Multifactor Authentication: Campus Deployment Case Studies

IAM Online
October 21, 2015 - 2 pm EDT

Paul Caskey, Internet2
Brad Judy, University of Colorado
CW Belcher, University of Texas at Austin
MFA Interop Working Group

Deliverables

- Assemble use cases that will motivate the deliverables of this working group
- Develop short list of widely deployed MFA technologies in higher education that will be in scope for the profile
- Define requirements for and draft MFA Interoperability Profile
- Develop and recommend scope and plan for adoption
- Present draft in session at Internet2 Technology Exchange in October 2015
- Publish final profile by November 30, 2015

Wiki: https://spaces.internet2.edu/x/CY5HBQ

List: mfa-interop@incommon.org

To subscribe to this list, email sympa@incommon.org with the subject line subscribe mfa-interop

Chair: Jacob Farmer, Indiana University
From 0 to 34,000 Multifactor Users in Six Months

InCommon IAM Online

Brad Judy

10-21-2015
JAN 2014 - MOTIVATIONS AND REQUIREMENTS
Requirements

• Mitigate common phishing
• Easy for end users
• Rapid deployment
• Flexible for other purposes (no specific use cases)
Things we considered

• Go manual
• Existing info MFA
• PIN or security questions
• “Risk based” MFA
• Tokens
• Phones
Support

- Support begins with Employee Services service desk
Data integrations

• Load ALL the users!!
  – Returning employee update issue

• Load ALL the phones!! (well, three of them)
  – Fixing international phone formats

HRMS → OSB → MDM → OSB → Duo
Functional integration

- Connecting GreyHeller ERP Firewall to Duo
Communications

It takes two
JULY 18, 2014 – GO LIVE
Multi-factor authentication debuts in the CU Resources area

The University of Colorado has debuted multi-factor authentication in the CU Resources section of the portal to improve protection of personal employee information stored there.

Colleges and universities are increasingly targeted by cybercriminals using fake "edu" email addresses. Following phishing attacks in late 2013, the university began working on a project to implement an authentication system that protected employee information while minimally disrupting portal usage.

Now, it takes two items—your password and your phone—to access sensitive information. Requiring two forms of authentication decreases the likelihood that others can access your data.

Please watch this one-minute video that will show you how to use the authentication system.

Find out more about multi-factor authentication >>

© Regents of the University of Colorado
Two-Factor Authentication

Device: CAMPUS1 (XXX-XXX-4293)

- Phone call
- Passcode

Log in

If you're having difficulties using this authentication page, please contact your departmental Payroll liaison or Employee Services. For more information about the two-factor authentication process, please visit this site: www.cu.edu/it-takes-two

Employee Services | University of Colorado
303-860-4200 | 655-216-7740 | employeeservices@cu.edu | www.cu.edu/ES
1800 Grant Street, Suite 400, Denver, CO 80203
One year stats

• 24,000+ people have used it
• 76,000+ authentication attempts
  – 16.5% failure rate = 63,000+ successful
  – 55% voice, 45% SMS (for successful)
• 120,000 telephony “credits” = $1,200
Problems encountered

• Duo UI didn’t like 100,000+ users/phones
• Data feed bumps (international number formatting, etc.)
• Still issues with bad phone numbers
• Duo account reps keep calling me about the 100,000+ users
NEXT STEPS
• HR/IT privileged user
• Student self-service
• Examining other use-cases with ERP Firewall options like field-level step-up MFA
• Implement new Duo delegated admin roles for service desks
UT Austin’s MFA Journey

IAM Online
October 21, 2015
Toopher Stage 1

• Needed to combat phishing attacks with an easy-to-use MFA tool that was quick to deploy
  – Had already tried using a second secret and other personal data but that encouraged more phishing

• Implemented Toopher March-July 2014

• First services protected by MFA:
  – W-2 access
  – Payroll bank routing info
Toopher Stage 2

• Added MFA to more services in Fall 2014:
  – Non-payroll bank routing info
  – Student emergency loans
  – Password administrative resets
• 38K active users (50K pairings since go-live)
• MFA via smartphone app, SMS, and pre-generated OTPs
Toopher Stage 3

- Planned major expansion in Summer 2015 to comply with UT System 2FA mandate:
  - VPN access
  - OpenAM & Shibboleth integration
  - PAM/RDP integration
- Halted due to lack of Toopher support from Salesforce
Next Steps

- Duo proof-of-concept with multiple campus groups – *Complete*
- Duo implementation:
  - Starting now
  - Go-live Spring 2016
  - Will minimize Duo/Toopher parallel operation to avoid user confusion
Tips & Lessons Learned

• Start with applications that resonate with leadership and users to get traction
  – Paycheck theft was a high priority issue for both campus executives and employees

• Acknowledge and prepare for user impact
  – Make sure leadership understands that some users will find MFA difficult or annoying
  – Document alternative ways to complete business processes when a user can’t complete MFA
Tips & Lessons Learned

• Partner with business areas that own apps to be protected – this isn’t just an “IT thing”
  – Requirements, testing, communication should all be joint efforts

• Beta test with targeted groups
  – Start with small group, survey them, adjust approach/process/documentation, then expand to larger and more varied groups
Tips & Lessons Learned

• Communicate, communicate, communicate
  – Talk to many stakeholders – faculty, students, HR reps, IT governance groups, developers, etc.
  – Stress to users that MFA is there to protect them and their information
Evaluation

Please complete the evaluation of today’s webinar

Upcoming Events

Next IAM Online – November 11, 2015

InCommon’s Future:
International, K-12, and Changing Demographics