Motivations and Policy Challenges of Multifactor Deployment

IAM Online
November 9, 2016

Brendan Bellina, UCLA
Matthew Dalton, University of Massachusetts Amherst

IAM Online is presented by InCommon, Internet2, and the EDUCAUSE Higher Education Information Security Council
Before we Begin - Laying the Groundwork for Multi-Factor Authentication (MFA)

Matthew Dalton, UMass Amherst IT

IAMOnline Nov 9, 2016
Define your Problem

- Compliance with PCI, HIPAA, or other
- Protection of Sensitive Areas
- Researchers protecting of assets
- Protection by Role
- Opt-In for everyone
- Required for Some, opt-in for the rest
- ...
Technology Selection

Features

Integrations

User Enrollment
# Features

## Authentication Methods
- One Time Pad
- Hardware Token
- Biometrics
- Phone Call
- SMS
- Application
- Certificate

## Other Features
- Step-Up Authentication
- Panic Button
User Enrollment

User Provisioning
- File Upload
- Active Directory
- LDAP

Second Factor Association
- Key Distribution
- Self Enrollment
Integrations

SSO
- Shibboleth
- SAML
- Active Directory

Network
- VPN

3rd Party Apps
- Wikis
- Blogs

Cloud
- Amazon
- Azure

Unix
- SSH

Programming Libraries
- PHP
- Python
Governance and Policy

For users:
- opt-in
- required

For systems:
- Single-Sign On
- Systems in scope

Based on:
- Risk, Compliance Objectives, Problem Definition
Questions?
Measured Rollout For Multi-Factor Authentication (MFA)

IAMOnline Nov 9, 2016

Brendan Bellina, bbellina@ucla.edu
Information Technology Services
About the UCLA MFA Project

- Managed by the IT Services Security Office
- Enterprise product license (Duo Security) allows common MFA platform across all UCLA account domains
- Multi-pronged approach with phased deployment

<table>
<thead>
<tr>
<th>UCLA Logon SSO</th>
<th>Campus at Large</th>
<th>IT Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shibboleth</td>
<td>Any interested campus department with local account space</td>
<td>IT Services VPN</td>
</tr>
<tr>
<td>Campus VPN</td>
<td>Active Directory, local systems, etc.</td>
<td>Application Development Tools</td>
</tr>
<tr>
<td>Self-service portal</td>
<td></td>
<td>Data Center Systems</td>
</tr>
<tr>
<td>BOL to provide user support</td>
<td></td>
<td>etc.</td>
</tr>
</tbody>
</table>

11
Who Uses MFA with UCLA Logon?

<table>
<thead>
<tr>
<th>User Population for UCLA Logon</th>
<th>Phase I</th>
<th>Phase II</th>
<th>Phase III</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>June 2016</td>
<td>Fall 2016</td>
<td>Spring 2017</td>
</tr>
<tr>
<td><strong>Users with Sensitive Access</strong></td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Employee</strong> (UCLA faculty and staff)</td>
<td>Opt-In</td>
<td>Opt-In</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Student</strong> (currently enrolled student)</td>
<td>Opt-In</td>
<td>Opt-In</td>
<td>Opt-Out</td>
</tr>
<tr>
<td><strong>Affiliate</strong> (parents, contractors, etc.)</td>
<td>Opt-In</td>
<td>Opt-In</td>
<td>Opt-Out</td>
</tr>
</tbody>
</table>
# Phased Plan for UCLA Logon MFA Adoption

<table>
<thead>
<tr>
<th>Phase I</th>
<th>Phase II</th>
<th>Phase III</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summer 2016</td>
<td>Fall/Winter 2016</td>
<td>Spring 2017 and beyond</td>
</tr>
<tr>
<td>• Turned on MFA in <strong>Web SSO</strong> and <strong>Campus VPN</strong> in June/July 2016</td>
<td>• Widen enrollment</td>
<td>• Switch to opt-out mode - MFA enrollment becomes default part of UCLA Logon account creation</td>
</tr>
<tr>
<td>• Enrollment by invitation</td>
<td>• Opt-in sign up for everyone</td>
<td>• Integrate MFA enrollment with the rest of UCLA Logon account management functions</td>
</tr>
<tr>
<td>• Dept Security Admin pilot</td>
<td>• <strong>Coordinated employee rollout by department</strong></td>
<td>• Continue to widen department and student body enrollment campaign</td>
</tr>
<tr>
<td>• Internal Audit</td>
<td>• Expand online help material as necessary</td>
<td></td>
</tr>
<tr>
<td>• IT Services</td>
<td>• Improve self-service MFA experience - simplify user experience</td>
<td></td>
</tr>
<tr>
<td>• Develop self-service enrollment tutorial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Close technical and procedural gaps</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Current MFA Statistics (as of October 31, 2016)

- Enrolled Users: 567
- # of 2FA devices registered: 1103 (includes unassigned tokens)
- # of Assigned Hardware Tokens: 90
- # of Landlines registered: 311
- # of Mobile Phones registered: 600
  - 62% iOS
  - 33% Android
- # of Telephony Credits used since launch: 20,559
- Total MFA Logins per day: ~ 1600
  - Average 2.8/user/day
Lessons Learned Since June 2016

Note: Enrollment to this point has been primarily to IT staff

• Once enrolled MFA use is straight-forward and non-problematic

• Daily MFA use quickly becomes routine after initial adjustment

• More people had trouble during enrollment with using their phones and app store passwords than anticipated

• Department IT support team will play a critical role in rollout success
Department Deployment 5 week Template

**Step 1**
- Complete pre-engagement assessment check list
- Assemble deployment team
- Sign up for rollout engagement

**Step 2**
Meet with IT Services teams:
- Finalize area-specific rollout plan
- Train support staff
- Prepare rollout communication
- Purchase tokens (if necessary)

**Step 3**
Carry out rollout plan
- Opt-in sign up
- Grow adoption
- Turn on mandatory enrollment

Start of week 1

End of week 5
Factors Considered When Selecting Departments

- # of employees
- Department support staff capability
- Number of non-desktop based employees
- Frequency of use of computer-based applications
- Conflicts with Academic and Administrative calendars
Resources

- UCLA Bruin OnLine MFA FAQ:
  https://www.bol.ucla.edu/shortcut/mfa
- UCLA Bruin OnLine MFA enrollment instructions:
  https://www.bol.ucla.edu/shortcut/kb/KB0012931
- UCLA Info Sec MFA @ UCLA:
  https://www.it.ucla.edu/security/resources/mfa-at-ucla
- Duo Security
  - End User Guide: https://guide.duo.com
  - Duo Push video (21 seconds):
    https://www.youtube.com/watch?v=tPLxe9HUDjY
  - Why MFA video (2 minutes):
    https://www.youtube.com/watch?v=e8o8qDpHkHE
IAM Online Evaluation and Ideas

Please complete a short evaluation of today’s presentation:

Have an idea for an IAM Online? We have a form available a calendar of upcoming sessions.
https://spaces.internet2.edu/x/toX8