Link to 2024 ACAMP Wiki

Advance CAMP Thu. Dec 12, 2024

Room - I

Session Title: Fed Compliance/Phishing resistant MFA

CONVENER: Shannon Roddy (LBNL), Gabor Eszes (UVA), Matthew Economou (RDCT)

MAIN SCRIBE(S): Julian Anderson (Oberlin College)

- Thank you! -MXE

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: ~30

DISCUSSION:

- Matthew: Topics to cover:
    - NIST 800-63-4 (e.g., phishing-resistant MFA) and how they map to:
        - REFEDS MFA adoption
        - REFEDS assurance adoption
    - SP onboarding (e.g., Albert's work)
    - Standards Bodies Participation
        - US gov't engagement
        - NSF/NIH requirements

Matthew: NIST SP 800-63-4

- Will change a few things about identity assurance/authenticator assurance
- Kyle Lewis (RDCT):
    - Auth assurance
        - Draft has some verbiage of phishing-resistant MFA not currently in standards

        - Means REFEDS will likely need to adapt in some way
    - Changes will likely help close gaps
    - Also, standard for IAL1 (NIST low) is likely to raise
- Ann West (Internet2): can we talk more a bit about risk-based approach
    - Kyle: federal gov't will have lag in cultural change b/c security folks are still compliance-oriented
        - Decision makers will have to accept levels of risk due to mission needs
    - Ann: trying to position InCommon federation/REFEDS standards as viable option for interacting w/ government, having identity/auth assurance
- Matthew: risk-based approach for Authorizing Officials (AOs) for sure
- Kyle: even with 800-63-3 today, gov't service providers can accept IAP high in lieu of IAL2

Phishing Resistant MFA

- Matthew: as a result of telecom network breaches, security folks pushing harder and harder to get away from SMS/voice OTP
- 800-63-4 has some verbiage about crypto strengths, etc., but REFEDS is missing some of this
- Scott Cantor (THE Ohio State):re: MFA Context in SAML, if the requirement for phishing-resistant MFA exists, it will have to be a new context class for REFEDS

MFA Signaling and Error Handling

- Hard to tell what happened when something went wrong from the SP perspective. (e.g., insufficient auth strength)
    - User can get stuck at the IdP, or the SP may get unknown errors.
- Can't easily restart auth flow when an error of some type happens
- As a government SP, we'll work around this by, e.g., not strictly requiring MFA and hoping that IdPs pass it to us so that we can avoid step up, but that's not sustainable.
- Scott Cantor: One specific case called for in SAML spec, etc.

REFEDS Assurance Adoption

- Matthew: Another piece of gov't compliance is identity assurance (tying digital identity to legal identity)
    - Think, e.g., big ole AUP banner about interacting with a government system
    - Scott Cantor: no incentive to effect change prompted by outside unless money changes hands (pay or withhold money). Thus, no interest at tOSU in identity assurance at all at this time

- Ann: how many folks are looking at buying identity verification systems?
    - Phil Smart (Jisc): enrollment proofing, MFA factor enrollment
    - Zacharias from ???: we'
    - Jon Miner (U of Wisconsin): full student and employee identity verification
    - Julian Anderson (Oberlin College): considering for password/MFA reset to avoid social engineering risks
    - Liam Hoekenga (UMich) - helpdesk - password / MFA reset, but hope to use it for assurance

US government engagement (Ann) / Standards bodies participation

- Ann: InCommon working w/ NIH for a while, but intensely since 2020; used InCommon to help w/ infectious disease research
- Eventually received official letter from NIH CIO: do more InCommon stuff! Get it out there!
- A couple of years later, NIH eventually moved researchers and grants administrators to InCommon implementation with requirement of REFEDS MFA assertion
- Also looking to map to assurance
- Dear Colleague letter from NSF circa October requiring researchers to move Login.gov profile to MFA factor w/i two weeks in order to continue using research.gov
    - NSF called InCommon and had prompt discussion; for those orgs that have used InCommon to auth to NIH resources, no further work needed!
    - "Never waste a good crisis"
    - Got in contact with further folks, including 800-63 drafters; said "we can help you", need to align requirements and have a timetable. Nothing that drives action quite like access to a grants management system.
    - Tentative "yes" to working together with those folks
    - Matthew: would any of the recommendations eventually become public? Ann: hopefully yes
- Matthew: CommEX might be a good way to get IdP and SP heads in the same room. Other places where we can participate (or encourage leadership to participate) in these kinds of discussions?
    - Scott Cantor: InCommon Expectations is the place we can work out recommendations to improve this, SPs should be recommended to send back NoAuthNContext if they can't satisfy rather than having the user stuck.
    - Matthew: CTAB is another place, among others (InCommon Expectations Wiki)… "we're desperate to hear from you"

- Albert Wu (Internet2): We know we will need to go back to REFEDS and ask for change, we need your input

SP Onboarding (Albert Wu, Internet2):

- Also working on a tool to help federal agency SPs are properly handling interactions
- One universal common ask: can you give us a test IdP with some test accounts?
- Exactly what they're planning to give. Mini-federation with test IdPs and various auth situations that potential new SPs can use
- We have a wireframe that Albert can demo, hoping to have this ready very soon

- Ann: when we did comms for Dear Colleague letter, we worked with certain orgs to help push message that if you're an InCommon school, you're already good to go
    - NIH also reaching out directly to researchers worked well
    - What doesn't work well (per data): when IT implemented MFA for NIH, not a huge delta in InCommon logins. Turns out that IT comms did not communicate particularly well with researchers.
- Alan buxey (MyUnidays): the problem isn't necessarily technology, it's people/policies/processes
- Joanne Boomer (Missouri): what were the experiences like to switch? Do we even know?
    - Differed depending on NIH vs NSF
- Albert: a large university system just put out a requirement to use Duo Verified Push, which sounds a whole like phishing-resistant MFA. Are you seeing more IdP-having institutions (schools, etc.) push for more phishing-resistant MFA? At least a half-dozen hands raised and nods.
- Julian (Oberlin): IT would love for college to adopt, but has difficulty with MFA adoption, often surrounding not wanting to put work stuff on personal devices. In addition, YubiKeys (& WebAuthn in general) are finicky in a lot of environments, resulting in lots of fallback to TOTP. Funding gap for, e.g., work-issued devices to use push-based auth
- Colin McCarthy (UWash): Mostly solved for students/faculty/staff, but significant problems with medical workers, it's not been convenient, and not practical to try to bring devices into treatment areas, etc.
- Dave Mak (Berklee) - Students from export-controlled countries, in complicated circumstances where they cannot own or use some devices, especially not during application process.
- Jim Basney (UIUC): Yubikeys cheaper than work phones, for example

- Chris Evans (Oregon State): we use Entra + Duo together and strongly enforced. Bought 2000 YubiKeys to help incentivize. Went from Duo to Entra to Entra + Duo w/i 6 months.
- Julian: We use YubiKeys as much as possible but have run into a lot of edge cases where they don't work with Okta (e.g., within an SP's embedded browser)

Matthew: **We need your voice!** In CACTI, CTAB, etc.

Also Matthew: "the last word is 'monkey'"