InCommon TAC Meeting 2016-05-17

Minutes

Attending:
Walter Hoehn, Michael Gettes, Tom Barton, Steve Carmody, Keith Hazelton, Scott Cantor, Janemarie Duh, Mark Scheible, Kim Milford, Jim Jokl, Albert Wu, Tom Mitchell

With:
Mike Zawacki, Nick Roy, Paul Caskey, Ann West, Steve Zoppi, Kevin Morooney, IJ Kim, Mike LaHaye, David Walker

Action Items

(AI) Nick Roy will write up strawman incident response proposal for handling vulnerable deployments listed in metadata, enumerating types of vulnerability classifications and the incident procedures for each, share with TAC for review. Note that this strawman should include an education component and also any supporting material

(AI) A communications plan is needed for the incident response plan, and, more generally, to promote standards. This should include an email campaign to explain in stark technical terms why the v3 upgrade needs to happen and encourage community transparency.

- Shib communications should include specifics (v3 supports MDQ, dates when outdated software will present a risk, specificity will help with urgency
- (AI) As part of this plan, Paul Caskey will send a message to the REN-ISAC security list
- The communications plan needs to include a component aimed at CIOs and CISOs

(AI) TAC formed a working group to review the TAC work list, fill in the details, adjust things for clarity, and assign rank/priorities. Volunteers are Mark Scheible, Steve Carmody, and Jim Jokl. The working group will complete its work in two weeks (June 3)

(AI) Steve Zoppi will create accounts (at bugs.internet2.edu) for members of TAC and include them in the relevant project(s).

Shib v2 to v3 Discussion

There was discussion among a smaller group, then the full TAC, concerning ramifications of IdPs not upgrading to Shib v3 and InCommon's role in encouraging upgrades. For example, should outdated IdP software cause any security or other types of threats, what is the federation's plan?

It appears that the FOPP allows InCommon to develop an incident response policy that includes circumstances under which federating software may have its entity descriptor(s) removed from federation metadata (see the PA and "Software Guidelines" in the wiki). However there is a question whether the FOPP does allow this, or if it would need to change to accommodate this.

The TAC has asked that InCommon staff develop an incident response process to address the removal of software entity descriptors and/or compromised key material from the InCommon metadata when their continued presence presents a substantial risk to other Participants. (AI) Nick Roy will write up strawman incident response proposal for handling this kind of situation, enumerating types of vulnerability classifications and the incident procedures for each, and share with TAC for review. Note that this strawman should include an education component and also any supporting material.

(AI) A communications plan is needed for this and, more generally, to promote standards. This should include an email campaign to explain in stark technical terms why the v3 upgrade needs to happen and encourage community transparency.

- Shib communications should include specifics (v3 supports MDQ, dates when outdated software will present a risk, specificity will help with urgency
- (AI) As part of this plan, Paul Caskey will send a message to the REN-ISAC security list
- The communications plan needs to include a component aimed at CIOs and CISOs

Other thoughts from the IdPv2 to IdPv3 discussion:

- There are potentially two topics here: 1) out of date software, and 2) software actively causing a security problem. If we address 1), it should be for all types of software, not just Shib
- An incident response plan will provide a process to address issues, and demonstrate to the community that we are prepared.

Joint Steering, TCIC Meeting

The day prior to the TAC meeting included a joint meeting of the InCommon Steering Committee and the TIER Community Investor Committee (TCIC).

"Deep Dive" - Kevin provided an overview of a recently held "deep dive," which involved four community members meeting with the trust/identity leadership. The meeting was intended to validate processes and resource needs and gaps. That review produced good momentum and next steps.

One key outcome is developing and communicating a holistic view of of everything T&I has on its plate - from campuses, to national, and international connections (including talking honestly about positives and challenge.

There also seems to be increased clarity on the importance of Shib and the connection now among TIER, InCommon and Shib. There may still be confusion about how the Shib Consortium works and how funding for Shib works.

Kevin and Klara Jelinkova will put together the next intensive review, solution paths, funding opportunities, resource priorities, and other follow up. That will happen prior to the beginning of July. A smaller group will then develop those findings into a plan. Kevin will also follow up with "deep dive" attendees to gauge their thoughts/activities between then and now.

Comments include:

- Steve Zoppi - This space has changed significantly in the last 18 months. The importance assigned to trust/identity by Internet2 is the hiring of a dedicated VP. We're in a dramatically different world, but we're also facing changes in expectations from campuses. We're in the next phase here, analogous to a tech startup going from release to sustainment of product.
- Paul - We need to be clear about our value proposition. For example, if I'm an SP why wouldn't I just go join a free UK federation and get included in the metadata aggregate for free? We need to have messaging to address that.

TAC Work Items

There was a discussion about evaluating and prioritizing the 2016 TAC work items, in relationship to the other processes, including TIER and InCommon overall priorities and how the landscape has changed. It will also be helpful to understand resource availability when setting priorities. Note there are two lists referred to below. One is the InCommon Priority Worksheet, developed by InCommon staff. The other is the draft TAC work list.

Some comments:

- TAC and InCommon need to be working in a common space on common projects. Directly work on both red and blue items from Priority Setting Worksheet and acknowledge any deltas. We also need to be clear on which items TAC is involved with. For example, TAC shouldn't worry about Service Now implementation - it should care with outcome as a result of that tool being used. In other cases TAC might be more concerned with process than results.
- TAC should give consideration to future issues to be faced in the next 3-4 years.The draft TAC work list includes projects in both the near-term, as well as further out.
- This process is intended to align time/resource constraints and to approach decisions more methodically, with room for unknowns and future iterations of work plans.
- Note that InCommon Ops need to support services we have, develop/refine services, and do what amounts to R&D for future tech. We don't have the cycles to do all of that. TAC helps provide a framework for R&E thought leaders to contribute portions of those latter two needs.
- Each item on the priorities list represents a task or project needed to move Trust and Identity forward. Each has a project document which backs up that decision making. In addition, we need to look at long-term costs of *not* adopting something like Service Now and a ticketing system.

Given the lack of time to review each work item in detail and assign priorities, TAC formed a working group to review the TAC work list, fill in the details, adjust things for clarity, and assign rank/priorities. Volunteers are Mark Scheible, Steve Carmody, and Jim Jokl. The working group will complete its work in two weeks (June 3).

There was a discussion about the requirements for tools to manage this type of work.

1. Need to differentiate requirements vs. features and include that determination in decision making process
2. Need a rigorous prioritization process
3. Need to communicate the work plan, including:
    a. Deadlines
    b. Whether efforts are opportunistic or strategic
    c. General work flow

Job 1: the process:

1. Someone gets an idea
2. We track the idea
3. Rate the idea
4. Prioritize compared against all the other ideas
5. Consider sequencing of the ideas in the collective
6. Once you have the natural order of things determine the size
7. Bring to bear the resources to be applied (if available)
8. Solicit for additional/external resources if needed

Job II: The Response (solution/tool): https://bugs.internet2.edu (Kanban)

The point of this approach is to tell a story of things we need to accomplish, to aggregate tasks into a narrative form, make that process visible to outside stakeholders, and show progress.

(AI) Steve Zoppi will create accounts (at bugs.internet2.edu) for members of TAC and include them in the relevant projects.

Next meeting

Thursday, May 26, 1 pm ET