Fachhochschule Rosenheim
Fachbereich Informatik
Prof. Dr. R. Hüttl

IT-Security

Übung 7

Identity and Access Management (IAM)

In dieser Übung betrachten das Thema der Authentifizierung und Autorisierung in Cloud Umgebungen. Dies wird durch sogenannte IAM realisiert.

Identity- and Access Management (IAM) lässt sich mit dem Begriff Identitäts- und Zugriffsverwaltung übersetzen. IAM stellt einen Oberbegriff für alle Prozesse und Anwendungen dar, die für die Administration von Identitäten und die Verwaltung von Zugriffsrechten auf verschiedene Applikationen, Systeme und Ressourcen zuständig sind.

Aufgabe 1: Authentifizierung mit Google IAP (Identity Aware Proxy) über OAuth

Falls sie eine Google Account besitzen können sie versuchen sich mit OAuth an einer eigenen Testanwendung zu autorisieren. Folgen sie dabei den Anleitungen unter https://cloud.google.com/iap/docs/authentication-howto?hl=de

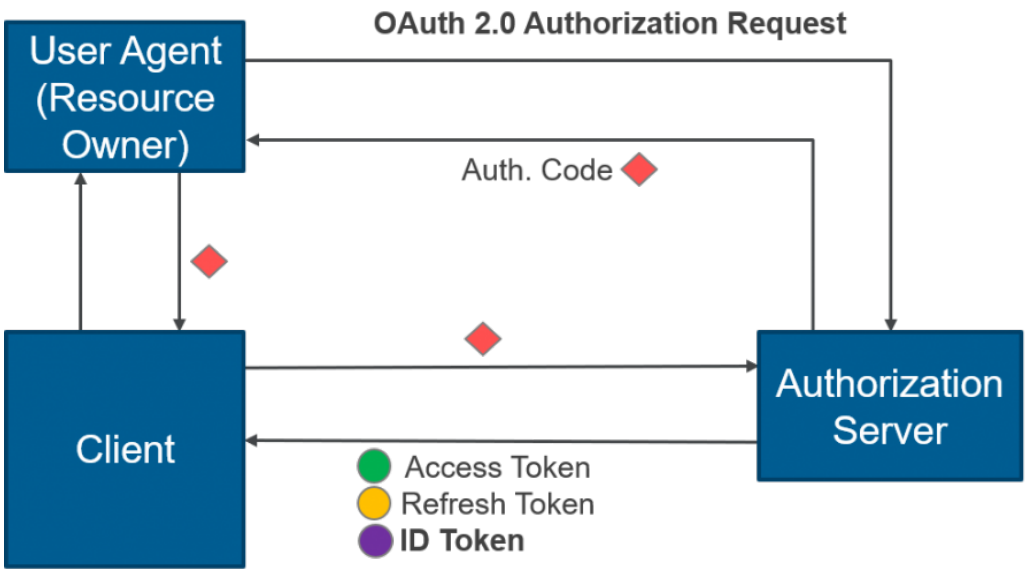
Dabei müssen sie

- ein Projekt anlegen
- eine Anwendung anlegen
- ein Dienstkonto anlegen
- einen OAuth Client mit Client-ID und Clientschlüssel erstellen
- einen Autorisierungscode holen
- mit **curl** einen **Access Token** (liefert Informationen zum Benutzer), einen **Refresh Token** (liefert bei Bedarf neuen Acces Token) und einen **ID Token** (liefert Zugriff auf Anwendungen) holen
- mit **curl** und dem ID Token auf die Anwendung zugreifen

Hinweis:

- Sie müssen sich das Command Line Tool **curl** zum Zugriff auf Server installieren
- Falls sie keinen Google-Account besitzen können sie sich einen Account anlegen

In der folgenden Abbildung sehen sie die Zusammenhänge und den Ablauf:



Quelle: https://www.oose.de/blogpost/oauth-openid-connect-und-jwt-wie-haengt-das-alles-zusammen-teil-2/

Der Ressource-Owner (angemeldeter Google User) holt einen Authorization Code für den Client:

```
https://accounts.google.com/o/oauth2/v2/auth?client_id=OTHER_CLIENT_ID&response_type=code&scope=openid%20email&access_type=offline&redirect_uri=urn:ietf:wg:oauth:2.0:oob
```

Der Client authentifiziert sich mit seiner ID und seinem Secret und holt sich mit dem Authorization Code über die OAuth-Api von Google die Token:

```
curl --verbose --data client_id=OTHER_CLIENT_ID --data client_secret=
OTHER_CLIENT_SECRET --data code= AUTH_CODE --data
redirect_uri=urn:ietf:wg:oauth:2.0:oob --data grant_type=authorization_code
https://oauth2.googleapis.com/token
```

Mit dem ID Token hat der Client Zugriff auf die Ressource (url):

```
curl --verbose --header 'Authorization: Bearer ID_TOKEN' URL
```

Aufgabe 2: Funktionen eines IAM

Neben Google IAP aus Aufgabe 1 gibt es weitere IAM für Cloud Umgebungen, z.B.

- Amazon AWS IAM https://aws.amazon.com/de/iam/
- Keycloak (OpenSource IAM) https://www.keycloak.org

Rechcherchieren sie im WWW was die wichtigsten Funktionen eines IAM sind.

Aufgabe 3: Risikomanagement bei einem IAM in einer AWS Cloud Umgebung

Ein Anbieter einer Cloud Native Umgebung hat eine Plattform zum Design, Entwicklung und Betrieb von Businessanwendungen auf Basis von AWS implementiert. Um nachzuweisen, dass er compliant (gesetzeskonform) für Bank- und Versicherungsanwendungen ist beauftragt er einen Seucrity-Audit.

Dazu wurde im erstenSchritt eine Risikonalyse gemacht. Der Cloudanbieter hat in seiner Plattform ein IAM integriert. Wir fokkusieren uns in unserer Aufgabe auf die Risikoanalyse des IAM.

In der Vorgabe haben sie die Liste der identifizierten Risiken.

Suchen sie für jedes Risiko Maßnahmen um das Risiko zu mildern.