Identity Management and Federated ID (Liberty Alliance)

ISA 767, Secure Electronic Commerce
Xinwen Zhang, xzhang6@gmu.edu
George Mason University

Identity

- Identity is the fundamental concept of uniquely identifying an object (person, computer, etc.) within a context (department, enterprise, country, global, etc.).
- Types
  - Local, corporate, national identity
  - Global identity often exists in technical world and is likely to be computer-generated.
Identity Management

- Security objectives
  - Keeping “bad guys out” and “good guys in”
- Identity management is for letting good guys in.
- IM within organization
  - To make sure organization employee’s authentication and authorization
- IM with inter-organizations
  - The ability to federate identity across organizations

Microsoft .Net Passport

- Centralized identity management architecture
- Manage unique IDs with every user
  - No need to for remembering multiple IDs and passwords
  - No special infrastructure is required
Liberty Alliance

- Multinational, multi-industry consortium
  - Over 150 companies, non-profit and government organizations from around the world
- Develops a set of open standards for federated network identity
- Extends security assertion markup language (SAML) to include additional security enhancements such as
  - Opt-in account linking
  - Simple session management
  - Global log-out capability
- SAML is a XML based security standard that provides a way of exchanging user authentication information

Liberty objectives

- Enable consumers to protect the privacy and security of their network identity information
- Enable businesses to maintain and manage their customer relationships without third-party participation
- Provide an open single sign-on standard that includes decentralized authentication and authorization from multiple providers
- Create a network identity infrastructure that supports all current and emerging network access devices
Federated Network Identity

- **Network Identity**
  - A **global set of user attributes** (username, password, preference info, etc.) constituting the various accounts

- **Circles of trust**
  - Businesses affiliate together into circles of trust based on Liberty-enabled technologies

- **ID Federation**
  - Users federate otherwise isolated accounts (local IDs)

- **Three actors**
  - **User**
  - **Identity Providers**
    - Service providers offering business incentives so that other service providers affiliate with them
    - usually the entry point into a Circle of Trust
  - **Service Providers**
    - Organizations offering Web-based services to users. (includes any organization on the Web)

Why Federation

- Federation is the way the world works today (drivers license, national ID, SIM cards…)
- Federation facilitates scalable, efficient, user-friendly, cross-domain Identity Management
- Without Identity Management, federation fails…
  - interactions and transactions become more difficult, if not impossible
- Federation is a foundation for pseudonymous and anonymous secure business relationships
  - Federation allows to identify an individual with two tags:
    - The tag of an Identity Provider and
    - The individual's Identity Provider specific tag
  - Can decrease, even eliminate, the need for a Global User ID
Federated Network Identity

Identity Federation - Example

User logs in at a Liberty-enabled Website
Identity Federation - Example

- User is notified of eligibility for identity federation and elects to allow introductions.

Identity Federation - Example

- User signs-on using his local service provider identity.
Identity Federation - Example

User is prompted to federate his local identities and selects "yes."

The Websites federate the user's local identities.
Single-Sign-On - Example

User logs in to identity provider's Website using local identity.

- User proceeds to service provider's Website, and his authentication state is reciprocally honored by the service provider's Website.
- No Identity provider identifier at service provider.
Liberty Functional Requirements

- Identity federation and defederation
- Authentication
  - Between IP, SP, and Users
- Use of pseudonyms
  - unique on a per-identity federation basis across all identity providers and service providers
- Support for anonymity
  - A service provider may request that an identity provider supply a temporary pseudonym that will preserve the anonymity of a Principal
  - A user does not need to consent a long term relationship with the service provider
- Global logout
  - notification of service providers when a user logs out at identity provider

Liberty Architecture

- Three components
  - Web redirection
    - Action that enables Liberty-enabled entities to provide services via today’s user-agent-installed base.
  - Web services
    - Protocol profiles that enable Liberty-enabled entities to directly communicate.
  - Metadata and schemas
    - A common set of metadata and formats used by Liberty-enabled sites to communicate various provider-specific and other information.
Liberty Architecture

Web Redirection

- HTTP-redirect-based
- Form-POST-based
- Cookies
HTTP-redirect-based Web Redirection

1. HTTP request (GET) by click a link
2. Response w/ status code of 302 (a redirect), alternate URI (ID provider) and a second, embedded URI of service Provider in location header.
3. HTTP request to ID provider w/ Service Provider URI.
4. Response w/ a redirect w/ service provider URI and optional second URI pointing back to itself.
5. HTTP request w/ optional ID provider URI.

HTTP Redirection - Example

- User arrives at service provider's website
HTTP Redirection - Example

• Redirect to the login page the identity provider

User

CarRentalInc

User

CarRentalInc

Airlines Inc

Airlines Inc

Redirect from http://www.aireline.com/logon

• User agent is redirected back to the service provider's website and provided usual access
Form-POST-based Redirection

- Steps changed from the http-redirection
  1. The service provider responds by returning an HTML form to the user agent containing an action parameter pointing to the identity provider and a method parameter with the value of POST. Arbitrary data may be included in other form fields. The form may also include a JavaScript or ECMAscript fragment that causes the next step to be performed without user interaction.
  2. Either the user clicks on the Submit button, or the JavaScript or ECMAscript executes. In either case, the form and its arbitrary data contents are sent to the identity provider via the HTTP POST method.

Form-POST-based Redirection: Example

- User arrives at service provider’s website
Form-POST-based Redirection: Example

- Service provider displays an embedded form
- The login info is conveyed to the identity provider with POST

Using cookies?

- Not used generally
  - Cookie keeps state of web browser not a user – can be impersonated by another user.
  - Normal setting is only cookie issuer can read the cookie – change may not be an option (lower the security settings)
  - Cook turned off in many user agents.
Web Redirection Issues

- Security vulnerabilities
  - Interception – cleartext communication
  - User agent leakage
- Limitation of overall size of URIs
- However, It enables distributed cross-domain interactions such as single-sign-on with current Internet infrastructure

Web Services

- Protocol profiles that enable Liberty-enabled entities to directly communicate.
  - Between identity providers and service providers
  - RPC-like protocol messages conveyed with SOAP.
  - For:
    - policy agreements
    - authentication negotiations
    - message protection mechanisms
    - service discovery and addressing
Metadata and Schemas

- A common set of metadata and formats used by Liberty-enabled sites to communicate various provider-specific and other information
  - Account/identity:
    - user handles (names) that
  - User authentication context:
    - Methods, mechanisms, protocols, etc
  - Provider metadata:
    - Identities, credentials, X.509 certificates, service endpoints

SSO and Identity Federation (1)

- User initiates federation of two identities.
Each provider creates entries in their user directories for user handles.
- Bilateral handle exchange is optional.
- Can have multiple handles for a user.
- A single handle for each service provider that has multiple Websites.

User directories of the identity provider and multiple service providers upon identity federation.

SSO and Identity Federation
(2)

SSO and Identity Federation
(3)
SSO and Identity Federation

A user with two identity providers federated to a service provider
- User's changes between identities
- Which ID provider is used?
- Need to remember to federate new SP to both IdPs
Identity Provider Introduction

- Having more than one ID provider, service providers need a means to discover which ID provider a user is using
  - Using ID provider's cookies
    - A cookie is often unable to be read by another provider
  - Using Common Domain to the circle of trust

Identity Provider Introduction – Using Common Domain (1)

1. User logs in to identity provider which redirects user agent to common domain.
2. Common domain service writes cookie.
3. User navigates to service provider site.
Identity Provider Introduction – Using Common Domain (2)

4. Service Provider redirects to common domain service which reads the IDP list from the cookie.

5. Common domain service redirects user agent back to service provider with IDP list embedded in the URL.

6. Service Provider prompts user if they would like to log in via the identity provider.

Single logout from an identity provider

1. User logs out.

2. Identity Provider logs user out from Service Provider A.

3. Identity Provider logs user out from Service Provider B.
Single logout from an identity provider

1. User logs out globally.

2. Service Provider A logs Identity Provider that user has logged out.

3. Identity Provider logs user out from Service Provider B.

Diagram:

- Service Provider A
- Identity Provider
- Service Provider B
- User