Tom Dopirak – tgd@cmu.edu

Monday June 15, 2009
Educause Camp on
Access Management

Building Blocks for Access Management

Please Note:

This file is a rough copy made from the original slides, which were much better formatted. The original slides included high resolution graphics and were not able to be uploaded to the wiki due to file size.

Agenda for the Day

- Identity & Access Management Framework - 10 minutes
- Why Bother? The Educause Survey - 5 minutes
- Policy and Guidelines - 5 minutes
- Basic Terminology & Process for Access Management - 30 minutes
- Preview and discussion - 10 minutes

Thanks

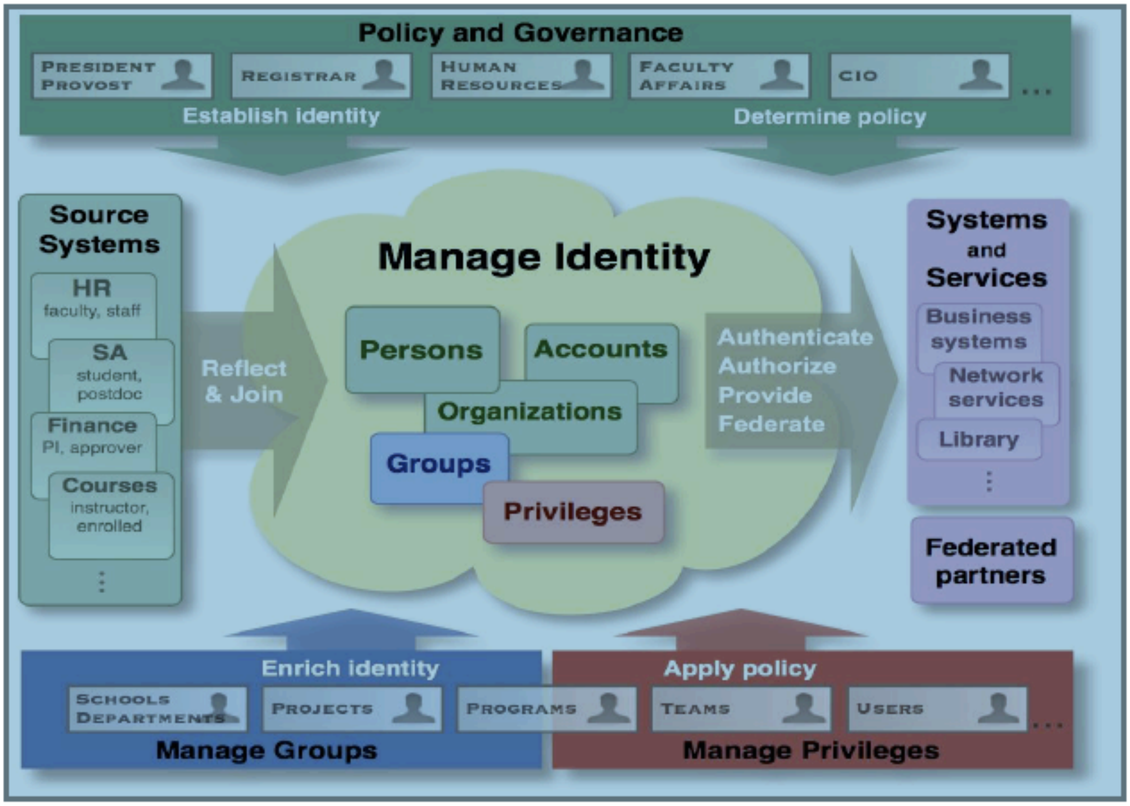
- Steal from the smart and give to the “not so smart yet” --
Robin “the Architect” Hood

Your Customers

How they see you

Identity and Access Management Roadmap

http://www.internet2.edu/middleware/resources.html



Rocks and Sticks and Mud
Some definitions

Identity Management

- Who are you ?
- How do we know that?
- What do we know about you ?
- What digital credentials do you possess and how

How well do you take care of them?

What is Identity Management (IdM)?

• Identity Management consists of the business processes
and technologies for managing the life cycle of an identity
• Enables organizations to facilitate and control their users' access to online
applications and resources while protecting confidential personal and
business information from unauthorized use.
• Uses delegated administration, workflow, rules, and policies
• Managed centrally and enforced locally
• Consistency of process
• Common implementation of best practices
• Provides centralized auditing and reporting
Carrie Regenstein – carrie1@cmu.edu

Access Management

- What are you authorized to do?
- Who authorized you to do so?
- How are services informed that you have access and how
is this enforced?
- Can you delegate your access to others ?
- How much of a service can you use?

Subjects and Privileges

Subject : An entity whose identifiers and attributes are managed by an Identity and Access Management practice.

Privileges amount to the sum of what a subject may do, as granted to them or inherited. Groups or roles do not have privileges, but instead provide a mechanism to confer privileges to all members of a group or role as individual principals.
In the context of a Privilege management system, Privilege is used to describe the combination of a subject or group, their current permissions, and any qualifications to those permissions.

Authority

A broad term that can cover most aspects of creating policies, guidelines and rules governing who has rights and privileges for an organization.

It includes the ability to control the dissemination of those rights, as well as an organization's responsibilities to enforce those rights. This is sometimes referred to as AuthZ (authorization), in contrast to AuthN (authentication).

It can also be used more specifically in a singular authorization situation to say whether a principal has "authority" to take an action. In this sense, authority and privilege can be used interchangeably.

It can also refer to a person or policy or rule that confers privileges to subjects, either directly by use of an access management system, or indirectly.

Access Management

“That part of Identity Management comprising the processes and tools used to associate privileges with subjects in accord with the wishes of Authorities.”

https://spaces.internet2.edu/display/macepaccman/MACE-paccman-glossary

Directory

“A directory is a specialized database that may contain information about an institution’s membership, groups, roles, devices, systems, services, locations, and other resources.”

http://middleware.internet2.edu/dir/metadirectories/internet2-mace-dirmetadirectories-practices-200210.htm

eduPerson and eduOrg

“eduPerson and eduOrg are LDAP schemas designed to include widely-used person and organizational attributes in higher education. They were developed, and are maintained, by the Internet2 MACE-Directories Working Group (MACEdir), a project of the Internet2 Middleware Initiative. These middleware activities are supported by Internet2 and EDUCAUSE.”

http://middleware.internet2.edu/eduperson/

A few important attributes

eduPersonAffiliation

Specifies the person's relationship(s) to the institution in broad categories such as student, faculty, staff, alum, etc. (See controlled vocabulary).
Permissible values faculty, student, staff, alum, member, affiliate, employee, library-walk-in

http://middleware.internet2.edu/eduperson/docs/internet2-mace-direduperson-
200806.html

eduPersonEntitlement

URI (either URN or URL) that indicates a set of rights to specific resources.

“A simple example would be a URL for a contract with a licensed resource provider. When a principal's home institutional directory is allowed to assert such entitlements, the business rules that evaluate a person's attributes to determine eligibility are evaluated there. The target resource provider does not learn characteristics of the person beyond their entitlement. The trust between the two parties must be established out of band. One check would be for the target resource provider to maintain a list of subscribing institutions. Assertions of entitlement from institutions not on this list would not be honored. See the first example below.

Examples:

eduPersonEntitlement: http://xstor.com/contracts/HEd123

eduPersonEntitlement: urn:mace:washington.edu:confocalMicroscope

Example applications for which this attribute would be useful”

√

Why care about access(privilege) management?

http://www.duke.edu/~rob/PrivManSurvey/
I2_PM_Survey_Final_Report.pdf

Internet2 Privilege Management Survey

“An overwhelming majority of sites (81%) indicated that they saw a need to develop privilege management policies; only a small fraction (6%) indicated that they already had such policies in place, supporting the hypothesis that a policy gap exists within higher education institutions that may interfere with the widespread adoption of centralized privilege management tools.”
≈

Develop Privilege Management Policies

Survey Results

Two thirds are dissatisfied with their
current Access Management
“Responding sites dissatisfied with their current privilege management approaches outnumbered those expressing full satisfaction with their current approaches roughly two to one”.
Sites are only partially centralized
“Responding sites reporting their privilege management strategies as partially centralized (with some critical applications using central privilege management and less critical applications fending for themselves) outnumbered others by almost three to one.”

More Survey Results

“Commonly cited problems respondents expected could be addressed through enhanced privilege management were delays and inaccuracies in the on-boarding and off-boarding of new institutional affiliates, the so•called “privilege snowball” effect, and the lack of transparency and audit ability in privileging practices and processes”.

On-boarding, off-boarding and changes of
roles are particular problems

Yet more results

“The most sought•after features in a privilege management solution were coarse•grained privileging based on broad user affiliations, target dependent privilege qualifications, and role• or group•based privilege management support. “

“The least sought•after features were support for manual override of automated privileging processes, timed or triggered attestations, and temporary privilege transfer”

A realistic approach

What Makes a Good Policy?

- Is high level, representing core values/principles

- Supports the mission of the University

- Stands the test of time (5, 10 even 15 years)...

- Is not technology specific (where technology is actually in the picture)

What Makes a Good Policy Approval Process?

- Includes vetting with university leadership

- Includes vetting with stakeholders

- Examines the impact on university mission and stakeholders

- Can be completed in a reasonable time frame

CMU Process

- Create initial draft of Information Security Policy
- Review with Vice Provost of Computing Services
- Review with Office of General Counsel
- Review with Executive Steering Committee on Computing
- Review & Approval by Management Team Light
- Review with Business Manager's Council and Staff Council
- Review with Departmental Administrators
- Approval of the Policy by President's Council
- Publication
- Communicate Publication of the Policy

Outline of a Policy

- Purpose -why have a policy
- Scope – what situations and people the policy applies to
- Maintenance – how it the policy amended , how is it revisited
- Enforcement – the impact of violating the policy
- Exceptions – how to get an exception
- Definitions
- Policies – the actual policy text
- Additional Information – other relevant resources
- Revision History

CMU Policy Roadmap

http://www.cmu.edu/iso/governance/index.html

1. Information Security Policy (done)
2. Roles & Responsibilities (done)
3. Data Classification (done)
4. Data Protection (under review)
5. Data Sanitization & Disposal (starting in the Fall)
6. Responding to a Security Breach (Starting in the Fall)
7. Policy Exceptions
8. Data Retention

CMU Guidelines

1. Guidelines for Appropriate Use of Administrator Access
2. Guidelines for Bulk Email Distribution
3. Guidelines for Copyright Violations
4. Guidelines for Data Sanitization and Disposal
5. Guidelines for Instant Messaging Security and Usage
6. Guidelines for Mobile Device Security and Usage
7. Guidelines for Open Mail Relay Security
8. Guidelines for Password Management
9. Guidelines for Proxy Server Security
10. Guidelines for Recursive DNS Server Operations
11. Guidelines for Web Server Security
12. Guidelines for Windows Administrator Accounts

Outline of a Guideline

- Purpose
- Applies To
- Definitions
- Regulatory Requirements – if any
- Guidelines
- Additional Information
- Revision History

Roles in the Information Security Policy

Director of Information Security- responsible for overall policy set and overall Authority.

Data Steward - a senior-level employee of the University who oversees the lifecycle of one or more sets of Institutional Data

Data Custodian – is an employee with operational responsibilities

An Introduction to Additional Terminology
The Student Billing Use Case

The Student Billing Use Case

Each month, CMU creates bills for 10,000 students that represent all of the transactions for that month. These bills are suitable for reading online and for printing. Each student can see all of their own bills and can delegate viewing of their bills to anyone with a CMU login or a login from a federated institution. In addition, there are less than 100 localbilling administrators on campus that can see individual student bills.

The local billing-administrator's access is based on college or department or degree enrollment of the student. For example, there may be one billing-administrator for the Tepper School of Business but a separate billing-administrator within that college for the Evening MBA program. At the University level there are less than 5 university billing administrators whom can see any student bill they desire. They are also responsible for designating local billing-administrators.

Roles

Roles – A collection of privileges usually related to a
task, responsibility or qualification associated with
an enterprise

- University-billing-administrator - can view the bills of all students, can designate local-billing-administrators for a set of bills, can view student delegations of bill viewing, can void bills that are incorrect. Acts as a data steward.

- Student - can view their own bills and delegate viewing of their own bills.

- Student-delegate - can view the bills of any student that delegates "viewing"
to them.

- Local-billing-administrator - can view the bills of any student that is enrolled in a department, college, or degree granting program over which they have been delegated "viewing" privileges, can void a students bill and see bills that have previously been voided.

Permissions

Permissions

- View-own-bills
- View-all-bills
- View-student-delegations
- View-selected-bills - usually accompanied by a membership rules that specifies what bills can be viewed
- Designate-local-billing-administrator - this designation is only valid for a fixed period of time and as long as certain attributes of the designee are constant
- Designate-viewer-of-own-bills

Use Case Table
Role University
Billing
Administrators
Local Billing
Administrators
Student Student
Delegate
Permission
View Own Bills x x
View All Bills x x
Delegate
viewing of bills
x
Delegate
Billing
Administration
x

Delegation

“The process used, or task performed, by a grantor to assign privileges to other subjects within the limits of its authority. A subject with delegated privileges does not have to perform any type of impersonation in order to exercise the privileges.”

The University-Billing-Administrator delegates viewing of some student bills to local-billingadministrators.

The student delegates viewing to their guardian.

Authorities

University-billing-administrator has complete authority over all students bills and who may view them

A Privilege Table

Subject Permission Rule

University-billingadministrator
Bill.view *
University-billingadministrator
Bill.delegate *
Mathdept-administrator Bill.view Where
student.dept='math'
Student S0 Bill.view Where Student-id=S0
Parent P0 of Student
S0
Bill.view Where Student-id=S0
and bill.dategenerated='
may 2009'
Student S0 Bill.delegate Where Student-id=S0

Grantor

A principal authorized to delegate some portion of its own
authority and that has exercised that privilege.
University-billing-administrator and Student are grantors
in this example

Assigning and losing Roles

- Derived from some authority
- System of Record and computed from Institutional data
- “granted” by an university official or their grantee
- Self – appointed if policy permits
- Removed by authority or attestation policy
- System of record changes data that implies role
- Grantor removed subject
- Calendar or timer based re-attestation occurs
- Opt-out where permitted

University-billing-administrator

- Directory Attributes Can be set as an attribute in the University Directory e.g. cmuPersonRoles contains the value CMU:StudentBilling:UniversityBillingAdministrator

- Groups If multiple people can be set as an attribute in each person record or recorded in a group e.g. CMU:StudentBillingUniversityBillingAdministrators contains DN of person

Local-billing-administrator

You can build a hierarchy of groups
names and examine
membership while agreeing on the name
or accomplish the
same thing with an attribute value
cmu:billing:dept-administrators:math
contains subject A0

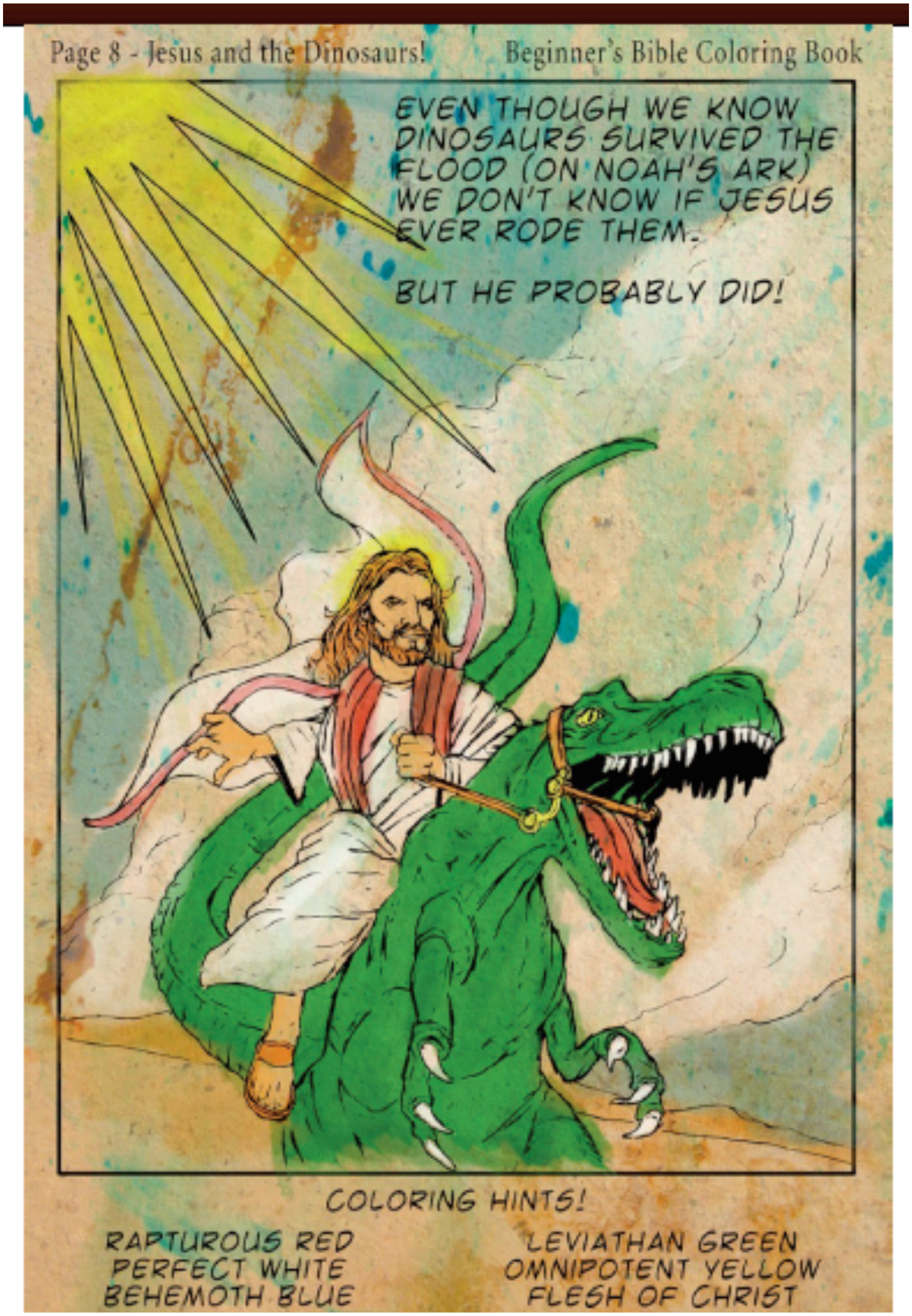
Local-billing-administrator

You can enumerate subject in privilege table or leave the group as the subject
Subject Permission Rule
A0 Bill.view Where
student.dept=‘math’
cmu:billing:deptadministrators:
math
Bill.view Where
student.dept=‘math’

The Rest of Camp

- Categorizing Access Management Challenges
- Use Cases , patterns and an overall methodology
- Discussion and lightning Rounds
- Attendee Use Cases and
- Solution Patterns applied to the Real World
- Matching Attendee Use Cases against solution patterns
- A Review of available tools and policy
- Looking Forward

Anything is possible


Page 8 - Jesus and the Dinosaurs!
Beginner's Bible Coloring Book
EVEN THOUGH WE KNOW DINOSAURS SURVIVED THE FLOOD (ON NOAH'S ARK) WE DON'T KNOW IF JESUS EVER RODE THEM.
BUT HE PROBABLY DID!
COLORING HINTS!
RAPTUROUS RED
PERFECT WHITE
BEHEMOTH BLUE
LEVIATHAN GREEN
OMNIPOTENT YELLOW
FLESH OF CHRIST

eduPersonPrincipleName

The "NetID" of the person for the purposes of inter-institutional authentication.

http://middleware.internet2.edu/eduperson/docs/internet2-mace-direduperson-200806.html