Institutional Data and the Role of Identity and Access Management

Mojgan Amini, Information Technology Services (ITS)
David Hutches, Jacobs School of Engineering

Campus IT Governance Committees

- History
    - Formed in mid-2015
- Rationale
    - Improve communication and collaboration among campus stakeholders and service providers.
    - Coordinate best practices for alignment of policies and procedures related to IT services.
    - Develop and shepherd both tactical and strategic solutions to campus information technology needs in targeted subject areas.
- Progress
    - Have produced a variety of actionable recommendations.
    - Fostered working groups to investigate specific projects in technical detail.
    - Established need and framework for coordinating activities among the committees.
    - Created common mechanism to ensure a productive feedback cycle to connect committee recommendations with service provider activities.
    - Most importantly: Laid the foundation for collaborative, cross-organizational communication channels that, at best, previously only existed in *ad hoc* form.

Campus IT Governance Committees

Collaborative development of best practices that encompass the people, processes, and technologies required to create and maintain consistent and approved standardization and availability of mission critical technologies across UC San Diego without regard to boundaries created by existing organizational structures:

- Data
  - Defining and managing access to all static, dynamic, and derived enterprise information.
- Identity and Access Management (IAM)
  - Who a user is and what resources she/he may access.
- Security and Privacy
  - Treatment of information systems and associated data as enterprise assets to protect against theft, damage, or exposure, and ensure compliance with guidelines and regulations.
- Service-Oriented Architecture (SOA)
  - System functions are exposed as loosely coupled, self-contained capabilities that are platform and language independent (versus a traditional, monolithic model).

What is Identity and Access Management?

- Broad definition: An administrative business process that
  - Uniquely and unambiguously identifies individuals and their associated attributes.
  - Brokers attribute-based access to systems, services, data, and other capabilities.
- Identity and Access Management systems typically include
  - ID repository - A directory of the personal data the system uses to define individual users.
  - Access lifecycle management- A set of tools for adding, modifying and deleting identity data.
  - User access regulation - Programmatic enforcement of security policies and access privileges.
  - Auditing and reporting - Verification and alerts related to changes to and operation of the identity and access management system, including records of usage by linked applications and services.
- Key point: Identity and Access Management is not merely a tool or collection of tools; it is a business process implemented as **mission critical infrastructure**.

Why is this important?

Strategically, there is currently no uniform, universally accessible mechanism to

- Uniquely identify the complete range of personnel affiliated with the University, nor the features associated with these personnel.
- Query for and verify basic access rights to be used as the subsequent authorization for campus systems, services, and data.

Summary of needs and issues

- Incomplete or inconsistent capabilities for flexible and fine grained access management for data and data-related services.
- Need for access to campus systems (both directly and by support personnel) outside the time window of a person's official campus affiliation.
- Numerous local IAM systems with varying, potentially conflicting attributes.
- Application and service development is impeded by reinventing infrastructure.
- Inconsistent or incomplete application of policies and procedures related to management of campus identities.
- Confusing user login experiences due to multiple account types (multiple authenticators).
- Inconsistent vendor single sign-on (SSO) integration.
- Overloading of production campus identity namespace by annual inclusion of tens of thousands of student applicant identities, the majority of which will ultimately be deleted.

What is the relationship between IAM and roles?

- Identity and Access Management is the foundation that underpins all other campus services.
- All of the most common and critical features that uniquely identify an individual affiliate of the University are collected in a single repository.
- From the atomic elements of a person's identity one constructs higher level abstractions such as the multiple (and changing) roles a person can have during his/her affiliation with the campus, a school/division, a department, a team, etc.

What’s the relationship between IAM and data?

- Not unlike the case with roles, it is out of fundamental identity characteristics that one constructs the abstract concept of data access.
- Disambiguates the roles of data steward and gatekeeper.
- Allows for the creation of arbitrary levels of granularity for data access as organizational needs dictate.
- Provides a more rigorous feedback mechanism to identify when data access systems work, when they do not, and why.
- Eliminates the inflexibility and change resistance associated with tightly coupled, monolithic systems.
- Reflects the modern best practices for software development and better supports agile deployment of tools for data access and analytics.

What’s next?

Principal observations/recommendations of the Identity and Access Management committee:

- The absence of a single, definitive, platform agnostic person repository with unique/permanent ID places the University at a strategic disadvantage and significantly impedes efforts to adopt a more agile, data-driven approach to research and education.
- Work must begin now to put in place a robust and scalable identity and access management system, which will serve as a basic infrastructural component upon which higher-level services and applications will be built.

Questions?