GENI and Federated Identity

Dr Ken Klingenstein
Director, Internet2 Middleware and Security

Comments

- Spirals or gyres
- Overheard
- Options
- Authz and groups and schema
- Beyond federated identity – federated *
  - The costs of federation
  - The costs of non-federation

Are They Spirals or Gyres

Turning and turning in the widening gyre
The falcon cannot hear the falconer;
Things fall apart; the centre cannot hold;
Mere anarchy is loosed upon the world,
The blood-dimmed tide is loosed, and everywhere

w.b. yeats- the second coming

Overheard at GEC7

- Just an experiment – reputation systems sufficient
- X.509 “special certs”
- Kerberos
- Federated identity and social identity
    - NIST 800-53 and 800-63
- Greatly expanding numbers of users shortly down the road

Options for Identity in GENI

- Anarchy
- Refactoring
- Adding a layer of abstraction
    - Costs
    - Benefits

Authorization

- The real deal
- Not identity munging
- Attributes and ABAC
- How far do groups go?
- What else is needed

Quick Attribute Nomenclature

- Attributes
  - Have syntax of the name (name-space) and semantics
  - Semantics get defined by a controlled vocabulary of values attribute can have and shared business rules for assigning values
- Schema
  - Collection of attributes
  - eduPerson is a starter set for R&E globally

Attribute Ecosystem elements

- Creation and storage of attributes
  - From source of authority, possible delgated
    - Enterprises and their legacy systems
    - Virtual organizations, clusters in GENI, collaborations
- Transport of attributes from storage to policy decision point (PDP)
    - Shib, SQL, LDAP, X.509
- Relying Party and their PDPs

What Modern Middleware can offer

- Creation and storage of attributes
  - Group management tools and interfaces
  - Some privilege management capabilities
  - Syntax and semantics experience
- Transports – Shibboleth/SAML, GridShib (Shib to X.509), LDAP
- Internet2 hasn't done PDP work beyond some activities in XACML for policy expression

R&E Federations

- Substantial deployments in many countries, including UK, Norway, Switzerland, Sweden, Japan, Australia, France, Denmark, Finland, Spain, Germany, Netherlands, etc. Coverage in a number of countries is now 100%.
  - Uses include roaming access, grid credentials, digital content access, wiki controls
- In the US, a national federation – InCommon – and others - Texas (three federations), UCTrust, CalState Trust, Libraries of Florida – Federation Soup

InCommon

- US R&E Federation,
- 200+ members - universities, service providers, government agencies, national labs, 5 M users
- Millions of assertions a day
- Access to controlled wikis, academic content (Elsevier, etc) clouds and Grids, services (student travel, testing, etc), Microsoft, Google Apps for Education, science portals,
- Access to national science and national medical resources
- Building multiple levels of assurance (LOA)
- Likely over half of the credentials in the room today work across InCommon

- www.incommonfederation.org

The Texas Lone Ranger in the past

The Texas Rangers now - federated

The Texas Rangers now sit in police cars and use Shibboleth to access state databases

The cost of federations

- Agreements
- Central facilitation of meta-data
- Dealing with privacy, especially internationally
- Schema, attributes and shared business practices

The cost of non-federations

- Agreements
- Dealing with privacy, especially internationally
- Schema, attributes and shared business practices
- Non-federated incident handling, especially internationally

Trust, Identity and the Internet

- The Internet was built for friendly behavior; that is not the current situation
- ISOC initiative to introduce trust and identity-leveraged capabilities to many RFC's and protocols
- http://www.isoc.org/isoc/mission/initiative/trust.shtml
- First target area is DKIM; subsequent targets include SIP and firewall traversal (trust-mediated transparency)

Non web applications

- Many non-web apps want federated identity – wireless roaming, videoconferencing, soft phones, SSH, Grids, next-generation Internet, calendaring, etc.
- Adding federated authentication and authorization to them is generally engineered on a per case basis.
- SAML and Oauth provides some specific solutions
- Project Moonshot, funded in Europe, looking to work through a general solution by extending IETF protocols

The Internet of things

- We have built the Internet of computers and now the Internet of people and identity; next is things.
- Federation is a powerful model – it provides a degree of local freedom but a scalable infrastructure; with interfederation it can reach Internet scale.
- Devices need to have identity, attributes, access control privileges, etc that tend to federate and also need to interact with identity federation.
- Next generation Internet work has many types of federations of circuits, of firewalls, of routers, etc.

The Attribute Ecosystem 属性之道

- Authentication is very important, but identity is just one of many attributes
- And attributes provide scalable access control, privacy, customization, linked identities, federated roles and more
- We now have our first transport mechanisms to move attributes around – SAML and federations
- There will be many sources of attributes, many consumers of attributes, query languages and other transport mechanisms
- Together, this attribute ecosystem is the “access control” layer of infrastructure