CACTI Meeting Public Minutes 6-March-2018

Attending

Members

- Chris Phillips, CANARIE (chair)
- Warren Anderson, University of Wisconsin-Milwaukee /LIGO
- Tom Barton, U Chicago
- Rob Carter, Duke
- Nathan Dors, U Washington
- Jill Gemmill, Clemson
- Ann Harding, SWITCH/GEANT
- Karen Herrington, Virginia Tech
- Todd Higgins, Franklin & Marshall College
- Christos Kanellopoulos, GEANT
- Les LaCroix, Carleton College

Internet2

- Kevin Morooney
- Ann West
- Steve Zoppi
- Emily Eisbruch

Regrets: Tom Jordan, U Wisc - Madison

DISCUSSION

Trust and Identity Roadmap - influencing the future

- A dialogue on the recent SAML security issue and the impact.
- XML Tooling that Shib and others reply on
- Is there an opportunity to improve things in the trust and identity space?
- What is the impact or ongoing impact to the T&I space (TIER?, FedOps?)
- LIGO: not much a hit from this security issue, updated packages with patches, LIGO has mostly internal encrypted traffic
- Campus perspective: hard to verify every SP covered by campus has been updated. Long tail. Impact is felt by the SP as well. Question: do we need a better mechanism to monitor SP operations?
- What kind of tools are available to see what version of software an SP is running? What are processes for enforcing trust within the federation?
- Tools -- depends on the threat and risk and what level of Penetration testing is done.
- There was an issue that the repositories providing patches were down for a period.
- IDP operator perspective: I must trust my SPs will perform the needed updates
- Baseline Expectations http://doi.org/10.26869/TI.34.2 talks about good security practices… this specific issue could be part of the community consensus process.
- Are all SPs alike from perspective of the federation? Services versus academic collaborations?
- SIRTFI participation can be a good indicator of trustworthiness. But SIRTFI is not complete. It requires people and infrastructure and mindset. https://refeds.org/sirtfi
- At some campuses, a lot of SPs are not members of InCommon
- Is CACTI the right place for this conversation within Internet2?
- It was noted that the InCommon federation is developing a stance on monitoring and how to address security incidents.
- Shannon Roddy, Security Lead for Trust and Identity, has reached out to InCommon participants to mitigate risk around security incidents such as ROBOT.
- ChrisP: need to operationalize security within federations
- tool - https://github.com/SAMLRaider/SAMLRaider
- Where could we advance security in T&I?
- Noted that TIER Security and Audit Working Group is in the CACTI workplan
- For next CACTI call, discuss what might be the outputs of a Security Working Group?

OIDC & interests in trust and identity

- Roland has reached out to ChrisP around leaving a solid foundation at The OpenID Foundation. http://openid.net/foundation/
- The OpenID Foundation is the home for other industry “profiles” of OAuth and OIDC, including the HEART (healthcare) profile, International Government Assurance (iGov) profile, and Financial API.
- Recall that OAuth and OIDC are complex frameworks
- Recall that a “profile” or “profiling” is “the process of adding to or modifying standards to tailor them for a specific use through changes such as additional requirements, making optional features mandatory, or specifying implementation details left unspecified in the original standard”
- Currently, the OIDC/OAuth working group is addressing this question as part of its “guide standardization” objective; see home page; the WG’s roadmap shows reviewing existing standards and profiles between Jan-May. Is iGov profile good enough, or do we need to rethink certain areas for our federation?
- Nathan: collecting learning materials around OIDC and existing profiles is also important. Some expertise gap.
- Could fit into the “identerati” part of CACTI charter/roadmap

- Reach out in our professional networks to find individuals who can do the kind of work Roland has done, such as create profiles and libraries.
- We may need an eduprofile to differentiate our sector from iGov

Nathan: additional expertise would be helpful on the OIDC-OAuth Deployment Working Group .
Would creating a profile for R&E under the OpenID Foundation reap a stronger result than doing it within our usual space?

Status on monthly reports from working groups

- First draft to be sent to CACTI on Friday morning. We're in the process of getting reports back from the WG chairs.

2108 Global Summit: CACTI is tentatively scheduled for Tuesday, May 8, 2018 at 7:30AM-8:30AM

Next CACTI Call: Tuesday, March 20, at 11am ET