Identity Management as the Security Perimeter: Creating Your Enterprise Strategy

William Cai, University of Chicago
David Walker, Scalable Privacy Project, Internet2
Mike Grady, Scalable Privacy Project, Unicon
Overview

● Introduction
● Enterprise Strategies for Identity Management
● Multi-Factor Authentication
● Deployment Patterns and Approaches
Getting to Know Ourselves
Do you have a Vision & Roadmap for your IAM Strategy?

Does it cover maturing authentication?

Do you have a methodology for access control?
How Long Will You Rely on Passwords for Sensitive Resources?

- We don’t rely on them now.
- 1 year
- 3 years
- 5 years
- Forever
Creating Your Enterprise Strategy
Build Your Strategy & Foundation

Understanding Your Risk and Aligning it to Your IAM Strategy:

- Data is our Asset
- Identity is our Perimeter
- Classification is our Control

Frameworks can help: IT General Controls, SANS CSC-20, NIST but apply them to your context.
Develop A Compelling Journey

Building your vision requires lots of marketing

Have a road-map to execute on your vision:

- Right amount of Governance at the right time
- Use your frameworks to help you build out your policies and controls
- Make your road-map meaningful to your stakeholders and customers
- Get people excited for your change; be a change agent
Specific Views in a Vision

Authentication is not the same as Authorization

Authentication - Meeting Silver Standards, Password Expiration, KBAs, Risk Based Auth, **Strong Authentication**

Authorization - **Privileged Access Mgmt, Access Reviews**, Access changes (granting & off-boarding)
Authorization

Have strategy of how you want to manage access - delegated, centralized, single toolset

Privileged Access Management has generally two major check in/check out approaches -
(1) session logging
(2) management of commands

Consider a Privileged Identity Lifecycle
Consider Access Reviews

Do you know who’s accessing your systems?

- Periodically validate access (yearly, quarterly, etc as needed)
- Access reviews during job role changes
- First few are account clean-ups
Multi-Factor Authentication
**Authentication Factors**

**Something you know**

**Something you have**

**Something you are**

**password**
MFA is using more than one factor

- Password is something you know
- Combine with something you have (or are), with growing # of choices/vendors:
  - Phone & mobile app based
  - Security tokens (hardware, USB, software)
  - Smart cards
  - Biometrics
Why Is Multi-Factor Authentication Important for Higher Education?
Passwords are Passé

- We try to shore up passwords
  - Length, complexity, frequent changes
- ...but we’re still subject to compromises
  - Phishing, cracked password files, key loggers
- We’ve made passwords more expensive, yet they are less ineffective.
  - Help desk calls
  - User frustration
More Reasons to Move beyond Passwords

● Greater online access to high-risk services
  ○ e.g., self-service payroll
● Compliance and regulations

“...ensure that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate. Within 18 months of the date of this order, relevant agencies shall complete any required implementation steps ...”

(White House Executive Order of 10/17/2014)
MFA Is Now a Viable Option

- MFA is easier to use
- MFA has more popular exposure
- Cost of technology and licenses decreasing
- Growing number of peer deployments
Higher Education Survey Results

- IAM Online webinar Sept. 2013: 75% of 120+ institutions indicated that within 5 years “using more than passwords for sensitive resources”
- MFA Cohortium institutions (45+) survey spring 2014: 80% within one year of “more than password”, with the other 20% within 3 years.
- Informal poll at beginning of Educause 2014 presentation aligned with MFA Cohortium survey results
Planning for Multi-Factor Authentication
Planning for MFA

- Make the Business Case
  - Risk assessment
  - Resources required
- Initial Deployment Options
  - Specific services
  - Campus SSO and/or VPN
- Establish Policy
  - Risk assessment
  - Authentication requirements
  - Token management and identity proofing
Selecting Technology - How Much Security Is Enough?

- Recover confidence lost in passwords
  - “Two Step” authentication, etc.

- Address higher security needs
  - OTP
  - “Push” mobile apps
  - FIDO U2F
  - PKI

- Assurance and compliance
  - InCommon Assurance Program
  - NIST 800-63
  - FIPS 140-2
Selecting Technology - SSO Options

- User opt-in
- Multi-factor for specific users
- Multi-factor for specific services
- Some options
  - Shibboleth: Multi-Context Broker
  - CAS: CAS-MFA (MFA extensions for CAS)
  - Incorporate into Active Directory
    - Office 2013/ADAL
Deploying Multi-Factor Authentication
An Emerging Deployment Pattern ....

- Pick a technology
  - Rely on User devices (mobile, phone)
  - Rely on cloud-based vendor
- Conduct a prototype/pilot
- Integrate into SSO
- Likely will need (eventually)
  - Hardware token option
  - Supplement the vendor-supplied enrollment/mgmt interface
    - e.g. print OTP list, register friend, ...
... An Emerging Deployment Pattern

- Start with core IT staff, then expand
- Begin to train support staff
- Deploy for early adopters (opt-in)
- Focus on developing marketing & communications
- Start work with service managers for mandatory use
- Deploy for all users
Operating Multi-Factor Authentication
Operational Issues

- Distribution of tokens
- Retiring tokens
- Periodic technology refresh
- Monitoring & metrics
- Help desk

---

The MFA Cohortium is collecting campus case studies and artifacts from campuses.
UChicago Implementation Details

- Four month project to implement 2FA
- Approximately 500 hours of work, valued at $48,000 total (including development, marketing/communications materials, web self service design)
- After release, drove adoption of service
UChicago Password Campaign

Multiple phases - (16,000 users in scope):

- 1276 tickets opened (8% of users)
- 650+ work hours (project & help desk)
- ~$35,000 in cost
- Positive feedback on passphrases
- Password change numbers went up as emails went out

Something culturally sensitive became normal...
MFA Cohortium
MFA Cohortium Basics

- About 50 institutions participated
- Representing roughly 1 million people
- Spring 2013 - Fall 2014, bi-weekly meetings
- Core work has finished, but perhaps another meeting or two
- Still collecting artifacts, stats as possible
Cohortium Resources

- The MFA Cohortium Wiki
  - https://wiki.cohortium.internet2.edu
- Case Studies
- Reference Materials & Artifacts/Examples
- MFA management console needs
- Presentations on campus deployments
  - Duke, Penn, Arizona, Stanford, Chicago, Johns Hopkins
Sample Cohortium Resources

- How Much Security Is Enough?
- Enterprise Deployment Strategies for Multi-Factor Authentication
- Diagrams providing a visual presentation of MFA Business Drivers, Deployment Decision Trees, and Integration (architecture) Patterns
- Multi-Factor Authentication Solution Evaluation Criteria
- Alternative Strategies When Multi-Factor Tokens Are Not Available
The Internet2 Scalable Privacy Project has helped to fund software that enables easier deployment of MFA:

- Shibboleth Multi-Context Broker (IdPv2)
  - IdPv3 -- efforts underway for recipe(s)
- CAS-MFA
- InCert
Questions?