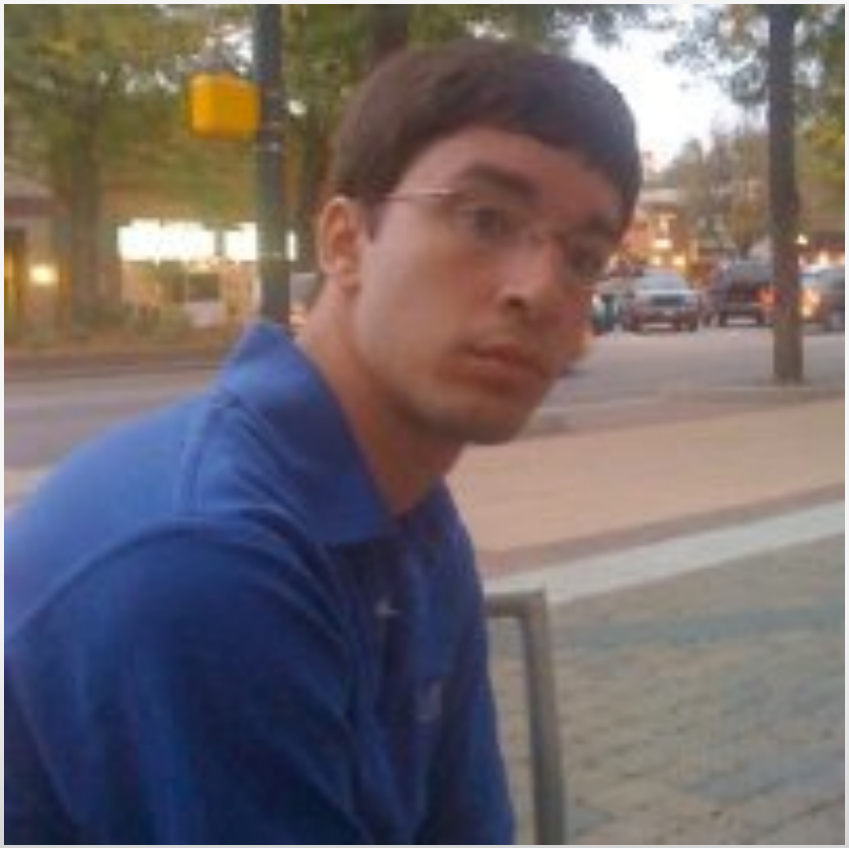
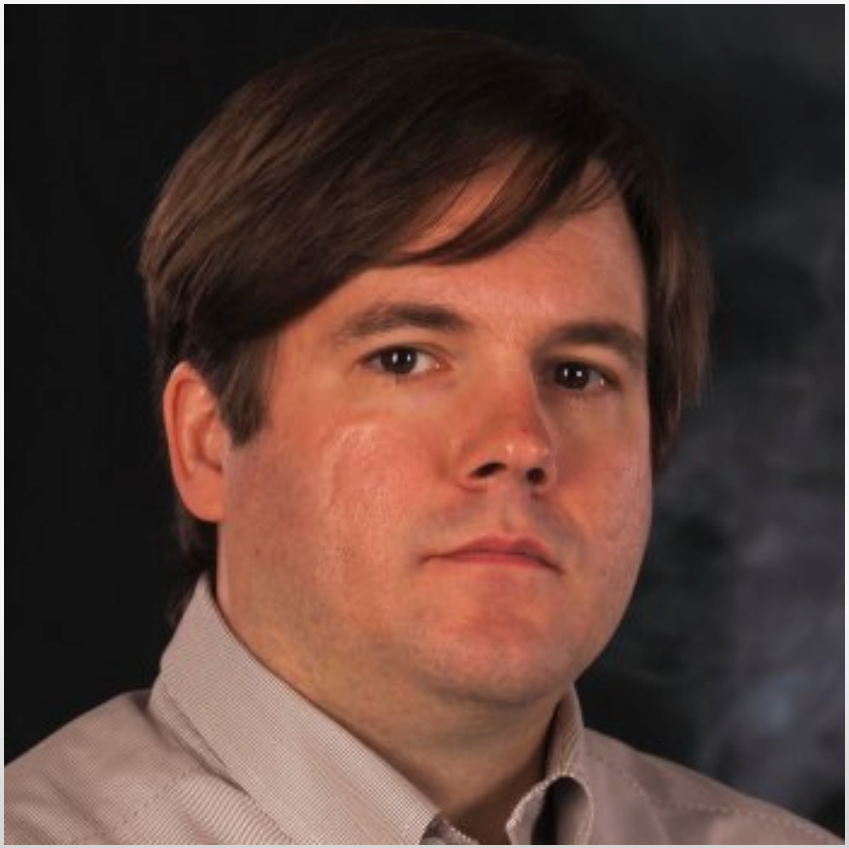
THE UNIVERSITY OF
CHICAGO



David Langenberg
IAM Architect
University of Chicago



Jonathan Johnson (Jj)
Software Developer,
IAM Consultant
Unicon, Inc.

Technical Overview

- v2 MCB
- v3 Spring Web Flows
- Duo for v3

v2 MCB

- Designed to cover most requirements
- Combination of hard coded functionality and custom XML schema
- Flexibility handled through Java development
- Designed specifically for Shibboleth v2

v3 Web Flows

- Gap analysis found that most functionality of the MCB can be done with v3
- Building blocks of services
- Tied together with external configuration
- Business logic moved out of compiled code

Duo for v3

- Pluggable -- Sane defaults that allow for easy drop in with a few configuration options
- Extendable -- The flow can be called from anywhere
- Overridable -- All configuration of the services and the flow can be changed by the deployer
- Community effort -- Developed with Unicon partners for the community

University of Chicago

- Shibboleth v2
- Working with Unicon
- Custom Work

Shibboleth v2

- Long-time user of Shibboleth
- Contributor to MCB Project
- Wrote a Duo authentication handler for MCB

Migration to v3 Goals

- Preserve all current functionality
  - Users can opt-in to forcing Duo
  - Services can force Duo
  - Support InCommon Silver via Password only
- Increase availability of service by eliminating dependencies
  - Memcached
  - External attribute sources
- Simplify build and enable deployment to foreign environments to which we have little control.
  - Dockerize

Implementation “Adjustments”

- Adjust provided Duo flow to support forceAuthn also forcing the user to re-enter their password.*
- Added some additional context-flow checking to enable us to handle silver even though the password flow returns PPT

*https://wiki.shibboleth.net/confluence/x/lYA9AQ

Gotchas & Current Issues

- ForceAuthn requests cause a double-login if the user does not have an existing SSO session (IDP-800)

- ECP Authentication does not work for users forcing Duo
  - Duo flow does not support passive authN

- When campus loses connectivity to Duo, the IdP fails closed

The Future

- Community driven efforts
- Other authentication methods
- Other types of plugins for Shibboleth

Resources

Duo Security: https://www.duosecurity.com/

Unicon Shibboleth v3 Duo Authentication:
https://github.com/Unicon/shib-mfa-duo-auth

Questions