June 28, 2013

AD-Assurance Notes from June 28

Michael Brogan, U Washington
Jeff Capehart, UFL
Eric Coleman, U Illinois
Eric Goodman, UCOP
Mark Rank, UCSF
Ron Thielen, U of Chicago
David Walker, Internet2/InCommon

Next Call

July 12 at Noon ET (unless someone has a reason to meet on July 5)
+1-734-615-7474 PREFERRED
+1-866-411-0013
0195240#

Agenda:

Discussion of changes to Cookbook before Community Review.

Action Items

- Edits to the current draft as described below in the notes.

Notes

- We decided to amend the appendix describing operational issues with running Bitlocker as part of a virtual machine guest OS. The new text will indicate that this can be resolved by running Bitlocker with the virtual machine host OS, instead of the guest OS.
- The "Configurations to address Passwords at Rest" section will be amended to indicate that the storage encryption mitigates the risk of an attacker gaining physical access to the storage media. Other controls, like file access permissions, are still needed.
- We discussed potential next steps if we don't get a satisfactory response from Microsoft about vulnerabilities in the NTLMv2 and Kerberos authentication protocols, as described in "Securing Authentication Traffic." We have no reason to believe that we will not get a satisfactory response, but we want to be prepared if we do. Unfortunately, there may be little we can do that isn't difficult and/or expensive to deploy. Here are some thoughts:
    - Require IPSEC for communication with domain controllers. This will not likely be an easy deployment, and it may not even be possible for old versions of Windows or non-Windows clients. A "monitor and mitigate" strategy is unlikely, as we do not believe that an indication of the use of IPSEC is available from the logs. It may be possible to move Silver-vetted people into subdomains with domain controllers that require IPSEC, but it would be a complex configuration.
    - Require multi-factor authentication. These seems to be the direction that federal government agencies are taking. Again, it's not cheap, but may be feasible for institutions for a small number of Silver-vetted people.
    - We need to understand Microsoft's strategic direction and roadmap for improving their authentication infrastructure. We know they know the issues; the question is how fast they're going to move.
- Since our next call would normally occur on the day between the Fourth of July and the weekend, we decided to cancel that call unless someone comes up with a reason to keep it.