LInk to 2020 ACAMP wiki

Title: The Future of Federation in a WebAuthn/FIDO2 World

With Webauthn/FIDO2 rapidly become an attractive authentication approach, the use of federation for SSO will diminish. While we were originally motivated by moving attributes, SSO and LOA and related authentication issues soon took all our time and effort. Can we get back to our roots and find new businesses around our trust fabric and our attributes?

Advance CAMP Wednesday Nov18,2020

1:20-2:10 pm ET

Room - Dining Hall

CONVENER: Ken Klingenstein

MAIN SCRIBE: Matthew Economou

ADDITIONAL CONTRIBUTORS: Jon Miner

# of ATTENDEES: 57

DISCUSSION:

- Ken K:
    - Comments on webauthn/fido?
    - Status of campus activities
    - Existential threat?
    - How else can federated trust be used?
    - Thoughts triggered by Rob's blog post: "How does WebAuthn and FIDO2 affect the future of federations?"

    - Lots of conversations about verifiable credentials
- Rob C:
    - BLOG POST LINK HERE :)
    - Duke integrating WebAuthn/FIDO2 with their IdP
    - Separate from that, realization that WebAuthn amounts to really easy, high value, high security, bilateral authentication solution for web-based stuff
    - WebAuthn gives user appearance of a kind of SSO, simplicity if nothing else
    - Why would SPs need to use federated identity when WebAuthn is so easy/secure?
    - What does WebAuthn do to traditional perspectives on Authentication Assurance Levels (AAL)?
    - Topic came up in CACTI several months ago
    - Federations have (1) trust fabric and (2) attributes. WebAuthn doesn't even try.
- Ken K:
    - "Shibboleth - will work for attributes" t-shirt (we stopped working on attributes..started working on LoA, MFA etc etc...maybe we're coming back to working on attributes?)
    - What's the rate of progress on WebAuthn?
- Leif J:
    - Gave similar presentation at TNC in Estonia
    - "Either provide attributes or you don't provide value"
    - WebAuthn adoption is slow due to lack of native (built-in) authenticators.
    - Magic happens when you don't have to buy anything.
    - Most extant deployments with Yubikeys.
    - Works with Android phones, Chromebooks, Windows 10.
    - Significant market gap with iOS.
    - Challenge becomes enrolling device instead of enrolling user
- Scott C:
    - "Easy" for commercial providers
    - But for campuses, the value from Duo is to handle all of that and provide user interface and provide user experience.
    - Big lift to do token management
    - Guesses it will be something IdPs do, not SPs do
- Leif J:
    - VOs/proxies might do it
- Matthew E:
    - Assurance becomes the key feature of federation in a SP- or VO-implemented WebAuthn world
- Ken K:
    - How to recover in the event of lost/stolen/revoked tokens?
- Matthew E:
    - Hard UX problem that even large companies don't get right, e.g., AWS.
- Shilen P:

    - To get to device registration page, one must use MFA, whether backup codes or Duo or another MFA device.
    - If no other devices, contact the Help Desk and validate IRL somehow.
    - Don’t have stats on how much the IRL backup happens.
- Johan P:
    - Use another IdP for step-up authentication?
- Scott C:
    - All this stuff is easy except the parts that aren’t, and those are out of scope. ;)
    - Centralized is a hard problem, and maybe we’ll end back up at the IdP authn model.
    - WebAuthN is all pairwise keys and there's no linking back together, it's a fundamental design feature.
- Matthew E
    - As vO operator, given up on trying to get attributes because of lowest common denominator problems.
- Ken K:
    - Not many people on call are dabbling in this at this point.
- Scott C:
    - WebAuthn doesn’t really get rid of passwords b/c of recovery.
- Tom J:
    - Accessibility issues, tech. needs to mature.
    - User experience was concerning
- Matthew E
    - Looking at it as a step-up option for VO for institutions that can't do AAL2, will try to enroll devices somehow and have to own the responsibility
    - Still in development
- Ken K:
    - Anyone else using WebAuthn with portals?
- Maartin K
    - Looking at it in EduID environment
    - (Ditto Leif)
- Leif
    - Hoping this will improve usability, having a mechanism for passwordless auth with the device everybody already has seems like it will work, avoiding everybody having passwords
- Rajesh P:
    - Looking at WebAuthn for improving progressive web apps
    - Going passwordless improves UX significantly
    - Big push esp. after pandemic
- Scott C:
    - Can’t sell improved UX to management due to other sunk costs surrounding device recovery
- Alan Buxey:

    - Client compatibility, account recovery and its all new to end users and unfamiliar to them (so lots of support requirements)
    - Think PC lab desktop environments and trying to get access to resources…
    - and physical visits to IT service desk for an account reset was fine last year….not so good this year
    - and then education of the users that their biometric data isn't being sent to the service for the login
- Matthew E
    - REFEDS MFA makes this useful
    - Scott: Need PIN for that? Otherwise it doesn't meet MFA?
- Leif J:
    - Running CTAP(?) over a slightly wider field radio network?
    - Bluetooth Low Energy (BLE) not very stable
    - Next big thing will probably be Apple's (essentially Touch/Face ID)
- Ken K:
    - Any concern about glancing at the phone to unlock being disruptive UX?
- Leif J:
    - Wrong to think about as another MFA, that's the wrong experience:
    - If accessing through phone, then you want the phone experience
    - If accessing through desktop, then you want whatever native authenticator is available on that OS
    - Fall back to asking a user to plug in a hardware token
    - Expectation from the users will progressively be that web apps trigger the right behavior for one's device
    - Won't always be without a PIN
- Scott C:
    - Sees phone as way around the problem, as it is a separate device that is valued by the user.
- Leif
    - Hearing that (people?) are moving away from phones in favor of hardware devices.
    - Hacking issues with BLE and other devices pushing back toward hardware.
- Ken K:
    - What's the adoption experience at Duke?
- Shilen P:
    - About 1500 users now
    - All employees/students must use Duo
    - WebAuthn not required
    - Rampup has been slow but steady
    - Only WebAuthn registrations allowed using devices capable of MFA
    - New features in phones has increased student registrations

From John Gasper to Everyone: (10:59 AM)
https://www.yubico.com/blog/getting-a-biometric-security-key-right/