From AD Groups to Grouper

By Erik Coleman and Keith Wessel
University of Illinois at Urbana-Champaign

Setting the Scene

- AD has been *de facto* central authorization store since 2000
- Thousands of groups managed in delegated department/unit OUs
- Required knowledge of LDAP tools or native AD tools
- No central management or auditing of membership or permissions
- Very few “reference” groups in AD
  - Limited to high-level affiliation groups
  - Managed by a scheduled PowerShell script

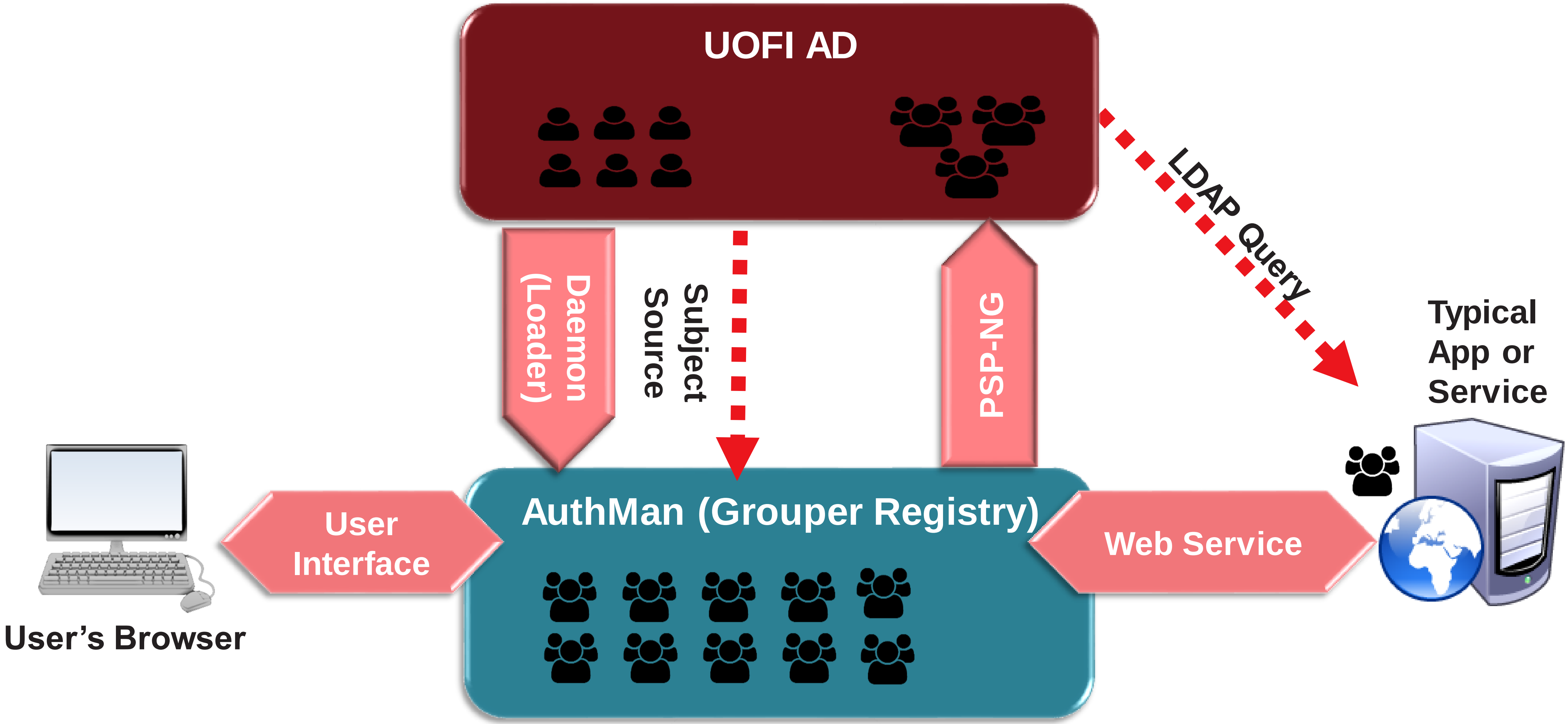
Along Comes Grouper

- First serious evaluations in 2015
- Provides easier management of groups
- Easy-to-use web interface for the non-technical
- Improved functionality
  - Include/Exclude Groups
  - Opt-in Groups
  - Attestation

The Move to Grouper: The Foundation

- AD will be subject source
- AD will also be group target
- Existing AD groups will not be migrated (but recreated)
- Infrastructure to deploy in AWS using TIER packaging
- Service branded as “Authorization Manager” or “AuthMan!”

Grouper Architecture at Illinois



The Move to Grouper: Phase I

- Reference groups built with Grouper LDAP loader jobs
- Groups can be optionally requested to sync to AD
- Synced groups pushed to flat OU=AuthMan
- Staff can request department/unit folders for delegation
- Individuals can create ad-hoc groups too

The Move to Grouper: Phase I-B - Real Use-Cases

- Include/Exclude group for VPN access
- Master Exclude group for Security service “shut off”
- AWS roles and account groups
- Duo MFA early opt-in group
- Authorizations for new web-hosting platform

The Move to Grouper: Phase II – Future Plans

- Campus Training and Onboarding Campaign
- Federated Grouper for external users (including our sister campuses)
- Support for "non-person" subjects in groups
- Test/Evaluate changes to group provisioning
  - Upgrade loader jobs to SQL queries against EDW
  - Consume messages directly from Banner
- Migrate class roster groups (huge undertaking!)