InCommon-Silver And Active Directory Domain Services

Warren Curry, University of Florida

Mark Rank, UW-Milwaukee

InCommon Assurance In One Slide

- 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.

Strengths vs Potential Risks

- Active Directory Domain Services:
  - widely deployed
  - complex and powerful

History AD DS/Silver Cookbook

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

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

Moving the project to a national level

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

Collaboration

- Participation and feedback from Microsoft
- 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

Microsoft®

What It Is

- 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 It's Not

- One size fits all
- A guarantee of success
- A complete analysis of Silver


UF
UNIVERSITY of
FLORIDA

UF AD DS Compliance

IAP sections addressed by UF changes:

- 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

NOTE:

- UF uses a distinct instance of MIT Kerberos to authenticate all shibboleth IdP access.
- AD DS is used to control internal desktops and client resources.
- Recent UF policy standard requires all web access to be operated through Shibboleth IdP.

UF AD DS Compliance Changes

Florida is following the following strategy to achieve secure authentication traffic with AD DS:

- Require LDAP data signing
- Disallow use of NTLMv1 (therefore requiring NTLMv2 or better)
- Require LDAP Simple Binds
- Management Reports for review and mitigation on a periodic and recurring basis.

UF AD DS Compliance Changes for InCommon Silver Requirements

By enabling the following GPO setting "Network Security: Do not store LAN Manager hash value on next password change" for clients, this will effectively disable storage of the LMHASH values of passwords.

Require signed LDAP traffic by setting the following GPO setting to enabled: “Domain Controller: LDAP Server signing requirements”

Deploy the GPO setting "Network security: LDAP client signing requirements" to clients, and require third party applications to be reconfigured to use SSL/TLS or signed SASL binds.

AD DS is not used with Federated InCommon Access but it is the same credential and must be considered when preparing for the Silver audit process. **No Weak Link !**

UF AD DS Compliance Changes for Silver

Deploy date for these changes is April 29th, 2012 !

Initial schedule was for mid January 2012 - we took it slow and built consensus through the campus community that the changes would be beneficial and were needed regardless of Silver.

Testing conducted uncovered a couple issues:

- **Data devices can be problematic some do not support NTLMv2**
- **Other devices printers, faxes, etc have issues and claim to support AD DS**
- **Mac issues: Health Center tests**
  - **applied the supplied GPOs to our separate test domain.**
  - **The test domain contains a domain controller and a separate Windows 2008 R2 server that houses file shares.**
  - **joined a iMac G5 (OSX 10.5.8), a MacBook Pro (OSX 10.5.8), and a MacBook Pro (OSX 10.7.3) to the test domain. We did not encounter any issues joining the devices to the domain and were able to successfully log into the MACs with domain accounts that did not exist on the devices already.**
  - **Once logged in with a domain account, we were able to connect to shares on the file server, access files, and update files. We created a security group in the domain and added users to it. We assigned this group access to one of the file shares and removed access from all other groups and users to the share. We were still able to add, remove, and update files in that share.**

Installed Wireshark on the Domain Controller and captured workstation login and file access traffic. The trace showed that the traffic was going over LDAP port 389 and not NTLM.


UNIVERSITY of WISCONSIN
UWMILWAUKEE

AD Cookbook and UWM

PD-http://en.wikipedia.org/wiki/User:Fubar_Obfusco

- 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
    - Cookbook integrated into the security plan for operations

Some “Tough Love”

- Turning risk assessment into security plan
- Tighten operational procedures
- Mitigate problem protocols
  - NTLMv1
  - LMHASH
  - LDAP

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

NASA Dryden Flight Research Center Photo Collection
http://www.dfrc.nasa.gov/gallery/photo/index.html
NASA Photo: ED99-45243-01 Date: 1999 Photo by: NASA

X-43A Hypersonic Experimental Vehicle - Artist Concept in Flight

Uses Beyond Certification

- Discussions in UW System to use the InCommon-Silver profile as a benchmark for credential assurance

- The AD Cookbook becomes part of the body of knowledge

DISCUSSION

Warren Curry (whcurry@ufl.edu)
Mark Rank (rankm@uwm.edu)

References

- 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