Deploying Multi-Factor Authentication with UCLA Logon

Common Systems Group Meeting

April 26, 2016
Multi-Factor Authentication (MFA)

- MFA is authentication requiring more than one type of assurance

- Common assurance factors:
  - Something you know, e.g., password
  - Something you have, e.g., smart card, cell phone, token
  - Something you are, e.g., biometric such as fingerprint
# About the UCLA MFA Project

- Managed by the IT Security Office
- Provides common good MFA platform (Duo Security) for all utilizing the UCLA account space
- Multi-pronged / phased deployment

## UCLA Logon
- Shibboleth
- Campus VPN
- Self-service portal
- BOL to provide user support

## Campus at Large
- Any interested campus department with local account space
- Active Directory, local systems, etc.

## IT Services
- IT Services VPN
- Application Development Tools
- Data Center Systems
- etc.
Duo Security Enterprise

- Allows both user pre-registration and Just In Time (JIT) account and device registration
- Partner with InCommon and Internet2
- Support for Smart Phone Apps (iOS and Android), SMS and Voice (at cost), and hardware tokens
MFA Login Flow with Shibboleth
MFA Login Flow with Shibboleth

User requests access to service → ID + Password Challenge → 1st Factor successful

1st Factor successful:
- No → Requested Access Denied
- Yes → Sensitive Resource: MFA for all users

Sensitive Resource: MFA for all users:
- No → Privileged Account: MFA for all resources

Privileged Account: MFA for all resources:
- No → Selective: MFA for this resource for this user

Selective: MFA for this resource for this user:
- No → Requested Access Denied
- Yes → 2nd Factor Challenge (smart phone app, SMS, voice, hardware token, etc.)

2nd Factor Challenge (smart phone app, SMS, voice, hardware token, etc.):

- No → Requested Access Denied
- Yes → MFA Policy Decision Point

MFA Policy Decision Point:

- Yes → Requested Access Granted
- No → Requested Access Denied
Demo
UCLA Logon MFA Deployment

MFA is added security to one's UCLA Logon. We recommend the use of both strong passwords and MFA for the UCLA Logon ID:

- If a user turns on MFA either by choice or by requirement, s/he will to sign in with MFA at all accepted authentication points.
- The two initial UCLA Logon MFA-enabled authentication points are Campus VPN and Shibboleth.
- If a Shibboleth-enabled application requires MFA, then its users will need to sign in with MFA to ALL Shibboleth applications as well as VPN.
- GOAL: All employee access through UCLA Logon will require utilization of MFA.
Who Uses MFA with UCLA Logon?

<table>
<thead>
<tr>
<th>Proposed</th>
<th>Phase I</th>
<th>Phase II</th>
<th>Phase III</th>
</tr>
</thead>
<tbody>
<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>

*Proposed Future State: MFA will generally be required (phased deployment) for UCLA Logon with (limited / TBD) Opt-Out exceptions*
UCLA Logon MFA Deployment Phase I


- Users of sensitive applications are required to enroll:
  - DACSS - Enrollment via DSA training sessions
  - Grouper (Role and Entitlement Management)
- Opt-in MFA enrollment is available for UCLA Logon user at my.logon.ucla.edu
- Rollout in May 2016
Deploying MFA to DSA’s

- Piloting training material with 30 DSA’s – May 2016
- Internal Audit to coordinate in-person training and registration event – June 2016
- IT Services training group is preparing video tutorial
- As DSA registers, s/he begins using MFA when signing into SSO.
- Mandatory MFA for DSA – July/August 2016, pending fiscal closing activities.
- IT Services Client Support and BOL Help desk to provide support; same as current DSA support
Increase User Education and Adoption.

- Education Campaign – Do the Right Thing
- Work with key business offices to prioritize additional applications and identify users with privileged access
- Monitor adoption trends, costs, and impacts
- Summer and Fall 2016
UCLA Logon MFA Deployment Phase III

Wide Spread Adoption.

- Change UCLA Logon creation process to automatically enable MFA enrollment. Opt-In becomes Opt-Out.
- At the right time, require MFA use for all employees.
- Winter 2016/Spring 2017 (estimate)
MFA Deployment in Campus VPN

- All enrolled UCLA Logon users will receive MFA challenge at VPN sign in.
- Works with CISCO AnyConnect Client as well as L2TP VPN client built into OSX, iOS, Android, Windows 7, Windows 10.
- Supports SSL, IPSec, and L2TP
## Opt-in MFA Enrollment

<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 2016</td>
<td>Winter 2016 and beyond</td>
</tr>
</tbody>
</table>

- **Phase I**
  - Purpose-specific site: my.logon.ucla.edu
  - Spread news via word of mouth – any UCLA Logon holder can sign up
  - Self-service online tutorial and FAQ
  - BOL Help Desk support - same support structure as other aspects of UCLA Logon ID/password support

- **Phase II**
  - my.logon.ucla.edu replaces all features of current logon.ucla.edu
  - All UCLA Logon holder will see MFA features
  - Encourage everyone to sign up
  - Campus-communication via web sites and emails
  - Expand online help material as necessary

- **Phase III**
  - Additional enhancements
  - Switching tool default to opt-out
  - Build MFA enrollment into UCLA Logon account creation flow
UCLA Logon MFA Deployment Summary

<table>
<thead>
<tr>
<th>Service</th>
<th>Supports MFA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shibboleth Single Sign-On</td>
<td>May 2016</td>
</tr>
<tr>
<td>Campus “BOL” VPN</td>
<td>May 2016</td>
</tr>
<tr>
<td>Campus Wi-Fi</td>
<td>No</td>
</tr>
<tr>
<td>(UCLA WIFI; eduroam)</td>
<td></td>
</tr>
<tr>
<td>UCLA Logon Active Directory (CLICC lab AD authentication)</td>
<td>Not Yet…</td>
</tr>
</tbody>
</table>
# Duo Security Cost

<table>
<thead>
<tr>
<th>Cost</th>
<th>Notes</th>
</tr>
</thead>
</table>
| **Annual Software Subscription and Support** | $88,000 per year  
- Covers all students, faculty, staff, and affiliates  
- Deployable to all UCLA account spaces*  
- Funded and managed through IT Security Office  
* Excludes medical and clinical care systems |
| **Telephony Credits** | $0.01 per SMS text  
$0.02 per phone call  
- Duo charges the university for SMS and phone calls.  
- Does not include telecom company phone charges  
- Credits are not sharable among different account types  
- Departments managing the account type (e.g., department AD) will be responsible for telephony credit charges |
| **Duo Tokens** | $20.00 per token  
- Cost to purchase USB token/UBKey  
- Only required if user cannot use phone  
- Departments will be responsible for employee token cost |
Questions?