Do we need an RPC security standard?

Atul Tulshibagwale, CTO, SGNL

IETF 114, July 24, 2022

Twitter: @zirotrust

Email: atul@sgnl.ai

RPC Security Today

- OAuth token at top-level component with specific scope and user authorization
- Other microservices use “service-to-service” trust (often using Mutual TLS)
- 3P API calls made with powerful “API keys” - OAuth tokens that can get access on behalf of any user within tenant
- Multi-cloud boundaries may require specialized “API keys” similar to 3P APIs

Issues with Today's RPC Security

- VPC compromise can enable attacker to have unlimited access
  - Various ways this can be achieved: Software supply chain, dev chain or privileged user compromise
- API keys can be abused to operate on behalf of any user within the tenant of a third-party SaaS platform
  - Obtained through VPC or SaaS credential compromise
- Multi-cloud deployments require everyone to "roll their own" security
- Higher level user and other context is lost in subsequent calls
  - Harder to make authorization decisions

Solution Requirements

- Preserve identity and scope
  - In calls at any level
  - Across 3P API calls
  - Across multi-cloud deployments
- Independently verifiable
- Immune to replay attacks
- Highly efficient

Possible Solution Properties

- Downstream tokens also bound to specific users and scopes - service cannot switch context
    - Further scope restriction in downstream calls
- Short-lived OAuth tokens - limit replay
- Bound to originating and destination services - explicit authorization
- Trust across 3P API and multi-cloud boundaries - interoperability
    - Token introspection
    - Common root of trust