Delegation in Microservice-Architekturen

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuerin: Dr. Annett Laube
Experte: Mathis Marugg (Die Schweizerische Post AG)

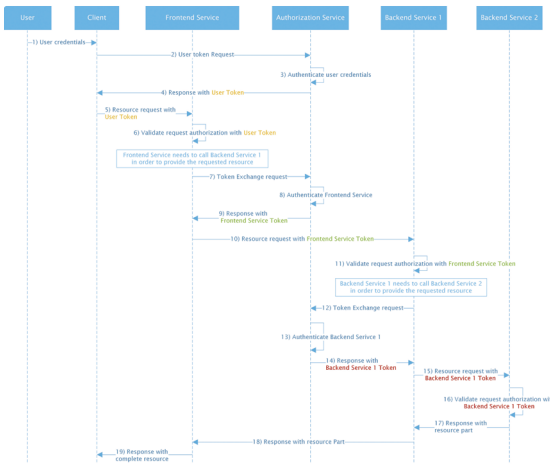
Heute folgen immer mehr Anwendungen den Prinzipien von Microservice-Architekturen. Im Rahmen dieser Arbeit wurde untersucht, wie die Identität des Benutzers und die damit verbundenen Berechtigungen bei der Kommunikation zwischen Microservices weitergegeben werden kann. Der implementierte Prototyp zeigt, wie das OAuth 2.0 Token Exchange-Protokoll als mögliche Lösung für diese Herausforderung funktioniert.

Aufgabenstellung

Microservice-Architekturen erlauben die Entwicklung von eigenständigen Services mit klar definierten Zuständigkeiten. Die einzelnen Services lassen sich mittels REST-Schnittstellen zu einem flexiblen und skalierbaren Gesamtsystem verbinden. Ein dabei oft unterschätztes Problem ist die Weitergabe der Identität des Benutzers durch die Service-Kette und die damit verbundenen individuellen Berechtigungen. Mit dem OAuth 2.0 Token Exchange-Protokoll arbeitet eine IETF-Arbeitsgruppe an einer möglichen Lösung. In dieser Arbeit sollte untersucht werden, ob die vorgeschlagene Lösung den Anforderungen des Identitäts- und Access-Managements gerecht wird. Dazu sollte das Protokoll prototypisch implementiert werden.

Vorgehen

Zu Beginn der Arbeit stand die Auseinandersetzung mit der Problemstellung und den technischen Grundlagen im Vordergrund. In einer zweiten Phase wurde der Protokoll-Entwurf eingehend studiert. Mögliche Antworten auf die Problemstellung sind darin nicht besonders prägnant formuliert. Folglich wurden die im Ansatz beschriebenen Token Exchange-Szenarien ausgearbeitet und visualisiert. Nach den Grundlagenarbeiten wurde eine konzeptionelle Systemarchitektur für die Prototyp-Implementation beschrieben. Auf dessen Basis wurde der Prototyp fortlaufend implementiert und mit der Protokoll-Spezifikation validiert. Die gewonnenen Erkenntnisse dienten als Grundlage für die abschliessende Bewertung des Protokolls.



Vereinfachtes Sequendiagramm zum implementierten Token Exchange-Ablauf.

Resultate

Auf Basis des MEAN-Technologie-Stacks (MongoDB, Express, Angular, Node.js) wurde eine eigene Microservice-Architektur implementiert. Ein Authorization Service unterstützt den Token Exchange gemäss Spezifikation. Zwecks Veranschaulichung wurden drei Resource Services zu einer Service-Aufruf-Kette kombiniert. Jeder Aufruf in der Kette erfolgt mit einem gültigen Access Token, das jeweils mittels Token Exchange beschafft wird. Der Prototyp ermöglicht die Simulation unterschiedlicher Token Exchange-Szenarien und zeigt die einzelnen Schritte mittels Logs an. Die gewonnen Erkenntnisse wurden zusammengefasst und ausgewertet. In Form eines Thread Models wurden potenzielle Angriffsvektoren und mögliche Massnahmen beschrieben. Weiterhin stellten sich einige Fragen, die für eine Nutzung in der Praxis relevant sind, zu denen aber der Protokoll-Entwurf (noch) keine Antworten liefert. Diese Fragen hat der Autor diskutiert und versucht, Antworten zu finden.

Fazit

Das OAuth 2.0 Token Exchange-Protokoll bietet eine funktionierende Lösung für die elementaren Bedürfnisse des Identitäts- und Accessmanagements in einer Microservice-Architektur. Jeder Microservice in einer Service-Kette erhält Informationen über die bereits durchlaufenden Services und den ursprünglichen Benutzer, der den Aufruf initiiert hat. Trotzdem müssen vor einer Umsetzung in der Praxis viele anwendungsfallspezifische Fragen geklärt und eine Kosten-Nutzen-Analyse durchgeführt werden.

Manuel Schmutz
manuel.schmutz@gmail.com