UMA telecon 2021-10-21

UMA telecon 2021-10-21

Date and Time

- **Primary-week Thursdays 06:30am PT; Secondary-week Thursdays 10:00am PT**
  - Screenshare and dial-in: https://zoom.us/j/99487814311?pwd=dTAvZi9uN0ZmeXJReWRrc1Zycm5KZz09
  - United States: +1 (224) 501-3316, Access Code: 485-071-053
  - See UMA calendar for additional details: http://kantarainitiative.org/confluence/display/uma/Calendar

Agenda

- Approve minutes of UMA telecon 2021-09-09, UMA telecon 2021-09-16, UMA telecon 2021-09-23, UMA telecon 2021-09-30, UMA telecon 2021-10-14
- IIW closing thoughts
- FHIR Vulnerability Review
- AOB

Minutes

Roll call

- Quorum: No

Approve minutes

- Approve minutes of UMA telecon 2021-09-09, UMA telecon 2021-09-16, UMA telecon 2021-09-23, UMA telecon 2021-09-30, UMA telecon 2021-10-14

Deferred

IIW closing thoughts

(see initial thoughts from last weeks minutes)

- a lot of SSI focus, main OAuth-y topics we're in relation to the interop/connection to SSI

FHIR Vulnerability Review

and how UMA could address, maybe a 1-2 page position

https://www.scmagazine.com/analysis/application-security/critical-flaws-found-in-interoperability-backbone-fhir-apis-vulnerable-to-abuse

https://www.healthcareitnews.com/news/cybersecurity-briefs-olympus-it-outage-fhir-vulnerabilities-and-more

Summary of articles: a white-hat security company (https://approov.io/) have looked at some health care mobile applications that access FHIR apis. Patients were authenticating against the API/EHR, however the applications were able to access all FHIR data regardless of the authenticated user. There were also issues raised around static client credentials embedded in the mobile applications (public SMART on FHIR app using confidential client creds?)

- no patient/RO segmentations, seems that any authenticated user could access the full API
  - coarse grained api access, no RO compartmentalization
- want apps to conform to their requirements and protect data

want to avoid a 'shut down access' reactive response

Potential Outline:

- summary of the issues found
- assumed oauth/oidc api model being used
  - identity is often an invitation model for EHRs
- present a uma architecture to show the fine grained RO resources
  - how that helps the FHIR API provider properly restrict access. only one patients at a time
  - direct responses to the 'Recommendations to FHIR API Owners"
  - use of high assurance identity
- other uma benefits

        - multiple idps, don't make the FHIR API provider deal with authentication/identity. UMA AS is connection between identity/authN systems and the FHIR AuthZ
        - sharing and delegation to Bob
- links to CARIN recommendations and app certification processes (eg as provided by AEGIS)

application of provider authZ setup to patient access

difference of patient/*.* (what they should've done) and user/*.* (what they did)

Patient empowerment group (hl7 group) is meeting and the article writer is presenting these findings.

Let's use confluence, **Alec will create a page and move these notes over then share the link on the mailing list**

AOB

- Delegation Use Cases
    - pp2pi (protecting privacy to promote interoperability) use cases, can we schedule a time to review. Nancy has the documents but can't share them
        - there is existing delegation use-cases documents that we may refresh/update: eg https://patientcentricsolutions.com/fileadmin/user_upload/Files/Report_UMA_Business-Legal_Framework_and_Use_Cases.pdf
    - summarize how UMA can be used to support these use cases. Delegation is viewed as hard, but can be addressed by trying to solve it and considering the use-case
    - This will be the main topic for next weeks call

- moving gdocs working docs to confluence, will create a working docs space in confluence to upload these docs
    - confluence has a 'import word doc' feature, need an approach for slide decks

Conference roundup

In person is coming back!

- Identity North
- HLTH: https://www.hlth.com/
    - in-person w/ 6000 people in attendance!
- FIDO Authenticate
- National Cyber Summit in Nashville
    - zero trust was a main topic
    - 2500 people!

Topic Candidates (from previous week's telcon)

- Delegation and Guardianship
- Outcome of user stories discussion
- PDP architecture includes the concept of governance registry/discovery
- TOIP/SSI are starting to define this ecosystem function
- ANCR records update
- Privacy as Expected/ANCR update : 2/3 weeks out (Sal?)

Attendees

As of October 26, 2020, quorum is 5 of 9. (Michael, Domenico, Peter, Sal, Thomas, Andi, Alec, Eve, Steve)

Voting:

1. Eve
2. Alec
3. Domenico

Non-voting participants:

1. Scott G, working with Healthcare team at Forgerock
2. Nancy
3. Vladimir
4. Scott

Regrets:

1. Steve