Trust in a Distributed Authentication Mesh

How to create trust and secure communication between distant authentication meshes

Graduate

Christoph Bühler

Introduction: The concept of the "Distributed Authentication Mesh" creates a foundation for dynamic authentication and authorization with diverging authentication schemes. Further, "Common Identities in a Distributed Authentication Mesh" defines and implements the common identity that is transported between services. The mentioned projects show with their respective Proof of Concepts (PoC), that it is possible to authenticate a specific identity and transfer it to other applications that do not share the same authentication mechanism.

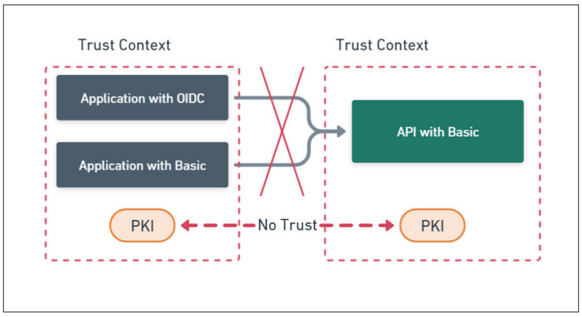
However, both projects are only distributed within the same trust zone. While still allowing the "zero trust" principle, the projects do not enable true "distribution".

Problem: In its current state, the Distributed Authentication Mesh is able to run inside the same trust zone with a shared common identity. The mesh handles the conversion of authentication information (such as an access token or a login/password combination) by transforming it into a shared format. A sender encodes the user ID in a JWT and signs it with its own private key. The receiver can then verify that the information is not modified and that the sender is part of the authentication mesh.

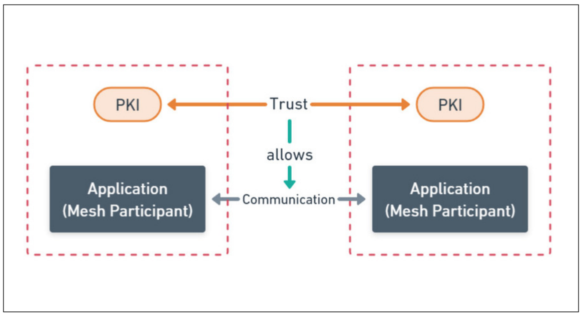
However, the connection between the participants is prone to attacks in multiple ways. The concept only works if all applications of the mesh are within the same trust zone (for example, in the same Kubernetes cluster behind the same API gateway). If part of the application runs on a different cluster, the same trust cannot be applied. An attacker may get their own key material from a mesh PKI and can pose as a valid participant of the mesh. Therefore, confidentiality and integrity are violated. Further, the receiving end of the communication has no possibility of verifying the sender of the message for certain.

Conclusion: This thesis contributes to the concept of the Distributed Authentication Mesh. It extends the already defined components with a contract repository and allows the mesh to be distributed over multiple trust zones, as the last image shows. With the additional concept of the contracts, the mesh participants can now safely communicate with distant (with mTLS encryption) parties and trust the provided identity. When a participant's proxy receives an HTTP request, and the mTLS connection has been established, the proxy can be sure that the source of the request is a genuine part of the authentication mesh.

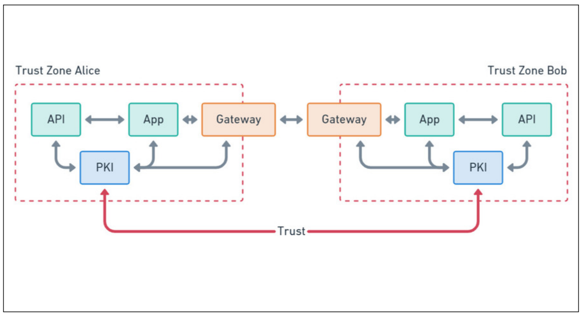
Without trust, the participants of two trust zones cannot communicate with each other over mTLS
Own presentment



A contract between the two zones allows mTLS connections between the participants
Own presentment


PKI
Trust
PKI
allows
Application (Mesh Participant)
Communication
Application (Mesh Participant)

Create trust between two separate trust zones
Own presentment



Advisor
Prof. Mirko Stocker

Co-Examiner
Leo Büttiker, yonesu GmbH, Olten, SO

Subject Area
Computer Science, Software and Systems