute Release
  - Effective and Informed User consent
  - Institutional control
    - E.g. negative permissions
  - Reducing friction in user experience
- CAR (Consent-Informed Attribute Release) from Duke and Internet2 is an open-source, protocol neutral example
- Data minimization – what is the practice
  - Blurred distinctions between application needs on required vs optional
  - Note the advertising cookie categorizations

Normative bundles of attributes

- Bundles are sets of attributes often used together for common use cases
- Purposes
  - For IDP release use, SP requests, end-user consent mechanisms
- Need to accommodate a variety of existing campus policies
  - Reassignment of identifiers such as email addresses
  - Variations in membership rules
  - Leads sometimes to sets of choices
- Primary existing example – Research and Scholarship (R&S)
  - Intended for federated login use for researchers
  - Shared user identifier, personal name, email address + optional affiliation
- New attribute bundles being discussed by Refeds

INTERNET 2

The art of practical access control attributes

- The Access Control Journey
  - Identity-based -> Role-based -> Attribute-based -> Policy-based
- eduPersonAffiliation
  - Coarse grain (faculty, student, staff, alum, member, affiliate, employee, library-walk-in)
  - Coarse semantics
- eduPersonEntitlements
  - Extensible syntax for community-centered semantics
  - May be only an IDP-computed value for exchange purposes
  - Fertile ground
- IsMemberOf
  - Single multi-valued attribute for Group memberships

INTERNET 2

Competencies, attributes and verifiable credentials

- Large number of use cases around certification, microdegrees, competencies, etc
- Important characteristics include composable assertions, off-line validation, mobility, etc.
- Challenges for verifiable credentials include
  - Lack of standards in wallets
  - Lack of standards in issuer authorization
  - User Identifiers and their binding strength

A few observations

- On the wire and the mapping of local to on-the-wire is what matters.
- With new attributes, make the space of values extensible
- Entitlements are underutilized as privacy-preserving
- Some technologies inherently cause lack of standardization (e.g decentralized identities)
- Fine-grain attribute use seems beyond the reach
- Anomalies for access control will happen – e.g. pubmed
  - How you get to the resource determines your privacy

Actionable Items for CNI community

- Pay attention to your institutional release policies
- Help create a purpose of use taxonomy for R&E
- Express needs for portals and fine-grain signaling of attribute needs
  - E.g. access control needs for subsections of wikis
- Community standards on required/optional attributes
- Help develop reporting utilities
  - https://wiki.refeds.org/display/CON/Consultation%3A+eduPersonAnalyticsID