CUWebAuth 2.0

Peter Bosanko
bosanko@cornell.edu

October 14, 2008

Greg Roth
gbr4@cornell.edu
CUWebAuth Features

• End-To-End Kerberos 5
• Integrated Authorization
• Easy, Flexible Integration (200+ Websites)
• Efficient POST Data Support
• Stateless, Scalable WebLogin Server
• WebDAV Support
• Automated Regression Testing
• Cross Platform (Linux, Solaris, BSD, Win32)
End-to-end Kerberos 5

- Multiple Kerberos Realm Support
- **Active Directory Supported**
- Kerberos Credentials Sent Through Browser.
  - GSSAPI Initial Context Token
- WebLogin isn’t a Credential Mint
  - Kerberos KDC Mints Credentials
- Multiple Domain Support
  - Credentials Aren’t in Domain Cookies
- Fat Client Can Bypass WebLogin Service
Flexible Integration

• Alternative Authentication Mechanisms
  ➢ No-prompt option

• Authorization
  ➢ Permit Portal

• Re-Prompting
  ➢ Based on Session Time
  ➢ Based on Credential Age

• N-Tier Support
  ➢ Proxy Portal

• Self Service ServiceID/Keytab issuance
Integrated Authorization

- HTTP Based
- Grouper / Permit Bridge
- Active and Static Content
- Active and Passive Application Control
- Lookup Cache
  - less load on central infrastructure
Future

• Shibboleth Bridge
• Two-Factor Authentication (RADIUS)
• User Delegation
• Support for other AuthN stores
• Client Certificates
• Browser Plug-In
CUWebAuth
Detail Slides
Supported Platforms

• Apache 2.2, Apache 2.0
  ➢ Binaries available for Linux (32 and 64 bit), Solaris, OpenBSD and Windows NT 5.1+ if you are using OpenSSL 0.9.8
  ➢ Source code available, works on OS X (last we checked).

• IIS 6, IIS 7
  ➢ Coming real soon now.
  ➢ Windows 2000 is no longer supported by Microsoft and does not receive security updates, so it makes a poor platform for a secured web server
Some Authorization directives

- require permit cu.employee cu.student cu.retiree
  - Restricts the page to members of one of those permits [old]
  - Your application also gets CUWA_GROUPS which lists the subset of the permits that the user has [new]

- CUWAInquire cu.employee cu.student cu.retiree
  - Your application gets CUWA_GROUPS which lists the subset the user has [new]. This doesn’t prevent any access.

- CUWAInquire all
  - CUWA_GROUPS includes all the permits that a user has.
  - Except it only shows permits that your ServiceID is authorized to see.
require noprompt

- If the user is authenticated, CUWA and REMOTE_USER variables are populated.
- Anonymous access is still allowed
- If the user has a non-expired single sign on session, the user is logged in.
  - As of 2.0.1.160
Candidates for noprompt

• Applications like confluence
  ➢ Public sites with users outside the Cornell community

• Applications with non-browser clients where any other mechanism breaks the application
  ➢ Hudson
  ➢ Fortify

• If the application should be restricted to the Cornell community, avoid noprompt.
Forcing Reprompts

• CUWACredAge X
  ➢ On initial access to WebAuth, disallow the use of a single-sign-on cookie that is more than X seconds old.

• CUWAInactivityTimeout Y
  ➢ A session that is inactive for Y seconds will be deleted and the user will be redirected to WebLogin. Depending on the value of CUWACredAge they might also be reprompted.
High Availability

or why webauth keeps connecting to weblogin

- Every 5 minutes, WebAuth contacts each weblogin server over SSL to port 443 and GETs the following files
  - /HA/servers
  - /HA/status

- Your site might go down during maintenance if you only configure one server.

- We reserve the right to add servers. Allow the entire class C subnet through your firewall.
CUWA Portal Permit

<location /CUWA/Permit>
  SetHandler cuwa_permit
</location>

Get /CUWA/Permit?netid=gbr4&permits=all http/1.0
200 ok
gbr4
cu.employee cit.staff cit.idm...
CUWL_DUMPCONFIG

• If you include the header
  ➢ CUWA_DUMPCONFIG: foobar
• We print the part of the configuration relevant to the request to your error_log. grep `\[foobar\]`
• Setting the directive cuwa.dumpcfg 100 will make that log message come out at [emerg]
• Helpful for debugging apache configurations
• wget --header “CUWA_DUMPCONFIG: foobar” url
• Introduced in 2.0.1.161
Quality Control

- Automated Build System
- Automated Test System
- Security Auditing
  - Fortify
Mailing Lists

- **CUWA-ANNOUNCE-L@cornell.edu**
  - Very low traffic announcement list.
- **CUWA-L@cornell.edu**
  - Discussion list. Low traffic.
CUWAPortal/Proxy Time Sequence
Arrows/boxes are the color of the HTTP request initiator.