Distributed Authentication Mesh*

Declarative Adhoc Conversion of Credentials

Christoph Bühler

xx.xx.xxxx

Abstract

foo bar stuff

Contents

List of Tables

List of Figures

1 Introduction

Modern cloud environments solve many problems like the discovery of services and data transfer or communiation between services in general. One modern way of solving service discovery and communication is a Service Mesh, which introduces an additional infrastructure layer that manages the communication between services (Li et al. 2019, sec. 2).

However, a specific problem is not solved yet: "dynamic" trusted communication between services. When a service, that is capable of handling OpenID Connect (OIDC) credentials, wants to communicate with a service that only knows Basic Authentication that originating service must implement some sort of conversion or know static credentials to communicate with the basic auth service. Generally, this introduces changes to the software of services. In small applications which consist of one or two services, implementing this conversion may be a feasable option. If we look at an application which spans over a big landscape and a multitude of services, implementing each and every possible authentication

*todo

mechanism and the according conversions will be error prone work and does not scale well[1].

The goal of the project "Distributed Authentication Mesh" is to provide a solution for this problem. TODO.

1.1 Project Context

This project aims at the specific problem of declarative conversion of credentials to ensure authorized communication between services. The solution may be runnable on various platforms but will be implemented according to Kubernetes standards. Kubernetes[2] is an orchestration platform that works with containerized applications.

The deliverables of this project may be used to ensure services can communicate with each other despite their different authentication mechanisms. As an example, this could be used to enable a modern web application that uses OIDC as the authentication and authorization mechanism to communicate with a legacy application that was deployed on the Kubernetes cluster but not yet rewritten.

- sidecar?
-

TODO.

2 State of the Art and Deficiencies

This section gives an overview over the current state of the art as well as the deficiencies according to the author. Following the description of the current situation, a definition of the should situation gives an overview of the purposed solution.

- Describe the IS situation.
- Describe the SHOULD situation.
- describe service mesh (image from referecne could be used)

Bibliography

Li, W., Y. Lemieux, J. Gao, Z. Zhao, and Y. Han. 2019. "Service Mesh: Challenges, State of the Art, and Future Research Opportunities." In *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*, 122–25. https://doi.org/10.1109/SOSE.2019.00026.

[1] According to the matrix problem: X services times Y authentication methods
[2] https://kubernetes.io/