

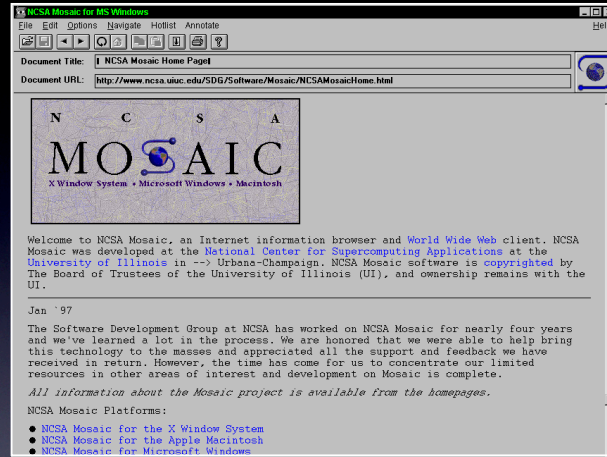
Web Authentication with Shibboleth

A view from the Flat East

Jon Warbrick
Computing Service
University of Cambridge
jw35@cam.ac.uk



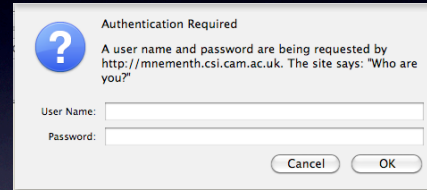
“Shibboleth, as a way to authenticate people to web sites, has been around in the UK for several years and yet many people don't know what it really does and some people still haven't heard of it. This session will take a quick look at the web authentication landscape, briefly consider what Shibboleth is and how it fits into this landscape, and take a look at what it has, is, and perhaps one day might be used for within the University of Cambridge.”



Once upon a time there was the web...

Once upon a time there was the web...and it was free and open and everyone was happy (and probably wore sandals and had beards).

...and then sites started to want to identify their visitors



Authentication Required

A user name and password are being requested by <http://mmenth.csi.cam.ac.uk>. The site says: "Who are you?"

User Name:

Password:

Cancel OK

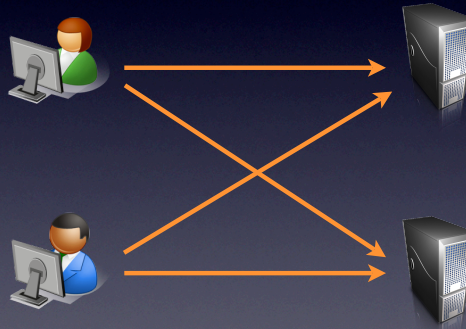
```
<Location /basic>  
  AuthType Basic  
  AuthName "Who are you?"  
  require valid-user  
</Location>
```

Obviously there are lots of good reasons for doing this:

- Making money
- Keeping things secret
- Providing personalisation

The joys of HTTP basic auth.

To each site its own users



But you are heading for a n -squared problem – password hell for users and administrators.

Organization-wide SSOs

- University of Cambridge Raven
- Oxford WebAuth
- Classic Athens (R.I.P.)
- Google
- etc, etc, ...

The web resource you requested requires you to identify yourself [help - why am I seeing this?]. This resource is provided by the website at www.maa.ac.uk. You should only proceed if you are happy to be identified to this site.

User-id:
Password:
 override login options for this session?

Always call your web browser when you have finished accessing services that require authentication. Do not disclose your Raven account to anyone and only enter it on web pages with URLs that start to begin /raven.maa.ac.uk. Please report attempts to obtain your password by other means.

University of Oxford Single Sign-On Login

The service you have requested is accessed via the University of Oxford Single Sign-On system.

Username:
Password: [Forgotten password?](#)

Please enter your Oxford username and password then click the "Login" button.

Not yet activated? [\[Activate a new account!\]](#)
[I don't know what to do!](#)

[Oxford University Computer Usage Rules and Etiquette](#)

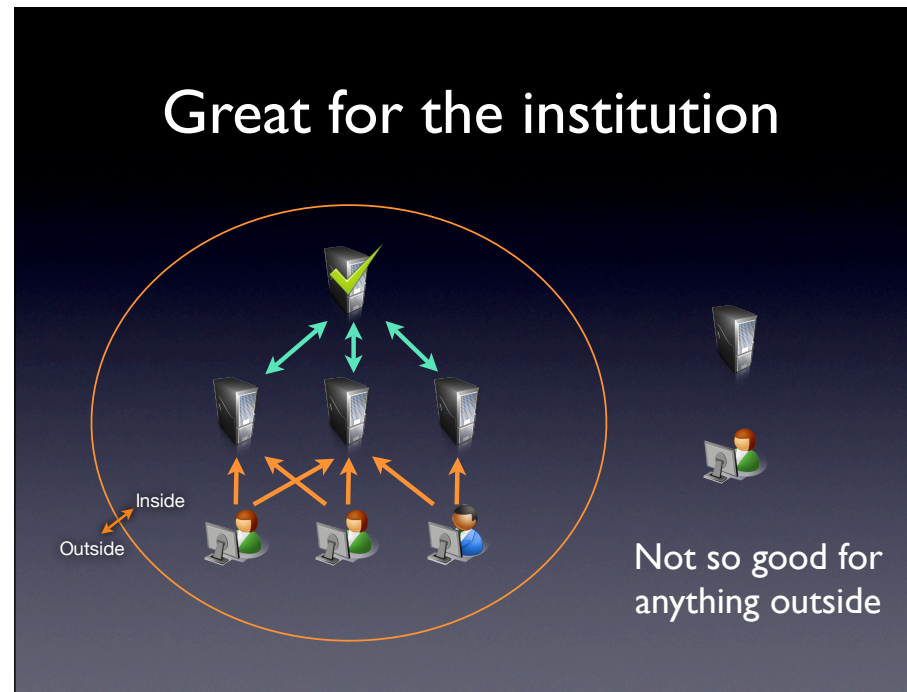
Sign in with your **Google Account**

Email:
Password:
 Stay signed in

[Can't access your account?](#)

So to address that, organizations all move to some sort of central authentication, probably doing some sort of SSO while you are at it.

Note that most of these leverage HTTP redirects so that passwords are only ever given to one recognizable service. This is at least a reasonable way to use passwords, despite the fact that **PASSWORDS DON'T WORK**, but that's another story.



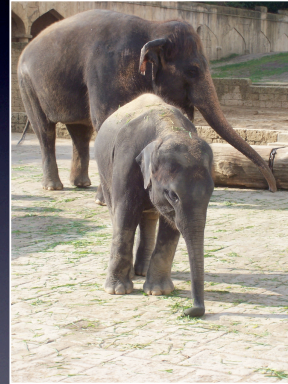
In this and subsequent slides, the orange line represents your institution's 'organizational' boundary

All this works quite well for people and servers within the organization, but isn't so good for people outside, nor for external servers. And note that people on the inside may not really notice this...

Note the assumption about one IdP.

Two elephants

- Data protection
- Trust



Once you start dealing with things outside the institution border you rapidly run into two big problems.

EU data protection legislation, and so our DPA, makes transferring ‘personal’ data somewhere between hard and impossible. Interesting in an education context the US have it if anything worse than we do (even though in all other contexts privacy may be non-existent).

The other problem is one of establishing trust. How can an external site know to trust you (and remember they will be dealing with us

Enter the Griffin

- AKA Shibboleth
- A Web Auth system designed to support (though not to require)
 - multiple IdPs
 - inter-organization use
 - privacy and anonymity
 - multiple attributes



A possible solution is Shib. Not quite clear what Shib is – potentially a protocol (though less so now with the move to SAML2), a reference implementation written by Internet2, or an architecture and policy framework.

Emerging chicken-and-egg situation – is Shib based on SAML, or SAML based on Shib?

Myth and Legends

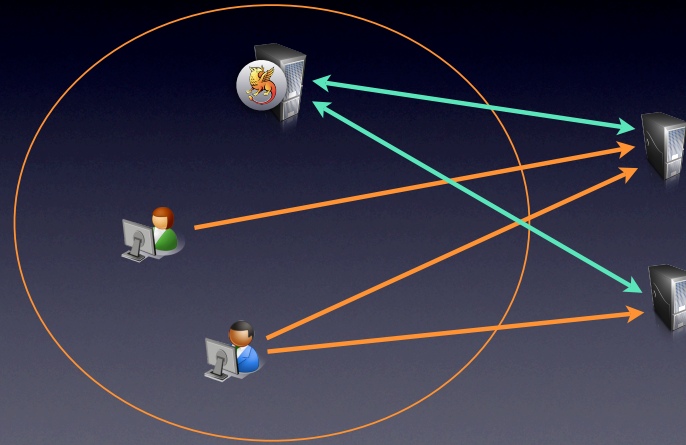
- Shib is only for e-Journals
- Only supports anonymity →
- Only supplied by Internet2
- Doesn't do standards
- Is really hard



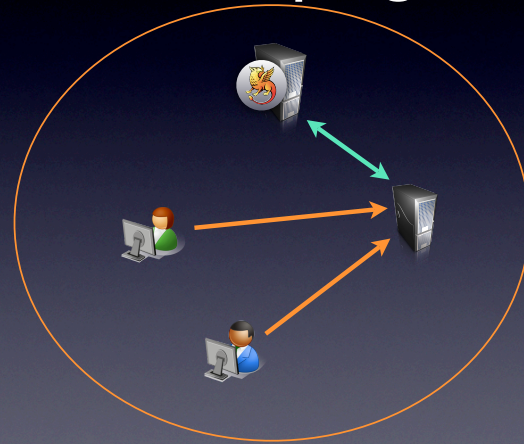
- E-Journals an early use case, and the one widely deployed in the UK
- The e-journals case tends to take advantage of the anonymity features, but you don't have to
- The reference implementation is by Internet2, but other implementations are springing up. The move to SAML2 in Shib2 opens up increased possibilities for interworkong with generic SAML S/W
- Shib 1 invented some new protocols and flows to support SP-first authentication. Everything that Shib needs is now part of SAML2
- It's not that hard. Really.

So, what can we do
with it?

E-Journals

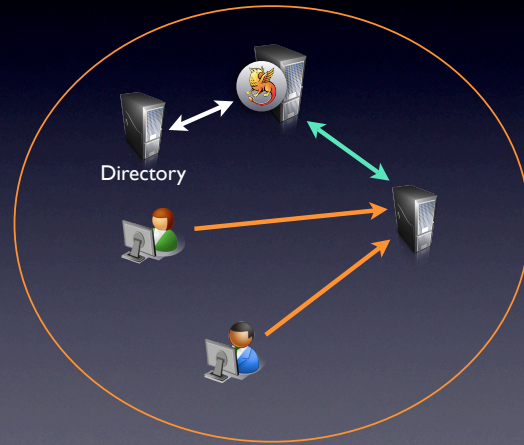


Standard web server plugins

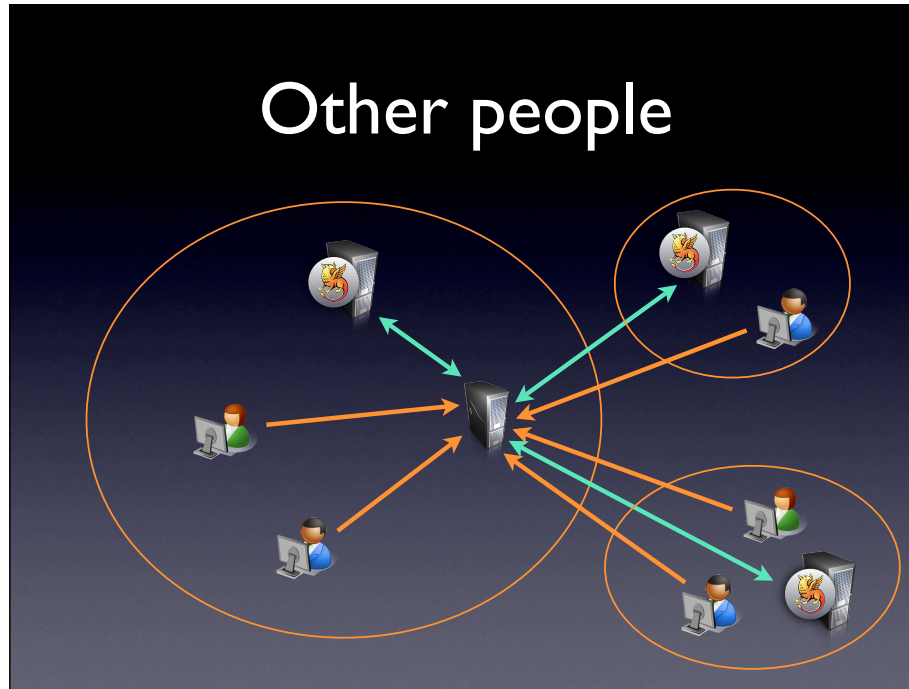


e.g. UofC have discontinued our Ucam WebAuth IIS plugin

Authorization decisions

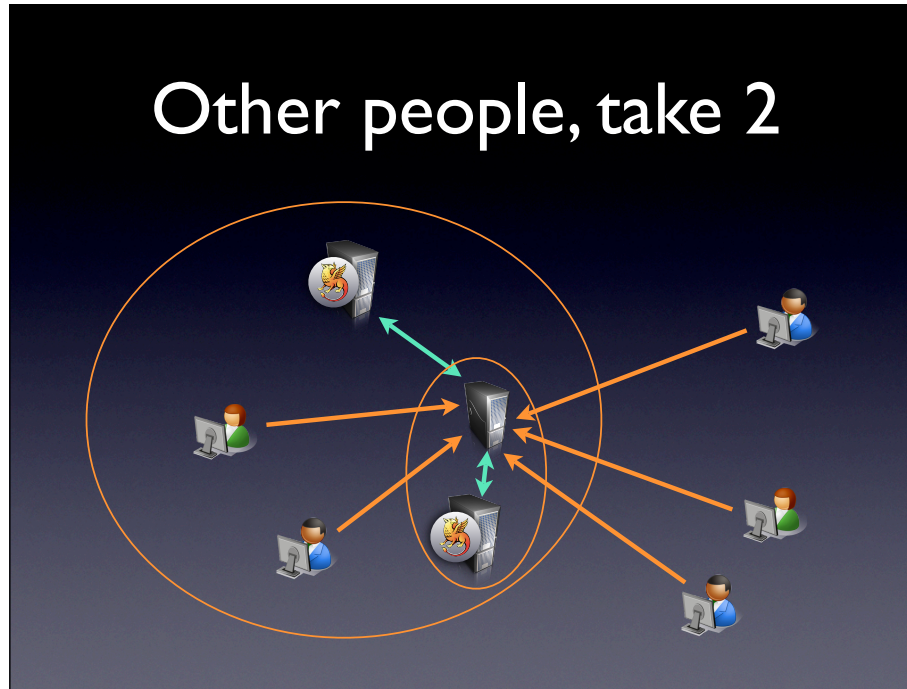


Other people



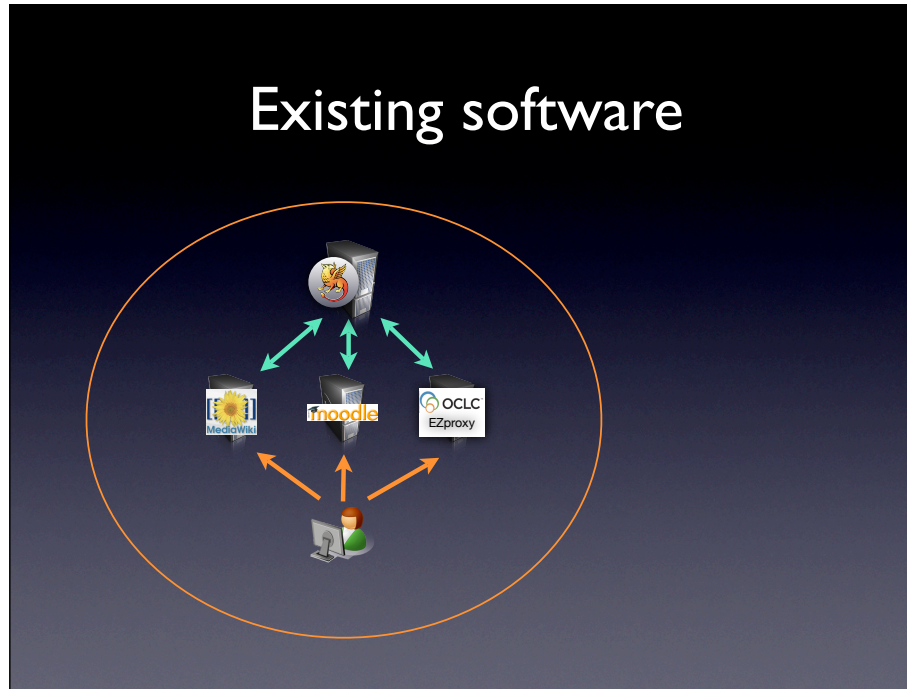
No ~~man~~ institution is an island

Other people, take 2



Anyone can run their own idP

Existing software

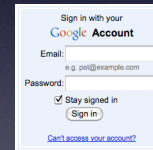


This slide is almost with out doubt out of date

VHS vs. Betamax



Facebook Connect



Google Friends Connect

Thanks for listening...

- There may be questions...
- ...including perhaps 'Why "Shibboleth?"





“On the Internet, nobody knows you are a dog...”

...but sites often want to know that you are the same dog as last time”





Credits

- 'In the Field', Julian Wearne, <http://www.flickr.com/photos/ikaink/4184787380>
- Mosaic screen shot courtesy of NCSA/University of Illinois <http://www.ncsa.illinois.edu/News/Images/>
- two elephants, Timo Heuer, <http://www.flickr.com/photos/upim/293676365/>
- Fire Breathing Mythical Dragon, Wili Hybird, <http://www.flickr.com/photos/walkadog/3484426248/>
- "On the Internet", by Peter Steiner, page 61 of July 5, 1993 issue of The New Yorker, (Vol.69 (LXIX) no. 20). Reproduced only for academic discussion, evaluation, and research.
- "Same dog as before": "[Tofu, online trust, and spiritual wisdom](#)" from the Pushing Strings" blog by Eve Maler.