Comments from Tom Barton - 2016-04-20

Subject:	[Assurance] comments on draft MFA Interop WG documents
Date:	Wed, 20 Apr 2016 15:36:52 -0500
From:	Tom Barton <tbarton@uchicago.edu>
Reply-To:	assurance@incommon.org
To:	assurance@incommon.org

Hi Colleagues,

It looks like an impressive group has done some really impressive work, and I'm, well, impressed!

I have a few questions and suggestions.

1. Since these profiles should eventually be adopted internationally in order to have greatest effect, I suggest addressing two aspects to remove potential barriers:

- Choose an identifier from the REFEDS namespace, and of course gain support and approval for allocating that value from REFEDS. Eg, "http://refeds.org/profile/mfa" and "http://refeds.org/profile/base-level".
- Remove "InCommon" from the names of the profiles themselves.

2. What is the source of the data in "MFA Technologies, Threats, and Usage", or, if it is sourced by the WG, what methodology and standards were used to arrive at this data? Associated suggestion is to put that material into the doc itself.

3. Big +1 for the manner in which you limited scope and focused!

4. Re the second main bullet in the "Independence of Factors" section of "Usage Guidance". What is the basis for the statement "Processes that allow a user to immediately register a new second factor (reregistration)
using only their “first factor” enterprise password are not secure." in the context of the specific risks identified in the "Risks that must be mitigated" section? Ie, should there be an analysis of those risks that is used to reach the conclusion that such reregistrations do not mitigate those risks, rather than an a priori statement of it being not secure?

5. Perhaps related to #4, the first main bullet in the "Independence of Factors" section of "Usage Guidance" contains the statement "Any factor that is directly accessible using the first factor is NOT considered a second
factor." Should that statement be sharpened to say something like "Any factor that is directly accessible by *unauthorized* use of the first factor ..."?

6. Did the WG consider whether or not it would be good to also define a corresponding entity category, signifying something like "this IdP supports this profile for some significant segment of its user population", or "this SP supports this profile for users in some of its security roles"? If so, would it be worthwhile to add a brief discussion of that proposition and the WG's conclusion to the Final Report, or if not, might that be an area for future work, to be added to the Recommendations section of the Final Report?

7. I understand that the base-level authncontext enables an SP to express that it prefers but does not require MFA, but I don't understand how it establishes "a base over which other profiles could be defined." Could you enlighten me?

Many thanks,
Tom


```
--
Tom Barton
Senior Director for Architecture, Integration, and Security
Chief Information Security Officer
IT Services
University of Chicago
+1 773 834 1700
```

Subject:	Re: [Assurance] comments on draft MFA Interop WG documents
Date:	Thu, 21 Apr 2016 13:23:57 -0700
From:	David Walker <dwalker@internet2.edu>
Reply-To:	assurance@incommon.org

To:	assurance@incommon.org

I've added some more thoughts below...

By the way, for those of you who may not have seen Monday's TIER release announcement, the MFA Interoperability Profile Working Group has asked that comments on its draft profiles and other documents be sent to assurance@incommon.org. Please take a look and weigh in on the conversation.

David

On 04/21/2016 12:13 PM, Eric Goodman wrote:

> *Hi Tom,*
>
> *Thanks for the detailed response!*
>
> *The workgroup did not explicitly discuss your email, so I'm trying to be good here and say "we" or "the workgroup" when referring to actual discussions that took place in the workgroup vs. "I think" when I'm giving my own opinion on a topic that was not explicitly discussed.*
>
> > *1.... I suggest [you]...Choose an identifier from the REFEDS namespace, and of course gain support and approval for allocating that value from REFEDS. Eg, "http://refeds.org/profile/mfa" and "http://refeds.org/profile/base-level".*
>
> *We agree with the approach. Note that the last bullet in the "Recommendations" document is to discuss this with REFEDS. I believe this was only not attempted given the time constraints on the deliverables. I'm confident that if appropriate consensus/approval from REFEDS can be achieved within a timeline acceptable to the AAC that the workgroup would be happy to see this done.*

Yes, that's exactly it. The charge from the AAC was for an InCommon profile, and we didn't have a lot of time after the group was reformed a couple of months ago. I certainly hope they can become REFEDS profiles with refeds.org-based URIs.

> > *2...What is the source of the data in "MFA Technologies, Threats, and Usage", or,*
>
> *Sourced by the workgroup.*
>
> > *if it is sourced by the WG, what methodology and standards were used to arrive at this data? Associated suggestion is to put that material into the doc itself.*
>
> *There was much discussion in the workgroup about how much technology-specific detail to put in the profile. We agreed to keep the profile rather technology agnostic, but at the same time we wanted to call out concrete technology use cases, which led to the creation of this page. In addition, while knew that this baseline MFA profile would allow a broad variety of technical MFA solutions, we wanted to call out how various 'additional factor' technologies/approaches address the authentication risks differently. This was both as general background and as possible groundwork for additional (e.g., "MFA Level 2") profiles in the future.*
>
> *Most of the risk analysis on that page was non-controversial at least among the members of the workgroup, but I don't think we had any formal references. That's not an argument that we shouldn't find references, just a statement that we didn't quote any specifically in the discussions.*
>
> > *4.... What is the basis for the statement "Processes that allow a user to immediately register a new second factor (reregistration) using only their "first factor" enterprise password are not secure." in the context of the specific risks identified in the "Risks that must be mitigated" section?*

This is a "slippery slope" item. We agreed to define the scope to be limited to the authentication process, which makes restrictions on registration processes technically "out of scope" for the profile. If we went into much more detail on one registration element, we risked bringing all sort of other "authentication-adjacent" (LoA, user vetting, etc.) issues into the discussion.

At the same time, everyone was dead set against seeing people allow such behavior. In the end, we went with to stating it here, even though from a normative standpoint it's not a requirement. I think the workgroup would be willing to add this as a requirement (i.e., in the profile rather than just advice in the usage guidance) if we could do it in such a way that didn't raise or confuse all of those other concerns.

> *...should there be an analysis of*
> *those risks that is used to reach the conclusion that such reregistrations*
> *do not mitigate those risks, rather than an a priori statement of it being not secure?*

I'm not sure what additional detail an analysis would cover in this case. The concern is that if possession of your password is sufficient to register a second factor, then possession of your password is effectively sufficient to authenticate as you, which makes the overall value of the authentication event equivalent to authentication with a password. Is that high level description what you are looking for, or is there a more detailed analysis you are suggesting?

> *5. Perhaps related to #4, the first main bullet in the "Independence of Factors"*
> *section of "Usage Guidance"*
> *contains the statement "Any factor that is directly accessible using the first*
> *factor is NOT considered a second*
> *factor." Should that statement be sharpened to say something like "Any factor*
> *that is directly accessible by*
> **unauthorized* use of the first factor ..."?*

I personally think adding "unauthorized" here muddies the point rather than sharpening it. If it were possible to independently determine whether the use of the first factor was authorized in an (any) authentication event, we wouldn't need additional factors. Basically, if authorized use of the password is possible, then unauthorized use is also possible; I'm not seeing what part of the statement you are trying to sharpen with the addition of the word "unauthorized" here.

(Note that unlike the reregistration you comment on above, in this case this language is clarifying the normative requirement "The factors must be independent, in that access to one factor must not by itself grant access to other factors," so at least in this case we can leave it as an a priori statement.)

Maybe we need to clean up the language here. The example was using a phone number as a second factor to a password. If that phone number is tied to a specific phone outlet, say in the user's office, then it's a good second factor. On the other hand, if that phone number can be claimed by a piece of VOIP software and a password, then it's not a good second factor, as the second factor is just another (or the same) password.

> *6. Did the WG consider whether or not it would be good to also define a*
> *corresponding entity category,*

Yes!

> *If so, would it be worthwhile to add*
> *a brief discussion of that proposition and the WG's conclusion to the Final*
> *Report, or if not, might that be an*
> *area for future work, to be added to the Recommendations section of the Final*
> *Report?*

> *We were trying to address that with this text in the first bullet of the Recommendations:*
>
> > *"The group did not think exposing “compliance” with the MFA Profile through the SAML metadata was helpful because no existing SP/IdP software is capable of leveraging such information to influence its use of the MFA profile."*
>
> *What additional detail are you thinking would be valuable to capture in the context of the report? It seemed to me that more detail would be getting a into IdP/SP software design considerations. Perhaps simply "options for leveraging such a compliance indicator to simplify SP configuration should be considered in the future"?*
>
> *Another possible point of confusion is that the workgroup discussed compliance both in the sense of "support" (my IdP is capable generate assertions that contain the specified AuthnContextClassRef values) and in the sense of "approval" (certification that my IdP's assertions using those AuthnContextClassRef values meet the profile requirements). I'm pretty sure that bullet is ambiguous, and would apply to both senses of term.*
>
> > *7. I understand that the base-level authncontext enables an SP to express that it prefers but does not require MFA, but I don't understand how it establishes "a base over which other profiles could be defined." Could you enlighten me?*
>
> *I think you caught us here. Originally, "base level" had some basic requirements associated with it (something along the lines of "the IdP operator complies with the InCommon POP"). That language was since removed, and now the context is really only there for technical SAML reasons. Perhaps we should change this to something more along the lines of:*
>
> > *"The intent of this profile is merely to simplify SAML conversations by establishing a named profile that has no explicit authentication requirements."*

+1, perhaps appending "...requirements to allow SPs to request a specific profile (*e.g.*, MFA) while being willing to accept anything else if the specific profile cannot be satisfied."

> *Thanks again for the feedback!*
>
> *--- Eric*