Report on FHIR API Vulnerabilities

Context:

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

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

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)

A recent report[1] by Approov found authorization vulnerabilities in the implementation of FHIR API access in app and third party FHIR aggregators. The main vulnerability found is that any authenticated user(patient) is able to access all data within the FHIR API – not only the data about themselves. This could be designed as "client-side authorization" where the relying party application is responsbily to properly restrict their access to to the API, either through queries or client side response filtering, in order to show only the authenticated users information. This authorization scheme is a major design error and highlight why server side policy decision and enforcement is essential to good security and privacy over the internet. Server-side authorization and scoped client access are the problems that OAuth and UMA were designed to address.

- these vulns show why strong authZ tools need to be easy to use/implement
- this api authZ is also common for provider FHIR access – that should also change to properly enforce patient directed record blocking
- <diagram to summarize vuln>

Draft Diagrams:

UMA is made to be additive to this ecosystem in order to enforce appropriate subject directed authorization of their record to the app, services, and other people they want to access their information.