Single Signon (SSO)

Experiences to Date

Faculty of Engineering

April 2017

Four Major Goals

- Users hate logging into every system they use and entering passwords multiple times per day
- Users leak passwords to phishers when they are accustomed to entering them frequently and on demand
- Systems may be compromised, and their password hashes stolen. Centralizing authentication can reduce that likelihood.
- Two Factor Authentication requires SSO in order to implement broadly

CAS – Central Authentication Service

- Often used as a simple SSO at universities
- At UW: Learn, MyHRinfo, ONA, etc.
- Relatively easy to implement for locally created sites
  - Apache mod_auth_cas
- Problems
  - Not many commercial applications are CAS compatible
  - Not possible to fully log one out of CAS-enabled sites
    - Compromise, firing, expelling
  - Too simplistic, cannot make assertions like:
    - Is an employee
    - Is a CS 232 student
  - lacks Two Factor Authentication (2FA)

SAML 1.1, 2
(Security Assertion Markup Language)

- A real SSO, solves most technical limitations of CAS (logout, 2FA, assertions)
- Version 2 released in 2005
  - the standard has settled in the intervening time
  - Considered a “heavy” protocol – a challenge to implement/debug
  - Most popular among big businesses (eg. Oracle, IBM, corporate apps)
- Open Source “Shibboleth” implementation used on campus
  - Well regarded concise implementation of SAML standards
  - Can be made interoperable with many products
    - Eg. Lynda.com
  - Not high availability, load balanceable or great performance
- MS ADFS implementation
  - Not as standards-based, but will be a force in community
  - Scalable, high availability
  - High cost to implement
  - MS Office365 integration

Several False Starts/Variants

- Whenever there is a good idea, we like to evolve, simplify or replace it

- There were several false starts and a few rethinks since the release of SAML
  - OpenID 1 and 2 were flops
  - OAuth1 and later OAuth2 were excellent for implementing authorization, but were not designed to implement authentication
  - JWT – JSON Web Tokens – a critical technology to the next step, totally replacing OpenID 1/2
  - SecureKey: lightweight simplified SAML used by US/Canadian governments
    - Because most of SAML is never used

OpenID Connect (OIDC)

- Ratified in 2015
  - Builds on successful OAuth2 and JWT, well known and understood technologies
  - Like SAML: logout, 2FA, assertions built-in
  - Backed by (alphabetically) Amazon, Cisco, Facebook, Google, HP, IBM, LinkedIn, Microsoft, Netflix, Oracle, others and in use ***today*** for all major social networks
    - YouTube, Gmail, Facebook, Netflix, LinkedIn, etc. and all associated apps
  - Much simpler to work with than SAML
    - easier for individual web sites to utilize: mod_auth_openidc
  - In 1½ years it has become the recommended choice, and the choice for new implementations
    - Next version of Desire2Learn will have OIDC
    - Unit4 integration with OIDC already available
    - Easy to replace existing CAS systems
    - Supports mobile clients too
    - Engineering / CS / the Portal going to use OIDC

Today’s Market

- Split between existing SAML and newcomer OIDC
  - Corporate apps more often have SAML
  - Social networking sites and mobile do OIDC
- Best option is to pick something(s) compatible with most players today and in the future by not limiting ourselves to one strategy
- Several SSO vendors support all three, some just SAML+OIDC
  - Gluu, OpenAM, Ping Identity

UWaterloo Landscape (unverified)

- ISS deployed SAML/Shiboleth (OSS, consortium)
  - Lynda.com
- TIS deployed SAML/Windows ADFS (Microsoft)
  - Office365, Unit4
- Portal deployed OIDC/Open Identity Server 3 (OSS)
- ISS deploying a production GLUU environment (OSS, commercial)
  - Supports CAS, SAML, OIDC concurrently
  - Engineering and CS/Math OAT/ASUS begin using
  - Portal plans to migrate to this

Thankyou