Design Criteria for Integrating Multi-Factor Authentication into Single Sign-On

David Walker
dhwprof@gmail.com
MFA Cohortium Meeting
6/26/2013

Background

- Study of user experience issues by InCommon Assurance Program with CI Logon, NIH, and Department of Education
- Product was an RFP for enhancements to the Shibboleth IdP, but the issues can be generalized for other single sign-on environments.

A Couple of Definitions

- **Authentication Method** - A specific method of authentication, such as "UC Davis Kerberos," or "Virginia Tech eToken."
- **Authentication Context** - A collection of criteria related to the trustworthiness of identity assertions. This includes an Authentication Method and other criteria, such as practices for identification and registration.
  - Authentication Context may be a well-known assurance profile like InCommon Bronze or Silver, or it may be locally defined.

Primary Use Cases

- The SP requires a specific Authentication Context.
- The SP requires one of a list of Authentication Contexts, presented in priority order. The service provided may vary, depending on the Authentication Context selected.

Issues

- Different Service Providers (SPs) require different Authentication Contexts.
- Some Authentication Contexts can be used to satisfy the requirements of others.
- Different authentication contexts may require different authentication methods.
- Not all users are able to use all authentication methods.
- We need to make this all work naturally in a single sign-on environment.

Another Issue

- The Identity Provider (IdP) presents a list of viable Authentication Methods to the user.
- Should a "pre-login" be required?
- Pros and Cons
  - The list of viable options may represent a security vulnerability.
  - Requiring pre-login allows the list of viable options to be tailored to the user.
  - Requiring pre-login might be an extra step for the user.
- Decision for the Shibboleth RFP was to make this a configuration option.

The Multi-Context Login Flow - 1

- 1 - The user browses to an SP.
- 2 - The SP requests identity information from the IdP. Authentication Context may be part of that request, depending on protocol.
- 3 - The IdP determines the Authentication Contexts that satisfy the SP's requirements, consulting:
  - The SP's specific requirements (either in its request, or configured in the IdP),
  - The IdP's configured hierarchy of Authentication Contexts, and
  - The user's allowed Authentication Contexts.

The Multi-Context Login Flow - 2

- 4 - If the SP's highest-priority Authentication Context is satisfied by an existing session with the IdP, that Context is returned to the SP.
- 5 - If not, the IdP presents the viable Authentication Methods to the user.
- 6 - The user selects one of the Methods and authenticates. The Context associated with the selected Method is returned to the SP.

Questions?

- *Assurance Enhancements for the Shibboleth Identity Provider (19 April 2013)*
  - https://spaces.internet2.edu/download/attachments/37650957/AssuranceReqShibIdP-19Apr2013.pdf
- David Walker <dhwprof@gmail.com>