Middleware: It’s Better Than Big E-mail Attachments

Lessons from the National Science Foundation’s Middleware Initiative

Jill Gemmill, UAB
Academic Computing / Computer and Information Sciences
This work is the intellectual property of the author. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.
Email Attachments???

- Send info to exactly the right people
- Don’t need to worry about where to store it
- Recipient has no difficulty locating the information
- We don’t need to share the same computer, the same system administrator, or same management to share data
- I could put it on a web site (extra work) but then it’s either public or I need to send out more passwords
With Middleware.....

- Placing information where the right other people can get to it should be easy
- Won’t need to carry a list of logins/passwords in your wallet
- Sharing information/resources should be easy
- Sharing your data/resources should be easily managed ....by you
About NMI

- National Science Foundation Middleware Initiative
- 2001-2004
- To help scientists and researchers use the Internet to effectively share instruments, laboratories and data, and to collaborate with their colleagues.
- Software; standardized methods and practices
NSF Middleware Initiative Release 3.0

NMI-R3 is out! Featuring the GRIDS Center Software Suite and NMI-EDIT Components, the latest NMI release integrates key software packages, standards, and best practices for science, engineering, and education. Downloads are free to the public. NMI releases arrive every six months -- in October and April -- to provide the stable, predictable middleware infrastructure that the community has identified as an important need. NSF issued a press release about NMI-R3.

InfoWorld Honors NMI Principal Investigators

InfoWorld magazine’s list of the top ten 2003 Innovators includes Ian Foster and Carl Kesselman of the NMI-funded GRIDS Center, with colleague Steve Tuecke of Argonne National Laboratory. The magazine cites them for "designing the most prominent grid architecture and releasing the accompanying open-source Globus Toolkit for building grids."
Grid Research Integration Deployment and Support Center

Define, Develop, Deploy, and Support an Integrated national middleware infrastructure supporting 21st Century science and engineering Applications

Enterprise and Desktop Integration Technologies

Jill Gemmill: 06/20/2003
Middleware should relieve your application of certain tasks
Why Middleware?

Once upon a time, there was a single computer with an operating system…..

- Root authority (superuser/administrator) –
  - knows location and availability of system resources
  - has list of all authorized users of the systems
  - Knows and manages all system resources
And Computing Looked Like This…

- My Lab Computer
- National Laboratory Supercomputer
- Library Computer Systems
- University Mainframe Systems
Then came the World Wide Web

- Think of amazon.com: you are logging in, with credentials hidden in cookies on your computer
- Change computers – oops, no cookies.
- Someone else uses your computer – maybe amazon thinks it’s you “Are you Jill Gemmill? If not, click here...”
Paradigm Shift

My Own Managed Computing Environment

Middleware replaces these Operating System functions:

- Login (authentication)
- Authorization (permissions)
- Process environment

- Session management
- Security
- Name space
Key Components of Middleware

- Identity / Authentication
- Authorization (Usage Policy Enforcement)
- Security
  - Access Control
  - Accounting/Logging
  - Encryption
- Resource Discovery and Management
Authentication

- Who are you?
- Sez who?
- We believe you – have a credential (session ID; signed application-specific credential; portable signed credential)

- In the Grid, access decisions are made on identity established ELSEWHERE
- AUTHORITATIVE sources for Identity are desirable
Universities have authoritative information in HR, Student, Alumni etc. systems

Standard naming and organization needed for use across organizations

LDAP Directory places information for standardized network access

UAB has implemented a central, authoritative LDAP Directory based on NMI eduPerson and LDAP Recipe
UAB Enterprise Directory Services

http://www.uab.edu/it/itd/blazerid_cycle.html
Middleware Program at UAB

- NSF ANI-022710 *ViDe.Net: Middleware for Scalable Video Services for Research and Higher Education*. Gemmill (PI), Chatterjee, Johnson, Verharen

- NSF EPS-0096193 *Alabama EPSCoR Cooperative Agreement: Internet2 Initiative* Griffin (PI), Cordes, Gemmill, Graves, Hancock, Shealy

- NSF ANI-0123937 via SURA-2002-103 *NMI Testbed Participant* Shealy, Gemmill
Authorization

- Now that we know who you are; what are you allowed to do? (Policy)
- Based on IDENTITY or GROUP MEMBERSHIP
- Example: You are a university student, therefore you can:
  - Use on-line library materials
  - Register for classes
  - Have an email address here.
Resource Allocation

- **What resources** do you need to accomplish what you are authorized to do?

- Example: You are a university student, therefore you can have an email address here. Resource needed: mailbox
Identity is Multi-valued

- Very few services requiring authentication are available to “everyone”
- GROUP memberships: Faculty; Enrolled in CS101; Biology Department; Paid member of IEEE; Collaboration partner in funded project; ..... 
- What about anonymous identity?
BlazerID Single Sign-On: Where We Are Today at UAB

- Single authoritative directory
- “White Pages”
- Microsoft Active Directory synchronization
- Oracle Initial Sign-On (no replication)
- Single management point for
  - Creating blazerid
  - password resets
  - user account creation/deactivation
What Applications can be “Middleware Enabled”? 

- Any application available via web (HTTP)
- System logins (eg UNIX)
- Videoconferencing software
- Computing resources (building “The Grid”)
PAM Architecture for UNIX authentication

- PAM stands for Pluggable Authentication Module
- Architecture for authentication/authorization
- Defined by SUN as part of DCE-OSF systems
- PAM enables administrator to select from a variety of authentication systems (/etc/passwd, LDAP, SQL, etc)
- Configurable and very powerful
An LDAP Module for PAM

- Acts as glue between LDAP and PAM
- PADL Software’s LDAP module for PAM on Unix Systems (pam_ldap)
  - www.padl.com
- Flexible and simple to configure
- Bundled with Linux distributions, must be downloaded & installed for Solaris
- See www.uab.edu/it/academic for instrux
NMI “Pubcookie”

- Pubcookie is an Apache (or IIS) web server module supporting single sign on and web initial sign on
- Content on the server is placed in a directory protected by pubcookie module
- Pubcookie requires signed credentials (the cookie) for access
- One login server manages all credentials
- Can be configured for LDAP, Kerberos, or UNIX login service
Using Pubcookie – the “Anti-Portal”

1. AUTHN

Web server A (Apache)

Web server B (Apache)

Web server C (IIS)

Web server D (IIS)

Campus Authentication Service

Login Cookie

1. AUTHN

2. AUTHZ

D Access Cookie

Private Key

Public Key

Pubcookie Login Server
Pubcookie Provides

- Web Initial Sign On for all campus web servers, for a configured time period (eg 24 hours)
- Anyone who can authenticate via your authoritative campus login service is approved for access
- Applications: library access; things for “everyone on campus”
- We put knowledge to work for Oracle sign on
Using Pubcookie for Existing Web Applications

- The Problem
  - Many Web Applications create their own authentication system
  - So, the user needs a username/password for each application

- The Solution
  - Pubcookie-enable those applications to use centralized username/password
Modifying Existing Applications

- We Pubcookie-enabled two open source applications
  - Bugzilla (Written in Perl)
  - PHPWebsite (Written in PHP)
- Similar changes were required for both applications
Modifications

- Remove old user login/password web form
  - Instead, Pubcookie authenticates the user
  - Authenticated users can proceed if they also have a Bugzilla or PHPwebsite account
- Change behavior of “Log Out” and “Change Password” pages
What about Group Membership? UAB Licensed Software Download

- **Problem**
  - Provide authenticated access to UAB licensed software
  - Students and faculty allowed, but not alumni/volunteers

- **Old approach**
  - IP based - no off campus access
  - VPN - difficult to setup for end user
Licensed Software Download Project

- Uses BlazerID and password for authentication
- Leverages eduPerson schema for usage reporting
- Implemented as Java Servlets and inherently cross-platform
- For performance reasons, only authentication is secured, not data transfer
- Source Code Available
  http://metric.it.uab.edu/cvsweb/website-auth/
Account Management Issues

- Remember, using pam_ldap solves password verification *only*, not account creation.
- Each user still needs the usual UNIX account definition:
  - BlazerID is the username
  - No password entry, disable local password
  - User id, groups, and home directory are locally defined
Current UAB Middleware target: Automatic resource allocation to authorized users

- Goal: Anyone at UAB enrolled in certain courses will have access to the campus Beowulf cluster
- Authentication: BlazerID/password used via PAM_LDAP
- Authorization: Validate course enrollment; automatically create login account (shell) if needed
- Extension: inter-realm version for multiple universities w. multiple authentication systems
Middleware for Videoconferencing Applications

- What does it take for some existing protocol to utilize middleware?
- Videoconferencing is an application naturally crossing administrative boundaries & requiring security.
- Not a web service
- H.323 ITU standard; SIP IETF standard
- Each protocol has existing authentication/security standards
Video Middleware Progress

- ITU-T has adopted our commObject schema (H.350 Directory Services for Multimedia)
- Will be submitted as informational RFC to IETF this summer
- Working on ITU-T security profile for H.323
- Sample endpoints and call servers using these directory services & authenticating with LDAP available by end of year
Remember old system?

- My Lab Computer
- National Laboratory Supercomputer
- Library Computer Systems
- University Mainframe Systems
Paradigm Shifts are not easy!!

Sidebar: What’s a portal?

Each has own Authentication And Authorization Services

- BIO Portal
- Library Portal
- Globus
- University HR/Finance/Student
“My Own Managed Computing Environment” *aka* the “uber realm”

- Everyone belongs under a single root authority
- Everyone uses same authentication system (Kerberos OR Microsoft Active Directory OR Passport OR Novell Directory Services OR Grid Security Infrastructure OR PKI…)
- Why?
  - Credentials hard to translate
  - Root needed for transfer of trust
To the Rescue: Federated Administration

- No root authority
- Many cooperating administrative domains
- Agreements negotiated as needed
- Authenticate with your authoritative home service
- Each realm chooses authentication service; don’t need to match
To the Rescue: Federated Administration (Cont’d)

- Your attempt to access a remote resource initiates transparent, standardized assertions about your identity and attributes from home to foreign realm.
- Access decision made by resource owner based on trust in credentials presented and referral to relevant policies.
- Uses Security Assertion Markup Language (SAML).
- NMI Shibboleth / PERMIS.
UAB Middleware Team

IT ACADEMIC COMPUTING
- David Shealy
- Jill Gemmill
- John-Paul Robinson
- Ramesh Puljala
- Rajani Sadasivam
- Aditya Srinivasan
- Zachariah Garner

Other IT Divisions
- Sheila Sanders
- Landy Manderson
- Joyce Iannuzzi
- Terry Tatum
- David Green
- Mike McBride