Introduction to Attributes

Nate Klingenstein
Internet2
ndk@internet2.edu

国立情報学研究所

２００７年６月１日

Attributes Structure

- An attribute is a single piece of information
- Usually a pair: a name, and a value

Name	Value
Last name	Klingenstein
Hair color	Brown (shaved)
Chess Club Member	No

Attribute Preparation

- Common attribute sets (Object Classes)
  - inetOrgPerson
  - eduPerson
- What do you need to know about an attribute?
  - Its name
  - Its value
  - What it's supposed to mean
  - Where it came from
  - And so much more...

Attribute Structure

- Attributes can be more complicated
- Some attributes have multiple values
  - “Billy Bob Thornton”
  - cn: Billy
  - cn: Billy Bob
- Attributes can also have internal structure
  - akiyama@cmc.osaka-u.ac.jp
  - Akiyama is the value
  - cmc.osaka-u.ac.jp is where he is from (scope)

Attribute Structure

- The information surrounding an attribute can affect its meaning too
- An attribute in an assertion I have means that attribute is about me, says the IdP
- Seems simple, but has big impacts
  - Removing attributes from assertions
  - Proxying, delegation
- The same attribute may take different forms in different environments

Attribute Structure

- LDAP

  eduPersonAffiliation: Member

- SAML 1.1

```
<Attribute AttributeName="urn:mace:dir:attribute-
def:eduPersonScopedAffiliation"
AttributeNamespace="urn:mace:shibboleth:
1.0:attributeNamespace:uri">
    <AttributeValue Scope="nii.ac.jp">
        Member
    </AttributeValue>
</Attribute>
```

SAML Attribute Naming

- urn:mace:dir:attribute-def:displayName
- urn:oid:1.3.6.1.4.1.5923.1.1.1.10
- https://supervillain.edu/attributes/inetOrgPerson/displayName

- Shibboleth uses different attribute names in SAML 2.0 and SAML 1.1
- Your application and directory will never see this, but your providers will

Attributes in Shibboleth

- Shibboleth can send and use any attribute
  - Including structured XML, but that's usually a bad idea
- Attributes are the main information delivered
  - It's dangerous to rely on authentication rather than attributes
- A set of default attributes is defined
  - Federations can set new or more defaults
- Attributes given to apps using standards

Attributes in Commercial SAML

- Support varies by vendor, but most don't use lots of custom attributes
  - Usually focused authentication or account linking rather than attributes
- Most make heavy use of NameIdentifiers
- Use additional fields in the SAML, such as NameFormat for Attributes
- Structured attributes like scope often cause problems
- Usually have an API

Attributes in ADFS & Cardspace

- ADFS has a pre-defined set of Microsoft attributes and can't use additional ones
- Cardspace also has default attributes, but it can be extended
- Cardspace identity card selection includes a set of attributes to be released
- It can also match attributes requested to attributes available

Attributes in OpenID

- There are no attributes in OpenID
- Drafts now exist that suggest some possibilities
- Other deployments are considering making the URL identifier parsable
  - https://example.com/employee/rescue/ndk
- In OpenID today, authentication and an identifier is all you get

Some Useful Attributes

- eduPersonScopedAffiliation
  - staff@supervillain.edu
- eduPersonEntitlement
  - urn:mace:dir:entitlement:common-lib-terms
- eduPersonPrincipalName
  - magneto@supervillain.edu
- cn
  - Erik Magnus Lensherr
- persistentId (eduPersonTargetedID)
  - Part of SAML 2.0 standard and usable for account linking & more

Attribute Assignment

- Everyone needs to understand an attribute
- Who's a student?
  - … is that exactly who?
- More names and values add options
  - But also add complexity
- Attributes should be chosen carefully
  - Understandable
  - Manageable

Attribute & Applications

- Many applications store lots of attributes about users already
  - Permissions, names, preferences, etc.
- Some applications are used to dealing with central attributes already
  - LDAP
- Other applications can do new things when they are given attributes
  - Preserve privacy, “least privileges”