Internet2 Trust and Identity Solutions Provider Webinar

Warren Leung, IAM Program Manager, UCLA
John Gasper, IAM Consultant, Unicon, Inc.

Shibboleth and Grouper at UCLA

UCLA At A Glance

- 53,000 employees (20,000 Health System; 33,000 campus)
- 40,000 students
- 670,000 UCLA Logon ID's
- 140,000 login attempts a day
- 550 registered SP's in Prod

Shibboleth at UCLA

- Used for internal SSO for UCLA and federated applications
- Provides high availability and redundancy with a fail over location
- UCLA has had a home grown SSO since 2000 and migrated to Shibboleth in 2007
  - We started with about 100 applications to migrate to Shibboleth in 2007. By the time migration was completed in 2009, we had 300 applications running with Shibboleth.

Grouper at UCLA

- Grouper is supplement and a potential successor to a legacy access control system
- UCLA's legacy access control system dates back to the early 90's
- Grouper was deployed in 2014 at UCLA
- Early Adopters
  - MyUCLA (Student Systems Portal) – Groups and roles are loaded into Grouper via web service or batch processes, which provision to our LDAP data store. Access is determined for a user at sign-in time when attributes are delivered by Shibboleth.
  - BruinCard (ID Card System) – Developed a home grown application that allows department administrators to manager door access. Group memberships are updated via web service and are provisioned into the BruinCard System.
  - Shibboleth MFA – More on that shortly

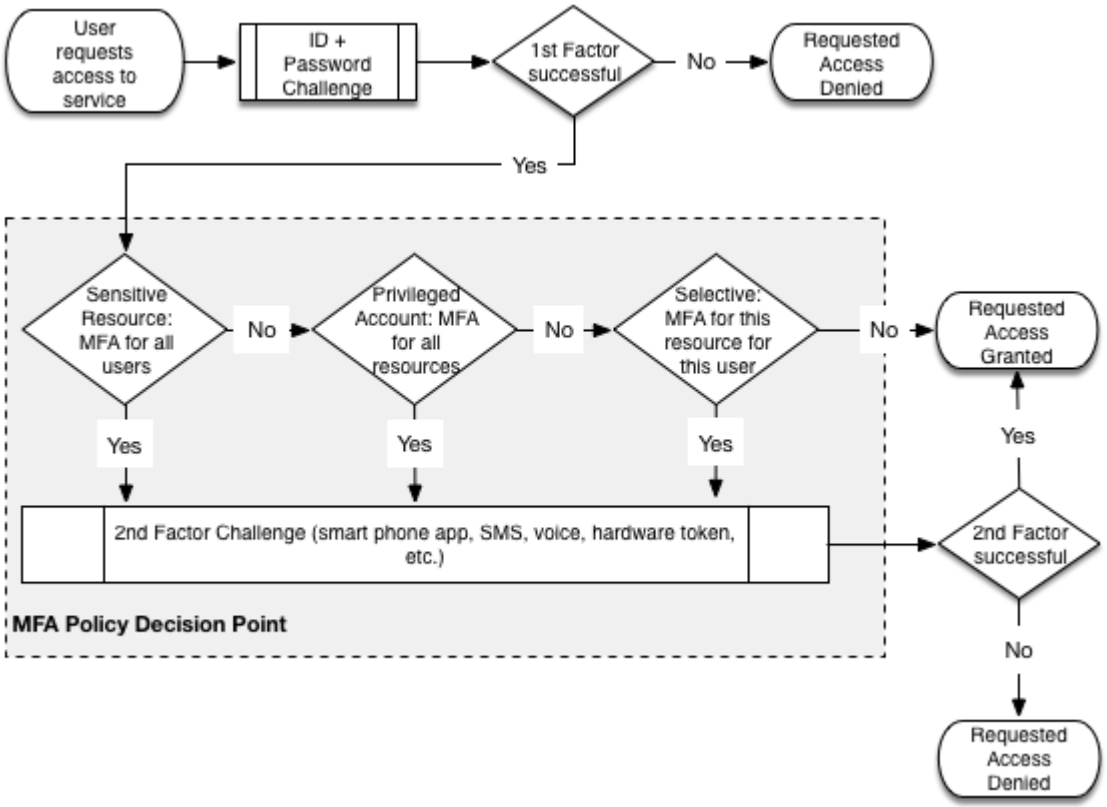
Growing Pains

- User experience and usability issues
  - Deploy a responsive, mobile focused user experience
  - “Rejecting replayed message” – Develop self guide instructions for users to resolve issues
- Support the other 20,000 employees
  - The majority of Health System’s employees do not have a UCLA Logon ID. However, there is a growing need for Health System employees to login to federated or UC wide applications via UCLA’s SSO.
- Grouper scaling issues
  - Batch loading processes would take hours and web service calls on large groups would timeout. After polling the community we decided to migrate from MSSQL to Oracle DB. We noticed huge performance increase.

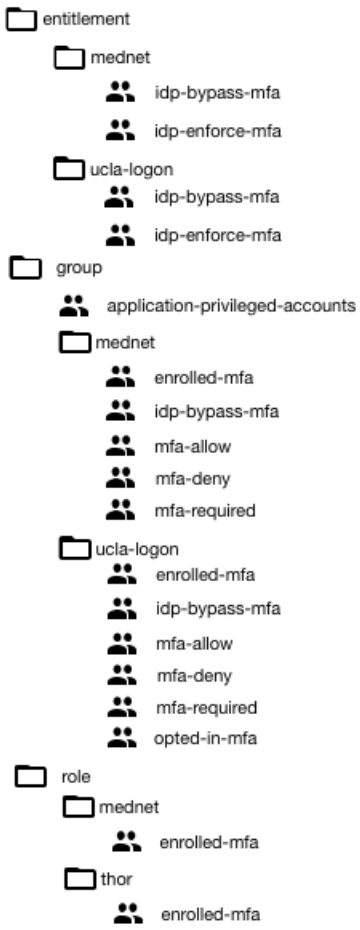
New Needs

- Migrate to Shibboleth v3
- Provide MFA Support
  - UCLA is a decentralized IT organization and unilaterally enforcing MFA would be a difficult challenge. Knowing this, we designed our solution to handle as many use cases as possible with the intention to also contribute back to the community. With our approach, we are able to phase in specific groups of users into MFA and hope to have all employees on MFA in early 2017.
  - MFA is enforced on your UCLA Logon ID rather than a specific application. Once you have enrolled in MFA, any application you sign into with Shibboleth will require MFA

MFA Login Flow with Shibboleth



MFA Groups


entitlement
mednet
idp-bypass-mfa
idp-enforce-mfa
ucla-logon
idp-bypass-mfa
idp-enforce-mfa
group
application-privileged-accounts
mednet
enrolled-mfa
idp-bypass-mfa
mfa-allow
mfa-deny
mfa-required
ucla-logon
enrolled-mfa
idp-bypass-mfa
mfa-allow
mfa-deny
mfa-required
opted-in-mfa
role
mednet
enrolled-mfa
thor
enrolled-mfa

Timelines

- 3/15 – 8/15 – User Experience Updates and Health Systems Support
- 11/15 – 6/16 – Shibboleth v3 and MFA
- 11/15 – 5/16 – Grouper migration from MySQL to Oracle DB

UCLA Enhancements

- Split Authentication Flow
- **Throttle Login Attempts**
- Display SP Info from RSS feeds
- Browser support sanity check: Enforce that JavaScript and Cookies are enabled.
- **Measure SAML generation time to monitor IdP performance.**
- **Assign a transaction ID at the first request and used for all subsequent requests. This transaction ID is logged in all idp-process.log entries.**
- **Customized SAML 1 & 2 POST binding response pages so that users see a friendly "Please Wait" instead of blank POST page.**
- Customized logout page: SP info displayed on logout page.
- Integration test used to validate these enhancements.

UNICON OSS SOLUTIONS FOR YOUR TOOLBOX

Most, if not all, are Apache 2 licensed.

UNICON®

Hazelcast Shibboleth IdP Storage Service

- Based on the P2P in-memory data grid, Hazelcast
- When client-side/cookies storage services are not enough, but other are too much.
- Sponsored by Portland State University
- https://github.com/UniconLabs/shibboleth-hazelcast-storage-service

OpenID Connect Plugin for Shibboleth IdP

- Authorization code and Implicit flows
- Dynamic discovery
- Administration and registration of OIDC RPs with the IdP.

- Sponsored by University of Chicago
- https://github.com/uchicago/shibboleth-oidc

Symantec VIP MFA

- Token Authentication
- OTP Authentication
- Push Authentication
- Risk based Authentication
- Sponsored by the University of Wisconsin – Whitewater
- Work is complete, but not generalized yet for open source.

Duo Security MFA

- Supports User Enrollment
- Invokable by user attribute, relying-party config, SP authnContextClassRef

- Sponsored by University of Pittsburgh
- https://github.com/Unicon/shib-mfa-duo-auth

Shibboleth IdP Authn Flows

Shib-CAS-Authn3

- Delegate user authentication to an external CAS Server.
- Passes relying party's entityId to CAS Server.
- Now supports returning attributes to the IdP.

https://github.com/Unicon/shib-cas-authn3

CCC-Split-Authn

- Support unique users coming from 2 different authn/attribute sources
- Configured to support two LDAP servers, but other types should be similar.

Sponsored by California Community Colleges
https://github.com/Unicon/ccc-shib-split-authn

Miscellaneous Projects

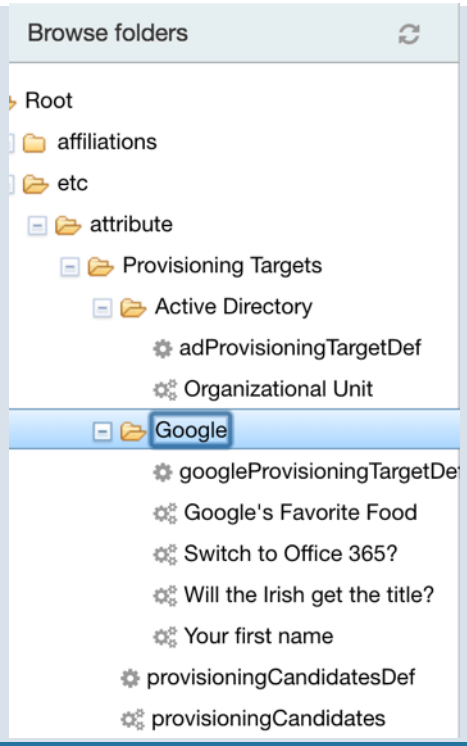
- Running Shibboleth IdP on the Azure Container Service:
  https://github.com/Unicon/shib3acs
  Sponsored by Microsoft
- Shibboleth IdP Development Environment:
  https://github.com/UniconLabs/shibboleth-idp-gradle-overlay
- Dockerized Shibboleth SP:
  https://github.com/Unicon/shibboleth-sp-dockerized
- AWS Lambda MDQ Server:
  https://github.com/Unicon/mdq-server-lambda

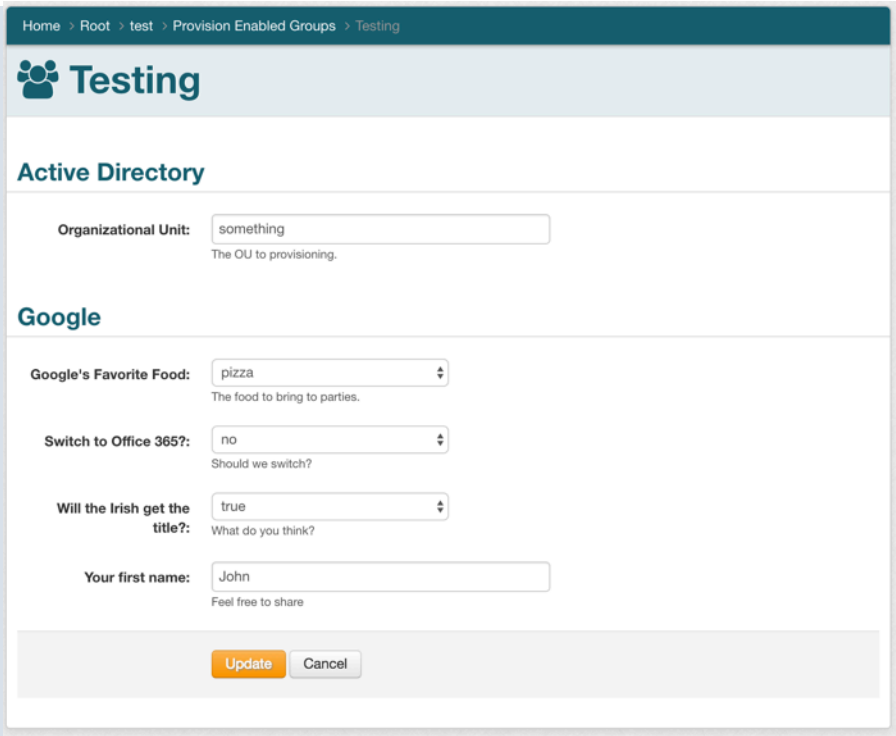
Grouper Custom Provisioning Target Form

- Dynamically builds a Group-specific form based on structured folders, attribute definitions, and attribute security settings.
- Good example of extending the Grouper UI

- Sponsored by Notre Dame
- https://github.com/Unicon/grouper-provisioning-target-ui

Grouper Custom Provisioning Target Form





Grouper Provisioners

Google Groups

- Supports multiple provisioner instances/configurations.
- Fine-grain control over which groups are provisioned.
- Configure Google's "advanced" group settings.

Sponsored by Oregon State University, additional work done by New York University

https://github.com/Unicon/googleapps-grouper-provisioner

Azure AD (Office 365)

- Security Groups Only
- Office 365 is planned but not scheduled.

Sponsored by Microsoft

https://github.com/Unicon/office365-and-azure-ad-grouper-provisioner

Dockerized Solutions for Grouper

Grouper Demo

Self-Contained:

- LDAP
- MySQL Server
- Grouper Loader
- Grouper UI & WS

•https://hub.docker.com/r/unicon/grouper-demo

Composable Images:

- Grouper Loader
- Grouper UI
- Grouper WS
- Grouper API (GSH)
- Images are ready to go!

•https://github.com/Unicon/grouper-dockerized

Unicon, Inc. is a leading provider of IT consulting, services, and support for education technology and works with institutions and organizations to find solutions to meet business challenges.

Unicon specializes in using open source technologies in the areas of:

- Identity and Access Management
- Student success/ Learning Analytics
- Learning Management Systems
- Portals

Unicon Services for IAM

- Consulting
- Strategic Assessment
- Systems Integration
- Custom Development
- User Experience
- Deployment
- Hosting
- Implementation Planning
- Branding
- Installation
- Configuration
- Support

Unicon is a Trust and Identity Solution Provider in the Internet2 Industry Program and an Industry Member of Internet2

UNICON®

Questions/ Answers

Contacts
Warren Leung
wleung@it.ucla.edu

John Gasper
jgasper@unicon.net