Web Authentication Protocol Flows
PIN & Shibb – CAS & OAuth

by Marlena Erdos
Oct 2014
Supporting materials for the Behind The Login Screen talk.
Shibboleth and PIN Protocol Flow Over HTTP

User tries to contact protected app:
http://example.com/App

Three stages of the interaction:
Session Initiation & Checking
AuthN Request & Response
Response Processing

Key entities are:
App
AuthN Protocol Module
Authentication Service

By Marlena Erdos with partial inspiration from Chris Bongaarts
User contacts app: http://example.com/App
AuthN module via HTTP GET

Module: If cookie sent, then retrieve session info based on cookie. Then look at session lifetime and inactivity timers. If no cookie or timer has expired prepare to issue authN request.

Module: Look up info for authentication service e.g. urls, certificate

Module: Look up info for Authentication Service e.g. urls, certs

Module redirects to AuthN service w/ AuthN Rqst via HTTP response with Redirect status code

Continued on next slide
Shibboleth AuthN Request & Response

AuthN Service
(Shib IdP, PIN Server, CAS, Server, Oauth Server)
aka “Identity Provider”

AuthN session storage

AuthN Rqst via GET. Any cookie for the AuthN service goes along as part of the HTTP GET request

AuthN Svc: If cookie sent, then retrieve session info based on cookie. Then look at session lifetime and inactivity timers for the requesting app! If no cookie or timer has expired, return the login page.

Login Page form html sent on HTTP OK response in the body!

Login info from user

Attribute Request

Attribute Response

AuthN Svc

IdP redirects to SP: authN response w/ attrs

Legend: Flows in Parens () are the second half of a redirect

Browser

Attribute Service (e.g. HU-LDAP)

Start Here
AuthN Request in HTTP redirect response

Web Server

AuthN Module

(IdP redirects to SP: authN response w/ attrs)

Continued on next slide

All materials by Marlena Erdos
Shibboleth Response Processing

Browser

<table>
<thead>
<tr>
<th>SP Module</th>
<th>Web Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP performs attr transformations</td>
<td></td>
</tr>
<tr>
<td>SP performs attr filtering</td>
<td></td>
</tr>
<tr>
<td>SP stores transformed attrs</td>
<td></td>
</tr>
<tr>
<td>SP redirects to original url; sets session cookie</td>
<td></td>
</tr>
<tr>
<td>SP looks up attr info based on cookie and stored info</td>
<td></td>
</tr>
<tr>
<td>SP sets environment variables for App</td>
<td></td>
</tr>
</tbody>
</table>

Request to http://example.com/app flows to app w/ attrs in environment variables

App makes authZ decision; Does other processing:

App returns response page to user

Legend: Flows in parens () are the second half of a redirect