Minutes of Assurance Call of 5-June-2013

Draft Minutes, Assurance Implementers Call, 5-June-2013

Attending

Ann West, InCommon
Mary Dunker, Virginia Tech
Wes Hubert, University of Kansas
Eric Goodman, UCOP
Mark Rank, UCSF
Diane Sheldon-ku, Duo Security
Dave Langenberg, U. Chicago
Brett Bieber, Univ. of Nebraska, Lincoln
Jeff Capehart, University of Florida
Steven Carmody, Brown
David Walker, InCommon
Mark Jones, UT Houston-HSS
Benn Oshrin, Spherical Cow Group
Emily Eisbruch, Internet2, scribe

DISCUSSION

Shib IdP Enhancements

The Shib IdP Enhancements RFP submission period has closed. Responses are being reviewed and announcement of the selected RFP should occur in about one month. The goal is that the work will be completed by the end of 2013.

https://spaces.at.internet2.edu/display/InCAssurance/InCommon+Assurance+Program#InCommonAssuranceProgram-RequestforProposal%3AShibbolethIdentityProviderEnhancements

CIC Assurance Documentation Grouphttp://bit.ly/Yu2erK

Jim Green, who has been leading the CIC Assurance Documentation group, has been reassigned to a new position at Michigan State University. New leadership is being sought for this group, which meets monthly to share experiences and documentation around Assurance adoption. Let Jim know if you can help.

Assurance Advisory Committee

Mary noted that the AAC appreciated the feedback that was provided on the May 8 Assurance Implementers call about campus impacts of making Bronze a baseline standard for InCommon IdPs. The AAC is exploring this idea and will report back.

In addition, the AAC has been discussing procedures for how an IdP must re-certify when there are changes to the spec. The only institution impacted in the increase from 1.1 to 1.2 is Virginia Tech. Virginia Tech is getting instructions from the AAC on how to recertify under 1.2. One aspect of this is that Virginia Tech will submit an Alternative Means about using the SafeNet eToken PRO multi-factor authentication solution.

Q: Is there a plan to change the POPs along with the proposal to require Bronze as the baseline for IdPs?

A: Ann: yes, there are a items in the IdP POP that are not covered by Bronze. How should we address those? Are there new items that should be included in the next generation POP? InCommon is reviewing the POP with AAC.

Q: What timeframe is being considered for requiring Bronze as the baseline for IdPs?

A: The current discussions center on Level 1 InCommon Members achieving Bronze in 18 months. IdPs in other tiers are given a longer time, with increments of six months being used for each additional pricing tier. Tiers are shown here: http://www.incommon.org/fees.html

David noted that POPs are hard to enforce, and easily become out of date, and that the Bronze Assurance program is more scalable.

"Failed Authentication Counter" Proposalhttp://bit.ly/1b1A1L7

Benn reviewed his "Failed Authentication Counter" proposal. The goal is to develop a more workable approach to the password entropy calculation requirements in the assurance profiles. The current requirements are not suitable for some institutions, such as UC Berkeley and NYU. The proposed "Failed Authentication Counter" approach is simpler; it counts the number of failed authentication attempts and takes action -- such as to lock out the credential -- when that count crosses a threshold.

Eric: The approach is fine. Wondering where this might fail and what could be done to mitigate those concerns.

Brett: This proposed solution is worth exploring. Would be interested in participating in a group to look at this.

It was noted that this proposal addresses attempts to guess a password, but it does not protect against stealing a password. What about looking at issues impacting the security of credential stores? It was agreed that it makes sense to have a parallel effort around best practices for credential store policies.

Moving forward, Benn will spin up a subgroup to look at this proposal.

AD Alternative Means Work

http://bit.ly/14CPlPuhttps://spaces.at.internet2.edu/display/InCAssurance/AD+Alternative+Means+-+2013

Eric reported that the AD Alternative Means Group is making good progress. The group's charge is to analyze using AD to comply with the IAPs, and develop guidance and specific pre-approved Alternative Means to bridge any gaps. The group has found that most of the topics are already covered in the AD Cookbook developed under the leadership of Nick Roy:https://spaces.at.internet2.edu/display/InCAssurance/InCommon+Silver+with+Active+Directory+Domain+Services+Cookbook

The AD Cookbook gives general advice in most cases, and this group is trying to be more specific on whether or not AD meets the requirements under certain configurations. Also when the AD Cookbook written, the spec was at 1.1 and there are some relevant changes with the new IAP 1.2. Important gaps for AD-specific issues are around support of insecure protocols for backwards compatibility. Some of the elements that were originally just recommended in the AD cookbook are now being required, such as using BitLocker or something like it to secure the AD Password stores.

StevenC said that there are campuses that are still running MIT Kerberos, often in parallel with AD. Is It possible for the AD Alternative Means group to separate out from the core AD document a subsection to refer only the protocols that AD adopted out of the K5 specs? Eric replied that the document could call out areas that apply to MIT Kerberos.

Ann: once the updates to the AD cookbook are farther along, we will send out info to the Assurance and InCommon participants lists and solicit for Community review.

SHA-1 Question

DaveL: SHA-1 won't be approved after Dec 31, 2013. This could cause a problem for InCommon Assurance, since few browsers support SHA-2

Ann: The AAC recently discussed this issue and the TAC will be having a discussion as well. Stay tuned.