MFA: Duo and Google 2-Step Deployments Compared

Rich Graves, Carleton and St. Olaf Colleges

Moderator: Tom Barton, University of Chicago
IAM Online April 12, 2017
2-Factor Landscape

- Best single mitigation against impact of phishing
- Passwords are often shared and many are easy to crack

- Good 2FA options exist with reasonable/no cost
- Pretty good user experience, with some effort
- Good integration with web apps, remote access, shell/console access
- Lots of Higher Eds are doing it
- REFEDS MFA Profile, based on InCommon MFA WG, defines standard federation signaling for services to request MFA

- Hard to protect some applications/systems with 2FA
2FA Road Map @ UChicago

| Protect privileged access to core business systems | Protect remote access to campus |
| Protect privileged access to IT systems | Protect paychecks & personal info |

Make part of net ID claim

2FA Adoption by Affiliation

- Faculty: 1316 (2FA), 217 (Not 2FA)
- Staff: 16429 (2FA), 3580 (Not 2FA)
- Student: 19181 (2FA), 777 (Not 2FA)
- Hospital: 8384 (2FA), 2977 (Not 2FA)

2FA Forecast - 2 Years

- Faculty: 133 (2FA), 0 (Not 2FA)
- Staff: 1400 (2FA), 20009 (Not 2FA)
- Student: 9919 (2FA), 10039 (Not 2FA)
Polls 1 and 2
MFA: Duo and Google 2-Step Compared

Rich Graves, Carleton and St. Olaf Colleges

IAM Online

April 12, 2017
Agenda

1. A tale of one city, with two liberal arts colleges

2. Google 2-Step and Duo
   
   Commonalities

   A solution for Google 2-Step (*not* just Authenticator) before InCommon IdP

   Some notable differences

3. From opt-in to mandate: usability and governance challenges
Experiment in sharing resources among colleges

Can “information security,” defined broadly, be done “better” and “cheaper” if Carleton and St. Olaf share an information security officer (ISO)?

- Assessment
- Basic training
- Policy
- MFA advocacy
- IDS and security ops
- Incident response
How do small colleges deal with MFA & IAM?

Might lack local expertise for extensive customization of a Shibboleth IdP

Expensive work to add MFA step-up to ERP applications not gonna happen

More likely to choose pure Google or MS options, though Carleton does Duo

But we have advantages:

More centralized, more forgiving

I see the full stack from VIP engagement, to IdP configuration, to user support

**St. Olaf had more MFA users March 2017 than UCLA had October 2016. Carleton has twice the adoption rate as UChicago.**
The big picture: Different technologies and engagement strategies employed at two very different colleges, yet the growth curve was similar.
Agenda

1. A tale of one city, with two liberal arts colleges

2. Google 2-Step and Duo

   Commonalities

   A solution for Google 2-Step (*not* just Authenticator) before InCommon IdP

   Some notable differences

3. From opt-in to mandate: usability and governance challenges
Poll 3
Google 2-Step Verification/Duo Two-Factor Options

- Push/Prompt app
- Authenticator app
- Phone call
- Text message
- U2F/Yubikey
- Printed OTP codes
- Hardware tokens (Duo only)

Security awareness training stresses the need for independent backup options.
Poll 4
Using Google 2-Step to sign on to Shibb/InCommon

Shibboleth supports a **RemoteUser** mode.

At St. Olaf, we sign in to an Apache proxy using Google and OpenID Connect (**mod_auth_oidc**), which in turn gets us to Shibboleth, which finally gets us to arbitrary InCommon SPs.

Microsoft shops could do this with the OpenID or SAML support in ADFS or Azure. Needed because ADFS can not (yet) consume InCommon metadata.

St. Olaf College won the Rube Goldberg Award in 2009 and 2012.
Google 2-Step (St. Olaf) v. Duo (Carleton)

Free

- Only Google-branded web authentication
- No help desk access; no useful admin access except for delayed reports and OU enforcement
- Hard to troubleshoot
- Only one Google Authenticator per account
- App-specific passwords supported
- Can’t whitelist IP address ranges
- Google Prompt issues especially on iOS

$2,860 for up to 2500 student FTE

- Branded, Windows RDP, VPN, RADIUS, LDAP, LastPass, JavaScript
- Full API and delegated help desk rights to view/edit devices and passcodes
- Full real-time logs
- Any # of devices can run Duo Mobile
- No app-specific passwords (but you seldom need them anymore)
- Can whitelist IP address ranges
- Duo Push is quite nice

Microsoft 2FA on par with Google 2-Step, except no Yubikeys
Duo onboarding and usability issues

New users seem to like the Google 2-Step experience more than Duo’s.

Separate layer, not pre-integrated like accounts.google.com.

Techies tend to like Duo because all the options are right there on the sign-in page; regular folks dislike it for the same reasons

“Remember me for X days” is not checked by default

At Internet2 TechExchange, most presenters said they would not allow “remember me” anyway, but we certainly do

“Automatically send push to primary device” conflicts with “Remember me”

That thing where you need to check a box to verify your phone number annoys
Google 2-Step usability and support issues

Help desk/admins/APIs have no ability to view/edit user 2-Step devices!

Streamlined enrollment interface with lots of white space is friendly and welcoming to new users. However,

Few people figure out how to enter multiple devices

Fewer still figure out that “Try another way to sign in” is where you go to select a backup device

“Google Prompt” (the Duo Push equivalent) is poorly advertised

Password expiration/change breaks Google Prompt on iOS

Deadline for users to enroll is very smooth. But via Luther College: If you create a new user in an OU where 2-Step is already required, they can never log in!!!

RFEs: Force Enable 2-Step on First Login and the second is Don’t Require Phone to Enable 2-Step
Agenda

1. A tale of one city, with two liberal arts colleges

2. Google 2-Step and Duo
   
   Commonalities
   
   A solution for Google 2-Step (*not* just Authenticator) before InCommon IdP
   
   Some notable differences

3. From opt-in to mandate: usability and governance challenges
Risk management: why are you doing MFA?

MFA *does* impose costs on your users. It *is* hard to learn. Be kind.

Huge difference between simple phishing resistance and non-repudiation. Select verification frequency and options accordingly.

**Security includes availability.** Don’t block students & faculty from Moodle.

Can you mitigate your biggest risks in other ways?

  - Don’t allow self-service payroll direct deposit change for some employees
  - “Knowledge based authentication,” demand SSN/DOB before showing W-2
  - Anomaly detection (geographic, unusual bank routing codes)
  - Redact SSNs on W-2s, 1098-T, 1095-C, etc.
  - By default, Google blocks “less secure apps” (IMAP/SMTP without OAuth)
Poll 5
Marginal cost increases as you approach 100%

Identity management: How do you define “all staff”? Adjuncts, athletics trainers, custodians, outsourced departments, emeritus faculty who teach one extension course, humanities research institute volunteers…

We added several analog phones to custodian break rooms that only had PCs

Mobile: Do people even know their iCloud and Android Store passwords?

Cans of worms: Do we help them reset the personal iCloud and Gmail account passwords that own their phones? Do we have a responsibility to configure 2-factor on private accounts? Do we have liability for accidentally unlinking private accounts from personal smartphones?

“Exchange” versus “Google” email setup

Brad Judy: Just use SMS/voice. Me: Wise advice for ERP step-up use case, but email needs mobile.
Talking about religion and politics, etc.

John & Todd story… your local pastor uses Google 2-Step, why don’t you?

Need for different presentations between Carleton and St. Olaf, see https://blogs.carleton.edu/rgraves/2016/10/05/2016-security-awareness-kickoff-slides/

St. Olaf chose to use Google 2-Step rather than Duo

Carleton chose not to follow through with making MFA mandatory for all staff “yet”

People in the same roles at each campus had very different views on MFA. Don’t take “because this is how my office works” at face value.
The inside story on various milestones

- Carleton’s President starts using Duo, then ITS “starts internal pilot”
- A few sysadmins have used Duo since 2011
- Carleton’s HR, Admissions, and Development opt in
- St. Olaf all-staff mandate

- St. Olaf IT chooses to support Google 2-Step broadly
- St. Olaf Training v2
- St. Olaf Training v1
- St. Olaf Security Awareness Training v1
- Mandatory for St. Olaf IT
- Carleton Opt-In Begins again
- Carleton Business Office
- Carleton Security Awareness Training v1
- Carleton’s President starts using Duo, then ITS “starts internal pilot”
- A few sysadmins have used Duo since 2011

1503 1504 1505 1506 1507 1508 1509 1510 1511 1512 1601 1602 1603 1604 1605 1606 1607 1608 1609 1610 1611 1612 1701 1702 1703
Carleton 23 45 80 59 45 41 47 46 45 42 44 45 52 87 96 118 115 114 117 183 189 251 272 290 309
St. Olaf 12 13 13 14 26 31 42 59 72 74 77 81 81 82 88 93 103 113 118 204 239 253 256 259 599
Q&A. What does “more security” look like?
Evaluate Today’s IAM Online

https://www.surveymonkey.com/r/IAM-Online-Apr-2017
2017 Technology Exchange Call for Proposal

Proposal deadline – April 28, 2017
https://meetings.internet2.edu/2017-technology-exchange/call-participation/

2017 Technology Exchange
October 15-19
San Francisco, California
InCommon Shibboleth Installation Workshops

Trainings will begin to shift to the TIER version of Shibboleth, likely starting in July.

- June 14-15, Denver, Colorado
- July 19-20, Easton, Pennsylvania
- November 7-8, Bethesda, Maryland
- TBA, Seattle, Washington
May IAM Online

The Shibboleth Consortium – Current State and Future Plans
May 10, 2017 – 2 pm ET