Shibboleth meets Buzzwords

SWITCH

Serving Swiss Universities

Chad La Joie
chad.lajoie@switch.ch

The Buzzwords

- User-centric Identity
- Zero-knowledge Proof
- OpenID
- Cardspace
- Geneva
- OAuth
- Google Wave
- Cloud/Grid/Distributed Computing
- Role/Attribute-Based Access Control

User-centric Identity

- Claim: All data about a person is property of that person and as such should be kept and controlled by that person.
  - Allows for freedom of movement from provider to provider
  - Allows for a consistent identity across sites
  - Allows individuals to choose what information they release to whom
- In practice though:
  - The user isn't authoritative for most of their data
  - Self-asserted data is inherently non-verifiable (in-band)
  - A consistent identity across sites means sites can correlate data and identify you as an individual
  - Most users can't operate an identity provider and so end up locking in to a particular provider anyways
- The goal should probably be to bring information release consent to organization-centric identity.
  - e.g. Shibboleth + uApprove

Zero-knowledge Proof

- “An interactive method for one party to prove to another that a statement is true without revealing anything other than the veracity of the statement.” - Wikipedia
- In this space ZKP is used to prove an identity without providing it.

$$\forall x \in L, z \in \{0,1\}^*, View_{\hat{V}}[P(x) \leftrightarrow \hat{V}(x,z)] = S(x,z)$$

- Usually involves a process where an operation that is “easy” to perform but requires knowledge of a secret, that is guessable, is performed over a set of inputs and the results verified.
  - The more iterations the less likely that the secret was simply guessed
- Often times seen as a way to allow a user to interact with an SP without the IdP knowing which SP it is.

OpenID

- OpenID claims to be the simple, user-centric, federated identity system.
  - User's have an OID provider that they run.
  - OID is a URL entered at the SP (removes need for a WAYF/DS)
  - Shibboleth 1-like authentication process occurs
  - Only proves ownership of URL
  - Extensions to protocol allow for some exchange of attributes
- Very few users can run their own OID provider
- Very few users can remember a URL as their identifier
- Information is self-asserted, trust is done via white/black list
- Much easier for developers to implement than SAML
- General litmus test "Would you be willing to give out the restricted information to a random person who asked?"
  - This is perfectly okay for **many** sites

Shibboleth + OpenID

- Work has begun to add OpenID 2 support to Shibboleth
- Initial release will be an IdP plugin
  - no SP support currently planned
- Supported Features:
  - Attribute Exchange 1.0, PAPE 1.0, Simple Registration 1.0
  - Will use XRD 1.0 (a spec to be finalized) for basic metadata
  - Will employ existing Shibboleth trust mechanisms
- Use of XRD and trust will mean a lack of interoperability with most existing OpenID service providers
  - The goal is to try and meet up with where OpenID technology seems to be converging, not to support legacy OpenID 1.0 deployments

CardSpace

- CardSpace generally refers to two things:
  - Microsoft's evolution of Passport in to a decentralized service
    - Known by Microsoft as the identity metasystem
  - Microsoft's client for the service
    - The only thing that Microsoft calls CardSpace
- Primary focus on avoiding phishing
  - The OS controls the UI during authentication
- Secondary focus:
  - Support for multiple authentication technologies: SAML, Kerberos, PKI, OpenID
  - Support for user-centric identity through unmanaged cards
  - Support for organization-centric identity through managed cards
  - Zero-knowledge interactions between identity and resource owners
- CardSpace is a client without a server

Geneva

- Microsoft's server-side implementation of the identity metasystem
  - Officially called Forefront (I think)
    - Website is a completely impenetrable wall of marketing
  - Spiritual successor to Active Directory Federation Services
    - but not interoperable with it
- It currently does not interoperate with other products
  - Microsoft is not using the Inforcase/Cardspace protocols given on their website
  - Microsoft is also not compliant with other standard specification
    - MS currently uses crypto algorithms that are not part of the XML digital signature spec and so XML-DSIG tools can't work with those signatures
    - MS is using a **higher** grade crypto, which would be good if it didn't break things
- Appears to integrate with Exchange and Sharepoint already

Shibboleth + Forefront (CardSpace/Geneva)

- Shibboleth already has a plugin that supports the published Infocard/CardSpace protocols

  https://spaces.internet2.edu/display/SHIB2/IdP+Infocard
- The absolute latest versions of CardSpace/Geneva is not compatible with these protocols
- Initial contact with MS has not provided any additional information
  - though a more direct call from the Shib team to the MS developers is planned for later this week

OAuth

- OAuth is an access delegation protocol.
  - You log in to Service B. Service B wants your information from Service A. You log in to A, get a token, and give it to B. B uses the token to get information from A.
- OAuth is independent of the means by which a user is authenticated or the format of the token.
  - So OAuth is orthogonal to federated identity management
- OAuth is currently under-specified
  - Creating interoperable implementations tends to be a trial-and-error exercise
  - IETF WG attempting to provide a more clear standard

    http://www.ietf.org/dyn/wg/charter/oauth-charter.html

Google Wave

- Wave is Jabber (XMPP) on ~~steroids~~ performance enhancers
  - "Email if it was thought up in the web 2.0 world"
- User-to-Wave-Provider authentication is unspecified
  - Currently, all wave apps seem to be web-based so standard web-based SSO solutions, like Shib, would work
  - Future applications will almost certainly not be web-based so the non-browser support issue comes up again
- It remains unclear how much this will take off. Technology has some very interesting features though.

Cloud/Grid/Distributed Computing

- My definition: An execution environment for services that is outside the service owners organization.
  - It's outsourcing... for servers.
- User-to-provider interaction is not specific, most today use a REST based mechanism.
  - Immediately runs into issue with any existing SSO solution
- Commercial systems like Amazon will likely not support other authentication for a very long time
- Current "grid" software almost exclusively uses X.509 and the Short Lived Certificate Service (SLCS) provides certs based on Shibboleth

Role-Based Access Control

- The determination of a principal's ability to act within a system based on a singular role.
  - Though the user may have more than one role.
- Very simple to program
  - if(string1.equals(ROLE))
- Difficult to analyze all aspects of the system and create roles in such a way that everyone gets what they need and not get what they don't.
  - Requires that you get a lot of information correct right at the start
  - Almost always turns in to a case where every single individual functions gets a unique role.
  - An HR system that uses RBAC, at a particular university in the US, currently has over 2,000 roles defined in it.
  - This was more roles than people using the system.

Attribute-Based Access Control

- The determination of a principal's ability to act within a system based on the entirety of their known identity.
- More complex to program because there are potentially a lot more things to check.
  - In practice most apps use ~3 attributes
- Removes the need to get things correct at the start
  - New data can be added, and old ones expired, over time
- An Attribute-Based Access Control that operates on a single attribute **is** a Role-Based Access Control system