Subverting OpenID: Intro to Net::OpenID::Server

Abram Hindle

Kitchener/Waterloo Perl Mongers
Canada
http://softwareprocess.es/
abram.hindle@softwareprocess.es

Identification

- Used to reduce abuse (spam/trolling)
- Attribute your comments or your work to yourself or others
- Enable community building by recognition of posters

Problems with Identity

- Impersonation
- Stalking
- Authentication
- Inconsistent profiles
- Multiple Logins

OpenID

- Protocol of ID authentication
- Decentralized
- Digital ID

Why do I care

- Avoid registration
- Avoid sharing a password with a website
- Post on blogs without registration
- Register for services

Context

- Historically many blogs allow anonymous or unverified posts
  - Just supply some information and you post.
    - Too much spam
      - Snarky posters
- Now every site under the sun wants you identify yourself
  - Too many passwords
    - too many accounts
      - too much information

Example 1/2

- To login to sprockets blog provide your OpenID URL
- sprockets grabs that OpenID URL
  - sprockets reads the headers for the provider info
- sprockets sends the OpenID provider a message that someone is trying to authenticate
  - they share a secret
- ...

Example 2/2

- your browser is redirected to your OpenID provider
- you login to your provider
- the provider redirects you back to return address that sprockets supplied, you carry a shared secret
- sprockets validates your shared secret and if valid lets you login as your OpenID user.

Where’s the distributed part?

- Your URL is generally under your control and can be any site you can change
- Your OpenID provider can be any open provider

What are the actual benefits to a user?

- Decentralized, you control your identity by sites you control
  - All you need is a web-page or an OpenID provider
- Lack of vendor lock-in
- You can avoid hassles of registrations

So it is great right?

- OpenID allows for easier social network analysis
- People can track your every move across multiple websites
- Your OpenID provider is aware of all site you visit
- You’re not protected from malicious site owners yet content on their site has your name on it.
  - false sense of security
- At least you’re responsible for your ID

But it doesn't seem it was designed this way!

- People make assumptions about OpenID!
  - You can trust an OpenID (no)
  - OpenID reduces spam (maybe, but not technically)
  - OpenID protects the identity of the user

So what's your point

- People trust OpenID
- People want me to authenticate and prove my identity
- I don't want to provide any identity
- I would rather post anonymously in 99.9% of the cases.
  - Social network analysis is creepy

Openid.aliz.es

- An OpenID provider
  - that validates everyone and their dog!
  - Anti-identity
    - But accepted at the front door
- Play on the assumptions of others about what OpenID is.
- http://openid.aliz.es/yourid here

Openid.aliz.es

- No “protection”
- Anyone can post as any openid.aliz.es user
- Often they can delete messages too
- Think of openid.aliz.es like spam.la
  - Throw away identity

Net::OpenID::Server

- Great Module
- Is meant to integrate with a wide variety of frameworks
- Attempts to control the OpenID auth part of the process
  - See code

Net::OpenID::Server Issues

- If you want to use it yourself you're going to have to implement the setup page
  - this allows the users to login

Net::OpenID::Server Issues

- Try to stick to the perldoc page
- Relies on BigInts and can be very slow
  - Diffie Hellman in BigInts for the shared secret negotiations
  - Install Math::BigInt::GMP
    - or install Crypt::DH::GMP::Compat (even faster)
- You need GMP

Shared host annoyances

- If you’re on a shared host and lack the necessary GMP version etc.
- install it to /local
- build your own Perl too (linking is a pain)
- Common prefix is easier to deal with that managing all the paths and using LIB_LD_PATH

OpenID doesn’t provide much in the way of safety

- Sure other posters have a hard time impersonating you
  - But the site admins don’t
- Site admins can be spammed by throwaway OpenID accounts

Resources:

- http://openid.net/
- http://search.cpan.org/
  - Crypt::DH::GMP::Compat
  - Net::OpenID::Server