

Enabling Applications to Use Your Identity Management System

Or “Why Mark began losing his hair at age 23”

Mark Earnest

The Pennsylvania State University

Where We Are Coming From

- ❑ Authentication: Kerberos V (DCE) - aka Access Accounts
 - ❑ “Friends of Penn State” Kerberos realm
- ❑ Authorization: Mostly application specific (user lists), some DCE group usage
- ❑ No web initial sign on
- ❑ Thankfully, the vast majority of Penn State uses the centrally managed Access Accounts

Central Authorization Today

- ❑ DCE Groups
- ❑ Provisioning occurs via a variety of means:
 - ❑ Triggered automatically - eg: new student registration
 - ❑ Controlled Manually - eg: User Managed Groups
 - ❑ Delegated authority to manage these groups

Central Authorization Tomorrow

- ❑ IBM Secureway LDAP
- ❑ LDAP Groups
 - ❑ Attributes & Groups (where each makes sense)
 - ❑ Retain User Managed Groups and delegated authority
- ❑ Direct LDAP calls? Shib-like Attribute Authority?

Case Study: Portal & Webmail

- Penn State Portal and Webmail
 - Authentication and Authorization are handled at the web server via mod_auth_dce
 - AuthN/AuthZ easily changed to a single sign on architecture that uses Apache modules
 - Only sticking point is that DFS is required. SSO must be able to pass a credential that can be converted into a DCE context

Case Study: eLion & Angel

- ❑ eLion - Student and Faculty Portal
 - ❑ UserID and password are obtained via a web form and passed off onto a DLL that authenticates via DCE - DCE creds needed for RPC call
- ❑ Angel - Course Management System
 - ❑ Similar to eLion, but does not require credentials
- ❑ Both require Friends of Penn State integration

Case Study: ISIS & IBIS

- ❑ ISIS & IBIS - Student and business logic
 - ❑ Relies on front end to provide authentication
 - ❑ Authorization is done via user lists stored in local database. (IdM stone age)
 - ❑ Complete re-architecture required to integrate with modern identity management system

Migration Solutions: Cosign

- ❑ Web based initial sign on architecture using Kerberos V
- ❑ Drop in web module for Apache or IIS
- ❑ Capable of issuing Kerberos service tickets
- ❑ Current direction for Webmail, Portal, and eLion

Making Cosign Work For Us

- ❑ Current requirements include access to DFS space (Portal, Webmail) and the ability to make an authenticated DCE RPC call (eLion)
- ❑ Using Paul Henson's DCE/OpenSSL patches, we modified cosign to convert K5 creds to DCE
- ❑ We also modified the Cosign ISAPI module to request K5 tickets
- ❑ We plan to modify Cosign to use our Friends of Penn State realm as well

Portal & Webmail Solutions

- ❑ Cosign with DCE credential conversion code.
- ❑ Still dependent on DCE/DFS
- ❑ Future plans include LDAP based authorization and neutral distributed filesystem requirements

Potential Angel Solutions

- Cosign + LDAP
 - LDAP portion needs to be written
- Shibboleth
 - Already exists and works
 - Is protecting attributes internally overkill?
- Either Solution requires significant work

Potential IBIS & ISIS Solution

- Server “Broker” component receives a K5 ticket from front end and calls a Policy Decision Module
 - Possibly XACML based policy descriptions
 - Validates ticket and retrieves LDAP attributes
 - Makes authorization decision before control is passed into the legacy applications

IBIS & ISIS Difficulties

- Typical nightmare application case: very old code, limited programmers, and mission critical applications
- Natural & ADABAS use their own authn/authz routines for access control and record locking
- Hard sell. Often no perceived need for this kind of architecture

Future LDAP Plans

- New Group Types
 - Dynamic Groups - Auto-generated based on results of a query
 - Nested Groups - Groups inside groups
 - Hybrid Groups - A combination of static, dynamic, and nested
- Fine grained access control to group lists

Signet? Grouper?

- We are watching these applications closely
- Grouper appears to duplicate the functionality we have built that assembles group membership data from various sources
 - We are watching more for ideas for our own system
- Signet is interesting to us because we currently do identity based group management, not role based

Additional Tricks

- SASL-CA
 - Similar to the KCA (kx509) but uses SASL to negotiate authentication method
 - Signs a short term client cert (digitalSignature key extension)
 - Cert can contain identifying information, or a Shibboleth persistent opaque handle for use with Attribute Authority
 - Originally developed as part of the Lionshare project

Questions/Comments

- ❑ My Email: mxe2o@psu.edu
- ❑ Presentation URL:
 - ❑ <http://www.personal.psu.edu/mxe2o>
- ❑ Thank you :)