Password as AAI attribute

A presentation about AAI blasphemy :-)

SWITCH

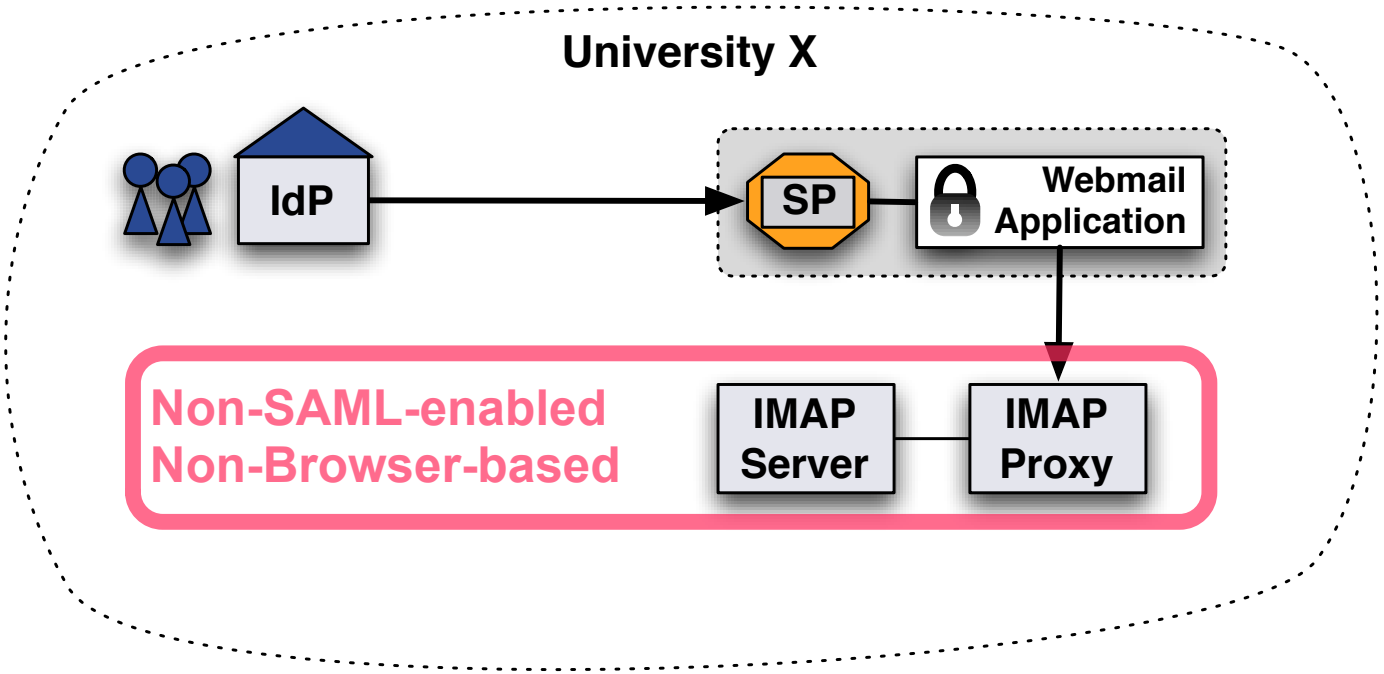
Serving Swiss Universities

Lukas Hämmerle
lukas.haemmerle@switch.ch

Bern, 16. September 2009

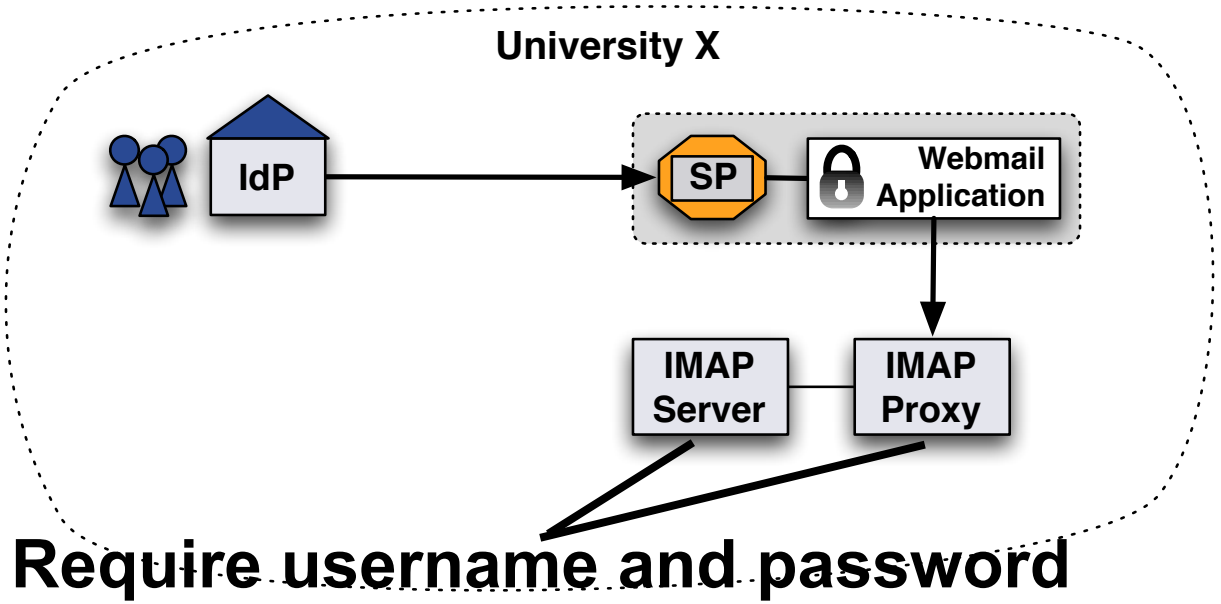
Scenario where AAI couldn't be used

Web applications like web mail cannot easily be AAI-enabled (yet) because there are **non-browser based** components involved that **don't understand SAML**.



A possible solution

Webmail could access IMAP if SP could provide user's IMAP login name and password...

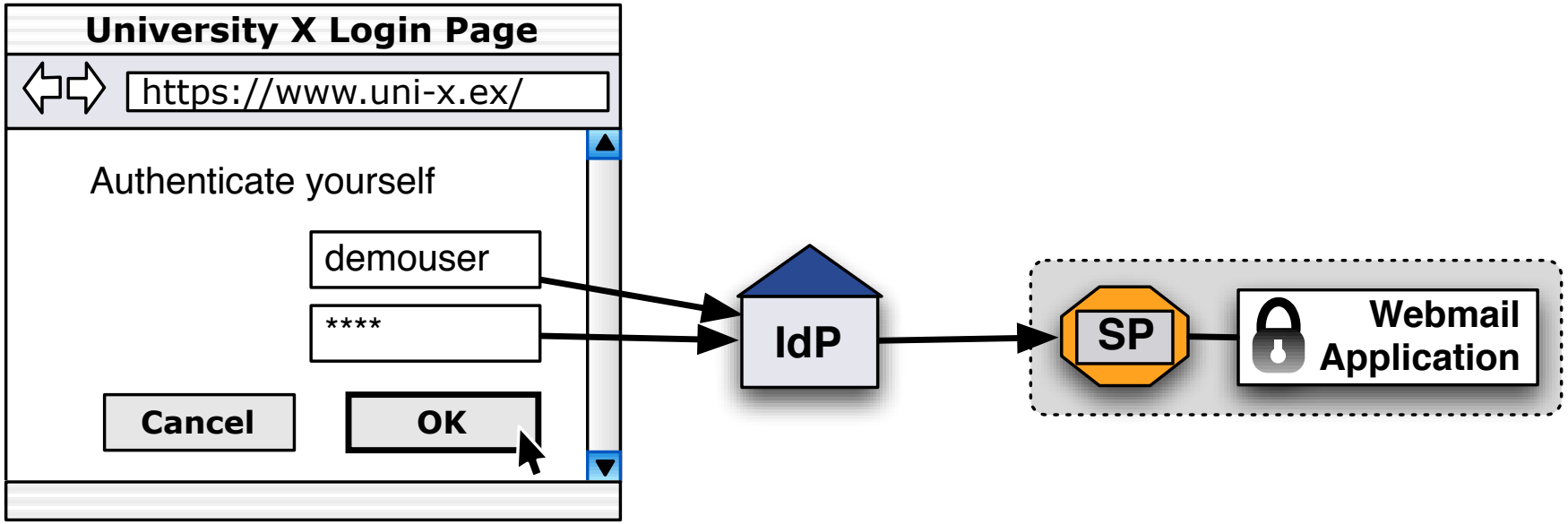


But password is not an AAI attribute and cannot be extracted from ActiveDirectory...

However...

... the password in AD/LDAP is not required because:

1. User enters password at IdP login page.
2. IdP can get access to the password
3. IdP then just needs to treat it as an attribute



And this actually works :-)

```
Attributes
Shib-EP-Affiliation: 1 value(s)
Shib-EP-Entitlement: 7 value(s)
Shib-InetOrgPerson-givenName: 1 value(s)
Shib-InetOrgPerson-mail: 1 value(s)
Shib-InetOrgPerson-mobile: 1 value(s)
Shib-Person-surname: 1 value(s)
Shib-Person-password: 1 value(s)
Shib-Person-telephoneNumber: 1 value(s)
Shib-SwissEP-HomeOrganization: 1 value(s)
Shib-SwissEP-HomeOrganizationType: 1 value(s)
Shib-SwissEP-UniqueID: 1 value(s)
persistent-id: 1 value(s)
```

The benefits

- Webmail and other internal applications also can be used with Single-Sign On
- One login name/password pair less for the users
- Fine-grained access control rules can be easily enforced

Requirements for password attribute

Identity Provider

- Shibboleth Identity Provider 2.1.3
- UsernamePassword handler must be used
- Scripted attribute definition in attribute-resolver.xml
- Filter rule in attribute-filter.xml that ensures password is only released to very specific internal services!
- retainSubjectsPrivateCredentials must be true in web.xml

Service Provider

- Attribute definition for password in attribute-map.xml
- Filter rule in attribute-policy.xml to accept password only from Home Organisation

Code example for attribute-resolver.xml

```
<!-- Add password as attribute-->
<resolver:AttributeDefinition id="password" xsi:type="Script" xmlns="urn:mace:shibboleth:2.0:resolver:ad">
  <resolver:AttributeEncoder xsi:type="SAML1String"
       xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
       name="urn:mace:dir:attribute-def:password" />
  <resolver:AttributeEncoder xsi:type="SAML2String"
       xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
       name="urn:oid:1.3.6.1.4.1.1466.115.121.1.40"
       friendlyName="password" />
<Script>
          <![CDATA[
importPackage(Packages.edu.internet2.middleware.shibboleth.common.attribute.provider);
importPackage(Packages.edu.internet2.middleware.shibboleth.idp.authn.provider);

// Create new password attribute
password = new BasicAttribute("password");

// Get subject
userSubject = requestContext.getUserSession().getSubject();

// Get credentials
i = userSubject.getPrivateCredentials().iterator();

if( i.hasNext() ){
  // Set password as attribute
  password.getValues().add(i.next().getPassword());
}
          ]]>
</Script>
</resolver:AttributeDefinition>
```

But keep in mind...

© Lord of the Rings

You shall not pass(word-enable)

services outside your organization boundaries and
you shall use this feature only very very carefully!

Quick Summary

- Password that user enters for authentication at IdP can be released as attribute by Identity Provider
  (even in the case of Active Directory)

- Allows shibbolizing web mail and other applications

- Should be used very carefully and only internally!

Please contact aai@switch.ch if you are interested.