Configure a Service Provider to Force Re-Authentication

Purpose

This document describes how to configure a Shibboleth Service Provider (SP) to force re-authentication of a user instead of using Single Sign-On (SSO).

Background

After a user is authenticated by the UW Identity Provider (IdP), they may be able to access other Shibboleth-protected applications without having to logon again for up to 12 hours. This SSO capability is one of the primary benefits of integrating a web application with Shibboleth. In some cases, however, an application may wish to force users to re-authenticate even if they present a valid session cookie. This is sometimes done for sensitive applications that want to reduce the risk of a valid user session at an unattended computer being used by another person to access data inappropriately.

Configuration

Forced re-authentication is configured in the `shibboleth2.xml` file. Where you make the changes within this file depend on how you've configured session initiation for your application.

Once you find the appropriate session initiator for your application, you will need to add `forceAuthn="true"` to that element. Three examples follow:

If your application uses the `<SSO>` element within `<ApplicationDefaults>`:

```
<SSO entityID="urn:mace:incommon:washington.edu" forceAuthn="true">
    SAML2 SAML1
</SSO>
```

If your application uses a `<SessionInitiator>` element within `<ApplicationDefaults>`:

```
<SessionInitiator type="Chaining" Location="/Login" isDefault="true" id="Login"
    entityID="urn:mace:incommon:washington.edu" forceAuthn="true">
</SessionInitiator>
```

If you have configured an application override for you application and want forced re-authentication to affect only this application and not other applications on the same web site, you would make the change to the `<SessionInitiator>` element within the `<ApplicationOverride>` element rather than within the `<ApplicationDefaults>` element.

See Also

- Shibboleth Project's SessionInitiator reference
- Shibboleth Project's ApplicationOverride reference