March 29, 2013

AD-Assurance Notes from March 29

David Walker, InCommon/Internet2
Michael Brogan, UWash
Jeff Capehart, UFL
Ron Thielen, UChicago
Joe Streeter, UW Madison
Eric Coleman, University of Illinois
Ann West, InCommon/Internet2

Next Call

April 5 at Noon ET
+1-734-615-7474 PREFERRED
+1-866-411-0013
0195240#
Agenda: Updates to AIs, matrix starting with 4.2.5.1

Action Items

David - Develop AM to abstract Ron's approach of using audit process lieu of technology controls.
Michael - Need reference regarding LDAP signing in 4.2.3.5
Michael - Add recommendation to ensure chosen configuration of services support Approved Algorithm encryption. in 4.2.3.6. 1b.

Cookbook Todos
Add guidance about methods to prevent transient password exposure to the Cookbook.

Notes

Ron's Alternative Means -

Primary concern centered on scope of population and diversity of services available. When the silver pop scope widens and the need to access more diverse services increases, the frequency that users will be bumped out of silver will increase. At Chicago, the initial silver pop is scoped to reserachers, not a large group. Ron has been watching the traffic using this technique for about a year and seeing roughly 400 individuals in the log, very few (or any?) of which are in the target pop. In the long run, one would need a better solution.

Washington is looking to tak the approach of preventing users from doing something that would make their cred non-compliant, such as using an old OS.

UI Issues

The rub is how to communicate about assurance to users. Lots of confusion about why they can't log in. At Chicago, they've developed an WHO AM I website where users can look at their credentials, click on a silver page, and see a series of statements with checked boxes corresponding to the criteria needed achieve it (or what they've done to degrade it).

One could couple Ron's audit process with user education on good and bad (compromising) credential behavior. If anyone has documentation on this, please share with Jim Green's documentation subgroup.

Ron is educating the department admins about this approach and giving them guidance the audit process and what needs to be done to reduce silver compromise such as upgrading OSes. His pitch is really about keeping up to date on modern security standards. Silver is influencing timing and exposes the issue, but isn't driving it. Good security practices are driving the changes.

Ron also mentioned another AM they're working on for supporting protected channels: deploy the service over a non-route-able layer 2 VLAN.

AI - David to develop AM to abstract Ron's approach of using audit process lieu of technology controls.

Matrix

4.2.3.4 - MS Question: Is there a filter in 2008 and later to decrypt and encrypt disk sectors as they are read?

4.2.3.5 - AI - Michael - Need reference regarding LDAP signing.

4.2.3.6

1b - AI - Michael to add recommendation to ensure chosen configuration of services support Approved Algorithm encryption.

Can't configure the environment, put them in a group policy that doesn't allow them to use faciltiiites that aren't silver compliant.

2. Disable non-compliant protocols. Encrypt LDAP binds; If you can't due to compatibility, monitor the traffic for clear binds (AM).

3. Applies regardless of technology. Any service using IdMs have to have policies and procedures that make sure they're doing the right thing. Making sure the logging is on for unsigned LDAP. AI - All - Add guidance about methods to prevent transient password exposure to the Cookbook.

- UFL uses Shib instead. Either requires now or will require services to register to connect.

- Washington requires Shib too and this works well for their internal apps. They still have issues with vendors that have built in LDAP Auth because it's so widely deployed across HE.