Zentrale und dezentrale Zugriffskontrolle in OAuth2 und OpenID Connect Systemen

OAuth2 und JSON Web Token (JWT) als Spezifikationen erlauben es http-Schnittstellen zu sichern. Der Ablauf ist folgendermaßen zu beschreiben: Ein Client erhält dadurch, dass sich ein Nutzer an einem Autorisationsserver authentifiziert einen Token, mit dem er auf Schnittstellen eines Ressourceservers zugreifen kann. Darüber hinaus ist es oftmals notwendig, Schnittstellen basierend auf Berechtigungen der Nutzer zu sichern. Grundsätzlich lässt sich das in dem Ressourceserver implementieren, allerdings kann das bei einer umfangreichen Applikationslandschaft mit verschiedenen Programmiersprachen und komplexen Zugriffsrichtlinien zu Unübersichtlichkeit und einen hohen Wartungsaufwand führen. Aus diesem Grund wurde 2016 „Open Policy Agent“ (OPA) entwickelt, das in einer einheitlichen und leicht verständlichen Sprache die Autorisierung von dem Resourceserver entkoppelt.

Diese Entkopplung hat allerdings zur Folge, dass der Resourceserver jedes Mal bei eingehenden http-Anfragen den OPA-Service um eine Entscheidung fragen muss, d.h. es besteht das Risiko von gravierenden Performanceeinbußen. Da bei einer hohen Last auf Schnittstellen diese i.d.R. durch horizontale Skalierung entlastet werden, können Performanceeinbußen äußerst kostspielig sein.

Um erstmalig zu untersuchen, inwiefern sich eine Entkopplung von Autorisierung mit OPA auf die Performanz und Sicherheit auswirkt, wurden zwei durch OAuth2 gesicherte http-Schnittstellen implementiert. In dem einen Testsystem geschieht die Autorisierung in der Applikation und in dem anderen durch einen OPA-Service. Außerdem wurde dabei die verschiedenen Deploymentmethoden von OPA berücksichtigt. Um die Performanz (unter Last) zu testen, wurde als Tool Apache JMeter verwendet und hierbei als zu betrachtende Metrik die Round-Trip-Time gewählt. Zudem wurde auf beiden Systemen die Sicherheit getestet mit Testfällen, mit denen versucht wird auf unerlaubte Weise Zugriff auf die Schnittstelle zu erhalten.

Dabei ist man zu dem Ergebnis gekommen, dass ….

- OPA per Docker-Container = ungefähr halb so schnell wie Autorisierung in Applikation, ausführliche Ergebnisse = TODO
- OPA und Resourceserver in Kubernetes Pod = TODO
- Sicherheit: TODO
- Bewertung hinsichtlich des CAP-Theorems: TODO