Minutes of Assurance Call of 2-Oct-2013

Draft Notes: Assurance Implementers call 2-Oct-2013

Attending
Ann West, Internet2/InCommon
Mary Dunker, Virginia Tech
Wes Hubert, University of Kansas
Eric Goodman, UCOP
David Walker, Internet2/ InCommon
Marlena Erdos, Harvard
Dedra Chamberlin, UC
Ron Thielen, University of Chicago
Michael Brogan, University of Washington
Jonathan Miner , University of Wisconsin
Waren Curry, University of Florida
Jeff Capehart, University of Florida
Chris Spadenuda, UW Milwaukee
Brian Arkills, University of Washington

DISCUSSION

Updated Version of InCommon Silver with Active Directory Cookbook
https://spaces.at.internet2.edu/x/dJSVAQ

The AD Assurance working group has released a draft of their updated version of the InCommon Silver with Active Directory Cookbook and is asking for feedback from the Community during the period of October 2 to November 8, 2013.

Please send feedback to the Assurance list or enter it on the table linked from:https://spaces.at.internet2.edu/x/dJSVAQ.

Background

David presented the background of the AD Cookbook effort. In 2012, a group worked on the InCommon Silver with AD Services cookbook. https://spaces.at.internet2.edu/x/w56KAQ

Since the 2012 AD Cookbook was finalized, the Bronze and Silver IAPs were revised from version 1.1 to version 1.2. This change to the IAPs triggered looking at the AD Cookbook again. Of particular interest was the wording change (to align with FICAM) from "industry standard algorithms" to "Approved algorithms."

The community was aware that ADDS (part of AD) uses many protocols that reflect the history of AD development over decades. Some of the AD algorithms are approved and some are not. Therefore, in March 2013, InCommon kicked off a community review of the InCommon Silver with AD Cookbook in light of the revised version 1.2 Identity Assurance Profiles and Framework. Issues are summarized here: http://tinyurl.com/kun6o89

Scope

The scope of the cookbook is AD with passwords for authentication that are selected by the end users. The cookbook does not address MFA and alternatives to passwords.
More about scope is here: http://tinyurl.com/mzua9eh

While there are some unresolved questions that the group posed to Microsoft, the Cookbook is now ready for review.

Additional Details on the Cookbook

Eric noted that the group did restructuring of the 2012 AD Cookbook to highlight important issues related to the version 1.2 IAPs.

One of the challenges occurred when there were different interpretations of the intent of the IAP. Some of the interpretation issues were clarified with the AAC and that proved helpful. The interpretations being used are explicitly spelled out in section 4 of the Cookbook: http://tinyurl.com/kun6o89

The Cookbook provides configuration requirements for password at rest, secure authentication traffic, and transmission of authentication secrets by the IdP. Input is welcome from those who have a chance to do testing. http://tinyurl.com/kr5wogs

The AD Cookbook attempts to be explicit on which requirements apply to IDP interactions and which requirements apply to IDP verifier interactions.

The Cookbook includes a "monitor and mitigate" alternative control for satisfying requirement 4.2.3.6.3. (related to use of LM and NTLMv1) https://spaces.at.internet2.edu/x/roGZAg

The group concluded that no alternative means are required to handle AD Assurance. Sample management assertions are provided http://tinyurl.com/lqpjwm7

Comments:

Brian noted that a concern at University of Washington was around password encryption, and the revised Cookbook is helpful in this regard.

Chris stated that based on his initial review, the revised Cookbook clarifies several important issues. Kudos to the team.

Jeff noted that U. Florida has had concerns about the IdP, Shibboleth, MD4 hash and RC4. The Cookbook is helpful in addressing those issues, especially as some parts of AD can now be excluded.

Mary Dunker, chair of the AAC, thanked the AD Assurance Group for their work on this Cookbook. This is a valuable resource for the community.

Next Steps

Ann noted two groups needs to look at the Cookbook

-AAC to do another review of the interpretations

-Ann will send the cookbook to Microsoft to get response to the open questions and the content itself

Hope to have those responses from AAC and Microsoft to discuss on the November Assurance Implementers call.

Feedback from the community is welcome. Closing date for review by community is Nov. 8, 2013.