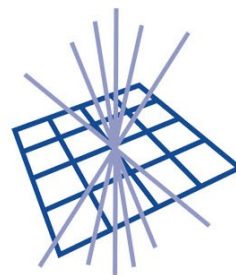


Security Middleware

Andrew McNab

University of Manchester

MANCHESTER
1824



GridPP
UK Computing for Particle Physics

Overview

- GridSite status
- CSRF
- Login pages
- www.gridpp.ac.uk

GridSite in use

- GridSite continues to be used for
 - Websites (eg GridPP!)
 - Web service hosting (eg WMproxy)
 - Grid security toolkit
(eg in gLite LB, CREAM)
 - Command line tools (eg CREAM WNs)

GridSite in GridPP3

- During GridPP3, intend to maintain GridSite and respond to requests for changes
 - eg new VOMS attribute handling
 - porting to later versions of Apache etc
- Rather than developing major new features **after** the current round of preparations for v 2.0

GridSite AURIs

- In the last year, we have made some major changes to the way GridSite handles credentials internally
- Now use generalised “Attribute URIs” which can be extended by developers or even site admins
- This has given options for new credential types (eg Kerberos) and has helped with CSRF...

CSRF

- “Cross Site Request Forgery” is a class of attacks against websites.
- Involves tricking authenticated users into carrying out actions
 - eg by clicking on a form button which submits a command to **another** website
 - If the user is already authenticated there, it might be possible to get Something Bad to happen

CSRF

- In the general web world, this means users with authentication cookies from, say, Google Mail.
- Several methods can mitigate this, including checking the Referer: header or using “double submit cookies”
- The problem is worse for us, since with X.509 certificates in browsers, users are always logged-in

GridSite and CSRF

- GridSite now implements a solution for this based on double-submit cookies
- Instead of authenticating users directly from X.509 certificates, we allow them to login with X.509 and give them a cookie in return
- To delete a file etc, their browser presents this cookie twice: in HTTP headers and in the HTML form contents, which stops CSRF attacks.

GridSite logins

- GridSite allows “automatic” logins from X.509
 - Get a cookie the first time you visit that session
- But also allows a separate login page, and this is the option which will be used for the new GridPP website
- At the bottom of each page, there will be a “Login” link which takes you to a login form...



GridPP Login Page - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://www.gridpp.ac.uk/login/ Google

 **GridPP**
UK Computing for Particle Physics

Home : Site Map : Grid Support : Website Help

Search

GridPP Login Page

Welcome back /C=UK/O=eScience/OU=Manchester/L=HEP/CN=andrew mc nab

This form allows you to login to the GridPP website using your X.509 user certificate.

Last modified Wed 12 March 2008 . [View page history](#)

You are /C=UK/O=eScience/OU=Manchester/L=HEP/CN=andrew mc nab

[Edit page](#) . [Manage directory](#) . [Switch to HTTP](#) . [Website Help](#) . [Print View](#) . Built with [GridSite 1.4.3](#)

GridPP Open Source Policy

 Science & Technology
Facilities Council



Done www.gridpp.ac.uk  

GridSite logins

- The login form will initially be very simple, with just a button saying “login” and the text “You are /CN=joe user” or whatever
- You press the button and are taken straight back to the page you were looking at: but now you have a login cookie and can edit pages
- In the future, can add options for username / password logins too (Shib, OpenID, Kerberos, etc)

Why a login page?

- The login form will be placed on a different virtual webserver: <https://login.www.gridpp.ac.uk/>
- This means we can have separate authentication zones to prevent escalation attacks.
 - eg J. User's cert is stolen; nasty Javascript put on his part of site; P.M.B. User looks at this and the Javascript then makes all the PMB docs world readable.

(How this works)

- You can share cookies between sites (eg <https://login.www.gridpp.ac.uk> and <https://www.gridpp.ac.uk>) but restrict what directories they are visible to (eg /pmb/)
- Since users can't upload nasty Javascript to <https://login.www.gridpp.ac.uk> they can't upload code to steal cookies via XMLHttpRequest (since **that** can't be used between sites, unlike cookies)

www.gridpp.ac.uk

- www.gridpp.ac.uk is being revamped:
 - Neasan has produced a new template and set of sections
 - Changes being made to blogs, news etc
 - We all need to revise lists of who can edit what zones (DN Lists, GACLs etc) ... **look out for forthcoming email about this**

Summary

- GridSite continues to be used for web services and websites
- Finalising AURIs and cookie-based logins
- GridSite 2.0 will wrap up all these features
 - Then move to maintenance
- www.gridpp.ac.uk being revamped, and will include all this