RPC Security Standard Requirement

Background Notes - Atul Tulshibagwale, Jul 26, 2022

I spoke to a few people after the OAuth WG meeting on Monday, Jul 25, 2022. I took some notes, which I would like to share here in order to facilitate the discussion in the side meeting

- My presentation from the IETF 114 OAuth WG Meeting is here.
- The problem is similar to / same as the “confused deputy problem” (described in AWS docs, or Wikipedia)
- There is no standard way of securing RPCs today. See this NIST publication (Aug 2019) for a good overview of best current practices.
- The MITRE proposal for token chaining may be relevant
- Any RPC security standard that we come up with should provide implementers with distinct benefits, and should not be onerous

Goals of a RPC Security Standard

It’s worth reiterating the goals of any standards effort here:

1. RPCs should preserve user and scope so that the “confused deputy problem” does not arise
2. Callers should be able to downscope the authorization of downstream calls
3. This should work across services / microservices belonging to the same organization, belonging to different organizations (typically through publicly documented APIs) regardless of whether this is happening within the same cloud platform provider or across multiple cloud platforms
4. If should be super efficient in order to not increase the latency or throughput of such a frequent action as a RPC