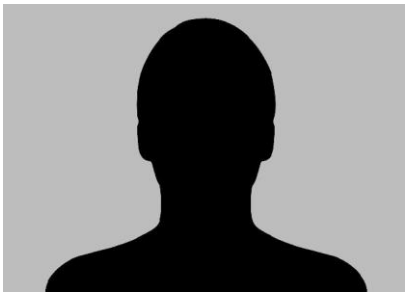
Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

InIT Institut für angewandte Informationstechnologie

# OAuth 2.0 und OIDC – Angriffe und Gegenmassnahmen

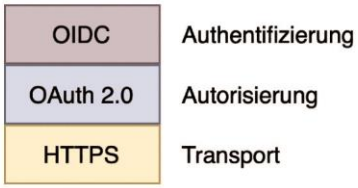


Diplomand
Lars Tönz

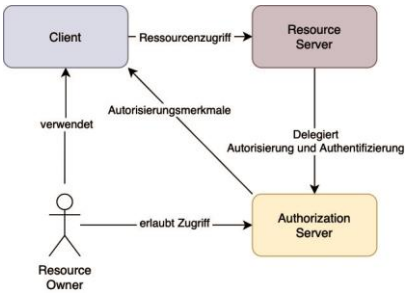
Dozent
Bernhard Tellenbach

Moderne Identity-and-Access-Management-Systeme müssen hohe Anforderungen an die IT-Security erfüllen und gleichzeitig einfach nutzbar bleiben. Die CAOS AG entwickelt eine Identity-and-Access-Management-Lösung und setzt dabei vorwiegend auf offene Standards. OAuth 2.0 und OpenID Connect 1.0 gehören aufgrund ihrer hohen Verbreitung zu den bedeutendsten Vertretern. Wie bei anderen Standards zum Teil auch basiert die Sicherheit der von OAuth 2.0 und OpenID Connect 1.0 beschriebenen Authentifizierungs- und Autorisierungsmethoden auf der Annahme, dass die dazu genutzten Kommunikationskanäle (z.B. Transport-Layer-Security-Kanäle) sicher sind und nicht durch einen Man-in-the-Middle (MITM) kompromittiert werden können. Im Unternehmensumfeld werden diese Verbindungen aber oft mit Hilfe von Proxys aufgebrochen, damit der Netzwerkverkehr von Sicherheitssystemen protokolliert und auf problematische Aktivitäten analysiert werden kann. Für Angreifer sind diese Proxys deshalb lohnenswerte Ziele, da an einem meist zentralen Punkt diverse schützenswerte Daten abgefangen werden können.

Diese Arbeit analysiert existierende Lösungsansätze zur Verhinderung einer Kompromittierung von Authentisierungs- und Autorisierungsmerkmalen im Falle eines MITM und präsentiert einen neuen Lösungsansatz. Keiner der existierenden Lösungsansätze ist in der Lage, die Problematik ohne Abstriche bei der Sicherheit oder praktischen Umsetzbarkeit zu lösen. Das präsentierte Konzept erweitert den Lösungsraum um eine Variante, die auf OAuth 2.0, OpenID Connect und einer neuen Browsertechnologie, dem ServiceWorker, basiert. Unter der Annahme, dass der Erstkontakt mit einem System nicht durch einen MITM kompromittiert wird, verhindert der vorgestellte Lösungsansatz die verwertbare Extraktion von Authentisierungsmerkmalen erfolgreich. Sämtliche Punkte des Konzepts werden in einem Prototypen auf Basis der OIDC-Library von CAOS AG erfolgreich belegt.




Für die Arbeit relevante Protokollschichten.




Rollen des OAuth 2.0 Protokolls, Quelle: oracle.com