Investigating OpenID

David Chadwick
University of Kent
UK
Authentication on the Internet

• The Original Internet of Yesteryear

• No authentication. Everyone is trusted. Everyone believes what they are told. Everyone is a good guy.
"On the Internet, nobody knows you're a dog."
The Internet Today

- No-one is trusted per-se
- There are lots of bad guys out there
- We need good authentication mechanisms
- We will only trust a limited number of users
- We will grant different access rights to different users
- We may have different levels of authentication and apply different trust/authorisation levels to these
- Enter Shibboleth. Phew, some relief
  - Attempting to bring some order into this distributed world of chaos
Enter OpenID

- **The Internet Today with OpenID**

- People can claim whatever ID they want (within reason). But does it matter?
- Some say Yes, I need to know which biological entity lies behind the Internet ID
- Some say No, I don’t care who you are (i.e. which biological entity) as long as it is the same entity using this particular Internet ID each time we communicate
Two Aspects to Authentication

1. The security technology that is used to prove you have the right to use the ID you are claiming (Computer Based Authentication Mechanism)

2. The binding of a biological entity to an ID at initial registration time (User Registration Mechanism)

Both are included in the current NIST Level of Assurance/Authentication (LOA) definitions
Strong Computer Based Authentication Mechanism

• **Digital signatures preferred!**

• Security is hard to get right.
  – Man in the Middle Attacks
  – Cryptography Attacks
  – Replay Attacks
  – Dictionary Attacks
  – etc.

• Leave it to the professionals. Use tried and trusted mechanisms. Don’t roll your own
Registration Mechanism

- This is under your control
- You register staff and students when they first arrive
- You validate their claimed identity (passport, driving license etc.)
- You validate their claimed qualifications (degree certificates etc.)
- You validate their character (police records, references etc.)
- You enter everything into your database and give them an Internet ID and an Authentication Mechanism
- Then users use their new Internet ID to access your University resources
What happens when they leave?

- They go through the whole process again with their new employer/institution
- Users collect lots of Internet IDs and Authentication Mechanisms
- Shibboleth does not help!
  - It is not a Registration Mechanism, it’s a federated Authentication Mechanism. It does not assign IDs to users, it helps in validating existing ones
- OpenID could help!
  - Users register themselves with an OpenID provider and get an Internet ID and Authentication Mechanism
Revised Registration Mechanism with OpenID

• This is still under your control
• You register staff and students when they first arrive
• You validate their claimed identity (passport, driving license etc.)
• You validate their claimed qualifications (degree certificates etc.)
• You validate their character (police records, references etc.)
• You validate their claimed OpenID and if it is acceptable
• You enter everything into your database
• Then users use their OpenID to access your University resources
Validating a Claimed OpenID

You need to know three things

1. User has the right to use the claimed ID
   • Get them to log in with it

2. User is the sole user of the claimed ID
   • Get them to sign for this (No different to using your current IDs)

3. What Authentication Mechanism is being used by the OpenID provider
   • How do you know today what authn mechanism is used by other Shib federation members? Is it good enough?
   • Short Term. OpenID providers need to publish their Authentication Mechanism in a Policy Document
   • Medium Term. Standard criteria for what to see in this policy document for different levels of authn. Audit system to be put in place to validate the level that is being claimed.
Dissecting the LOA

• Existing NIST LOA needs splitting into two
• Level of Computer Based Authentication (LOCBA)
  – Performed by the OpenID Identity Provider
• Level of Registration (LOR)
  – Performed by the Service Provider

• Once we have metrics for these in place and they are being used, SPs can start to use OpenID for valuable resources
JISC OpenID Project

• The project is combining structured interviews, technical evaluation, and working demonstrators to address the following:
  • What OpenID is and is not
  • What other institutions have already been doing with it
  • What applications can be foreseen in the short and medium term
  • How OpenID relates to the UK Access Management Federation
  • Whether OpenID may be applicable to services using licensed data
  • How the forthcoming integration of CardSpace with both OpenID 2.0 and Active Directory might affect the large number of institutions that presently use Active Directory as a major component of their identity management
  • Whether or not there is a forseeable path from institutionally-managed identities to institutions providing trusted attributes about public, user-centric identities
Progress to Date

• Questionnaire developed and starting to be answered
  – Responses so far are negative about using OpenID for accessing anything of value, but some willing to use it for very low value apps.
  – More volunteers requested please
  – Email me at d.w.chadwick AT kent.ac.uk

• Technical evaluation of OpenID
  – Biggest weakness is its open to phishing attacks, same as Shibboleth

• Starting to answer the questions as highlighted in this presentation and developing short and medium term views

• Have built an OpenID-Shibboleth gateway for users to play with to access an EDINA service
  – User contacts Shibboleth SP, chooses OpI-Sh gateway in WAYF, then from there is redirected to OpenID to authenticate, and then back to the Shibboleth SP
  – Will be live within a week or two.
Any Questions ???