Authorization

Willard Rafnsson

IT University of Copenhagen

In this assignment, we see how to control the operations of authenticated users, such that unauthorized operations are denied. The goal is to gain experience with access control, to know how to implement such controls in software.

Problem 1 : ACL (Ambient Authority)

`alice` can read and write to the file `a`, read the file `b`, and execute the file `c`. `bob` can read `a`, read and write to `b`, and has no access to `c`.

Part 1 Write access control lists for this situation. (~ 2 sentences)

Part 2 Write capability lists for this situation. (~ 2 sentences)

Part 3 Say you need to, on the one hand, *a)* revoke all `write` permissions to a specific file, and on the other hand *b)* revoke all `write` permissions of a specific user. In these two scenarios, what is the difference between access control lists and capability lists, in terms of what you need to do to achieve the desired effect? (~ 2 sentences)

Part 4 As `root`, create a directory `alice-bob-acl`, create the above files `a`, `b`, and `c`, and remove all permissions for everyone from these files. Then, add the above-described permissions into the access control lists of the files. `tar` the result (see commands below), and include the `tar`ball in your submission. Useful commands:

To remove all permissions from user, group, and other, on file `f`:

```
chmod ugo-rwx f
```

To create user `alice`,

```
adduser alice
```

To `tar` and un-`tar` a directory *while preserving ACLs*:

```
tar --acls -cpf alice-bob-acl.tar alice-bob-acl
tar --acls -xpf alice-bob-acl.tar
```

Problem 2 : DAC (Authentication in Microservices)

OAuth is a protocol for scenarios where a user wishes to authorize an app to access their data in another app (DAC). Its most widespread application today, is for implementing authentication in a microservice architecture; by authorizing an app to access your (identity-)data in another (identity-provider-)app—something only you can do—you effectively authenticate yourself to the app. An identity in an identity provider effectively becomes a SSO for all apps authorized, and all those apps benefit (for free) from MFA support for that identity. OIDC—a thin layer on top of OAuth—facilitates this.

In this problem, we gain familiarity with authentication in microservice architectures (a prerequisite to authorization).

Setup: Auth0 is a service for creating and configuring identity providers (identity-as-a-service, IaaS). You will use this service to create an identity provider. You will then have our custom client use said identity provider to authenticate users. Do the following:

1. *Create identity provider*: Sign up for a personal account[1]. Login, go to Settings. In the Settings part therein, pick "AmaSoft Inc." as the Friendly Name, use their logo[2], and Save.
2. *Create client*: Download our custom client[3] from the course webpage.
3. *Register client with identity provider*: Create a new Application in Auth0. Call it "PayBud Inc.", pick Native as the application type, and head straight to its Settings. Use its logo[4], and complete steps 1-3 in the guide mentioned in footnote 3 to configure it. Make note of `domain` & generated `client id` and `client secret`.
4. *Configure client*: Set variables in `.env` appropriately (`ISSUER_BASE_URL` is `domain`).
5. *Start client*: `npm install` and `npm start`.

You can now access the client through `http://localhost:3000` (note `http`). Pick a user e-mail address, say, alice$X$@mailinator.com (where X is some string you pick).

Part 1 Who or What is the 1) resource owner, 2) client, 3) authorization server and 4) resource server? (use these terms correctly in the following). (~ 4 sentences)

Part 2 Create a new user account for the chosen e-mail address (Login → Sign up). Then log into that account. Explain what happened when you logged in; what sends what message to what? (Include the names of the entities). (~ 10 sentences)

Hint: All the steps of the OAuth authorization code flow.

Part 3 Enable MFA in the identity provider (Security → Multi-factor Auth), by enabling "one-time password" and Require Multi-factor Auth: Always. Log out and in again to add a 2nd factor (e.g. Microsoft Authenticator). Then log out and in again. Explain which steps are added & where in the protocol run from **Part 2**.(~ 2 sentences)

[1] `https://auth0.com/signup`

[2] `https://www.willardthor.com/amasoft.jpg`

[3] `https://auth0.com/docs/quickstart/webapp/express` that we have slightly modified.

[4] `https://www.willardthor.com/paybud.png`

Problem 3 : MAC (Auth<u>o</u>rization in Microservices)

In this problem, we gain familiarity with auth<u>o</u>rization in microservice architectures.

Open Policy Agent (OPA) is an engine, run as a microservice or library, which can be configured to enforce an access control policy. Given an INPUT query, an OPA evaluates it, together with DATA relevant to policy decisions (e.g. state), against a POLICY, and outputs a decision. Head to OPA playground[5], and pick the ABAC example.

Understanding INPUT & DATA

Part 1 In POLICY, what do the following evaluate to?

1. `input.action` (~ 1 sentence)
2. `data.user_attributes`[`input.user`] (~ 1 sentence)
3. `data.pet_attributes`[`input.resource`] (~ 1 sentence)

Understanding POLICY

Part 2 The OUTPUT of a policy evaluation is a record with up to 8 attributes. Justify your answer to the following by referencing POLICY, INPUT and DATA.

1. what is the (data-)type of all 8 possible attributes? (~ 1 sentence)
2. when is `action_is_{read, update}` true? (~ 1 sentence)
3. when is `user_is_{owner, employee, customer}` true? (~ 1 sentence)
4. when is `user_is_senior` true? (~ 1 sentence)
5. when is `pet_is_adopted` true? (~ 1 sentence)
6. when is `allow` true? (~ 1 sentence)

Querying POLICY

Part 3 We will ask for the value of `allow` in the following. To justify your answer, trace the value of `allow`, i.e. "`allow` is true if X is true, which is true if Y is true, ..." (you can replace "true if X is true" by "implied by X").

1. Consider the default INPUT.
   What is the value of `allow`? (~ 1-3 sentence)
2. Change the `user` attribute in the INPUT to `alice`.
   What is the value of `allow`? (~ 1-3 sentence)
3. Change the `user` attribute in the INPUT to `dave`.
   What is the value of `allow`? (~ 1-3 sentence)

Changing POLICY

Part 4 Change the policy such that any user is allowed the action `eat` of animals that are less than or equal to 2 years of age[6].

1. Give example INPUT with action `eat` where `allow` is true.
2. Give example INPUT with action `eat` where `allow` is false.

[5] `https://play.openpolicyagent.org/`

[6] you may assume that the pet shop is in China, if that makes you feel better.