InCommon Silver
With Active Directory Domain Services

Building A Community-Sourced Cookbook
Nick Roy – The University of Iowa
Mark Rank and Chris Spadanuda – The University of Wisconsin-Milwaukee
Ann West – InCommon
Topics for Today

• What is InCommon Silver?
• What is the AD Cookbook for Silver?
• Case Study from UW-Milwaukee
What is InCommon Silver?
It’s All About Assurance

Assurance
• a positive declaration intended to give confidence; a promise: [ with clause ] : *he gave an assurance that work would not recommence until Wednesday.*

Identity Assurance
• the ability for a party to determine, with some level of certainty, that an electronic credential representing a person can be trusted to actually belong to the person.
Federated Transactions

Services Relying on External Identities:
- I need to trust you to manage online identities for me?
- What are my risks?
- What are the odds and the degree of harm?

Parties need agreed-upon criteria for identity assurance

InCommon Assurance Program: Responding to Government Requirements

- 2004: USG defines 4 Levels of Assurance (NIST 800-63)
- 2009: USG Identity, Credential and Access Management (ICAM)
  - Establishes criteria for trust framework providers to enable interaction with federal agencies
  - InCommon Approved Trust Framework Provider
- Oct 2011: Federal CIO Memo mandating use of FICAM-approved externally-issued credentials. NSF, NIH, etc.
Program Basics: Documents

- Identity Assurance Assessment Framework
- Identity Assurance Profiles
  - Bronze (Level 1)
  - Silver (Level 2)
- Legal Addendum
  - Privacy criteria from ICAM

Want more background? See assurance.incommon.org
InCommon Identity Assurance Profiles

- Business, Policy and Operational Criteria
- Registration and Identity Proofing
- Credential Technology
- Credential Issuance and Management
- Authentication Process
- Identity Information Management
- Assertion Content
- Technical Environment
History

- CIC CIOs: All CIC schools will achieve InCommon Silver by Fall of 2011
- The CIC Identity Management group started a Silver assurance project
- Areas of focus
  - Documentation
  - Registration Authority Processes
  - Authentication Technology and Processes
Active Directory Domain Services

- AD is prevalent in higher education
- Institutional net IDs and passwords often provisioned to AD
- AD is likely in scope for your Silver assessment
Authentication-specific areas of Silver

- 4.2.3.4 Stored Authentication Secrets
- 4.2.3.5 Protected Authentication Secrets
- 4.2.5.1 Resist Replay Attack
- 4.2.5.2 Resist Eavesdropper Attack
- 4.2.5.3 Secure communication
How To Get To Silver

- Active Directory is widely deployed
- Its strengths are also potential risks
- Active Directory is complex and powerful
Background: Active Directory DS and InCommon Silver
The AD DS/Silver Cookbook

- I presented a number of technical hurdles with authentication and Silver at the Fall, 2010 Internet2 member meeting
- Many of these issues were rooted in our Silver gap analysis of Iowa’s AD environment
- Began work to document solutions in January, 2011 within the CIC IdM group
The CIC Reaches Out

- We needed a lot of cooks in the kitchen
- Lots of others looking at the same questions
Widening Participation

- Getting feedback from Microsoft was essential
- Vetting our recommendations
- Opening it up to the entire InCommon assurance community
Moving the project to a national level

- More eyes on a project like this are better
- Goal to donate the documentation to InCommon
Added Partners

• A (hopefully complete) list of schools involved:
  - Iowa, Minnesota, Univ. of Chicago, UW-Madison, UW-Milwaukee, Penn State, Ohio State, Univ. of Florida, Univ. of Washington, Carnegie Mellon, UT Austin, Texas A&M, North Carolina State, University of California

• At least two schools actively implementing strategies defined in the cookbook: UW-Milwaukee and Univ. of Florida
The Cookies

- A list of things to think about carefully
- An interpretation of the assurance profiles in the context of AD DS
- A set of suggestions
- Not proscriptive or definitive
What’s In It?

- The Cookbook only covers those sections that present problems unique to Active Directory.
- Not those that are generally applicable to all password-based authentication, such as password complexity.
What It’s Not

- One size fits all
- A guarantee of success
- A complete analysis of Silver
Some Concrete Examples
Context

- UWM has long history in area of health related research...
  - College of Health Sciences
  - College of Nursing
  - Helen Bader School of Social Welfare
- UWM is also the new home for the Joseph J. Zilber School of Public Health, Wisconsin’s first accredited school of public health.
We pay attention...

UWM RESEARCH EXPENDITURES
Fiscal Year 2010
FEDERAL SOURCES – By Agency ($29.66 million)

- NSF 32.4% $9,601,874
- NIH 31.4% $9,301,661
- FED – Other 5.5% $1,624,042
- Defense 6.2% $1,832,138
- Education 8.1% $2,401,666
- EPA 1.4% $422,470
- Agriculture 1.7% $504,204
- NOAA 2.6% $766,823
- Energy 4.7% $1,402,767
- DHHS – Other 5.1% $1,503,959
- Transportation 1.0% $302,199
Timeline

- 2006 – UWM Research Growth Initiative kicked off
- 2009 – IAM funded to support research
- Jan 2010 - IAM Program established – AD is a service without a home
- Summer 2010 – WG formed and AD upgrade identified as top risk to operation
- Dec 2010 – AD administrator hired
- Spring 2011 – AD upgraded to 2008 R2
- Summer 2011 – IAM Group formed
- Summer/Fall 2011 – UWM InfoSec Office conducts risk assessment with input from early draft of cookbook
Where does AD Cookbook come in?

- UWM Operates two synced credential stores
  - OpenLDAP – A topic for a different time
  - Active Directory
    - Centrally Maintained
    - Coordinated using operation team reporting to IAM Steering Committee
Moving Forward - Our Plan

- Leverage the operational team structure
- Use AD Cookbook as guideline
- Utilize information gained via recently completed risk assessment of AD environment
- Conduct a pre-audit to validate our fit-gap
- Prep our auditor
Securing Authentication Secrets

- 4.2.3.4 Stored Authentication Secrets
- 4.2.3.5 Protected Authentication Secrets
Attacks

• 4.2.5.1 Resist Replay Attack
• 4.2.5.2 Resist Eavesdropper Attack
Securing Communication

- 4.2.5.3 Secure communication
More AD work to consider

- Multi-Factor
- Endpoint hardening
- Transport hardening
- Application use of AD
- Remote site build out
- Decentralized IT needs
- Audit
- For UWM, the value of the community effort is a set of practical guidance
Some Final Thoughts

We’d love to get your feedback and experiences with implementation
Send feedback to assurance-adsilver@incommon.org
Discussion

• The Cookbook: https://spaces.internet2.edu/x/w56KAQ
• Contact us –
  Assurance mailing list: assurance@incommon.org
• AD/Silver feedback: assurance-adsilver@incommon.org
• Assurance website: assurance.incommon.org
Shibboleth Workshop Series
http://www.incommon.org/educate/shibboleth/

April 12-13 – Columbia, Missouri

July 16-17 – Baltimore, Maryland

InCommon Confab – April 26-27, 2012
Scaling Community Trust
www.incommon.org/confab2012.html

Crystal Gateway Marriott, Arlington, Virginia

Learn how the InCommon community is using trust services to enhance users’ experiences and scale online relationships.

Register today!
Evaluation
Please complete the evaluation of today’s IAM Online:

IAM Online Announcement List
Email sympa@incommon.org with the subject: subscribe iamonline

Thank you to InCommon Affiliates for helping to make IAM Online possible.

Brought to you by InCommon, in cooperation with Internet2
and the EDUCAUSE Identity and Access Management Working Group