InCommon TAC Meeting 2016-07-07

Action Items from June 23

(AI) Chris Misra will draft language for the FOPP, which will then be vetted by TAC and ultimately recommended to Steering

(AI) Steve will incorporate the proposed changes to the “TAC Response to Priority Planning” and send the revised document to TAC no later than June 27 for comment. The document will be finalized after the close of business on June 29 and will be sent to Kevin Morooney for consideration.

(AI) Steve will contact TAC members about draft charters for items on the TAC Work Plan in time for the July 7 TAC call.

Minutes

Attending: Tom Barton, Steve Carmody, Tom Mitchell, Mark Scheible, Jim Jokl, Scott Cantor, Kim Milford, Keith Hazelton, Albert Wu

With: Dean Woodbeck, Nick Roy, David Walker, IJ Kim, Ian Young, Tom Scavo, Mike LaHaye, Paul Caskey, Ann West

Action Items

TAC agreed to recommend the FOPP changes to Steering and will propose to InCommon management that incident response procedures be created and an incident response plan be documented, perhaps with the help of one or more campus security officers (and others as needed). (AI) Steve Carmody will send notes to Steering and InCommon management with these recommendations.

Approval of Minutes from June 23

Approved to make public

Ops Update

Upgrades that are in progress

1. Upgrading to Shibboleth xmlsectool 2.0.0
2. IJ has completed a major overhaul of the FM software stack
    a. secure linux 7.2
    b. Apache v2.4.6
    c. Ruby on Rails v4.2.6
    d. Ruby v2.2.4
    e. Postgres v9.5
3. New database server will be installed in the coming weeks
4. Federation Manager code now committed in Internet2's Github Enterprise account, working with a software development firm on a review of the code there.

To support the Steward Model, major changes to the Federation Manager are required. IJ has a prototype. IdP mdui:DisplayName will be editable. Will have multiple IdPs per organization (will be an undocumented feature).

The Ops Advisory Group recommends that Ops implement the following Interfederation Technical Policy rules:

1. Modify import filter check_idp_non_saml2
    a. Require HTTP-Redirect OR HTTP-POST (instead of focusing on HTTP-Redirect)
2. Modify import filter check_shib_regscope
    a. Continue to filter any IdP entity descriptor with a regexp scope
    b. Implement a whitelist of approved regexp scopes
3. Implement import filter check_duplicate_scope
    a. Filter imported IdP metadata having a scope belonging to an IdP registered by InCommon
4. Implement import filter check_dup_display
    a. Filter imported IdP metadata with duplicate <mdui:DisplayName> values

IdPv3 upgrade communications

- “Office hours” to answer questions about upgrading to Shibboleth IdP3 - today and July 12

FOPP Suggested Text About Incident Response

After discussion at the last TAC meeting, Chris Misra reviewed the FOPP looking for a place that addresses security, with an eye toward inserting language allowing the InCommon Federation to take action should a security situation arise. He recommends this change to section 10.3.1:

> 10.3.1 Suspension for reasons of security
>
> A Participant may request the suspension of any Federation services in the case of Administrator credential compromise, participant key compromise, or other security compromise within the Participant's systems. This request may be made via e-mail or telephone from the Executive or Administrator and will be verified by InCommon using trusted communication channels. Suspension may include processes such as revoking credentials, or removing or modifying Metadata.

If InCommon suspects any compromise or negligence on the part of a Participant, it will make reasonable efforts to contact Participant ~~to verify Participant's status~~. In the case of a significant security incident that poses an unacceptable risk to InCommon or other Federation participants, InCommon may take immediate remediation actions commensurate with the impact of the incident. ~~For example, a non-responsive Administrator's account may be suspended for the security and safety of Participant's Metadata if InCommon suspects an Administrator is no longer active and its repeated attempts at contact go unanswered.~~

Chris also recommended developing a document that would include InCommon's incident response procedures, that would be approved by both TAC and InCommon Steering.

Action Item

TAC agreed to recommend the FOPP changes to Steering and will propose to InCommon management that incident response procedures be created and an incident response plan be documented, perhaps with the help of one or more campus security officers (and others as needed). (AI) Steve Carmody will send notes to Steering and InCommon management with these recommendations.

Status of TAC Work Plan

https://docs.google.com/spreadsheets/d/1-08e_nWxbxbsQsFuQiOsh_G-zqAvXf7T4Ka7dF3Ai8c/edit#gid=0

Steve Carmody provided an update on a number of items in the TAC work plan, including:

- The IdP of Last Resort work has been moved to REFEDS; Keith Hazelton is leading the IOLR working group for REFEDS: https://wiki.refeds.org/display/GROUPS/IoLR
- "Document Interop Steps for Popular SPs" - There was discussion about gathering input from the community on which SPs would be on this list. In addition, an IdP that wanted to document their work with a high-profile SP would be welcome (and encouraged) to do so. All of this material should end up in one place on the wiki, along with the CIC Cloud Cookbook and similar existing items.
- The federation interoperabilty profile has moved to Kantara, but it is important for the community to continue to be involved in this process.
- Deployment profile - This would revolve around updating the SAML2int profile
- Compliance - This item is about developing a tool for testing services on their compliance with interop and deployment profiles (and potentially baseline practices). This is high on management's list. A working group could be formed to work with Roland on using Fed-Lab.
- Per-entity Metadata Working Group - Scott Koranda agreed to chair and has had strong interest from the community
- Beyond SAML - Steve Carmody has talked with a community member about potentially chairing a group that would look at OAuth and OIDC

Next Meeting - Thurs., July 21, 2016 - 1 pm ET