Practical Identity Access Management

Lessons From the Field
John Benninghoff
Introduction

• My background
• Lessons learned from designing & building IAM/SSO solutions
• Reflects my personal experience only
• Working with government organizations
• Focus on getting access to the system
Why do you need an IAM system?
Traditional IAM

- One Constituency
  - Join
  - Change Jobs
  - Reviewed
  - Leave
Government IAM

• Three Constituencies:
  • Government
  • Public
  • NGOs
Buying an IAM Product
IAM Products

- They’re all expensive
- They’re all platforms
- They all require professional services

- Lesson: choose one you can support. Have the professional services team picked out when you buy.
The User Experience
Getting a User ID

Apple ID

Create Your Apple ID

One Apple ID is all you need to access all Apple services. Already have an Apple ID? Find it here:

- name@example.com
- password
- confirm password
- first name
- last name
- birthday

Security Question 1
- answer

Security Question 2
- answer

Security Question 3
- answer

These questions will be used to verify your identity and recover your password if you ever forget it.
Enrollment

• Getting a User ID
• Identity Matching
• Identity Verification
Enrollment: Getting a User ID

• Public: self-service enrollment
• Government: use existing IDs
• NGOs: requesting an ID OR through federation
Login Screen: Single ID

Who do you want to be today?

☐ Case Worker
☒ Benefits Applicant
☐ Assistor
Enrollment: Getting a User ID

• Public: self-service enrollment
• Government: use existing IDs
• NGOs: requesting an ID OR through federation

• Lesson: a person could have 3 or more User accounts
• Lesson: a user account is not a person
Enrollment: Identity Matching

• Identity Matching: comparing 2 or more records to determine if they represent the same person
• Problem for public only (generally) to link a user to “their” data
• Even harder problem than IAM
• Identity matching in banking
Enrollment: Identity Matching

CitiMortgage

Link Your Mortgage Accounts
Access your Citigroup accounts all in one place.

Already Linked to My Profile
Account Number: XXXXXXX Nickname: Home

Link to My Profile
*Required fields
Citi mortgage account:
Account Number: XXXXXXX
State: -- Select --
Zip Code: 

Return to View My Profile In Continue

TTY Services available: Dial 711 from the United States, Dial 1-866-280-2250 from Puerto Rico.

First mortgage loans are originated by Citibank N.A. NMLS ID 412951
First mortgage loans are serviced by Citigroup, Inc. NMLS ID 415188

Copyright © 2016 Citigroup Inc.
Enrollment: Identity Matching

- Identity Matching: comparing 2 or more records to determine if they represent the same person
- Problem for public only (generally) to link a user to “their” data
- Even harder problem than IAM
- Identity matching in banking

- Lesson: IAM shouldn’t do identity matching but should record results of ID matching
Enrollment: Identity Verification

• Verifying a user’s claimed identity

• Government users are verified at time of hire
• NGO users are verified through a process
• Public users must prove who they are
Enrollment: Identity Verification

Which of the following vehicles have you owned?
A. 2005 Ford Taurus
B. 2014 Chevrolet Malibu
C. 2010 Toyota Prius
D. 1998 Audi TT
E. None of the above
Enrollment: Identity Verification

• NIST 800-63-2 discusses in detail

• Lesson: verify identity after granting a User ID but before granting access

• Lesson: provide a manual identity verification process
Enrollment: 3 phase approach

1. Getting a User ID
2. Identity Matching
3. Identity Verification
Logging In (finally!)
Logging In

• User ID for logging in
• User accounts may span multiple systems
Logging In

Identity & Access Management System

Application

IAM User DB

Application

App User DB

Application

App User DB

Application

App User DB
Logging In

• User ID for logging in
• User accounts may span multiple systems
• Unique ID for user account
• Single Sign-on:
  • Traditional
  • SAML
  • OAuth
Lesson: don’t use case-sensitive usernames!
Lesson: each constituency needs a unique user ID namespace
Lesson: Use an IAM-specific unique identifier for user IDs
Lesson: Use SAML today, also consider OAuth
Managing Access
## Getting Access: Role Mapping

<table>
<thead>
<tr>
<th>IAM Role</th>
<th>Application Role</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>External User</td>
</tr>
<tr>
<td></td>
<td>Applicant</td>
</tr>
<tr>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Internal User</td>
</tr>
<tr>
<td></td>
<td>Case Worker</td>
</tr>
<tr>
<td></td>
<td>View Only</td>
</tr>
</tbody>
</table>
Getting Access

• Lesson: manage coarse-grained authorization in IAM, fine-grained authorization in the applications
• Lesson: start with fewer roles
Removing Access

• Public: user IDs are “never” disabled
• Government: disable upon termination
• NGOs: disable by process

• Lesson: Manage costs of public users by disabling inactive or abandoned user accounts
Changing & Reviewing Access

• Vision: automated, end-user driven request process
• Request – Notify – Approve – Grant
Questions?

email: john@transvasive.com
twitter: @jbenninghoff @transvasive