Common Identities in a Distributed Authentication Mesh

Definition and Implementation of a Common Identity for Secure Transport

Student

Christoph Bühler

Problem: The “Distributed Authentication Mesh” is a concept to dynamically convert authentication information (such as access tokens from OpenID Connect) to other authentication schemes (like HTTP Basic). In contrast to “Security Assertion Markup Language” (SAML), the concept does not require all participants to share the same authentication scheme. It eliminates the requirement to introduce code changes into existing applications such that they can support other authentication schemes.

A central part of the mesh is the “common language format.” This format is eminently important to the mesh because it delivers the users’ identity to other participants. While the previous project included the concept of the mesh and implemented a Proof of Concept to modify HTTP headers, it did not provide a definition or implementation for the common language format.

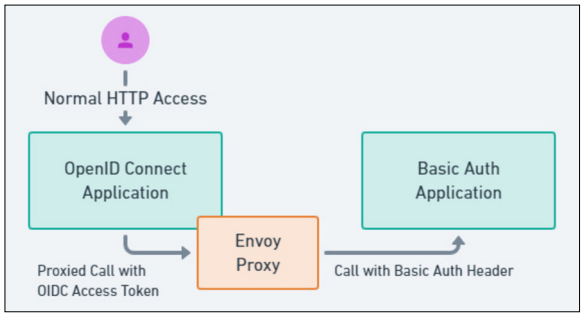
This project targets the topic of the common language and analyzes several possibilities for such a format. The project also defines the objects that must be transmitted between mesh participants. The concept of the mesh is extended with a “Rule Engine” that improves the security and versatility of the mesh. Additionally, this project implements the “Distributed Authentication Mesh” as open-source software such that it can be operated on Kubernetes. The conclusion provides further information about the project and possible topics of follow-up work.

Conclusion: This project further improved the core concept of the “Distributed Authentication Mesh” proposed in a former project. The goals of this project were the definition and implementation of the “common language format” and a complete implementation in a cloud environment (i.e. “Kubernetes”).

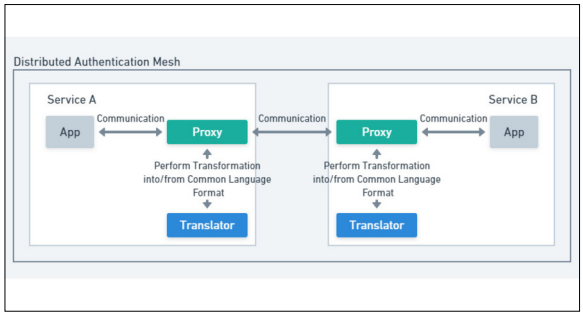
Several formats (such as structured formats or certificates) were analyzed to see if they are suitable for a common language between communicating parties. The comparison derived "JWT" (JSON Web Tokens) as a good fit for the job.

The implementation for Kubernetes is open-source and can be found on GitHub (https://github.com/WirePact). The organization contains an Operator, two translators, and the public key infrastructure for the authentication mesh.

Dynamic conversion of authentication information.
Own presentment



The common language between mesh participants.
Own presentment



Examiner
Prof. Mirko Stocker

Subject Area
Computer Science, Software and Systems