Identity and Access Management:
A Centralized Approach

Robert Stanfield, Interim Director
Benjamin Lewis, Security Analyst
Jeffrey Smith, Security Analyst
Identity and Access Management Office

**Mission:** To provide a consistent, University-wide means of identifying Purdue University constituents for the purpose of granting access to resources while ensuring an individual’s privacy.
Identity and Access Management Office

**Vision:** To coordinate the activities of identity assignment and role-based access across the University.
• What we do
  – Centralized Provisioning Service
    • Career Account for servers and applications
    • Used by ITaP and 13 Departments
  – Centralized Authentication and Authorization
    • LDAP, RADIUS, Web Services
    • Used by ITaP and 25+ Departments
• Themes
  – Problems Purdue Was Facing
  – PUID – an SSN replacement
  – Account and Namespace Unification
  – Centralized Provisioning Service
  – Centralized Authentication & Authorization
  – IAM Office
• Problems Purdue Was Facing
  – Central IT, multiple accounts per person
  – Distributed IT, multiple identities in multiple systems, departmental systems, etc.
  – Provisioning and de-provisioning delays
  – Only common key was SSN
  – Sensitive identity data transmitted to various areas across campus
• **Realization: the Purdue Person**
  – One account per person
  – Ability to access Purdue resources using a single credential

• **Requirements: Unification**
  – Assignment of a unique key
  – Consolidation to a single account
• PUID – an SSN replacement
  – In 1996, central IT began a project to replace the SSN in Purdue systems with a unique, numeric identifier
  – The PUID provides a key to tie identity across disparate systems
  – One person, one PUID
  – Formatted as 00000-00000
  – Luhn check digit
  – No intrinsic value - it’s just a number
PUID System / PUID Assignment

- Student Identity Data
- Personnel Identity Data
- Other identity data providers
- I2A2 system
- Other Systems
- SSN remediation
• PUID – Lessons Learned
  + Good identity assignment is hard, but worth it
  + Quick SSN remediation would have been impossible without it
    – Adoption should have been pushed much earlier. A single security incident drove widespread adoption
    – Consult with legal
    – Put clear and concise policies in place first
• Account and Namespace Unification
  – In 1997, our vision was to adopt a single login and password for the majority of academic systems
  – In 1997, we undertook a major effort to combine multiple logins per person into one single login
  – In 1998, our vision was to provide early access to incoming students during our day-on-campus activity
  – By 1999, most namespace unification complete
• Account and Namespace Unification – Lessons Learned
  + End-user experience - a single login and password
  + Was the groundwork for adoption of a single login credential

  – Voluntary process - required account coordination to access services
  – It took a long time
  – Help desk (support) issues
• Access Management Infrastructure

• Components
  – Centralized Provisioning Service
  – Centralized Authentication and Authorization
• Centralized Provisioning
  – Developed a centralized provisioning service called ACMAINT
  – Used to manage access to systems and applications
  – Account management is automated
ACMaint Architecture

- Hosts
- Users
- Accounts

Database

- Database Daemon (dbd)
- Packet Daemon (packetd)

- Client (passwd)
- Administrative Client (AH)
- Service
- Server

- Users
- Accounts
Provisioning System Architecture

- Database
  - Meld ID Data
  - Role Assignment
    - De-assignment
  - Role Reconciliation
- Input for ACMaint Administrative Client (AH)
- Personnel
- Student Identity Data
• Centralized Provisioning – Lessons Learned
  + Key infrastructure component for managing a single credential across systems
  + We own it – flexibility
  + Cost and time reduction
  + Identity data not distributed

– Least common denominator
– Weakest link
• Access Management Infrastructure

• Components
  – Centralized Provisioning Service
  – Centralized Authentication and Authorization
• Centralized Authentication & Authorization
  – In 1996, single authoritative service for authentication and authorization
  – Vision was a centralized service for access control for web-based and other applications
  – Developed a solution accessed through standard protocols such as LDAP and RADIUS
I2A2 architecture

- Network clients (apache, etc.)
- I2A2 network service daemons (LDAP, RADIUS, custom protocol)
- I2A2 database managers (lookup, authentication, authorization)
- PUID / other identity data
- I2A2 "Cloud"
• Centralized Authentication - Lessons Learned
  + Key infrastructure component
  + Cost and time reduction
  + Further helped unify namespace
  + We own it – flexibility
  + Security benefits

– Custom, only used by Purdue
• Future - IAM Office
  – One place for managing identity and access
  – Combining business and IT functions
  – Central management of IAM projects
  – Committee governance
Things done wrong

- Separate areas providing services
- Delayed PUID adoption (SSN remediation)
• Things done right
  – End-user experience
  – Build it and they will come!
  • Centralized automated provisioning
  • Centralized authentication and authorization
  – No charge for services
  – Cost and time savings
  – Security benefits