June 14, 2013

AD-Assurance Notes from June 14

Eric Goodman, UCOP
Ron Thielen, U of Chicago
David Walker, Internet2/InCommon
Jeff Capehart, UFL
Michael Brogan, UW
Ann West, Internet2/InCommon

Next Call

June 21 at Noon ET
+1-734-615-7474 PREFERRED
+1-866-411-0013
0195240#

Agenda:

Discussion of changes to Cookbook before Community Review.

Action Items

- Eric Goodman will edit the Cookbook according to today's discussion.

Notes

- **Introduction:** We will move the paragraph about versions of Windows Server that we are addressing from the "IAP Requirements Reviewed" section to the Introduction.
- **Configurations to address Passwords at Rest:** The "Remove Insecure (LMHASH) Stored Secrets" subsection will be recast as highly recommended, but not necessary for Silver compliance, assuming that the preceding "Encrypt the Password Store Using 3rd Party Tools" subsection has been implemented.
- **Configuration to Secure Network Traffic:** We are still undecided on the viability of RC4 ciphers for Kerberos and NTLMv2. Here are the issues:
    - RC4 is not an approved algorithm, but the IAP's standard is that exploits "impractical." They are probably impractical right now, but it's hard to tell how long they will be. We need input from Microsoft on how they would address an exploit, for which versions of Windows, *etc*.
    - We do not have consensus on whether the information communicated over the network during authentication is one of the following. Microsoft can help us determine this, and then we need to decide whether we believe that an exploit is "impractical."
        - passwords / authentication secrets,
        - hashes of passwords or authentication secrets, or
        - hashes of session-dependent values, using passwords or authentication secrets in the algorithm, but not transmitting them.
- We are starting to be blocked by lack of information from Microsoft. Ann continues her efforts to set up a call, now with support from John Krienke and Shel Waggener, but we might want to start making some assumptions about likely Microsoft responses (which we would still verify) in order to make progress on the Cookbook.