May 17, 2013

AD-Assurance Notes from May 17

David Walker, InCommon/Internet2
Eric Goodman, UCOP
Jeff Whitworth, UNC Greensboro
Rob Gorrell, UNC Greensboro
Ron Thielen, U Chicago
Jeff Capehart, UFL
Mark Rank, UCSF
Ann West, I2/InC (scribe)

Next Call

May 24 at Noon ET
+1-734-615-7474 PREFERRED
+1-866-411-0013
0195240#

Agenda:

Action Items

- Mark to send out a strawman endorsement statement that the group will iterate on in email.
- Brian to clarify whether one can tell the difference between NTLM v1 and v2 in the logs.
- David to draft an alternative means statement about NTLMv2 and RC4/HMAC.
- Ron to draft a statement about client caching of credentials.
- Ron will look into whether SysKey uses approved algorithms.

Notes

Alternative Means: Monitor and Mitigate

For those with a different case, this provides enough of a template that others can use to address their own use case. Chicago to submit it, endorsed by those on the AD-Assurance call that approved it (and others that follow suit on email). AI - Mark to send out a strawman endorsement statement that the group will iterate on in email. Ron will then add this statement to his proposal and send to the AAC.

Next Steps on Cookbook

Eric's proposal

- Organization - Pull out the why so that implementers see clearly what they have to do. Move reasoning to appendices. - Eric Goodman

- Password Stored at rest - pull out entropy - Eric Goodman

   - Is SysKey use an Approved Algorithm? If so, then it's an alternative to Bitlocker. - Ron will look into this; we'll also ask Microsoft.

- AM and reference language regarding NTLM v2 and RC4-HMAC. - David Walker

- Client cashed credentials. Clients are out of scope, but you need to address them. - Ron Thielen

- Add Monitor and Mitigate AM language/reference. - Eric Goodman

Meeting with Microsoft

Brian and Ann contacted Microsoft about meeting with the AD-Azure PM,