

The New Infrastructure

Internet 2 - EA Meeting
Baltimore, March 2000

Steve Carmody
Brown University - CIS

Recommending a Strategy

Ideas for Today (Larry did Tomorrow)

Goals and Objectives

- ◆ A managed environment
- ◆ An integrated environment
- ◆ Delegated day to day management of the environment
- ◆ Effective distribution of information from the fundamental data elements of the university
- ◆ ... in a heterogeneous environment
- ◆ Summary of the current situation
- ◆ Use brief bullets, discuss details verbally

Today's Topics

- ◆ Planning for the Enterprise
- ◆ Managing the Enterprise
- ◆ Understanding Infrastructure Requirements

Planning for the Enterprise

- ◆ Establish Standards, consistent with the emerging practice in higher education
 - ◆ Identity (how many....)
 - ◆ Naming
 - ◆ Contents
 - ◆ Use of Attributes
 - ◆ ACLs - permissions on the various attributes

(more) Planning

- ◆ Scaling the problem
 - ◆ The new community
 - ◆ Size of name space(s)
 - ◆ Longevity
 - ◆ Groups
 - ◆ Centrally maintained... with tweaking
 - ◆ Departmental
 - ◆ Individual

(more) Planning

- ◆ Compatibility of various environments
 - ◆ Contents of DN
- ◆ Browsing the directory
 - ◆ What you see is based on permissions
- ◆ Cross domain
 - ◆ Directory of directories

Managing the Distributed Environment

- ◆ The registry (the meta-directory)
 - ◆ A global view ...
 - ◆ Life cycle management of identity and privileges
 - ◆ Reconcile identity, and multiple relationships with university
 - ◆ Authoritative source for attributes
 - ◆ May need information that is NOT stored in operational systems (eg organizational hierarchy)

(more) Managing the Environment

- ◆ The Directory
 - ◆ Evolving from a white pages service (organized around people)
 - ◆ ... to a key infrastructure component supporting directory enabled applications
 - ◆ Need for formally identified business rules
- ◆ Synchronization of multiple directory/authentication services
 - ◆ Security concerns
 - ◆ The devil is in the details (eg name changes)

Authentication

- ◆ The process of verifying the claimed identity of a client or service
- ◆ Need to abstract authentication out of (web based) applications
 - ◆ Fewer signons
 - ◆ It is often easier (faster) for a new framework to implement its own directory, security than to leverage a common infrastructure (political)
 - ◆ Multiple security domains

Authorization

- ◆ The process of verifying that the authenticated identity has been granted permission to perform the requested operation on the requested object
- ◆ Central versus delegated management
- ◆ Protection model
 - ◆ Deny all versus Allow all
- ◆ Central revocation

(more) Authorization

- ◆ The start of abstracting authorization out of applications
 - ◆ File systems
 - ◆ Web servers
- ◆ REAL Issues
 - ◆ Different name spaces
 - ◆ Granularity
 - ◆ Different models for managing authorization

Understanding Infrastructure Requirements

- ◆ A simple example
- ◆ Web Access Control

Simple Situation

- ◆ Basic Authentication
- ◆ Users and groups defined on the web server
- ◆ File space/ web space - different permissions structures

Enterprise Infrastructure

- ◆ Multiple constituencies
 - ◆ Central (www.X.edu)
 - ◆ Administrative applications
 - ◆ Distributed web servers (departmental and individual)
- ◆ Leverage a central infrastructure
 - ◆ (Managed) identity within the enterprise
 - ◆ Authentication
 - ◆ Groups
- ◆ Avoid basic authentication

(more) Enterprise Infrastructure

- ◆ Single sign-on enterprise wide
- ◆ Mobile users
 - ◆ Kiosks
 - ◆ As guest on ? Machine
- ◆ Administrative Systems
 - ◆ Multiple identities (one per application ?)
 - ◆ Complex Authorization

(more) Enterprise Infrastructure

- ◆ Distributed Environment
 - ◆ Machines NOT to be trusted
 - ◆ Cannot perform certain functions from these machines
- ◆ Building Credentials
 - ◆ Optional
 - ◆ Needs appropriate authorization to include certain attributes
 - ◆ Static values or attributes from user object
 - ◆ Clear or opaque

Enterprise Infrastructure - Version 2

- ◆ New communities - redefinition of community
 - ◆ Applicants
 - ◆ Alum's
 - ◆ Parents
 - ◆ Friends
 - ◆ E-commerce
- ◆ Cross domain
 - ◆ What is trust?
 - ◆ Who do you trust
 - ◆ Interpret digital identities between sites

(more) Version 2

- ◆ New browsing devices
 - ◆ Web phones
- ◆ Portals
 - ◆ Single signon
 - ◆ Portal acts as your proxy
 - ◆ Contents customized, based on your affiliation
 - ◆ Contents customized, based on YOUR choices
 - ◆ Requires storing profile information

(more) Version 2

- ◆ External Licensed Resources
 - ◆ Pseudo-nonumous
 - ◆ Authority certificates
- ◆ Use of roles to manage privileges
- ◆ Central revocation
 - ◆ To control liability

(more) Version 2

- ◆ Shrink wrapped web based applications
 - ◆ IMS
 - ◆ Calendaring
- ◆ Requirements
 - ◆ Create additional schema, attributes
 - ◆ Required “dedicated” DS?
 - ◆ Aligning with authentication and authorization?
 - ◆ Add other types of resources/ objects to directory?

(more) Version 2

- ◆ Leveraging the directory
 - ◆ DEN
 - ◆ Managing distributed servers
- ◆ The Directory as part of the administrative applications infrastructure
 - ◆ Card entry to buildings

Questions