Link to 2022 ACAMP Wiki

Advance CAMP Thu. Dec. 8, 2022

Room - 3

Session Title: Can't trust this

CONVENER: Michael Gettes (wsg Tom Barton)

MAIN SCRIBE(S): Chris Bongaarts, Mike Zawacki

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: 25

DISCUSSION:

- Michael: Currently a pervasive perspective (esp at state gov't level) of "why should we trust other organizations?" (specifically identity data like username)
- Michael: Concerned that those state players are both well resourced and suspicious of Federations. So they are content to buy off-the-shelf software, but many vendors can't do multilateral federating or meet baseline expectations. Want to take the temperature in this room - your experiences?
- Rob Carter (Duke): Is it "can't trust this" or "won't trust this"?
    - Michael G: it's both.
    - Rob: More one than the other? Each has different implications, needs to be addressed differently
    - MaryM (cirrus identity): I'd like to hear who's getting pushback. I'm having good engagement with CIOs, especially when you emphasize accountability, attribution, ability to
    - Tom Jordan (wisc): Use cases that resonate most are use cases where we can take away support burden, especially for users who are only intermittently using services. (e.g. hospital workers who only use system once a year; having a local account is needless extra work for everyone)5

- Mary M: At Duke one thing that brought me into identity was the need for ease of logging in. If you make account creation easy and logging in hard, they'll just recreate accounts constantly. Also, architecting for revocation strengthens value
- Amy Butler (U of Montana): We recognized that we have a security access issue. Single layer networks are huge risk, but often deployed because it's easy. Federation addresses that
    - Michael: Is it a multi/single layer question or is it about appropriate access to the network
    - Amy: More about appropriate access. Ease of maintenance - self signed certs etc.
- Stephen Fox (ProvisionIAM): Have to be able to articulate the risk when talking to other stakeholders. Don't want to allow a guest to log in and get to some critical piece of your architecture. Separating access by risk of the resources - ensure critical systems are protected. That risk speaks to C level folks
    - Michael: In my experience deprovisioning is problematic. Creates security risks and can drive the perspective of "why trust this", back to the starting point. Collaboration is key to what we do, need to make C* understand that.
    - Stephen Fox (ProvisionIAM): You look at problem, articulate problems in terms of money
    - Gabo@UVAr: Pushback often related to conflation of identity and access. Having low quality identity has low risk if it doesn't confer access on its own. Key is authorization, and the ability to revoke access
    - Mary: I think ID verification is important, but most (all!) of the breaches we see aren't people creating new identities but existing accounts that get hijacked. Need to be able to suss out suspicious use (e.g. anomalous activity, multiple logins with a single account, etc) and revoke those accounts proactively.
    - Tom J: You haven't talked about the value of the information you're protecting. Can do you that?
    - Michael: Access to HR data, databases, management of research $, websites where collaboration happens, control of resources & instrumentation etc.
    - Chris B (UMN): You don't have a lot of guests using the HR system though right?

        - Michael: No. and contractors process of account creation is highly manual.
        - Chris B: Can you separate use cases out? THe science sites are probably of more interest to collab than some of the infrastructural systems.
- Tom J: Looking at this through the CISO lens, figuring out what categories of risk require what category of system/design considerations. Need to learn how to articulate that in CISOese
        - Tom B: Purpose of the CISO is to enable the mission of the organization. Understanding the purpose of the organization is key in figuring out how to approach the CISO. Context is everything here. There are common guard rails (money, budget, compliance, etc) but worth considering unique aspects of org's mission. U Chicago primary mission is research. So consider quality of accounts (assurance?), (witness NIH here). All of these things are possible. Lots of ways to approach this. If you get to "no" there are several main possibilities:
            - Just don't know - help them understand more of mission
            - Regulated environment - decide whether to trust idp or not based on required controls. Federation poses challenge, but can restrict idps (white/black list).
        - Marc Wallman (ND State): To what extent is this sort of critical thinking involved in pushback? Is it more reflexive? What's the nuance here?
            - Michael: We're speaking rationally about irrational responses to problems. My understanding is that a lot of these conversations have been had, approaches tried, but are still getting pushback. Seeing this at other places too. Concerned about loss of capability. So how do we make our collective case better to the world? We have
        - Maarten Kremers: What happens if they go to Google, etc? Can drive users "underground" to make things workable.
        - Dan Malone (Cal Poly) We don't use SPs - there's serious resistance to releasing our data. Don't want a generic policy for release. They want to control everything.
        - Chris B: Sounds like the opposite of the problem originally stated
        - Jared (Kent STate) : I would not underestimate the concerns expressed here. Have to look at the reasons behind these concerns. Consider a research project - how much should be made public, how much made

private. Don’t want to stop people from joining in, accessing resources, but do want to be able to identify who comes in, accesses resources. There’s a whole legal structure around dealing iwth breaches, abuses, etc. Solution could be more granularity of access control. Also think about who’s setting the policy. Will that impact ability to finely manage access rules? Often policy setting is centralized.

- Stephen Fox (ProvisionIAM): Need to list requirements for participation/use of Federation. Figure out permission levels around information/data release. Need ot be able to identify every single objection, negotiate, figure out their allowable level of risk, frame the conversation out from there.
- Mary: Everything is subjective from a security point of view. Leadership that’s pushing back think they’re being rational. To sell an idea you need to find how some problem/issue is relevant and how Federation solves for that. Make incremental moves
- Gabor: I wonder if it would be valuable to demonstrate that there is a lot of “underground” credentialing and highlight that to CISO/C level people
- Michael: In many cases they’re aware of problem (and federation solutions!) but see it as justification to lock down more
- Rob: Does SLAC support eduroam
- Michael: Yes
- Rob: That signals some willingness to Federate in a different context
- Lots of labs have different policies on this so hard to say "oak ridge does federation".
- MikeZ: Do they know eduroam is a federation?
- MikeG: It's not though
- MikeG: When wallets take over the world and vendors fall over themselves to implement, they'll see our value.
- TomJ: WHen he hit pushback we can push against that, or find an advocate in another part of the org/from an external org.
- TomB - when we take the time to understand where someone is coming from, even if you don't agree, you can find common ground
- Michael: They’re saying “it’s everything, Shut It All Down” that’s irrational
- JonM (wisc): Maybe find a Bigger organization to push from the other side (eg, NIH and Assurance)
- Amy: Can you make the case of dollars lost if they don’t Federate?

- Marc W: To Tom's point, it's a methodological approach that wins through. Need to do analysis, understand your audiences, risk benefits, costs, etc.
- Michael: Consider that there's a lot of vendor solutions that feel easy but don't do things like multilateral Federation, won't implement cause they don't see the value there. other key capabilities.
- Stephen Fox: At lower levels you'll find objections - if you can bring them over, that's an ally.
- Researchers are onboard with federation but are not persuasive enough to convince CISO.
- Paul: Ken talked abou the pressures that make CISOs risk averse. They'll see attribute release as a threat and refuse.
- Michael: Landscape is complicated, CISO can be opposed, CIO can be for, etc.
- Rob: It feels like at some point in the past we saw a split between identity and security people. Identity folks aren't talking to security folks about security benefits of Federating. How do we get that general conversation going?

ARTIFACTS / LINKS