Fine-grained Transactional Authorization Working Group Charter

Working Group Name

Fine-grained Transactional Authorization (FTA)

Background

Interactive and Batch Invocations

Independently running software components, referred to as services here, often depend on other services to perform parts of their tasks. These tasks may be initiated either interactively, when a user or robotic principal invokes a service or they may be initiated as a part of a bulk operation, i.e. a batch process.

Synchronous or Asynchronous Invocations

Within any interactive or batch service invocation, the invoking entity may expect that the invoked service needs to return information in a short period of time. If such an expectation exists, then the invocation is said to be synchronous, otherwise it is considered to be asynchronous.

Trust Boundaries

A trust boundary is a computational and networking environment that has a homogenous administrative structure and homogenous management capabilities. A single trust boundary may have multiple services running within it, but any single service operates entirely within one trust boundary.

A trust boundary could represent a specific tenant in a cloud platform belonging to a single organization, or a data center operated by an organization. Tenants owned by the same organization but residing in different cloud platforms represent different trust boundaries because of the lack of homogeneity in their management environments.

RPCs

Remote Procedure Calls (RPCs) are the basic communication mechanism between services that run either within the same trust boundary or across trust boundaries. RPCs may be synchronous or asynchronous.

Call Chain

When a service is called by another service, it represents the next step in a sequence of calls that originate with the initiating principal or batch process. The sequence of calls starting with this initiating entity and ending with the present RPC as received by the called service is the call chain.

Zero-Trust

A traditional trust model relies on breaking the network into different zones, and assumes that the network inside the datacenter is a trusted network. That proved to be a flawed assumption, because as soon as an attacker was able to compromise one entity in the network, the attacker had access to the rest of the datacenter entities.

Zero-Trust is a trust model where every entity, e.g., user, application, device, is by default not a trusted entity, until it proves its identity. Another fundamental principle of Zero-Trust is the least privilege principle, which dictates that each entity must be provided with the minimal permissions it needs to perform its function properly.

Purpose

The goal of the Fine-grained Transactional Authorization Working Group (the WG) is to enable services within the same trust boundary and across trust boundaries to securely and interoperably convey authentication, least-privilege, fine-grained authorization, call chain, and call context information in communication between independent services.

Scope

The WG will define the following:

- A framework for communicating identities across trust boundaries (to the extent required to communicate authorization information)
- A mechanism for services to securely communicate the following information about communication between services

    - Preserve Identity of the initiating principal
    - Service identity of the calling service
    - Service identities of participants in the call chain
    - Authorization scope defined by the caller
    - Authorization scope defined previously called services in the call chain
    - Argument context defined by the initiating principal
    - Argument context defined anywhere in the call chain

Out of Scope

- Defining a naming convention for identities
- User or robotic principal authentication
- Policy framework or language

Proposed Deliverables

The WG will define specifications that cover the scope defined above. This may include

- A specification that defines how identities may be communicated across trust boundaries
- A specification that defines how information (defined in the “Scope” section) relating to an RPC is conveyed between services that reside either in the same trust boundary or across trust boundaries

Anticipated Audience or Users

- Developers building systems that include multiple services
- Cloud platform providers
- Authorization platform providers

Language

English

Method of Work

TBD

Completion Milestones

The following qualities are necessary to declare that work in this working group has concluded

- Rough consensus in the WG on deliverables
- Ratification of deliverables through a standards body such as the IETF OAuth WG

- No / little outstanding feedback from outside the WG regarding the deliverables
- No / few new items to be considered to revise the deliverables

Proposers

- Atul Tulshibagwale, CTO, SGNL
- Erik Gustavson, Co-founder and CPO, SGNL
- Rifaat Shekh-Yusef, Senior PM @ Okta, Chair OAuth WG @ IETF
- Michael Jenkins, Secure Protocol Standards Lead, NSA-CCSS
- Pieter Kasselman, Identity Standards Architect, Microsoft
- Dean H. Saxe, Senior Security Engineer, AWS Identity, Amazon Web Services