CACTI Public Meeting Notes from 23-July-2019

CACTI call of Tuesday, July 23, 2019

Members

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

Internet2

- Kevin Morooney
- Ann West
- Steve Zoppi
- Nick Roy
- Jessica Coltrin
- Emily Eisbruch
- Mike Zawacki

Regrets:

- Marina Adomeit, GEANT
- Tom Jordan, University of Wisc - Madison

Pre-Reads

- **https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Announcing-the-public-preview-of-Azure-AD-support-for-FIDO2/ba-p/746362**

Reminders/longer term

- **Slide deck for value proposition for research for the Trusted Access Platform (Jill and Ann)**

Discussion

TechEx 2019 in December in New Orleans https://meetings.internet2.edu/2019-technology-exchange/

  - FIM4R on Sunday
  - REFEDs on Monday
  - Day and time for the CACTI meeting at TechEx not yet confirmed
    - Would a breakfast CACTI meeting, at 7am, work?
    - Or meet from 6pm-8pm? Prefer morning
    - There are too few lunch slots for all the side meetings requesting lunchtime

- Main Business
  1. T&I Hackathon September 2019: https://wiki.refeds.org/pages/viewpage.action?pageId=44959235

  - Reading: https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Announcing-the-public-preview-of-Azure-AD-support-for-FIDO2/ba-p/746362

  - Discussion around **WebAuthN/FIDO2/Strong Authentication**
    - When (not if!) Microsoft accomplishes this, what are the implications for Trust and Identity and what kind of insights do we have?
    - Nick, interesting, worth following, worth eliminating passwords where we can. Not sure how rebinding tokens will be handled in the new approach. What about SSH and eduroam and authentication for other non web things?
    - Rob: Microsoft document does not cover initial binding. Transition from using password to FIDO2 is complex.
    - Similar/same problem to account linking for social logins. Need to trust something that is not ours. There are remote alumni who can't just be handed a token or a key.
    - It's a matter of time until passwordless becomes a reality. But how many years/months from now?
    - Microsoft may make a shift where campuses must support passwordless approach for users to access their outlook account.

- If Microsoft flips a switch that is a big deal.
- Office365 is just one corner of our world
- How do we want to push and support passwordless?
- Similar to the discussions around MFA
- It's possible that users will push for passwordless everywhere
- Will there be other passwordless technologies, in addition to FIDO?
- Nick: we have spent a long time supporting passwords. Baking upgrade path into a hardware device is problematic
- Smaller institutions need to use cloud services due to more limited staff. Pivot from MFA to "strong authentication." Tokens will replace passwords. Our community doesn't have a corresponding process yet.
- Christos: somewhat skeptical, people like usernames and passwords. Binding between person and token is not yet defined. In September 2019, GEANT will launch a pilot, to get a feel of how the user base will react.
- Nathan: U Washington has **integration w multiple cloud environments and with open source environments**. Will likely do a mix of DUO and Microsoft technologies, may enable thru open source, like Duke. Interesting to see if passwordless world will increase attacks on people to get their token. Are we reducing safety?
- It's important for Service Providers that Identity Providers take on this. So service providers don't need to be identity experts
- Duke is fully federating. U. Washington has some concern that some services don't allow full federation. May need to sync some services. This may require WebAuthN
- Rob: In passwordless environment, what does this mean for syncing of hashes? Might Microsoft remove the option of federation?
- If Microsoft removes option of Federation, this could be a competitive disadvantage.
- TomB: the federation linkage and skews are profitable, making it less likely that Microsoft will back off from federation.
- Could be a brushfire, remains to be seen
- So far not a lot of concern being voiced at board level
- How does passwordless change MFA? Webauthn versus MFA?
- Should we stop saying MFA and start saying **strong authentication**?
- WebAuthN could be the 2nd factor. Will password remain the 1st factor? TBD
- WebAuthN can help with standardization across browsers
- You get the proof of possession with WebAuthN
- Phone hardware is part of the equation, and the security the phone provides may vary depending on phone brand
- Man in the middle attacks are a risk.
- In some places MFA will be necessary, in some places WebAuthN will shine
- At Virginia Tech, there was much work on MFA, using Duo. It was a large effort. Currently some Identity Team members and others are looking at WebAuthN. Unlikely that Virginia Tech will step away from MFA any time soon.
- Small colleges have limited leverage to push back against Microsoft. Can't jump on another train. Challenge to support multiple cloud environments.
- Windows 10 authentication to Azure , potential for immediate playback on campus
- People can leverage on campus authentication as basis for their IDP

- What are the **implications for eduroam in a passwordless environment**?
- Trend to move towards ETLS already? MikeZ will look into statistics on that.

- Perhaps we should to start thinking about implementing WebAuthN in a few places.
- Are there implications for InCommon Trusted Access Platform?
- Shibboleth should start to support WebAuthN
- For enrollment and verification, for the whole solution
- There is a Ubico office in Bellville, WA, Nathan could open a discussion with them

- Todd : looking for solution and approach that works for broadest base of needs and constituents

eduroam Advisory Committee charter

- consultation is live, ends tomorrow, Wed July 24
- ChrisP, MikeZ, Nick, Ann will discuss next steps

- Status Updates

1. Close-out of MACE-DIR transition to REFEDS
    a. URN registry transfer - status

1. Topics being tracked

a. Background: https://lists.refeds.org/sympa/arc/refeds/2019-07/msg00010.html
b. TAC is tracking and formulating thoughts on it.
c. Scott Cantor believes there is very little impact from this, but load balancers where cookies contain relay state will be a much bigger problem.
a. https://techcrunch.com/2019/06/03/apple-sign-in-privacy/
    i. OIDC open letter: https://www.zdnet.com/article/openid-foundation-says-sign-in-with-apple-is-not-secure-enough/
a. Build on last meetings outcomes focusing on the 5 areas we highlighted :
    i. infrastructure, services to end users, software dev, infrastructure as a service, and outreach and education
    ii. Focus of conversation: to identify high priority items/quick wins in the above areas
- Same Site Chrome browser update cause grief (Nick or maybe Nathan?)
- "Sign In With Apple": WUWT?
- Continue prioritizing CACTI FIM4R recommendations (Chris/Jill)

- ID Pro (Chris has next touch point)

Next Call: Tuesday, August 6, 2019