COMP08011 Distributed Systems Project 2019

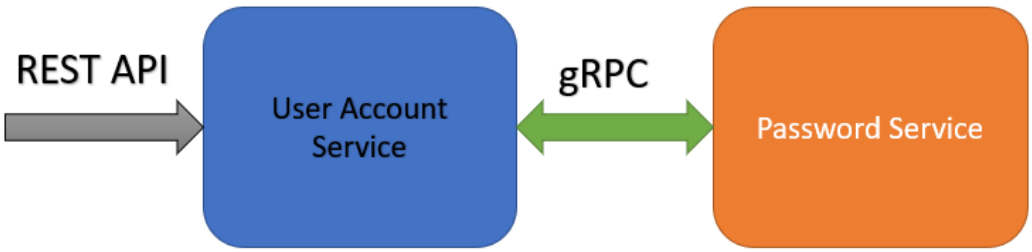
Part 1: Password Service with gRPC

Overview

The purpose of this project is to gain practical experience in interprocess communication protocols used in modern distributed systems. You'll build a distributed user account management system in two parts. Each part of the project will involve developing a service which will be able to connect to other services via APIs. Each service will be submitted separately. The two interconnected services you'll develop are as follows:

- Part 1: gRPC Password service
- Part 2: RESTful User Account Service

The overall system architecture is shown below.



Part 1: Password Service

Storing user passwords in plain text is poor security practice. Best practice is to store a salted hash of the user's password, along with the salt used to generate the hash. When a user attempts to authenticate with their password, a system can check if the password is valid by generating a hash of the password along with the salt, and comparing it with the

stored hash. See `https://crackstation.net/hashing-security.htm` for more details on password hashing.

In Part 1 you'll develop a Password Service which will provide the password hashing and verification services described above. Your service will expose a gRPC API with two methods:

method	input	output
`hash`	userId, password	userId, hashed password, salt
`validate`	password, salt	boolean indicating password validity

The `userId` and `password` input parameters to the `hash` and `validate` methods should be of type integer and string respectively. You are free to determine the other types as you see fit. Note that in Part 2 you'll be storing the hashed password and salt returned from the `hash` method. The `hash` method includes userId on input and output because we will be calling the method asynchronously in Part 2 and will need the userId on the asynchronous response.

Helper Code

Utility methods for generating and verifying cryptographically secure salted hashes of passwords in Java are available at
`https://gist.github.com/john-french/9c94d88f34b2a4ccbe55af6afb083674`.

Part 2 and Grading

The User Account Service you'll develop in Part 2 will be a client of the gRPC Password Service you develop in Part 1. Parts 1 and 2 be graded together after the submission of Part 2 by running the two services you have submitted and verifying that they work end to end.

Part 1 Deliverables

Your submission for Part 1 should comprise a .zip file containing:

- your gRPC Password Service packaged as an executable jar file. It should be possible to run the service using the command `java -jar your-service.jar`.
- a README text file containing
  - additional instructions for running the service (command-line parameters etc.)
  - the URL of the git repository containing your source code

In addition, your git repository should contain a tag called `part1` indicating the commit that you submitted.